



governmentattic.org

"Rummaging in the government's attic"

Description of document: National Security Agency (NSA) Military Cryptanalytics Part III by Lambros D. Callimahos, October 1977

Requested date: 07-July-2012

Release date: 09-December-2020

Posted date: 04-January-2021

Note: This document as released by the National Security Agency ends at letter "C" of the index, on page 656

Source of document: FOIA Request
National Security Agency
Attn: FOIA/PA Office
9800 Savage Road, Suite 6932
Ft. George G. Meade, MD 20755-6932
Fax: 443-479-3612 (ATTN: FOIA/PA Office)

The governmentattic.org web site ("the site") is a First Amendment free speech web site and is noncommercial and free to the public. The site and materials made available on the site, such as this file, are for reference only. The governmentattic.org web site and its principals have made every effort to make this information as complete and as accurate as possible, however, there may be mistakes and omissions, both typographical and in content. The governmentattic.org web site and its principals shall have neither liability nor responsibility to any person or entity with respect to any loss or damage caused, or alleged to have been caused, directly or indirectly, by the information provided on the governmentattic.org web site or in this file. The public records published on the site were obtained from government agencies using proper legal channels. Each document is identified as to the source. Any concerns about the contents of the site should be directed to the agency originating the document in question. GovernmentAttic.org is not responsible for the contents of documents published on the website.



NATIONAL SECURITY AGENCY
FORT GEORGE G. MEADE, MARYLAND 20755-6000

FOIA Case: 68177B
9 December 2020

This responds to your Freedom of Information Act (FOIA) request of 7 July 2012 for "a copy of Military Cryptanalytics, Part III, by Lambros D. Callamahos. Please review the sections marked as classified for possible declassification and release." A copy of your request is enclosed. Your request has been processed under the FOIA and the document you requested is on the enclosed CD. Certain information, however, has been deleted from the enclosure.

Some of the withheld information has been found to be currently and properly classified in accordance with Executive Order 13526. The information meets the criteria for classification as set forth in Subparagraph (c) of Section 1.4 and remains classified SECRET as provided in Section 1.2 of Executive Order 13526. The information is classified because its disclosure could reasonably be expected to cause serious damage to the national security. Because the information is currently and properly classified, it is exempt from disclosure pursuant to the first exemption of the FOIA (5 U.S.C. Section 552(b)(1)). The information is exempt from automatic declassification in accordance with Section 3.3(b)(1) of E.O. 13526.

In addition, this Agency is authorized by various statutes to protect certain information concerning its activities. We have determined that such information exists in this document. Accordingly, those portions are exempt from disclosure pursuant to the third exemption of the FOIA, which provides for the withholding of information specifically protected from disclosure by statute. The specific statutes applicable in this case are Title 18 U.S. Code 798; Title 50 U.S. Code 3024(i); and Section 6, Public Law 86-36 (50 U.S. Code 3605).

Since these deletions may be construed as a partial denial of your request, you are hereby advised of this Agency's appeal procedures.

You may appeal this decision. If you decide to appeal, you should do so in the manner outlined below. NSA will endeavor to respond within 20 working days of receiving any appeal, absent any unusual circumstances.

- The appeal must be sent via U.S. postal mail, fax, or electronic delivery (e-mail) and addressed to:

NSA FOIA/PA Appeal Authority (P132)
National Security Agency
9800 Savage Road STE 6932
Fort George G. Meade, MD 20755-6932

The facsimile number is 443-479-3612.
The appropriate email address to submit an appeal is
FOIARSC@nsa.gov.

- It must be postmarked or delivered electronically no later than 90 calendar days from the date of this letter. Decisions appealed after 90 days will not be addressed.
- Please include the case number provided above.
- Please describe with sufficient detail why you believe the denial of requested information was unwarranted.

You may also contact our FOIA Public Liaison at foialo@nsa.gov for any further assistance and to discuss any aspect of your request. Additionally, you may contact the Office of Government Information Services (OGIS) at the National Archives and Records Administration to inquire about the FOIA mediation services they offer. The contact information for OGIS is as follows:

Office of Government Information Services
National Archives and Records Administration
8601 Adelphi Rd. - OGIS
College Park, MD 20740
ogis@nara.gov
877-684-6448
(Fax) 202-741-5769

Sincerely,

A handwritten signature in black ink that reads "Ron Mapp". The signature is written in a cursive style with a large "R" and "M".

RONALD MAPP
Chief, FOIA/PA Office
NSA Initial Denial Authority

Encls:
a/s

~~SECRET~~

NATIONAL SECURITY AGENCY

MILITARY CRYPTANALYTICS

Part III

By

LAMBROS D. CALLIMACHOS

October 1977

Classified by DIRNSA/CHCSS (NSA/CSSM 123-2)
Exempt from GDS, EO 11652, Cat 2
Declassify Upon Notification by the Originator

National Security Agency
Fort George G. Meade, Maryland

~~SECRET~~

~~SECRET~~

NATIONAL SECURITY AGENCY

MILITARY CRYPTANALYTICS

Part III

By

LAMBROS D. CALLIMAHOS

October 1977

Classified by DIRNSA/CHCSS (NSA/CSSM 123-2)
Exempt from GDS, EO 11652, Cat 2
Declassify Upon Notification by the Originator

National Security Agency
Fort George G. Meade, Maryland

~~SECRET~~

Give me an ounce of civet, good apothecary, to sweeten my imagination.

—Shakespeare.
(King Lear, Act IV, Sc. 6)

Preface

1. I wish to acknowledge my indebtedness to William F. Friedman in drawing upon portions of his early work, "Military Cryptanalysis, Part III," for much of the material treated in Chapters I–V. Chapters IV–XI are revisions of seven of my monographs in the *NSA Technical Literature Series*, viz.: Monograph No. 19, "The Cryptanalysis of Ciphertext and Plaintext Autokey Systems"; Monograph No. 20, "The Analysis of Systems Employing Long or Continuous Keys"; Monograph No. 21, "The Analysis of Cylindrical Cipher Devices and Strip Cipher Systems"; Monograph No. 22, "The Analysis of Systems Employing Gearing Disk Cryptomechanisms"; Monograph No. 23, "Fundamentals of Key Analysis"; Monograph No. 15, "An Introduction to Teleprinter Key Analysis"; and Monograph No. 18, "Ars Conjectandi: The Fundamentals of Cryptodiagnosis."

2. I also wish to acknowledge my indebtedness to Francis T. Leahy for keeping me out of statistical mischief, and to Bruce W. Fletcher for his expert assistance in the final proofreading, and for checking the cryptograms and the various diagrams.

—L. D. C.

(b) (1)
(b) (3) -18 USC 798
(b) (3) -50 USC 3024 (i)
(b) (3) -P.L. 86-36

TABLE OF CONTENTS

MILITARY CRYPTANALYTICS, PART III

Aperiodic Substitution Systems

<i>Chapter</i>	<i>Page</i>
I. Introduction	1
1. Preliminary remarks. 2. General remarks on cryptographic periodicity. 3. Effects of varying the length of plaintext groupings. 4. Primary and secondary periods; resultant periods. 5. Cryptographic principles of aperiodic systems. 6. Fundamental cryptanalytic considerations in the solution of aperiodic systems.	
II. Systems using constant-length keying units to encipher variable-length plaintext groupings	7
7. General remarks. 8. Aperiodic encipherment produced by plaintext sequences grouped according to word lengths. 9. Solution when known cipher alphabets are involved. 10. Solution when unknown cipher alphabets are involved. 11. Solution by means of idiomorphs and the probable-word method. 12. Solution by means of isomorphs. 13. Additional remarks.	
III. Systems using variable-length keying units to encipher constant-length plaintext groupings	25
14. General. 15. Plaintext interruptor systems. 16. Ciphertext interruptor systems. 17. Systems employing externally generated or determined keys. 18. Solution when known cipher alphabets are employed. 19. Solution when unknown cipher alphabets are employed. 20. Additional remarks.	
IV. Ciphertext autokey systems	41
21. The cryptography of autokey encipherment. 22. Solution of ciphertext autokeyed cryptograms when known cipher alphabets are employed. 23. Principles of solution by frequency analysis. 24. Example of solution by frequency analysis. 25. Solution by means of isomorphs. 26. Solution of isologs involving the same pair of unknown primary components. [REDACTED]	
28. Further remarks on ciphertext autokey systems.	
V. Plaintext autokey systems	75
29. Preliminary remarks on plaintext autokeying. 30. Solution of plaintext autokey systems when known cipher alphabets are employed and the introductory key consists of a single letter. 31. Solution of plaintext autokey systems involving known cipher alphabets when the introductory key consists of several letters. 32. Analysis of a case involving unknown components. [REDACTED]	
34. Analysis of digital plaintext autokey systems. 35. Concluding remarks on autokey systems.	
VI. Systems employing long or continuous keys	121
36. Preliminary remarks. 37. Depth and its exploitation. 38. Solution of a single cryptogram involving known primary components and an unknown plaintext running key. [REDACTED]	
41. Recovery of plain texts and the unknown primary components from a number of messages in flush depth. [REDACTED]	

<i>Chapter</i>	<i>Page</i>
VII. Cylindrical cipher devices and strip cipher systems	151
45. General. 46. Reconstruction of unknown cipher alphabets. 47. Analysis of cryptograms involving known alphabets but with unknown keys. 48. Further remarks.	
VIII. Systems employing geared disk cryptomechanisms	173
49. Introduction. 50. The Wheatstone cipher device. 51. Analysis of the Wheatstone cipher device. 52. The Kryha cipher machine. 53. Analysis of the original Kryha machine.	
[REDACTED]	
IX. Fundamentals of key analysis	227
56. Convenient sources of key. 57. Manual key generation methods. 58. Mechanical and electronic key generators. 59. General analytic approaches. 60. Analysis of key in a double transposition cipher. [REDACTED]	
62. Concluding remarks.	
X. Teleprinter key analysis	263
63. General. 64. Teleprinter key generation methods. 65. Analysis of combination streams. [REDACTED]	
XI. Principles of cryptodiagnosis	323
71. General. 72. The basic steps in diagnosis. 73. The diagnostician and his attributes. 74. Embarking on the unknown cryptosystem. 75. Preliminary actions in attacking the unknown cryptosystem. 76. First step: manipulating the data. 77. Second step: recognizing the phenomena. 78. Third step: interpreting the phenomena. 79. [REDACTED]	
[REDACTED] Post mortem.	
XII. Concluding remarks	415
81. Special cases of aperiodic encipherment. 82. Analysis and solution of a first case. 83. Analysis and solution of a second case. 84. Final remarks.	
APPENDICES	
1. De Profundis; or the ABC of Depth Reading	437
2. Synoptic Tables, Cipher Device M-94	447
3. Tables of the Poisson distribution	463
4. Table of the Binomial distribution for $p = \frac{1}{10}$	537
5. Plaintext and random material for sampling purposes	553
6. Basic letter frequency data, 24 foreign languages	561
7. Problems—Military Cryptanalytics, Part III	611
INDEX	653

(b) (1)
 (b) (3)-18 USC 798
 (b) (3)-50 USC 3024 (i)
 (b) (3)-P.L. 86-36

(b) (1)
(b) (3) -18 USC 798
(b) (3) -50 USC 3024 (i)
(b) (3) -P.L. 86-36

CHAPTER I
INTRODUCTION

	Paragraph
Preliminary remarks.....	1
General remarks on cryptographic periodicity.....	2
Effects of varying the length of plaintext groupings.....	3
Primary and secondary periods; resultant periods.....	4
Cryptographic principles of aperiodic systems.....	5

1. Preliminary remarks.—*a.* This text constitutes the third in the series of six basic texts on the science of cryptanalytics.¹ The first two texts together have covered most of the necessary fundamentals of cryptanalytics; this and the remaining three texts will be devoted to more specialized and more advanced aspects of the science.

b. It is assumed that the cryptanalyst reader has studied *Military Cryptanalytics, Parts I and II*, and is familiar with the cryptologic terminology, concepts, principles, and techniques of solution of the various cryptosystems treated in those texts. *This general background is a necessary prerequisite to the thorough understanding of the principles expounded in this and the succeeding volumes.* Where appropriate, however, reference will be made to particular portions of the first two volumes; the reader would be wise to have these volumes handy when undertaking the study of this present text.

c. The text immediately preceding this one dealt with various types of periodic polyalphabetic substitution, commonly called *repeating-key systems*. It was seen in these repeating-key systems how a regularity in the employment of a limited number of alphabets, or even the employment of a complete set of alphabets in succession as in a progressive alphabet system, results in the manifestation of periodicity or cyclic phenomena in the cryptogram, by means of which the latter may be solved. The difficulty of solution is directly correlated with the type and number of cipher alphabets employed in specific examples.

d. Two procedures might suggest themselves to an enemy cryptographer for consideration if he realizes the foregoing circumstances and he thinks of methods to eliminate the weaknesses inherent in repeating-key ciphers. First, noting that the difficulties in solution increase as the length of the key increases, he might consider employing much longer keys as a means of increasing the security of the messages. Upon second thought, however, if the enemy cryptographer recognizes that, as a general rule, the first step in the solution of these ciphers consists in ascertaining the number of alphabets employed, it might seem to him that the most logical thing to do would be to use a procedure which will avoid periodicity altogether, eliminating the cyclic phenomena that are normally manifested within cryptograms of periodic construction, and thus foil even a first step towards solution. In other words, the cryptographer might progress from the use of rather short repeating keys (of perhaps no more than a dozen letters or so) to the use of key phrases of, let us say, 25-40 letters or thereabouts; subsequently, he might embark upon the use of keying procedures which would have the effect of producing keys of a length approximately equal to that of the average message being enciphered; and finally, he might advance to a stage of keying sophistication wherein the key consists of hundreds or thousands of elements, or even of an infinite number of elements (as, for example, in autokey systems).

¹ Before the echoes of the first sentence of this third volume have died down, the distinction between the *science* of cryptanalytics and the *art* of cryptanalysis should be re-emphasized. The cryptanalyst pursues studies along general and detailed lines, in order to equip himself technically for the duties of the moment or of the future. This parallels quite closely the technical studies of a violinist, who progresses from elementary exercises to the études of Kreutzer and Rode and finally to the Caprices of Paganini; in the meanwhile, the violinist has also studied various solo works and chamber music as a means of enhancing his comprehension and appreciation of music in general. All that a technical background does for the violinist is to give him the means of artistic expression or synthesis of musical thoughts from the coding of clefs, keys, and notes; all that a technical background does for the cryptanalyst is to give him the means for imaginative expression or synthesis of plaintext meanings from the coding of systems, keys, and characters. See also in this connection footnote 5 on p. 3 of *Military Cryptanalytics, Part I*.

e. At this point in our discussion it would be well to examine two terms defined in the previous volume:

- (1) *periodic system*. A system in which the enciphering process is repetitive in character and which usually results in the production of cyclic phenomena in the cryptographic text.
- (2) *aperiodic system*. A system in which the method of keying does not bring about cyclical phenomena in the cryptographic text.

The foregoing are *practical* definitions—nobody in his right mind (and that of course includes all of our readers)² would classify a Hagelin C-38 system³ as periodic just because it really *is* periodic with a finite cycle of 26x25x23x21x19x17 or 101,405,850; nor would the same right-minded individual quibble with the classification of a system as aperiodic if the length of the key is only 1000 letters and messages very rarely exceed that length. In brief, what we are in effect saying is that, even if a system embraces in its principle a fixed cycle or period, unless the period is considerably shorter than the messages being enciphered (thus permitting the manifestation of cyclic phenomena), the system may nevertheless for all practical purposes be considered as aperiodic *since the solution of a message is not predicated on writing the cipher text on several superimposed cycles and then solving the cryptographic depth thus produced*.

f. In this text we shall first examine varieties of aperiodic (as just defined) polyalphabetic substitution systems; then we shall study methods of extending or lengthening short mnemonic keys, followed by systems using lengthy keys (to include digital and teleprinter systems). Subsequently, we shall study methods of solution of some typical cryptomechanisms and cipher machines, and aperiodic combination systems. The text proper will end with a discussion of principles of key analysis as applied in manual and machine cryptosystems, followed by an extensive treatment of cryptodiagnosis. The appendices include useful cryptologic and cryptomathematical reference material, concluding with a course of problems designed to insure comprehension of the principles expounded in this volume.

2. General remarks on cryptographic periodicity.—*a*. When we consider the nature of periodicity in polyalphabetic substitution systems, we note that it is composed of *two* fundamental factors, because there are in reality *two* elements involved in its production. We have appreciated the fact that periodicity necessitates the use of a keying element employed in a cyclic manner; now we begin to realize that there is also another element involved, *viz.*, that unless the key is applied to constant-length plaintext groupings, no periodicity will be manifested externally in the cipher text, despite the repetitive or cyclic use of a constant-length key. This realization is quickly followed by the idea that possibly all periodicity may be avoided or suppressed by either or both of two ways: (1) by using constant-length keying units to encipher variable-length plaintext groupings, or (2) by using variable-length keying units to encipher constant-length plaintext groupings.

b. In the usual types of polyalphabetic substitution systems, successive letters of the repeating key are applied to successive letters of the text. With respect to the employment of the key, the cryptographic process may be said to be *constant* or *fixed* in character. This is true even if a single keying unit serves to encipher two or more letters at a time, provided only the groupings of plaintext letters are constant in length. In all such cases of encipherment by constant-length groupings, the apparent length of the period (as found by applying the factoring process to the cryptograms) is a multiple of the real length and the multiple corresponds to the length of the groupings, *i.e.*, the number of plaintext letters enciphered by the same key letter. It is to be noted, however, that all these cases are still periodic, because *both* the keying units and the plaintext groupings are constant in length.

3. Effects of varying the length of plaintext groupings.—*a*. Now let us consider the effects of making either one or the other of these two elements *variable* in length. Suppose that the plaintext groups are made variable in length and that the keying units are kept constant in length. Then, even though the key may be cyclic and may repeat itself many times in the course of encipherment, external periodicity is suppressed, *unless the law governing the variation in plaintext groupings is itself cyclic, and the length of the message is greater than that of the cycle applicable to this variable grouping*.

² To scholars of English who experience a quick intake of breath at this point, the author hastens to clarify that the parenthetical phrase is intended to modify only the four immediately preceding words.

³ Cf. pp. 458-464 of *Military Cryptanalytics, Part II*.

b. As an example illustrating the italicized portion of the preceding sentence, let us suppose the correspondents agree to use reversed standard cipher alphabets with the key word SIGNAL, and that in the encryption the message is divided into groups as shown below:

S	I	G	N	A	L	S	I	G	N	A	L	S	I	G
1	12	123	1234	12345	1	12	123	1234	12345	1	12	123	1234	12345
C	OM	MAN	DING	GENER	A	LF	IRS	TARM	YHASI	S	SU	EDO	RDER	SEFFE
<u>Q</u>	<u>UW</u>	<u>UGT</u>	KFAH	UWNWJ	L	HN	<u>ARQ</u>	NGPU	PGNVF	I	TR	OPE	RFER	OCBBC
N	A	L	S	I	G	N	A	L	S	I	G	N	A	L
1	12	123	1234	12345	1	12	123	1234	12345	1	12	123	1234	12345
C	TI	VET	WENT	YFIRS	T	AT	NOO	NDIR	ECTIN	G	TH	ATT	ELEP	HONES
L	HS	QHS	WOFZ	<u>KDARQ</u>	N	NU	NMM	YIDU	OQZKF	C	NZ	NUJ	WPWL	EXYHT
S	I	G	N	A	L	S	I							
1	12	123	1234	12345	1	12	123							
C	OM	MAS	WITC	HBOAR	D	SC	OMM...							
<u>Q</u>	<u>UW</u>	<u>UGO</u>	RFUL	TZMAJ	I	AQ	UWW							

Cryptogram

<u>QUWUG</u>	TKFAH	UWNWJ	LHN <u>AR</u>	<u>QNGPU</u>	PGNVF	ITROP	ERFER	OCBBC	LHSQH
SWOFZ	<u>KDARQ</u>	NNUNM	MYIDU	OQZKF	CNZNU	UWPWL	EXYHT	<u>QUWUG</u>	ORFUL
TZMAJ	IAQUW	W...							

The cipher text in this example shows a tetragraphic and a pentagraphic repetition. The two occurrences of $QUWUG_c (=COMMA_p)$ are separated by an interval of 90 letters; the two occurrences of $ARQN_c (=IRST_p)$ by 39 letters. The first repetition ($QUWUG_c$), it will be noted, is a true periodic repetition, since the plaintext letters, their groupings, and the key letters are identical. The interval in this case, if counted in terms of letters, is the product of the keying cycle, 6, and the grouping cycle, 15. The second repetition ($ARQN_c$) is not a true periodic repetition in the sense that both cycles have been completed at the same point, as is the case in the first repetition. It is true that $ARQN_c$, representing $IRST_p$ both times, is a *causal* repetition produced by the action of the same combination of key letters, I and G, but the enciphering points in the grouping cycle are different in the two occurrences. Repetitions of this type may be termed *partially periodic* repetitions, to distinguish them from those of the *completely periodic* type.

c. When the intervals between the two repetitions noted above are more carefully studied, especially from the point of view of the interacting cycles which brought them about, it will be seen that, counting according to *groupings* and not according to single letters, the two pentagraphs $QUWUG_c$ are separated by an interval of 30 groupings. Or, if one prefers to look at the matter in the light of the keying cycle, the two occurrences of $QUWUG_c$ are separated by 30 key letters. Since the key is but 6 letters long, it has gone through 5 cycles. Thus, the number 30 is the product of the number of letters in the keying cycle (6) and the number of different-length groupings in the grouping cycle (5). The interaction of these two cycles is like that of two gears in mesh, one driven by the other. One of these gears has 6 teeth, the other 5, and the teeth are numbered. If the two gears are adjusted so that the teeth marked "1" are adjacent to each other and the gears are caused to revolve, these two teeth will not come together again until the larger gear has made 5 revolutions and the smaller one 6. During this time, a total of 30 meshings of individual teeth will have occurred. But since one revolution of the smaller gear (=the grouping cycle) represents the encipherment of 15 letters (when translated in terms of letters), the 6 complete revolutions of this gear mean the encipherment of 90 letters. This accounts for the period of 90, when stated in terms of letters.

d. The two occurrences of the other repetition, $ARQN_c$, are at an interval of 39 letters; but in terms of the number of intervening groupings, the interval is 12, which is obviously two times the length of the keying cycle. In other words, the key has in *this* case passed through two cycles.

e. In a long message enciphered according to such a scheme as the foregoing, there would be many repetitions of both types discussed above (the completely periodic and the partially periodic) so that

the cryptanalyst might encounter some difficulty in his attempts to reach a solution, especially if he had no information as to the basic system. It is to be noted in this connection that if any one of the groupings exceeds, say, 5 letters or so in length, the scheme may give itself away rather easily, since it is clear that *within each grouping the encipherment is strictly monoalphabetic*. Therefore, in the event of groupings of more than 5 or 6 letters, the monoalphabetic equivalents of telltale words such as ATTACK, BATTALION, DIVISION, would stand out. This system is most efficacious, therefore, with short groupings.

f. It should also be noted that there is nothing about the scheme which requires a regularity in the grouping cycle such as that embodied in the example. A lengthy grouping cycle guided by a key of its own may just as easily be employed; for example, the *number* of dots and dashes contained in the International Morse signals⁴ for the letters composing the 25-letter key phrase DECLARATION OF INDEPENDENCE might be used. Thus, A (. -) has 2, B (- . . .) has 4, and so on. Hence:

D E C L A R A T I O N O F I N D E P E N D E N C E
3 1 4 4 2 3 2 1 2 3 2 3 4 2 2 3 1 4 1 2 3 1 2 4 1

The grouping cycle is 3+1+4+4+2+ . . . , or 60 letters in length, and if the same phrase is used as a repeating key the total period would of course be 60, since after the encipherment of 60 letters the first key letter would be used again to encipher 3 letters, and so on, repeating the cycle. Suppose, however, that the foregoing 60-element keying pattern were used in conjunction with a different literal sequence for the actual key letters, say the 38-letter phrase CONSTITUTION OF THE UNITED STATES OF AMERICA. The period would then be the least common multiple of 38 and 60, or 1140 letters. This system might appear at first glance to yield a fairly high degree of cryptographic security; but this is not the case, as we shall presently see.

4. **Primary and secondary periods; resultant periods.**—a. It has been noted that the length of the complete period in a system such as the foregoing is the least common multiple of the length of the two component or interacting periods. In a way, therefore, since the *component* periods constitute the basic elements of the scheme, they may be designated as the *basic* or *primary* periods. These are also *hidden* or *latent* periods. The *apparent* or *patent* period, that is, the complete period, may be designated as the *resultant* or *secondary* period. In certain types of cipher machines there may be more than two primary periods which interact to produce a resultant period; also, there are cases in which the latter may interact with another primary period to produce a tertiary period, and so on.⁵ The *final*, or *resultant*, or *apparent* period is sometimes the one which is usually ascertained first as a result of the study of the intervals between repetitions. This may or may not be broken down into its component primary periods.

b. Although a solution may often be obtained without breaking down a resultant period into its component primary periods, the reading of many messages pertaining to a widespread system of secret communication is much facilitated when the analysis is pushed to its lowest level, that is, to the point where the final cryptographic scheme has been reduced to its simplest terms. This may involve the discovery of a multiplicity of simple elements which interact in successive cryptographic strata.

5. **Cryptographic principles of aperiodic systems.**—a. A discussion of the methods for avoiding periodicity was contained in the preceding text.⁶ A brief résumé of these methods is given below:

- (1) Elements of a fixed or invariable-length key are applied to variable or irregular-length groupings of the plain text.
- (2) Elements of irregular-length (variable-length) key are applied to regular and fixed groupings of the plain text.
- (3) The principles of (1) and (2) are combined into a single system.

⁴ Cf. p. 23, *Military Cryptanalytics, Part I.*

⁵ An example of a cipher machine with several interacting latent periods is the Hagelin C-38. This machine produces in effect at any given moment six simultaneous reversed-standard-alphabet monoalphabetic substitutions in all 26 combinations of their presence or absence. The activity of each contributing monoalphabetic substitution is strictly periodic, with cycles of 26, 25, 23, 21, 19, or 17, conforming to the six regularly stepping pinwheels of the stated sizes. The total cycle of the machine is the product of the six relatively prime numbers, but the presence of individual subcycles constitutes one of the serious weaknesses of the machine.

⁶ Cf. par. 99, *Military Cryptanalytics, Part II.*

(4) The key does not repeat itself; this is brought about either by constructing a nonrepeating key, or by employing the key in a special manner (such as in plaintext- and ciphertext interruptor systems and plaintext- and ciphertext autokey systems).

b. From the standpoint of cryptographic mechanics, aperiodic systems may be divided into two main classes, viz.:

(1) Systems in which the key elements are not in any way determined or influenced by any elements of the plain or cipher text; and

(2) Systems in which the key elements are generated or governed by the plain text being enciphered or by the resultant cipher text.



⁷ Cf. par. 65 (on p. 157) of *Military Cryptanalytics, Part II.*



(b) (1)
(b) (3) -18 USC 798
(b) (3) -50 USC 3024 (i)
(b) (3) -P.L. 86-36

CHAPTER II

SYSTEMS USING CONSTANT-LENGTH KEYING UNITS TO ENCIPHER VARIABLE-LENGTH PLAINTEXT GROUPINGS

	Paragraph
General remarks	7
Aperiodic encipherment produced by plaintext sequences grouped according to word lengths.....	8
Solution when known cipher alphabets are involved.....	9
Solution when unknown alphabets are involved	10
Solution by means of idiomorphs and the probable-word method.....	11
Solution by means of isomorphs.....	12
Additional remarks	13

7. **General remarks.**—*a.* The system described in subpar. 3*b* is obviously not to be classified as aperiodic in nature, despite the incorporation into the cryptosystem of a variable which in that case consisted of irregularity in the length of one of the two elements (key text and plain text) involved in polyalphabetic substitution. The variable there was subject to a law which in itself was periodic in character.

b. To make such a system truly aperiodic (under the definition given in subpar. 1*e*), by elaborating upon the basic scheme for producing variable-length plaintext groupings, would be possible, but impractical. For example, using the Morse code method illustrated in subpar. 3*f* for determining the key and simultaneously the lengths of the groupings, one might employ the text of a book; and if the book is longer than the message to be enciphered, the cryptogram would certainly show no periodicity as regards the intervals between any repetitions which might occur. However, as already indicated, such a scheme would not be very practical for regular intercommunication between a large number of correspondents, for reasons which are quite apparent. Encipherment and decipherment would be slow, cumbersome, onerous, and very subject to error; the book would have to be safeguarded as would a code book; and, unless the same key text were used for all messages, methods or indicators would have to be adopted to show exactly where encipherment begins in each message. Therefore a simpler method is desirable for producing constantly changing, aperiodic plaintext groupings.

8. **Aperiodic encipherment produced by plaintext sequences grouped according to word lengths.**—

a. The simplest method for producing aperiodic plaintext groupings is encipherment according to the actual word lengths of the message being encrypted. Although the *average* number of letters composing the words of any alphabetical language is fairly constant, *successive* words comprising plain text vary a great deal in this respect, and this variation is subject to no law.¹ In telegraphic English, for example, the mean length of words is 5.2 letters; the words may contain from 1 to 15 or more letters, but the successive words vary in length in an extremely irregular manner, no matter how long the text may be.

b. As a consequence, the use of word lengths for determining the number of letters to be enciphered by each key letter of a repetitive key suggests itself to a cryptographer as soon as he comes to understand the way in which repeating-key ciphers are solved. For, he asks, if there is no periodicity in the cryptograms, how can the letters of the cipher text written in 5-letter groups be distributed into their respective monoalphabets? And if this very first step is impossible, how can the cryptograms be solved? We shall see.

9. **Solution when known cipher alphabets are involved.**—*a.* Despite the foregoing rhetorical questions, the solution is really quite simple when the cipher alphabets involved are standard alphabets or are otherwise composed of known sequences. All that is involved is the completion of the plain-component sequence (preceded by, if the situation so demands, conversion into plain-component equivalents). In monoalphabetic substitution systems, all of the words of the entire message come out on a single gen-

¹ It is true, of course, that the differences between the vocabularies of two writers are often marked and can be measured. These differences may be subject to certain laws, but these laws are psychological rather than mathematical. See Rickert, E., *New Methods for the Study of Literature*, University of Chicago Press, Chicago, 1927.

eratrix in the completion diagram; in the case of the system discussed in subpar. 8b, since the individual, separate words of a message are enciphered by different key letters, *these words will reappear on different generatrices of the diagram*. All the cryptanalyst has to do is to pick them out; he can do this once he has found a good starting point, by using a little imagination and following clues afforded by the context.

b. As an example, let us consider the following intercepted message:

S U H P Z T C E P L G L Q K C X H V K M V J L Z A K X W H A
Y T O W N H B A F E X A V E Q A U V Z I E B P O B

In the course of routine study of the message, the plain-component sequence is completed for the first 15 letters of the cryptogram, on the assumptions of direct and reversed standard cipher alphabets, as shown in Figs. 2a and b, respectively, below:²

S U H P Z T C E P L G L Q K C
T V I Q A U D F Q M H M R L D
U W J R B V E G R N I N S M E
V X K S C W F H S O J O T N F
W Y L T D X G I T P K P U O G
X Z M U E Y H J U Q L Q V P H
Y A N V F Z I K V R M R W Q I
Z B O W G A J L W S N S X R J
A C P X H B K M X T O T Y S K
B D Q Y I C L N Y U P U Z T L
C E R Z J D M O Z V Q V A U M
D F S A K E N P A W R W B V N
E G T B L F O Q B X S X C W O
F H U C M G P R C Y T Y D X P
G I V D N H Q S D Z U Z E Y Q
H J W E O I R T E A V A F Z R
I K X F P J S U F B W B G A S
J L Y G Q K T V G C X C H B T
K M Z H R L U W H D Y D I C U
L N A I S M V X I E Z E J D V
M O B J T N W Y J F A F K E W
N P C K U O X Z K G B G L F X
O Q D L V P Y A L H C H M G Y
P R E M W Q Z B M I D I N H Z
Q S F N X R A C N J E J O I A
R T G O Y S B D O K F K P J B

FIGURE 2a

S U H P Z T C E P L G L Q K C
H F S K A G X V K O T O J P X
I G T L B H Y W L P U P K Q Y
J H U M C I Z X M Q V Q L R Z
K I V N D J A Y N R W R M S A
L J W O E K B Z O S X S N T B
M K X P F L C A P T Y T O U C
N L Y Q G M D B Q U Z U P V D
O M Z R H N E C R V A V Q W E
P N A S I O F D S W B W R X F
Q O B T J P G E T X C X S Y G
R P C U K Q H F U Y D Y T Z H
S Q D V L R I G V Z E Z U A I
T R E W M S J H W A F A V B J
U S F X N T K I X B G B W C K
V T G Y O U L J Y C H C X D L
W U H Z P V M K Z D I D Y E M
X V I A Q W N L A E J E Z F N
Y W J B R X O M B F K F A G O
Z X K C S Y P N C G L G B H P
A Y L D T Z Q O D H M H C I Q
B Z M E U A R P E I N I D J R
C A N F V B S Q F J O J E K S
D B O G W C T R G K P K F L T
E C P H X D U S H L Q L G M U
F D Q I Y E V T I M R M H N V
G E R J Z F W U J N S N I O W

FIGURE 2b

c. In the diagram in Fig. 2b we note the word CAN at the beginning of one generatrix, then in the very next six columns the words YOU and GET in two other generatrices. That we should get some three-letter words on various generatrices is not particularly remarkable; (note the short words produced purely by accident in the generatrices of Fig. 2a) but that these words should follow one another in direct sequence in succeeding columns, and that the three words in question should be in excellent *contextual relationship* to form a plausible and *convincing* sentence beginning such as "CAN YOU GET . . ."

² One of the first things, if not the very first, to be done to a cryptogram in an undiagnosed system is the completion of the plain-component sequence on the basis of standard alphabets. In certain cases a solution is sometimes achieved by this means that would be impossible by any other. The completion is painless if accomplished by sliding strips; its probability of success in an isolated case is small, but the ratio of the time expended to its potential value is very large. This is a typical illustration of the application of the maxim of the experienced cryptanalyst: "Try the simplest thing first."

is more than remarkable (= a probability of .01 of random occurrence)—it is astonishing (= random probability of .0001).³

d. From here on the rest of the solution follows easily. If the cryptanalyst comes to a temporary halt (as in the example in Fig. 2b) in recovering further words on the generatrices, he can search in subsequent positions of the generatrix diagram for more words to be disclosed, and then he can fill in the missing portions from context and take another look at the generatrices. Or, it might be simpler if the cryptanalyst recovers a fragment of the specific key for the message, and then expands this key by steps to assist in reading the rest of the plain text. For example, in the case under discussion the cryptanalyst would get U, N, and I as key letters⁴ for the successive words of the plain text CAN YOU GET; these letters suggest the words UNION, UNITED, UNIVERSITY, etc. The complete solution is given below, with the recovered specific key being UNITED NATIONS.⁵

U N I T E D N A T I O N S
CAN YOU GET IN TOUCH WITH SECOND DETACHMENT STOP LINES OUT OF ORDER
SUH PZT CEP LG LQKCX HVKW VJLZAK XWHAYTOWNH BAFE XAVEQ AUV ZI EBPOB

The only minor difficulty of such a solution is that of making the first step and getting a good start on a word. If the words are short it is rather easy to overlook good possibilities and thus spend some time in fruitless searching. However, solution must come; if nothing good appears at the beginning of the message, search should be made in the interior of the cryptogram or at the end.

10. Solution when unknown cipher alphabets are involved.—a. It has been seen from the foregoing that solution of cryptograms involving word-length encipherment by standard alphabets is rather trivial, not because there is any magical quality about standard alphabets, but because the components are *known sequences*. If any other components had been used, say a plain component based upon a HYDRAULIC keyword-mixed sequence and a cipher component based on a QUESTIONABLY keyword-mixed sequence, and if these components were *known*, the problem would have been pursued in exactly the same way, *viz.*, conversion of the cipher letters of the cryptogram into their plain-component (HYDRAULIC . . . XZ) equivalents and completion of the plain-component (HYDRAULIC . . . XZ) sequence.

b. But what if one or both of the components are unknown mixed sequences? The simple procedure of completing the plain-component sequence obviously cannot be used. Since the messages are poly-alphabetic, and since the process of factoring cannot be applied, it would seem that the solution of messages enciphered in different alphabets and according to word lengths would be a difficult matter. Nevertheless, as is about to be demonstrated, the solution, even of a single message, is not nearly so difficult as first impression might lead one to imagine; the *modus operandi* will be explained in pars. 11 and 12.

11. Solution by means of idiomorphs and the probable-word method.—a. The first case to be studied involving unknown alphabets will be one wherein the original word lengths are retained in the cryptogram; this case will be discussed not because it is often encountered in practical military cryptography, but because it affords a good introduction to the usual case in which the original word lengths are no longer in evidence in the cryptogram, the latter appearing in the customary 5-letter groups. If the words

³ We must never forget that probabilities are influenced by the *amount* of material under examination; if we looked at *enough* material, it might not be at all astonishing if we obtained even a 10-letter word by accident. In all the probability considerations in this text, unless otherwise stated it is assumed that we are dealing with a limited amount of traffic, limited enough so that a probability of .01 is remarkable, and a probability of .001 exciting.

⁴ The key letters are assumed to be under A_p as the index letter. Throughout this text, whenever encipherment processes are under discussion, the pair of enciphering equations commonly referred to as characterizing the so-called Vigenère method will be understood unless otherwise indicated. This method involves the pair of enciphering equations $\theta_{k/2} = \theta_{i/1}$; $\theta_{p/1} = \theta_{c/2}$. That is, the index letter, which is usually the initial letter of the plain component, is set opposite the key letter in the cipher component; the plaintext letter to be enciphered is sought in the plain component and its equivalent is the letter opposite it in the cipher component. See in this connection subpar. 13f of *Military Cryptanalytics Part II*.

⁵ This is the specific key as recovered from this single message. It is quite possible that the complete key is UNITED NATIONS ORGANIZATION, UNITED NATIONS SECURITY COUNCIL, etc.; a longer message would prove whether the key is UNITED NATIONS used repetitively, or whether it is a phrase beginning with these two words.

of a message are enciphered monoalphabetically, the true and complete idiomorphs of word patterns will be patent, regardless of the identity of the particular alphabet used in the encryption of each word. These idiomorphs and word lengths can then be used as a basis for the probable-word method of attack.

b. Let us study the following low-echelon ground message in which the actual word lengths have been preserved in the cipher text:⁶

IUITD QHIWE LVCGWPCLZ RP NIV GYPYSYCV NC IXHCXWUJ ORS ZXH
GRPPRVQDOB SE OKYNMMHKV GUJLTN MYIN WZ IVURNI CLSWZVHS

We note some strong idiomorphic sequences, in particular the following:

- (1) IUITD
aba
- (2) GYPYSYCV
abaca
- (3) GRPPRVQDOB
abba
- (4) OKYNMMHKV
abcddea

Looking up these patterns in idiomorph lists,⁷ and guided by the delimitations of the words, we arrive at the following assumptions:

- (1) IUITD
ENEMY
- (2) GYPYSYCV
DIVISION
- (3) GRPPRVQDOB
BATTALIONS
- (4) OKYNMMHKV
ARTILLERY

The cipher values of these plain-cipher equivalencies are entered into a sequence reconstruction matrix of four levels (representing the four word assumptions), as follows:

P:	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	
(1)									I												T	U				D	
(2)							G				Y											V	C		S		P
(3)	R	G									Q		V		O	D									B	P	
(4)	O							H			N		M											K	Y		V

FIGURE 3a

Noting in lines (2) and (3) that the intervals between the letters G, V, and P are the same in both cases, we can assume direct symmetry⁸ of position. In a few moments our reconstruction matrix will look like this:

P:	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
(1)	S	H	B	P	I	N				M	R	G	T	U	K	Y	Q				V	C	O	D		
(2)	M		R	G	T	U	K	Y	Q			V	C	O	D	S	H	B	P	I	N					
(3)	R	G	T	U	K	Y	Q				V	C	O	D	S	H	B	P	I	N					M	
(4)	O	D		S	H	B	P	I	N			M	R	G	T	U	K	Y	Q			V	C			

FIGURE 3b

c. The rest of the plain text can be recovered either by (1) completion of the plain-component sequence, insofar as possible, in order to reveal further plaintext fragments which may be expanded and thus make possible the filling in of additional values in the cipher component, or by (2) recovery and expansion of the partial specific key for the message. An important additional step in solution is the recovery of the missing letters in the cipher component by analysis of the construction of the component in cases of systematic derivation. These points will be taken up in order in the subparagraphs below.

⁶ Foolish as this may be, it has happened in operational practice.
⁷ Cf. Appendix 3, *Military Cryptanalytics, Part I*.
⁸ Cf. par. 28, *Military Cryptanalytics, Part II*.

(1) Let us complete the plain-component sequence on the second and third words of the message, after first converting the cipher letters into their plain-component equivalents (where known), using for this purpose the uppermost cipher alphabet given in Fig. 3b. This is shown in the illustration below:

<u>IUITD</u>	<u>QHIWE</u>	<u>LVCGWPC LZ</u>
ENEMY	SBE	VWL DW
	TCF	WXM EX
	UDG	XYN FY
	VEH	YZO GZ
	WFI	ZAP HA
	XGJ	ABQ IB
	YHK	BCR JC
	ZIL	CDS KD
	AJM	*DET LE
	BKN	EFU MF
	*CLO	FGV NG
	DMP	GHW OH
	ENQ	HIX PI
	*FOR	IJY QJ
	GPS	JKZ RK
	HQT	KLA SL
	IRU	LMB TM
	JSV	MNC UN
	KTW	NOD VO
	LUX	OPE WP
	MVY	PQF XQ
	NWZ	QRG YR
	OXA	RSH ZS
	PYB	*STI AT
	QZC	TUJ BU
	*RAD	UVK CV

FIGURE 4a

<u>LVCGWPC LZ</u>
GVWL DW
HWXM EX
IXYN FY
JYZO GZ
KZAP HA
LABQ IB
MBCR JC
NCDS KD
ODET LE
PEFU MF
QFGV NG
RGHW OH
SHIX PI
TIJY QJ
UJKZ RK
VKLA SL
WLMB TM
XMNC UN
YNOD VO
ZOPE WP
APQF XQ
BQRG YR
CRSH ZS
DSTI AT
ETUJ BU
FUVK CV

FIGURE 4b

<u>LVCGWPC LZ</u>
HVWL DW
IWXM EX
JXYN FY
KYZO GZ
LZAP HA
MABQ IB
NBCR JC
OCDS KD
PDET LE
QEFU MF
RFVNG NG
SGHW OH
THIX PI
UIJY QJ
VJKZ RK
WKLA SL
XLMB TM
YMNC UN
ZNOD VO
AOPE WP
BPQF XQ
CQRG YR
DRSH ZS
*ESTI AT
FTUJ BU
GUVK CV

FIGURE 4c

The generatrices with the most plausible possibilities for the continuation of plain text are marked with an asterisk. If the context of the message cannot be gotten from this diagram, what we can do is to take the third word, LVCGWPC LZ, and assume that the letters for which we have no plain-component equivalents in the first cipher alphabet of Fig. 3b represent one of the eight missing plaintext letters, G, H, J, P, R, T, U, or Z. If we assume that the first letter (L_c) of this word represents G_p (on the first or conversion row of the generatrix diagram just beneath the ciphertext letters), we obtain the result shown in Fig. 4b; when we try $L_c=H_p$, as shown in Fig. 4c, we obtain an excellent plaintext tetragraph on the third generatrix from the bottom, and see that the word is ESTIMATED. The newly recovered values in the cipher alphabet will aid in establishing the remaining unknown letters in the generatrix diagrams for other words of the message.

(2) For the second method, let us refer again to Fig. 4a. The key letter used to encipher the first word, ENEMY, is S_k (assuming A_p to be the index letter in the usual Vigenère equation), since $I_c=E_p$. Now for the second word, if $Q_c=C_p$ (one of the asterisked good generatrices for this word), the key is Y_k ; if $Q_c=F_p$, $\theta_k=U$; and if $Q_c=R_p$, $\theta_k=H$. The first key digraphs thus formed, SY, SU, and SH, are all compatible as English word beginnings. For the third word of the message, considering the two asterisked generatrices in Fig. 4a, if $V_c=D_p$, $\theta_k=Q$; if $V_c=S_p$, $\theta_k=P$. Therefore the first three key letters are now resolved as SYP or SUP; SYP is quickly discarded, and SUP should be followed by an E, I (less likely), P, or R, suggesting words such as SUPERIOR, SUPPORT, or SUPREME. A quick check on the message establishes that, with $\theta_k=R$, the fourth word deciphers to AT_p . Proceeding in this fashion, we are able to recover the key and simultaneously the plain text in record time.

(3) In cases wherein the cipher component has been constructed in some systematic manner, analysis of its derivation will make possible recovery of the component in its entirety after a sufficient number of values has already been placed correctly.⁹ What constitutes "a sufficient number of values" depends upon the type of construction of the component, as well as the vagaries of the particular situation at hand. Taking for example the cipher component as established in Fig. 3b,

S H B P I N . . M . R G T U K . Y . Q . . V C O D . .

we observe the digraphic fragments BP and GT. If these are a part of a transposition-mixed sequence, the mechanics of the system would indicate that the fragments are part of the diagram B . . . G,
P Q R S T

which means that three of the letters CDEF lie in order between B and G, and that directly above them are the letters composing the key word for the transposition matrix. However, since R immediately precedes the G in the sequence, it appears that R is part of the key word and not part of the remaining

H Y D R

alphabetic portion. Thus the fragmentary matrix B . . G can be reconstructed, from which, with but
P Q S T

little imagination, the key word HYDRAULIC may be seen emerging, so that the entire component is derivable from the following diagram:

4 9 3 7 1 8 6 5 2
H Y D R A U L I C
B E F G J K M N O
P Q S T V W X Z

d. By means of the foregoing methods, we can establish that the primary components are the following:

P: A B C D E F G H I J K L M N O P Q R S T U V W X Y Z
C: A J V C O D F S H B P I N Z L M X R G T U K W Y E Q

The complete message and the specific key are given below:

S U P R E M E C O U
ENEMY FORCE ESTIMATED AT ONE DIVISION OF INFANTRY AND TWO
IUITD QHIWE LVCGWPCLZ RP NIV GYPYSYCV NC IXHCXWUJ ORS ZXH

R T O F T H E U (NITED STATES)
BATTALIONS OF ARTILLERY MOVING WEST OF NEWTON JUNCTION
GRPPRVQDOB SE OKYNMMHKV GUJLTN MYIN WZ IVURNI CLSWZVHS

Now that the components have become known sequences, the solution of subsequent messages enciphered with these components but with different specific keys is a simple matter, involving only a conversion of the cipher letters into their plain-component equivalents and a completion of the plain-component sequence. This point required re-emphasizing because in actual operational problems it is frequently forgotten.

e. The example in subpar. b involved a case of direct symmetry of position. If both the plain and the cipher components had involved mixed sequences, indirect symmetry of position would have

⁹ For a treatment of the cryptographic mechanics of systematically mixed sequences and their cryptanalytic recovery, see par. 51 (on pp. 86-90) of *Military Cryptanalytics, Part I*.

applied.¹⁰ As an example of such a case, let us suppose that the cipher text of the message in question had been different, and that the sequence reconstruction matrix in Fig. 3a had been the following:

∅	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
1					H								U	L												O
2				J							P			Y	D			U		I						
3	R	C									L		U	M	N				Q	S						
4	O			W						S		Q						N		C						K

FIGURE 5

(1) We observe the proportion AR (∅-1, 3-1) = ON (∅-15, 3-15) which is duplicated in AR (∅-1, ∅-18) = ON (4-1, 4-18);¹¹ this is indicative that symmetry extends to the ∅ line, and therefore that the plain and cipher components are identical sequences. Consequently, we are able to chain to the ∅ line, deriving the following sets of partial chains:

∅-1 E H M U N L Y O
 ∅-2 O D J V I P N Y S U
 ∅-3 A R B C I L U O N M T S Q
 ∅-4 A O E W I S L Q R N T C Y K

FIGURE 6

(2) We note that the fragmentary chains ONM and TSQ of the ∅-3 set appear to be parts of a keyword-mixed sequence in reverse; so, proceeding with the graphical method¹² of indirect symmetry, we assign to these chains the notation →, and then we arbitrarily assign the notation ↓ to the ∅-2 chains. The four sets of fragmentary chains will then be amalgamated into the diagram shown in Fig. 7a, below.

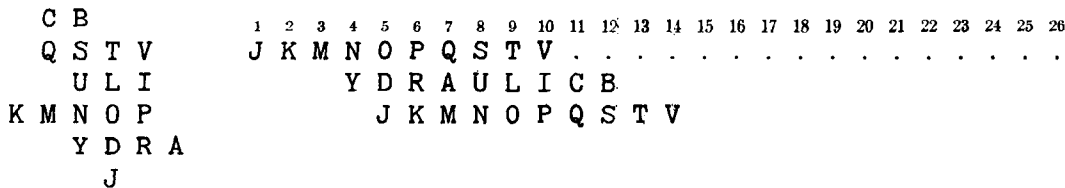


FIGURE 7a

FIGURE 7b

This diagram may then be expanded into that shown in Fig. 7b, consisting of the integration of two major chains tied together by the vertical VIP relationship.

(3) Now noting in Fig. 7b the sequence VCS on a diagonal and the letters S.V in the top row, we realize that the distance V to C when measured on the primary component should be 12, i.e., one-half of the distance (24) between V and S on the top row. Consequently, we may place the C at a position 12 spaces to the right of the V, which permits us to expand our diagram into the following:

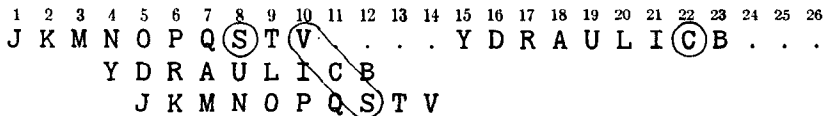


FIGURE 7c

(4) The fragmentary chains EH and EW in Fig. 6 could have been placed in their proper positions earlier in Figs. 7a-c; however, in order to illustrate a point, we have delayed their amalgamation until now. We note that the ∅-1 chains in Fig. 6 are at a decimation of -10 in the sequence in Fig. 7c; there is only one possible placement of the letters E and H at this interval, which then fixes the position of the

¹⁰ Cf. Chapter VI, *Military Cryptanalytics, Part II*.
¹¹ This notation has been discussed in footnote 2 on p. 92, *Military Cryptanalytics, Part II*.
¹² Cf. par. 46, *Military Cryptanalytics, Part II*.

last unused letter, W, the placement of which heretofore could have been ambiguous. These letters fit into the reconstructed sequence as follows:

J K M N O P Q S T V W . . H Y D R A U L I C B E . .

It is a pleasure to use, without encountering a risk of cavilation the word "obvious"¹³ as regards the positions of the missing letters:

J K M N O P Q S T V W X Z H Y D R A U L I C B E F G

f. The immediately preceding example treated a case of identical sequences proceeding in the same direction for the plain and cipher components. If the cipher component had run in the reverse direction, or if the components had been two different [unknown] mixed sequences, indirect symmetry would still have applied, with the exception (and a very important exception indeed) that chains to the Ø line would have been excluded, all chaining being done within the matrix. This prohibition would result in the situation that not only would a single short message encrypted in such a system be well-nigh unsolvable, but that even if we had a long message or a small volume of traffic, it would probably be necessary to make a fairly large number of assumptions, all correct, before there would be enough data available to permit their manipulation and exploitation by indirect symmetry.

g. Now that we have understood the details of solution of cases wherein the true word lengths have been preserved, we will take up the situation wherein the cipher text has been transmitted in its usual form of 5-letter groups.

(1) Let us suppose that we have a number of messages, all of which are known to have been enciphered monoalphabetically by word lengths with the same pair of unknown primary mixed components and (although this is not a vital consideration) in the same message key.¹⁴ Five messages have been selected from the aggregate because of the presence of polygraphic repetitions between them; the beginnings of these messages are shown in Fig. 8a, below:

1. G K B S A M K U H Q P J C G K K L J H K C F V T Y . . .
2. A L E J Q A K G L Y L W H R H C D H K U V B V P V . . .
3. S T T J U M A M K U Z I U V S V N R L Z O K L Z P . . .
4. L K Q A M G I J E U M G P J C G K K L J H B E K V . . .
5. B K J U A I E S A A S B R H S L Y L W H H Q Y E P . . .

FIGURE 8a

¹³ The reader is reminded of the pithy anecdote on the word "obvious" quoted in footnote 11 on p. 6 of *Military Cryptanalytics, Part I*.

¹⁴ If this latter fact had not been known, it could have been conjectured, from an examination of the I.C.'s of groups of columns, that the same message key was used for all the messages. In the particular example in Fig. 8a, the I.C. of the first 5 columns (taken collectively) is 1.56, while that of the first 10 is 1.76, and thereafter the I.C. drops off very rapidly even though we are adding more data to our distribution for evaluation. The grouped I.C.'s for the first N columns are summarized in the diagram below:

N	I.C.	N	I.C.
5	1.56	12	1.53
6	1.55	15	1.33
8	1.73	20	1.37
10	1.76	25	1.24

The reason for the low I.C.'s of the first 5 and the first 6 columns is that the sample was insufficient to portray what we expect of English plain text; on the other hand, the reason for the high I.C.'s of the first 8 and the first 10 columns is that the beginning words of these messages probably exceed the average length (5.2 letters) of all English words.

(2) The 5-letter and 9-letter repetitions have the length and idiomorphic patterns of ENEMY and ARTILLERY, respectively. Taking into account that the average word length in telegraphic English plain text is 5.2 letters, it appears that both of these words were probably enciphered by the third letter of the message key,¹⁵ although the relative numerical identity of the particular alphabet is really of no concern to us at the moment. On the basis of the idiomorphic beginning, Message No. 3 could start with the word AMMUNITION, making the 4-letter repetition TION which is cryptolinguistically titillating; the first word of Message No. 1, LOCATION, comes immediately thereafter, which is followed by COUNTERATTACK at the beginning of Message No. 5, HOSTILE at the beginning of Message No. 4, and THRUST at the beginning of Message No. 2. From the solution of the first three words of these five messages, and with the concurrent exploitation of the direct symmetry manifested, the primary cipher component is established as

S H B P I . Z L M . R G T U K W Y E Q A J V C . D F

(3) The key letters (under A_p) of the first three alphabets are S, U, and P. The rest of the solution proceeds either by the generatrix method as outlined in subpar. 11c(1), or by analysis of the key as illustrated in subpar. 11c(2). The complete texts of the message beginnings are shown in Fig. 8b, below:

1. G K B S A M K U | H Q | P J C G K K L J H | K C F V R T . . .
 L O C A T I O N | O F | A R T I L L E R Y | E M P L A C
2. A L E J Q A | K G | L Y L W H | R H C D H K U | V B V P V . . .
 T H R U S T | B Y | E N E M Y | A R M O R E D | E L E M E
3. S T T J U M A M K U | Z I U V S | V N R L Z O K L Z | P . . .
 A M M U N I T I O N | T R A I N | S C H E D U L E D T
4. L K Q A M G I | J E U M G | P J C G K K L J H | B E K V . . .
 H O S T I L E | H E A V Y | A R T I L L E R Y | S H E L
5. B K J U A I E S A A S B R | H S | L Y L W H | H Q Y E Z | . . .
 C O U N T E R A T T A C K | O N | E N E M Y | R I G H T

FIGURE 8b

(4) It may be seen from the foregoing example that the general theory of idiomorphic attack and the probable-word method remains the same for 5-letter texts as it is for text divided into bona fide word lengths; only the details of the execution differ. Where a small volume of homogeneous traffic is at hand, and something is known about the correspondents and the nature of the messages, solution should pose no problems (other than usual cryptanalytic headaches concomitant with operational situations of minor systems in which only a few messages are available).

12. Solution by means of isomorphs.—a. The phenomenon of isomorphism and an illustration of the exploitation of isomorphs in cipher text were covered in the previous volume.¹⁶ In practical cryptanalysis the phenomena of isomorphism afford a constantly astonishing source of clues and aids in solution. The alert cryptanalyst is always on the lookout for situations in which he can take advantage of these phenomena, for they are among the most interesting and most important in cryptanalytics.

¹⁵ We have already noted that the common plain-cipher equivalencies E_p=L_c and Y_p=H_c in the two words establish the fact that these words were enciphered by the same alphabet.

¹⁶ Cf. par. 71, *Military Cryptanalytics, Part II*.

b. Let us consider the case of word-length encipherment involving an unknown pair of primary components, the cipher text being transmitted in the customary 5-letter groups. The following cryptogram is available for study:

```

L H J J T   Y Z L D X   Z H Y P H   Z F O C X   L I M D F   G O O B D
-----
P F Q X X   Q G Y J P   R X G J G   L T S R M   K S P G Z   Z I J F P
-----
K E F G J   I M K H X   W I Y D C   C T A U E   E D T F K   H U N F Z
-----
H S G R G   E G J K L   I B W X W   D V B B O   W T D X S   T V W M T
-----
F B D J Z   I Y Z B E   X X X X X

```

c. There are no long polygraphic repetitions in evidence. An isomorphic search,¹⁷ however, uncovers several isomorphic sequences indicated by the dotted lines above; these are grouped into the following two sets of isomorphs:

- | | |
|-------------------------------|-------------------|
| Set "A" | Set "B" |
| (α) L H J J T Y Z L D X Z H Y | (δ) D F G O O B D |
| (β) P G Z Z I J F P K E F G J | (ε) T A U E E D T |
| (γ) D V B B O W T D X S T V W | |

If these isomorphs are causal isomorphs, i.e., isomorphs produced by the different encryptions of identical plaintext sequences, then the relationships between corresponding letters of the isomorphs reflect the relationships between different juxtapositions or slides of a cipher component against a plain component; these relationships, latent in the isomorphs, may be made patent through the mechanics of indirect symmetry.

d. The partial chains derivable from these isomorphs are given below:

```

α-β: L P   H G   Y J Z F   T I   D K   X E
α-γ: L D X S   H V   J B   Z T O   Y W
β-γ: P D   G V   Z B   I O   J W   F T   K X   E S
δ-ε: B D T   F A   G U   O E

```

Using the graphical method of indirect symmetry, these partial chains may be amalgamated into the diagrams shown in Figs. 9a and b, below. We note in Fig. 9a the $\leftarrow \begin{matrix} 1 \\ 2 \end{matrix}$ relationship of the letters XZ, ST,

OP, and EF, and conclude that the cipher component must be a keyword-mixed sequence. We now expand the diagram of Fig. 9a by placing the W in position diagonally ahead of the XZ, and we duplicate the remaining letters in their proper position with respect to the W just placed a moment before; this

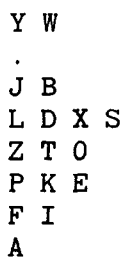


FIGURE 9a

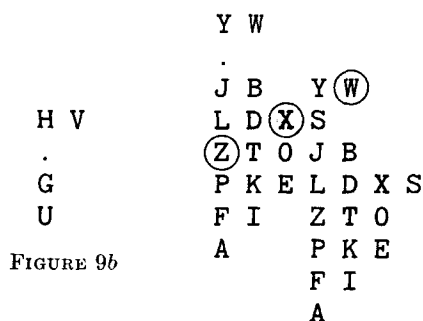


FIGURE 9b

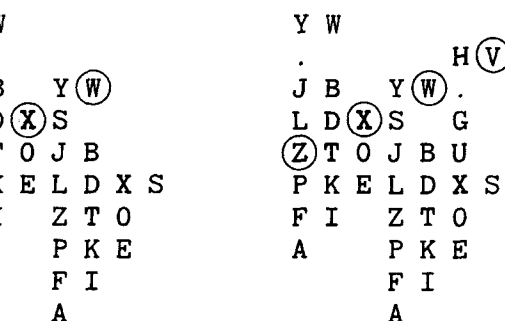


FIGURE 9c

FIGURE 9d

¹⁷ For a systematic method of searching for isomorphs, see footnote 7 on p. 174 of *Military Cryptanalytics, Part II*.

is shown in Fig. 9c. This facilitates placing the diagram of Fig. 9b into the array (on the basis of the VWXZ diagonal), resulting in the final diagram shown in Fig. 9d. From this latter figure, the original cipher component, minus 5 letters, may be chained out:

1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26
 B E F G J K . . O P . S T V W X Z H Y D . A U L I .

Our old friend HYDRAULIC.

e. We have the sequence for the cipher component, but now what? We could assume the plain component to be the normal sequence, direct and then reversed, and we could convert the first few cipher letters into their plain-component equivalents on these hypotheses and then complete the plain-component sequence; if we are correct in our assumption, a plaintext word would be revealed on one generatrix, another word on a different generatrix, etc. We could also assume the plain component to be the same as the cipher, in the same or in the reverse direction, and we could complete the plain-component sequence accordingly. All of these attempts fail, so it means that we are faced with a plain component of unknown composition. We have the cipher component at hand, it is true, but *unless we know or can deduce the motion of the cipher component*,¹⁸ it will be impossible for us to convert the cipher text into monoalphabetic terms; in other words, the original cipher is already reduced as far as it will go. Plaintext assumptions are now an absolute necessity.

f. It can be seen by referring to the two sets of isomorphs in sub-par. c that Set "A" has the complete idiomorphic pattern for COMMUNICATION, and that Set "B" has the idiomorphic pattern contained in ARTILLERY. If the now known cipher component is set down and the plaintext equivalents for the first occurrences of the assumed COMMUNICATION and ARTILLERY are recorded in the rows labelled P₁ and P₂ of the diagram below, direct symmetry of position will of course apply, provided that there

C:	H	Y	D	R	A	U	L	I	C	B	E	F	G	J	K	M	N	O	P	Q	S	T	V	W	X	Z
P ₁	O	N	A						C						M						U				T	I
P ₂		R								E	T	I			A				L	Y						

is a tie-in letter between the sequences; there happen to be three such letters, so that the plain component may be expanded as follows:

O N A . L Y C M . R U E . T I

Since there are manifested the phenomena of a keyword-mixed sequence in the plain component, we may further expand the sequence into the following:

O N A . L Y C D F G H J K M . R U E . T I

If the key word for the sequence cannot be guessed from this partial sequence, we might finish the solution by a modification of the method indicated in subpar. 11c(1), with the difference that, in this case, not only will some of the cipher letters not have plain-component equivalents, but also that the plain component itself will have gaps in its sequence in the plain-component completion diagram. After the key word (QUESTIONABLY) for the plain component has been recovered, the solution can be completed by the generatrix method, keeping in mind the reconstruction of the message key as a means of quick

¹⁸ See in this connection subpar. 71d on p. 175 of *Military Cryptanalytics, Part II*.

analysis after a few letters of the key have been derived. The complete decipherment of the message is shown below:

S		T		R		I	
L H J J T	Y Z L D X	Z H Y	PH	Z F	O C X	L I	M D F G O O B D
C O M M U	N I C A T	I O N	W I	T H	F I R	S T	A R T I L L E R
K	E	W		H		I	L
P	F Q X X	Q G	Y J P	R X G J	G	L T S R	M K S P G Z Z I J F P
Y	W I L L	B E	T H R	O U G H	C	O R P S	A N D C O M M U N I C
	E	T		H		E	
K E F G J	I M K H	X	W I Y D C	C T A U E	E D T F	K	H U N F Z
A T I O N	W I T H	S	E C O N D	A R T I L	L E R Y	T	H R O U G
I		R		O		N	
H	S G R G	E G J K	L	I B W	X W	D V B B O	W T D X S T V W M T
H	D I V I	S I O N S	S	T O P	N O	C O M M U	N I C A T I O N A F
	S						
F B D	J Z	I Y Z B E	X	X X X X			
T E R	M I	D N I G H	T				

FIGURE 10

The key for the message, under Q_p as the index letter, is "STRIKE WHILE THE IRON IS . . . (HOT?)"¹⁹

g. In connection with the solution of the problem in this paragraph, let us take a closer look at the isomorphs listed in subpar. c. These are given below, together with their plaintext equivalents:

	Set "A"	Set "B"
	<u>C O M M U N I C A T I O N</u>	(A) <u>R T I L L E R</u> (Y)
(α)	L H J J T Y Z L D X Z H Y	(δ) D F G O O B D
(β)	P G Z Z I J F P K E F G J	(ε) T A U E E D T
(γ)	D V B B O W T D X S T V W	

In case it had escaped attention before, note the ciphertext fragments XZHY, EFGJ, and STVW at the ends of the isomorphs of Set "A". These three tetragraphs, transparent in the cipher text, are actually fragments of the keyword-mixed sequence constituting the cipher component. The reason for their presence is not hard to find: the plaintext equivalent of the isomorphs ended with TION and the letters TION happened to be a fragment of the keyword-mixed sequence constituting the plain component. (Note also, from Set "B", that AU must also be in sequence in the cipher component.) This information would have been of assistance to us in the chaining process pursued in subpar. d; for pedagogical reasons, however, we delayed drawing attention to this situation until now. Needless to say, this situation or a recognizable variation of it could be of considerable assistance in the solution of a difficult problem of only a few messages in actual operations.

h. One more very important facet of isomorphism should be discussed at this point. Let us suppose that we have recovered the cipher component of the message under study through the exploitation of isomorphs as just demonstrated; but let us suppose that the two plaintext assumptions (COMMUNICATION and ARTILLERY) were insufficient to disclose enough of the sequence for the plain component to permit its facile recovery.²⁰ Additional plaintext assumptions are necessary, but we seem to have milked the

¹⁹ Hot.

²⁰ This would be the case if the plain component were not a keyword-mixed sequence but were, let us say, a transposition-mixed sequence.

cipher text dry with the two cribs we have already placed. The problem confronting us is how to make further "educated guesses" that might display a trace (or more, we hope) of erudition.

i. Since the cipher component has become a known sequence, let us set it down, numbering its elements serially from 1 to 26, as follows:

1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26
H Y D R A U L I C B E F G J K M N O P Q S T V W X Z

Let us first replace the letters of the cipher text by their numerical equivalents according to the HYDRAULIC sequence. We will then take a delta or lateral difference stream²¹ from these numerical values, by subtracting each number from the following one;²² however, instead of recording the numerical difference, we will record the literal equivalent of this numerical difference according to the HYDRAULIC sequence above. The result of this process is shown in Fig. 11, below:

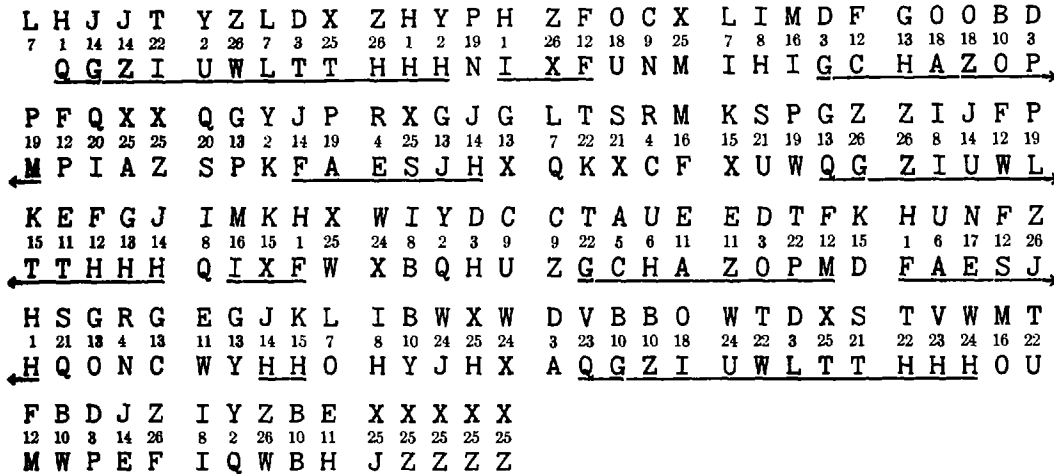


FIGURE 11

j. We can see, by comparing Fig. 11 with the original plain text as given in Fig. 10, that the delta stream has revealed all of the polygraphic repetitions of trigraphs or better in the underlying plain text.²³ Note the IXF repetition in the delta stream, which means that the ciphertext sequences PHZF and IMKH must represent the same plain text (probably the word WITH, since it is a four-letter repetition following COMMUNICATION); the PHZF and IMKH sequences are actually isomorphic, but we were unable to recognize them as such until now. Also note the delta repetition FAESJH, which means that the ciphertext sequences YJPRXGJ and KHUNFZH (an isomorphic pair whose isomorphism we were unable to trust before, because of a lack of sufficient corroborative values in the isomorphic repetition pattern) must represent the same plain text (in this case, the assumption of the word THROUGH would be permitted). Note further the HH digraphic fragment in the delta stream, which means that GJK_c must represent ION_p (from COMMUNICATION); since this is not preceded by T_p, the assumption of S_p, and therefore DIVISION is encouraged. With these plaintext values and those which follow as a direct result of our analysis thus far, it would be a simple matter to reconstruct the plain component almost in toto and the plain text of the message in its entirety.

13. Additional remarks.—a. One of the practical difficulties in employing systems in which the keying process shifts according to word lengths is that in handling such a message the deciphering clerk is often not exactly certain when the termination of a word has been reached, which results in the loss of time and effort. For instance, in deciphering a word such as INFORM, the clerk would not know whether he now has the complete word and should shift to the next key letter or not; the word might be INFORMS,

²¹ The application of delta stream techniques to the solution of digital cipher systems has been illustrated in Chapters XI and XII of *Military Cryptanalytics, Part II*.

²² In this process, subtraction is performed mod 26: i.e., if we are to subtract a large number from a smaller, we add 26 to the smaller before subtraction. For example, 1-7=(1+26)-7=20=Q in the scale above. 26 is equivalent to 0 in this modulus, so that 14-14=0=Z.

²³ The plaintext repetitions are foreshortened by one letter in the delta stream; e.g., COMMUNICATION, a 13-letter word, appears as a 12-letter sequence in the delta stream.

INFORMED, INFORMING, INFORMAL, INFORMATION, etc. The past tense of verbs, the plural of nouns, and terminations of various sorts capable of being added to word roots would give rise to difficulties, and the latter would be especially troublesome if the messages contained a few telegraphic errors to boot. Consequently, *word separators* are often adopted to circumvent this source of trouble.²⁴ These separators usually consist of an infrequent letter, such as X_p or Q_p, which is placed after every word of the plain text and is encrypted along with the rest of the message.²⁵

(1) When word separators are employed and this fact is once suspected or discovered, their presence is of as much aid to the cryptanalyst in his solution as it is to the clerks who are to decipher the messages. As an example, let us study the following cryptogram:

IWJIR	NPTXS	FIWCM	SDFEW	SBLXQ	LBHFL	TYIFD	UVLUL	JRLYG	HRZYI
FMZXD	GRMCR	SWPTX	SFIWC	KAMWZ	XLXWQ	BAARN	FLTVQ	AMQDZ	LWUQK
GQZZO	IHMIR	OLOMI	DXZFG	PLKIS	CAHQZ	MGNWX	BTIYQ	BDLTP	NPQUD
LYLGU	FINSX	LOHZA	SXAFD	XTFIZ	PJXMM	QDCPE	WYIBZ	QGHBH	RXDTX
IOOLU	IKVGC	MGITZ	HWDRG	GIWMY	RZWNP	FDCEM	YFASY	PJWHX	JZGWW
XFQXO	TMCNA	UUEJJ	IKVGH	RZYIP	MWIDL	RDCWI	PGAQC	SACWP	

Collateral information indicates that the cryptosystem involves monoalphabetic encipherment by word lengths, a word separator being used to signal the change to a new key letter; the key letters themselves form a plaintext word as a mnemonic key.

(2) If the encipherment is by word lengths and a word separator is used, the average length of words should be 6.2 letters. Since a key word is used to control the selection of alphabets, if a polygraphic repetition of significant length is present in the cipher text, the interval between the first and second occurrences should give a fair indication of the length of the key, unless there are repeated letters in the key and these polygraphic repetitions happen to be produced by identical key letters in *different* positions in the key word. We note the 8-letter repetition P_{TXSFIWC} at an interval of 56 letters; this would seem to indicate that the key word is $\frac{56}{6.2}$ or 9 letters long, give or take a letter. Since there is another

polygraphic repetition present, G_{HRZYI} at an interval of 224 letters, the division $\frac{224}{6.2} = 36 = 4 \times 9$ furnishes corroboration of the length of the key word, and dispels fears that these repetitions may have been produced by identical key letters in different positions in the key word.

(3) When word separators have been used, the first and last letters of long polygraphic repetitions are most likely to be word separators;²⁶ consequently, in the case of the first repeated sequence, P_{TXSFIWC} (representing either the second or third word of the message), P_c and C_c should represent the word separators. Now if the cipher text of the message is written out in lines of 50-60 letters or so using the repeated sequence P_{TXSFIWC} as a sort of base, we might be able to pick out the successive word separators; this is shown in the diagram below:

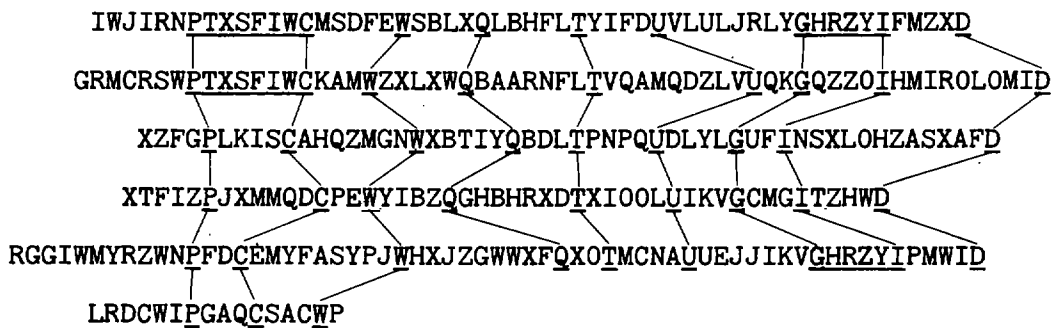


FIGURE 12

²⁴ See the discussion on word separators in subpar. 100d of *Military Cryptanalytics, Part II*.

²⁵ Occasionally, *unenciphered* word separators are encountered, there being employed for this purpose a character not otherwise used in the cryptographic scheme.

²⁶ The occasional exceptions would be cases of the partial repetitions arising from pairs of words such as **INFORMS** and **INFORMATION**, wherein the initial letters of the ciphertext repetitions would represent a word separator, but the final letters would represent M_p, the last letter of the root word.

Note that the next-to-last separator, I_c , was preferred to a preceding Z_c (also a possibility as a word separator) because of the final letter of the GHRZYI repetition. With the word divisions now known, it is an easy matter to make plaintext assumptions based on word lengths and idiomorphs; the rest of the solution is left to the reader as an exercise.

(4) The foregoing example involved but a single message and a relatively short message key so that during the encryption five complete cycles of the message key were employed; it was this re-use of the keying sequence that permitted a solution. It is obvious that, regardless of the length of the key, if we had five or six messages or so in the same key, we could have written them out over one another and by careful scrutiny we could have determined the word separators much in the same fashion as was illustrated by the diagram of Fig. 12, above.

b. The systems thus far discussed are all based upon word-length encipherment using different cipher alphabets. Words are markedly irregular in regard to this feature of their construction and thus aperiodicity is imparted to such cryptograms. But variations in the method, aimed at making the latter somewhat more secure, are possible. Instead of enciphering according to natural word lengths, the irregular groupings of the text may be regulated by other agreements. For example, suppose that the numerical value (in the normal sequence) of each key letter be used to control the number of letters enciphered by the successive cipher alphabets. Depending then upon the composition of the key word or key phrase, there would be a varying number of letters enciphered in each alphabet. If the key word were PREPARE, for instance, then the first cipher alphabet would be used for 16 (=P) letters, the second cipher alphabet, for 18 (=R) letters, and so on. Monoalphabetic encipherment would therefore allow plenty of opportunity for telltale word patterns to manifest themselves in the cipher text. Once an entering wedge is found in this manner, solution would be achieved rather rapidly.

c. If the key of the system described in the foregoing subparagraph is short, and the message is long, periodicity will be manifested in the cryptograms, so that it would be possible to ascertain the length of the basic cycle (in this case, the length of the key) from a single message, despite the irregular groupings in encipherment. The determination of the length of the cycle might, however, present difficulties in some cases, since the basic or fundamental period would not be clearly evident because of the presence of repetitions which are not periodic in their origin. For example, suppose the word PREPARE were used as a key, each key letter being employed to encipher a number of letters corresponding to its numerical value in the normal sequence. It is clear that the length of the basic period, in terms of letters, would here be the sum of the numerical values of $P(=16) + R(=18) + E(=5) + \dots$, totalling 79 letters. But because the key itself contains repeated letters and because encipherment by each key letter is monoalphabetic, there would be plenty of cases in which the first letter P would encipher the same or part of the same word as the second letter P, producing repetitions in the cipher text. The same would be true as regards encipherments by the two R's and the two E's in this key word. Consequently, the basic period of 79 would be distorted or masked by aperiodic repetitions, the intervals between which would not be a function of, nor bear any relation to, the length of the key. Cases are frequently encountered in which a fundamental periodicity is masked or obscured by the presence of ciphertext repetitions not attributable to a fundamental cycle; the experienced cryptanalyst is on the lookout for phenomena of this type, when he finds in a polyalphabetic cipher plenty of repetitions but with no factorable constancy which leads to the disclosure of a short period. He may conclude, then, either that the cryptosystem involves several primary periods which interact to produce a long resultant period, or that it involves a fairly long fundamental cycle within which repetitions of a non-periodic origin are present and obscure the phenomena manifested by repetitions of periodic origin.²⁷

d. A logical extension of the principle of polyalphabetic encipherment of variable-length plaintext groupings is the case in which these plaintext groupings rarely exceed 4 letters, so that a given cipher alphabet is in play for only a very short time, thus breaking up what might otherwise appear as fairly long repetitions in the cipher text.

²⁷ See also in this connection footnote 8 on p. 26 of *Military Cryptanalytics, Part II*.

(1) For example, suppose that the letters of the alphabet to be used as key letters are arranged in the order of their relative frequencies in English plain text, and are set off into four groups of 5, 6, 7, and 8 letters, respectively, as follows:

E T N R O	A I S D L H	C F P U M Y G	W V B X Q K J Z
Group 1	Group 2	Group 3	Group 4

Suppose that a key letter in Group 1 means that one letter will be enciphered; a letter in Group 2, that two letters will be enciphered; and so on. Suppose, next, that a rather lengthy phrase were used as a key; for example, I KNOW NOT WHAT COURSE OTHERS MAY TAKE BUT AS FOR ME GIVE ME LIBERTY OR GIVE ME DEATH. Suppose, finally, that each letter of the key were used to control the number of letters to be enciphered by the selected alphabet, according to the scheme outlined above. Such an enciphering scheme, using the HYDRAULIC . . . XZ primary cipher component sliding against a normal plain component, would yield the following groupings:

Grouping:	2	4	1	1	4	1	1	1	4	2	2	1	3	1	3	1	2	1	1	1	2																		
Key:	I	K	N	O	W	N	O	T	W	H	A	T	C	O	U	R	S	E	O	T	H																		
Plain:	T	W	E	N	T	I	E	T	H	R	E	G	I	M	E	N	T	H	E	A	D	Q	U	A	R	T	E	R	S	N	O	W	L	O	C	A	T	E	D
Cipher:	H	R	P	Y	I	V	S	E	A	K	Y	R	X	R	Z	E	N	A	Y	H	R	S	X	T	Z	Y	G	C	W	P	Q	Z	U	C	G	O	K	A	R

Grouping:	1	1	2	3	2	3	1	2	4	1	4	3	1	2	2	3	1	1																				
Key:	E	R	S	M	A	Y	T	A	K	E	B	U	T	A	S	F	O	R																				
Plain:	N	E	A	R	H	E	A	D	Q	U	A	R	T	E	R	S	O	F	F	O	R	T	Y	S	E	C	O	N	D	R	E	G	I	M	E	N	T	. . .
Cipher:	W	I	S	F	V	Q	M	I	S	T	Y	P	K	C	T	L	D	Q	Q	X	H	D	I	Y	B	I	Q	C	I	T	X	H	Q	W	M	A	V	

(2) Here it will be seen that any tendency for the formation of lengthy repetitions would be counteracted by the short groupings and quick shifting of alphabets. Before a long plaintext passage can be enciphered by *exactly* the same sequence of key letters, an interval of exactly 135 letters (the sum of the values of the letters in the key phrase) or a multiple thereof must intervene between the two occurrences of the plaintext passage.²⁸ When, however, a repeated plaintext passage is at an interval of only one or two letters off from 135 or a multiple of 135, there can occur in the system under discussion a phenomenon of intermittent coincidences; i.e., coincidences not among all the ciphertext letters representing the repeated plaintext passage, but among only a few of these ciphertext letters. As an example, let us consider the following message beginnings of two messages in flush depth:

Grouping:	2	4	1	1	4	1	1	1	4	2	2	1	3	1	3	1	2	1	1	1	2																			
Key:	<u>I</u>	<u>K</u>	<u>N</u>	<u>O</u>	<u>W</u>	<u>N</u>	<u>O</u>	<u>T</u>	<u>W</u>	<u>H</u>	<u>A</u>	<u>T</u>	<u>C</u>	<u>O</u>	<u>U</u>	<u>R</u>	<u>S</u>	<u>E</u>	<u>O</u>	<u>T</u>	<u>H</u>																			
Msg "A":	T	W	E	N	T	I	E	T	H	R	E	G	I	M	E	N	T	H	E	A	D	Q	U	A	R	T	E	R	S	N	O	W	L	O	C	A	T	E	D	. . .
Cipher "A":	H	R	P	Y	I	V	S	E	A	K	Y	R	X	R	Z	E	N	A	Y	H	R	S	X	T	Z	Y	G	C	W	P	Q	Z	U	C	G	O	K	A	R	
Msg "B":	F	I	F	T	Y	F	I	R	S	T	D	I	V	I	S	I	O	N	H	E	A	D	Q	U	A	R	T	E	R	S	I	S	M	O	V	I	N	G	. . .	
Cipher "A":	G	M	Q	I	G	Q	X	C	M	N	H	U	F	Z	J	U	F	E	A	A	H	I	S	M	C	Z	Y	T	V	W	L	C	U	Z	C	L				

The word HEADQUARTERS is offset one position to the right in Message "B" with respect to its position in Message "A". (This same situation would arise if the second occurrence of HEADQUARTERS in Message "A" were at an interval of 136 letters from the first occurrence, or 271 letters, or any other multiple of 135 plus one more letter.) If we set down the cipher equivalents of the two occurrences of HEADQUARTERS under the plain text, we have the following:

<u>H</u>	<u>E</u>	<u>A</u>	<u>D</u>	<u>Q</u>	<u>A</u>	<u>R</u>	<u>T</u>	<u>E</u>	<u>R</u>	<u>S</u>	
<u>A</u>	<u>Y</u>	<u>H</u>	<u>R</u>	<u>S</u>	<u>X</u>	<u>T</u>	<u>Z</u>	<u>Y</u>	<u>G</u>	<u>C</u>	<u>W</u>
<u>A</u>	<u>A</u>	<u>H</u>	<u>I</u>	<u>S</u>	<u>M</u>	<u>C</u>	<u>Z</u>	<u>Y</u>	<u>T</u>	<u>V</u>	<u>W</u>

²⁸ Note that, in the case of this particular key, two occurrences of a 14-letter plaintext passage could receive identical encipherments at two different positions of the key at which there are identical fragments (GIVE ME) in the key phrase; the intervals between these repeated ciphertext sequences would have nothing to do with the length of the period.

We notice that the cipher equivalents agree only in the first, third, fifth, eighth, ninth, and twelfth letters. The repetitions here extend only to one or two letters; longer repetitions can occur only exceptionally. The two encipherments yield only occasional coincidences, i.e., places where the cipher letters are identical; moreover, the *distribution* of the coincidences is quite irregular and of an intermittent character. This phenomenon of intermittent coincidences, involving coincidences of single letters, pairs of letters, or short sequences (rarely ever exceeding pentagraphs) is one of the characteristics of this general class of polyalphabetic substitution, wherein the cryptograms commonly manifest what appears to be disturbed or distorted periodicity.

e. As has already been noted, in aperiodic systems wherein the key is determined or generated *apart* from the plain text being enciphered (as is the case of the example in the foregoing subparagraph), cryptographic depth is possible; therefore the analyst may be able, if keying conditions permit, to superimpose messages and solve the resultant superimposition. On the other hand, in systems wherein the plain or cipher text influences or governs in any way the selection of keys, cryptographic depth is usually impossible of establishment, except in very special circumstances.

f. The essence of the systems described in this chapter really comprises *monoalphabetic* substitution in irregular, and usually small, segments; nevertheless, these segments were large enough to permit of their isolation and exploitation. As the size of these segments decreases, ultimately to units of single letters, so does the difficulty of solution increase—but not beyond the potentials of cryptanalysis, as will shortly be demonstrated.

CHAPTER III

SYSTEMS USING VARIABLE-LENGTH KEYING UNITS TO ENCIPHER
CONSTANT-LENGTH PLAINTEXT GROUPINGS

	Paragraph
General.....	14
Plaintext interruptor systems.....	15
Ciphertext interruptor systems.....	16
Systems employing externally generated or determined keys.....	17
Solution when known cipher alphabets are employed.....	18
Solution when unknown cipher alphabets are employed.....	19
Additional remarks.....	20

14. General.—a. The systems treated in the preceding chapter incorporated simple methods of eliminating or avoiding periodicity by enciphering variable-length groupings of the plain text, using constant-length keying units; the essence of those systems was really *monoalphabetic* encipherment by sections,¹ the sections comprising irregular-length plaintext groupings. In subpar. 2a, however, it was pointed out that periodicity can also be suppressed by applying variable-length keying units to constant-length plaintext groupings; the essence of such systems is polyalphabetic substitution applied to the plaintext units (usually single letters). One such method consists in *irregularly interrupting* the keying sequence, if the latter is of a limited or fixed length, and recommencing it (from its initial point) after such interruption, so that the keying sequence becomes equivalent to a series of keys of different lengths. Thus, the key phrase BUSINESS MACHINES might be expanded, by a particular keying convention, into a series of irregular-length keying sequences, such as BUSI/BUSINE/BU/BUSINESSM/BUSINESSMAC, etc. Various schemes or prearrangements for determining the type or character of the interruptions may be adopted. Several typical methods will now be described.

b. There are many methods of interrupting a keying sequence which is basically cyclic and which therefore would give rise to periodicity if not interfered with in some way. These methods may, however, be classified into six general cases as regards what happens after the interruption occurs.²

Case I: The keying sequence merely stops and begins again at the initial point of the cycle.

Case II: Certain elements of the keying sequence may "stutter" or be repeated a fixed or a variable number of times.

Case III: One or more of the elements in the keying sequence may be omitted from time to time irregularly.

Case IV: The keying sequence irregularly alternates in its direction of progression.³

Case V: The keying sequence irregularly alternates in its direction of progression, and, in addition, certain elements of the keying sequence may be repeated one or more times.

Case VI: The keying sequence irregularly alternates in its direction of progression, and, in addition, one or more of the elements in the keying sequence are omitted from time to time irregularly.

c. The foregoing methods may, for clarity, be represented graphically as follows. Suppose the key consists of a cyclic sequence of 10 elements represented symbolically by the series of numbers 1, 2, 3, . . . 0. Indicating an interruption by a vertical line,⁴ we show in Fig. 13, below, the relationship between

¹ See in this connection subpar. 84b(1) on p. 220 of *Military Cryptanalytics, Part I*.

² In addition to these cases, a "septimum quid" could be listed, as a catchall for "everything else," which includes progressions so irregular as to defy classification.

³ It is to be noted that this fourth case could be treated as though it were a special form (with irregularly occurring small or large skips) of the third case.

⁴ What *specifically* brings about the interruption is here not stated, nor for that matter does it concern us at the moment. Suffice it to say that, whatever the cause of the interruption, it is not a function of the plain or of the cipher text, but is in this case predetermined by an external convention with steps 3, 1, 6, 7, 5, 8, 2, 4, 9 . . .

the letter at each position of the message and the identity of the element of the keying sequence in the six general cases discussed above.

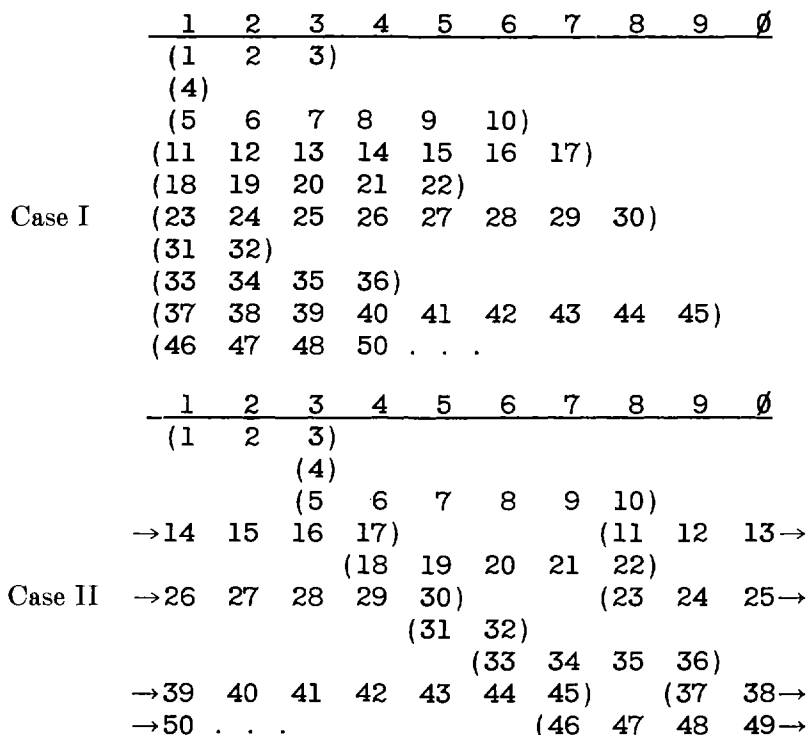
Letter No.	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25
Key elements, Case I:	1	2	3	1	1	2	3	4	5	6	1	2	3	4	5	6	7	1	2	3	4	5	1	2	3
Key elements, Case II:	1	2	3	3	3	4	5	6	7	8	8	9	0	1	2	3	4	4	5	6	7	8	8	9	0
Key elements, Case III:	1	2	3	5	7	8	9	0	1	2	4	5	6	7	8	9	0	2	3	4	5	6	8	9	0
Key elements, Case IV:	1	2	3	2	3	4	5	6	7	8	7	6	5	4	3	2	1	2	3	4	5	6	5	4	3
Key elements, Case V:	1	2	3	3	3	4	5	6	7	8	8	7	6	5	4	3	2	2	3	4	5	6	6	5	4
Key elements, Case VI:	1	2	3	5	7	8	9	0	1	2	4	3	2	1	0	9	8	0	1	2	3	4	6	5	4

Letter No.	26	27	28	29	30	31	32	33	34	35	36	37	38	39	40	41	42	43	44	45	46	47	48	49	50
Key elements, Case I:	4	5	6	7	8	1	2	1	2	3	4	1	2	3	4	5	6	7	8	9	1	2	3	4	5
Key elements, Case II:	1	2	3	4	5	5	6	6	7	8	9	9	0	1	2	3	4	5	6	7	7	8	9	0	1
Key elements, Case III:	1	2	3	4	5	7	8	0	1	2	3	5	6	7	8	9	0	1	2	3	5	6	7	8	9
Key elements, Case IV:	2	1	0	9	8	9	0	9	8	7	6	7	8	9	0	1	2	3	4	5	4	3	2	1	0
Key elements, Case V:	3	2	1	0	9	9	0	0	9	8	7	7	8	9	0	1	2	3	4	5	5	4	3	2	1
Key elements, Case VI:	3	2	1	0	9	1	2	4	3	2	1	3	4	5	6	7	8	9	0	1	3	2	1	0	9

FIGURE 13

Note that in Cases III and VI the amount of skip is here portrayed as being constant. This is not a necessary condition in these keying methods; the amount of skip could have consisted of irregular jumps as established by the keying convention employed.

d. If we *knew* just when the interruptions take place, and if we also knew the exact nature of the effect of each interruption,⁵ then the successive ciphertext sections of encrypted messages in the foregoing six cases could be properly superimposed so as to be in true cryptographic depth. In the diagrams below, the digits in the top line represent the ten keying elements, while the numbers 1-50 underneath this line represent the positional identities of the first 50 ciphertext letters.



⁵ These two points could have been determined either through physical compromise of a cipher machine incorporating such principles, or through the *analytical* compromise of a cryptosystem.

1	2	3	4	5	6	7	8	9	∅
(1	2	3)		(4)		(5	6	7	8→
→ 9	10)		(11	12	13	14	15	16	17)
	(18	19	20	21	22)		(23	24	25→
→26	27	28	29	30)		(31	32)		(33→
→34	35	36)		(37	38	39	40	41	42→
→43	44	45)		(46	47	48	49	50	. . .

1	2	3	4	5	6	7	8	9	∅
(1	2	3)							
	(4)	(5	6	7	8	9	10)		
(17	16	15	14	13	12	11)			
	(18	19	20	21	22)				
←27	26	25	24	23)			(30	29	28←
							(31	32)	
					(36	35	34	33)	
→41	42	43	44	45)		(37	38	49	40→
←49	48	47	46)						50←

1	2	3	4	5	6	7	8	9	∅
(1	2	3)							
		(4)							
		(5	6	7	8	9	10)		
	(17	16	15	14	13	12	11)		
	(18	19	20	21	22)				
←28	27	26	25	24	23)			(30	29←
								(31	32)
					(36	35	34	33)	
→41	42	43	44	45)		(37	38	39	40→
. . .	50	49	48	47	46)				

1	2	3	4	5	6	7	8	9	∅
(1	2	3)		(4)					
→ 9	10)					(5	6	7	8→
←14	13	12	11)				(17	16	15←
→19	20	21	22)						(18→
←28	27	26	25	24	23)			(30	29←
	(31	32)							
	(36	35	34	33)					
→45)	(37	38	39	40	41	42	43	44→	
←48	47	46)							50 49←

Obviously, if we did not know when or how the interruptions take place, then the successive sections of keying elements cannot be superimposed as indicated above.

e. The interruption of the fundamental cyclic keying sequence usually takes place according to some prearranged plan or convention. The *identity* of the plaintext letters being enciphered might be involved in the determination of the interruption (as in plaintext interruptor systems);⁶ or the identity of the ciphertext letters might be a factor (as in ciphertext interruptor systems); or, finally, the interruption of the fundamental cyclic keying sequence might be predicated upon a separate convention,

⁶ In the Wheatstone cipher device the interruption of the keying sequence of the 26 cipher alphabets used in sequential progression is predicated upon the relative *position in the plain component* of a plaintext letter with respect to the *position* (in the plain component) occupied by the next plaintext letter to be encrypted. (See Chapter VIII in this connection.)

mechanism, or prearrangement, without regard to the plain text or the cipher text. Some basic methods of interruption will now be taken up, using a short mnemonic key as an example.

15. **Plaintext interruptor systems.**—a. Suppose the correspondents agree that the interruption in the key will take place after the occurrence of a specified letter in the plain text, after which the key begins anew at its initial position.⁷ Since there is nothing fixed about the time the interruption will occur—it will take place at no fixed intervals—not only does the interruption become quite irregular, following no pattern, but also the method never reverts to one having periodicity. Let us assume that the correspondents have agreed upon R_p as the interruptor letter, and that they are using the normal sequence for the plain component and the HYDRAULIC . . . XZ sequence for the cipher component. If the mnemonic key phrase is BUSINESS MACHINES, this key would be interrupted by the occurrences of R_p as in the following example:

Key: B U S I N E S S M A C H I B U S B U S I B U S I N E
Plain: A M M U N I T I O N F O R F I R S T A R T I L L E R
Cipher: B O L Y R P J D R O J K X K J F Y X S X D J U P S Y

Key: B U S I N E S S M A C H I N E S B U B U S I N E S S M A C H I
Plain: Y W I L L B E L O A D E D A F T E R A M M U N I T I O N F O R
Cipher: I Y D P Y F X U R A F A E N M J J V B O L Y R P J D R O J K X

Key: B U S I B U S B U S I N E B U S I N
Plain: T H I R D A R T I L L E R Y S T O P . . .
Cipher: D G D X G U F D J U P S Y I W J T U

The final cipher text, in groups of five letters, would be the following:

B O L Y R P J D R O J K X K J F Y X S X D J U P S Y I Y D P
Y F X U R A F A E N M J J V B O L Y R P J D R O J K X D G D
X G U F D J U P S Y I W J T U . . .

It will be noted that the two long polygraphic repetitions are at intervals of 44 and 34, respectively, which intervals have nothing in common with 16, the length of the basic, uninterrupted period.

b. Instead of employing an ordinary plaintext letter as the interruptor letter, one might use a 25-letter plain component, combining I with J, and then use the 26th character (J) as a null plaintext letter which is inserted at random by the encipherer to serve as the interruptor letter. Note the following example:

Key: B U S I N E S S M A B U S I N E S S M A C H I N E S B U S B U S I N
Plain: P R O C E E D T O J R O A D I U N C T I O N S I X T W O J F I V E J . . .

c. It is obvious that repetitions would be plentiful in cryptograms of this construction, regardless of whether a letter of high-, medium-, or low-frequency is selected as the signal for key interruption. If a letter of high frequency is chosen, repetitions will occur quite often, not only because that letter will certainly be a part of many common words, but also because it will be followed by words that are frequently repeated; and since the key starts again with each such interruption, these frequently repeated words will be enciphered by the same sequence of cipher alphabets. This is the case in the first of the two foregoing examples. It is clear, for instance, that every time the word ARTILLERY appears in the cryptogram the cipher equivalents of TILLERY must be the same. If the interruptor letters were A_p instead of R_p, the repetition would include the cipher equivalents of RTILLERY; if it were T_p, ILLERY, and so on. On the other hand, if a letter of very low frequency were selected as the interruptor letter, then the encipherment would tend to approximate that of normal periodic substitution, and repetitions would be plentiful on that basis alone. Of course, the intervals between the repetitions in any of the

⁷ This is Case I of subpar. 14b.

...going cases (except perhaps that in which the plaintext interruptor is a letter of very low frequency) would be markedly irregular, so that periodicity would not be manifested.

16. Ciphertext interruptor systems.—a. In the systems of the preceding paragraph, a plaintext letter serves as the interruptor letter. But now suppose the correspondents agree that the interruption in the key will take place immediately after a previously agreed-upon letter, say Q_c, occurs in the cipher text. The key would then be interrupted as shown in the following example:

Key: B U S I N E S S M A C H I N E S B U S I N E S S M
Plain: A M M U N I T I O N F O R F I R S T A R T I L L E
Cipher: B O L Y R P J D R O J K X T P F Y X S X B P U U Q

Key: B U S I N E S S M A C H I N B U S I N E S S M A C H B U
Plain: R Y W I L L B E L O A D E D A F T E R A M M U N I T I O
Cipher: H R N M Y T T X H P C R F Q B E J F I E L L B O N Q O Q

Key: B U S I N E S S M A C H B U S I N E S S M A
Plain: N F O R T H I R D A R T I L L E R Y S T O P . . .
Cipher: V E C X B O D F P A Z Q O N U F I C G J R Q

The cipher text in 5-letter groups is as follows:

B O L Y R P J D R O J K X T P F Y X S X B P U U Q H R N M Y
T T X H P C R F Q B E J F I E L L B O N Q O Q V E C X B O D
F P A Z Q O N U F I C G J R Q

b. In the foregoing example, there are no significant repetitions; such as do occur comprise only digraphs, several of which are purely accidental. But the absence of significant, long repetitions is itself purely accidental, for had the interruptor letter been a letter other than Q_c, then the phrase AMMUNITION FOR (which occurs twice) might have been enciphered identically both times. If a short key is employed, repetitions may be plentiful. For example, note the following, in which S_c is the interruptor letter:⁸

Key: B A N D S B A N D S B A N D S B A N D S B A N B A N D S B B A
Plain: F R O M F O U R F I V E T O F O U R F I F T E E N W I L L B E . . .
Cipher: K T A K Z W X I I D A C B N Z W X I I D K W S J O G E U S E C

c. This last example gives a clue to one method of attacking this type of system. There will be repetitions within short sections, and the interval between them will sometimes permit ascertaining the length of the basic key. In such short sections, the letters which intervene between the repeated sequences may be eliminated as possible interruptor letters. Thus, in the foregoing example, we can deduce that the length of the basic key is 5 letters, and that the cipher letters A, C, B, and N may be eliminated as interruptor letters. By extension of this principle to the letters intervening between other repetitions, one may more-or-less quickly ascertain what ciphertext letter serves as the interruptor.⁹

d. The ciphertext interruptor might be a letter which is not otherwise used in the cryptographic scheme; for example, the plain component might be a 25-letter sequence (combining I and J) and the cipher component a 25-letter sequence excluding, let us say, Z. This letter Z may then be inserted in appropriate places in the cipher text to signal the interruptions in the keying cycle. In some cases such a special interruptor letter may be used in addition to a ciphertext interruptor which arises from the bona fide encryption of a plaintext letter, as a means of insuring that interruption of the keying cycle will take place frequently enough to suit the cryptographer or his procedures-prescribing superiors.

⁸ Note that the periodic repetitive phenomena manifested would also have arisen in a plaintext interruptor system, if the interruptor had been, let us say, A_p—or, for that matter, any other letter not present in the fragment FOURFI VETOFOURFI.

⁹ The method described in this subparagraph may also be applied in the case of plaintext interruptor systems, with certain modifications.

(For that matter, there is nothing to bar the use of two or more letters as interruptors in the usual manner, in either plaintext interruptor or ciphertext interruptor systems.)

17. **Systems employing externally generated or determined keys.**—*a.* In subpars. 3*b* and *f* we have seen two examples of keying procedures which do not depend upon conventions affiliated with identities of plaintext or ciphertext letters, but which are established by an independent, external keying convention. The keying methods of subpar. 3*b*, if modified to incorporate variable-length *polyalphabetic* keying units (as contrasted with the variable-length monoalphabetic keying units illustrated in that example), could take on a form such as the following:

S	IG	GNA	NALS	ALSIG	L	SI	IGN	GNAL	NALSI	A	LS	SIG	IGNA	GNALS
1	12	123	1234	12345	1	12	123	1234	12345	1	12	123	1234	12345
N	AL	LSI	SIGN	IGNAL	G	NA	ALS	LSIG	SIGNA	I	GN	NAL	ALSI	LSIGN
1	12	123	1234	12345	1	12	123	1234	12345	1	12	123	1234	12345
S	IG	GNA	NALS	ALSIG	L	SI	IGN	etc.						
1	12	123	1234	12345	1	12	123							

Similarly, the keying method of subpar. 3*f*, modified to embrace the aspect of variable-length polyalphabetic keying units, could be transformed into one of the following, among other possibilities:

- (1) D E F/E/C D E F/L M N O/A B/R S T/A B/T/I J/O P Q/N O/O P Q/F G H I/. . .
- (2) D E C/E/C L A R/L A R A/A R/R A T/A T/T/I O/O N O/N O/O F I/F I N D/. . .

b. The foregoing methods have as their purpose the establishment of keys of fair length from a short mnemonic key. There are other simple methods for accomplishing this, as illustrated in the examples which follow. Let us consider the mnemonic key HYDRAULIC, and derive from it a numerical key:

H Y D R A U L I C
4 9 3 7 1 8 6 5 2

We may now take the key letters in numerical-key order, and in groupings as determined by the numerical key, so that the original key of only 9 letters is expanded to one of 45 letters. Thus:

- (1) A/C H/D R A/H Y D R/I C H Y D/L I C H Y D/R A U L I C H/
U L I C H Y D R/Y D R A U L I C H/

Two other methods of deriving 45-element key sequences from the basic 9-letter key word are shown below:

- (2) H Y D R/Y D R A U L I C H/D R A/R A U L I C H/A/
U L I C H Y D R/L I C H Y D/I C H Y D/C H/
- (3) H Y D R A/H Y D R A U L I C/H Y D/H/H Y D R A U L I/
H Y D R A U L/H Y D R /H Y D R A U/H Y/

Method (2) is essentially the same as (1), except that the key fragments are taken in the order in which they appear in the key word. Method (3) involves taking the successive sections of the numerical key, these sections terminating with the successive numbers 1, 2, 3, . . . of the numerical key.¹⁰

c. Many other methods exist for the establishment of keys consisting of variable-length keying units. Furthermore, some of these methods merge into the domain of methods of lengthening or extending keys in general, apart from any considerations of variable-length keying units. Several of the most important of these methods will be discussed in subsequent chapters of this text.

18. **Solution when known cipher alphabets are employed.**—*a.* (1) Let us suppose that a particular cryptosystem has been in use for some time, and that the general nature of the system and the cipher

¹⁰ This method is equivalent to an interrupted-key columnar transposition system. See in this connection subpar. 51*h* on p. 89 of *Military Cryptanalytics, Part I.*

alphabets have become known, either through successful cryptanalysis or through light-fingered techniques coming under the formal term of "physical compromise," which includes among its manifold tachydactylurgic aspects that which has been referred to colloquially as "wastebasket cryptanalysis."¹¹ Only the specific key to messages remains unknown. The cipher text is examined for repetitions, and an attack is made on the basis of searching for a probable word. Thus, taking the cryptogram in subpar. 15a as an example (quoted here below for convenience), suppose the presence of the word ARTILLERY is suspected.

B O L Y R P J D R O J K X K J F Y X S X D J U P S Y I Y D P
X F X U R A F A E N M J J V B O L Y R P J D R O J K X D G D
X G U F D J U P S Y I W J T U . . .

Attempts are made to locate this word, basing the search upon the recognition of an intelligible key; we will assume in this case that the cipher component is the HYDRAULIC . . . XZ sequence sliding against the normal sequence for the plain component.

(2) Beginning with the very first letter of the message, we juxtapose the word ARTILLERY against the cipher text and ascertain the key letters. Thus:

Key: B H J Q P I B F U
Cipher: B O L Y R P J D R
Plain: A R T I L L E R Y

Since this "key" is certainly not intelligible text, the assumed word is moved one letter to the right and the test repeated, and so on until the 19th position in the text is reached.¹²

Key: S I B U S I N E B
Cipher: S X D J U P S Y I
Plain: A R T I L L E R Y

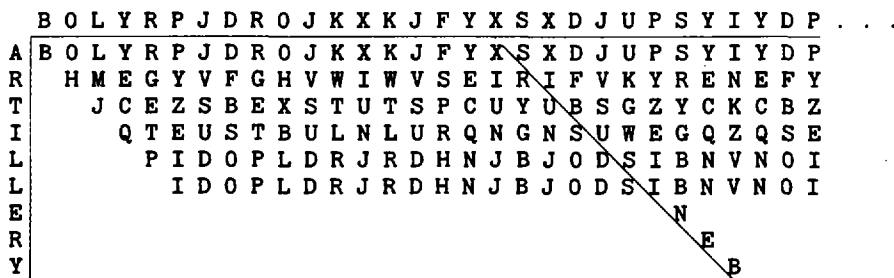
(3) The sequence BUSINE suggests BUSINESS; moreover, it is noted that the key appears to be interrupted both times by the letter R_p. The key may now be applied to the beginning of the message, to see whether the whole key or only a portion of it has been recovered. Thus:

Key: B U S I N E S S B U S I N E S
Cipher: B O L Y R P J D R O J K X K J . . .
Plain: A M M U N I T I U M T H I E T

(4) It is obvious that BUSINESS is only a part of the key. But the first word of the message is plainly AMMUNITION. When this is tried, the key is extended to BUSINESS MA . . . This key crib is now slid through the rest of the cipher text and the remainder of the message is quickly deciphered and the entire key recovered.

¹¹ This is really not stealing. For the pure in heart, this should be thought of as conversion of raw data, and that the parties so generously supplying these raw data are, unknowingly, cooperating in government work.

¹² In actual practice, the search for the placement of the probable word would have been accomplished by means of the following diagram (see in this connection subpar. 22d on pp. 41-42 of *Military Cryptanalytics, Part II*):

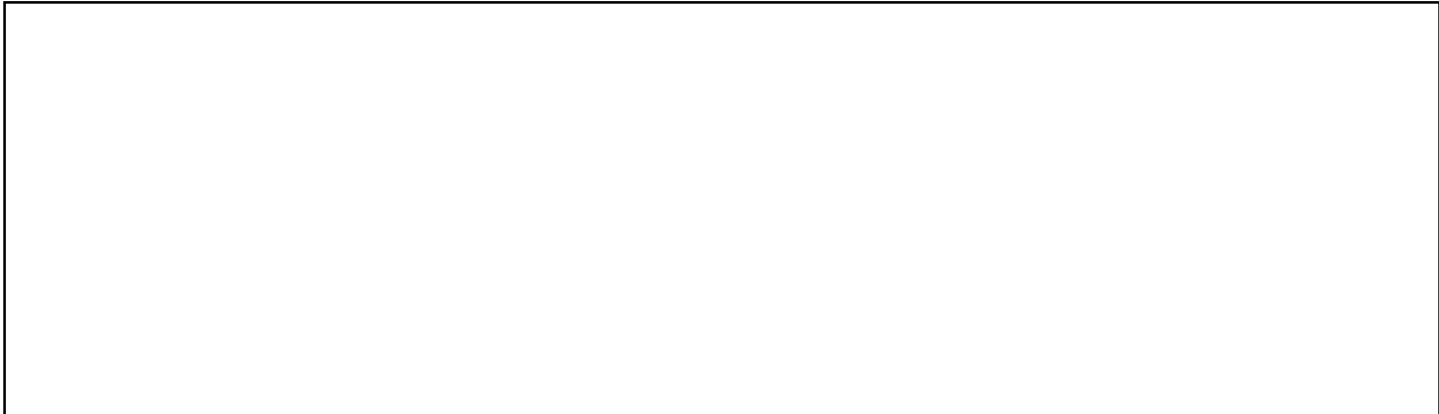


~~SECRET~~

(b) (1)
(b) (3)-18 USC 798
(b) (3)-50 USC 3024 (i)
(b) (3)-P.L. 86-36

~~SECRET~~

(b) (1)
(b) (3)-18 USC 798
(b) (3)-50 USC 3024(i)
(b) (3)-P.L. 86-36



d. (1) Another technique, if we know or can assume the method of key interruption (e.g., a skip over one element of the key after the occurrence of a previously designated ciphertext letter, in this case W_e), involves writing out the modified cipher text of a single message on trial widths in order to see if any cyclic properties are present in the basic, uninterrupted key. We can then determine statistically when the correct cyclic write-out is reached by the application of a technique discussed in the preceding text.¹⁶ As an example, let us assume the following message is at hand:

G S W W T R H Z D W G L N U J W X R W R H N Q L S Y X T E V
G C V B W C W Z U V I A V F G X X F N P H G P H A M I K D R
V C T E A V C A W G J I C G G C I S N S I V C J B S Z S R W
V L K Z R J B H C C C A Y Q V W J M R L W T L R S D J X F N
Z Z I A F M Q J C X

(2) If we know the method of interruption and also the identity of the ciphertext interruptor,¹⁷ we would write out the appropriately modified cipher text on various widths, testing each hypothesis in turn, until a satisfactory I.C. is reached for an entire columnar array. For example, if we know that the enemy is using key words and phrases from 11 to 40 letters in length as the basic key sequence, we would begin by writing out the modified cipher text (on the assumption of W_e as the interruptor letter) on a width of 11 as shown below, together with the appropriate ϕ values for the computations:

1 2 3 4 5 6 7 8 9 10 11
G S W . W . T R H Z D
W . G L N U J W . X R
W . R H N Q L S Y X T
E V G C V B W . C W .
Z U V I A V F G X X F
N P H G P H A M I K D
R V C T E A V C A W .
G J I C G G C I S N S
I V C J B S Z S R W .
V L K Z R J B H C C C
A Y Q V W . J M R L W
. T L R S D J X F N Z
Z I A F M Q J C X
 ϕ : 6 6 4 2 4 2 12 6 6 14 2 $\Sigma\phi=64$
N: 12 11 13 12 13 11 13 12 12 12 9

(b) (1)
(b) (3)-18 USC 798
(b) (3)-50 USC 3024(i)
(b) (3)-P.L. 86-36

(3) The row of numbers immediately beneath the write-out represents the ϕ values of the columns; the row beneath the " ϕ " row, labelled "N", represents the number of letters in the columns. Since there

¹⁶ Cf. Subpar. 18e on pp. 28-31 of *Military Cryptanalytics, Part II*.

¹⁷ If worst came to worst, we could test each of the 26 letters in turn as the ciphertext interruptor. This testing, coupled with the writing out of the cipher text on the various widths, would be quite laborious and time-consuming by manual methods; data processing machine techniques would here be very useful.

column have undergone the same kind of treatment by the same elements (plain and cipher components of the cipher alphabet).”²⁰ It follows that, even if the repeating key is very long, if there are many short cryptograms all enciphered by exactly the same key and each message begins at the same point in the key, the distributions applicable to the successive columns of text can be solved.²¹ Even in aperiodic systems, if there is available a number of messages starting out in the same key which then diverges in the course of encipherment according to the nature of the cryptosystem, this *solution by superimposition* may be applicable in particular cases, so long as the key divergence is not too radical for cryptanalytic comfort.

b. Let us study the following beginnings of 30 messages, passed between correspondents known to have used various types of aperiodic keying:

- | | |
|---|---|
| 1. Y F W F M R I Q M X X E L M J . . . | 16. G O E Q B Q O T L E S A C R B . . . |
| 2. H W W T T E C T D O Z F D O V . . . | 17. W T S R G X M Z T V S J Q L X . . . |
| 3. T P Y F K S O V W I H F N C J . . . | 18. W T E V F C I B T S P R C A T . . . |
| 4. Y P E P S N L S K Z N V T J B . . . | 19. Z C V Y M B V N Y W Q U Z G U . . . |
| 5. E A Q U Z D V E S K C I U P A . . . | 20. Z C T T Z W C T T I K H Q U T . . . |
| 6. Z C G M W T N B I M K U S N L . . . | 21. Z C C T S N E S K O U B M P T . . . |
| 7. E P D O Z F D O V B I L V L W . . . | 22. A F E S J O N K T D V E S K C . . . |
| 8. E P T L E S A C R B M P T P J . . . | 23. Z C F F D T N P F D H D T P F . . . |
| 9. W M L S O T O Z E E J Z G V K . . . | 24. V Z I E X R X R F F U N T Q E . . . |
| 10. Z C F F D C F R J W H L P D T . . . | 25. E P S N L S K L O H W P T R G . . . |
| 11. H C Q E D T P Y I L N R E M V . . . | 26. Y T S V W L S T L E S A C R B . . . |
| 12. C L C T Z I K S O E O Z C T T . . . | 27. W A Z X Z Q A C H Q U T L S T . . . |
| 13. H C Q E F D K I F Q W O C L M . . . | 28. N O F T Z N L H Q U T J H Z A . . . |
| 14. E P T W K S U Z N V V A U C S . . . | 29. V R C W K M O L N X W S D O L . . . |
| 15. Z A B M Z H G O F X Q I G M M . . . | 30. S P R C P F X E O J C Q F W M . . . |

²⁰ *Military Cryptanalytics, Part II*, subpar. 65a.

²¹ Cf. subpar. 65b, *Military Cryptanalytics, Part II*.

The presence of digraphic and polygraphic repetitions in the initial columns could mean that the messages start out in flush depth, and the presence of offset repetitions could be an indication of shifts in the keying sequence. Frequency distributions for the columns are made and are shown in Fig. 16, below, accompanied by their I.C.'s:

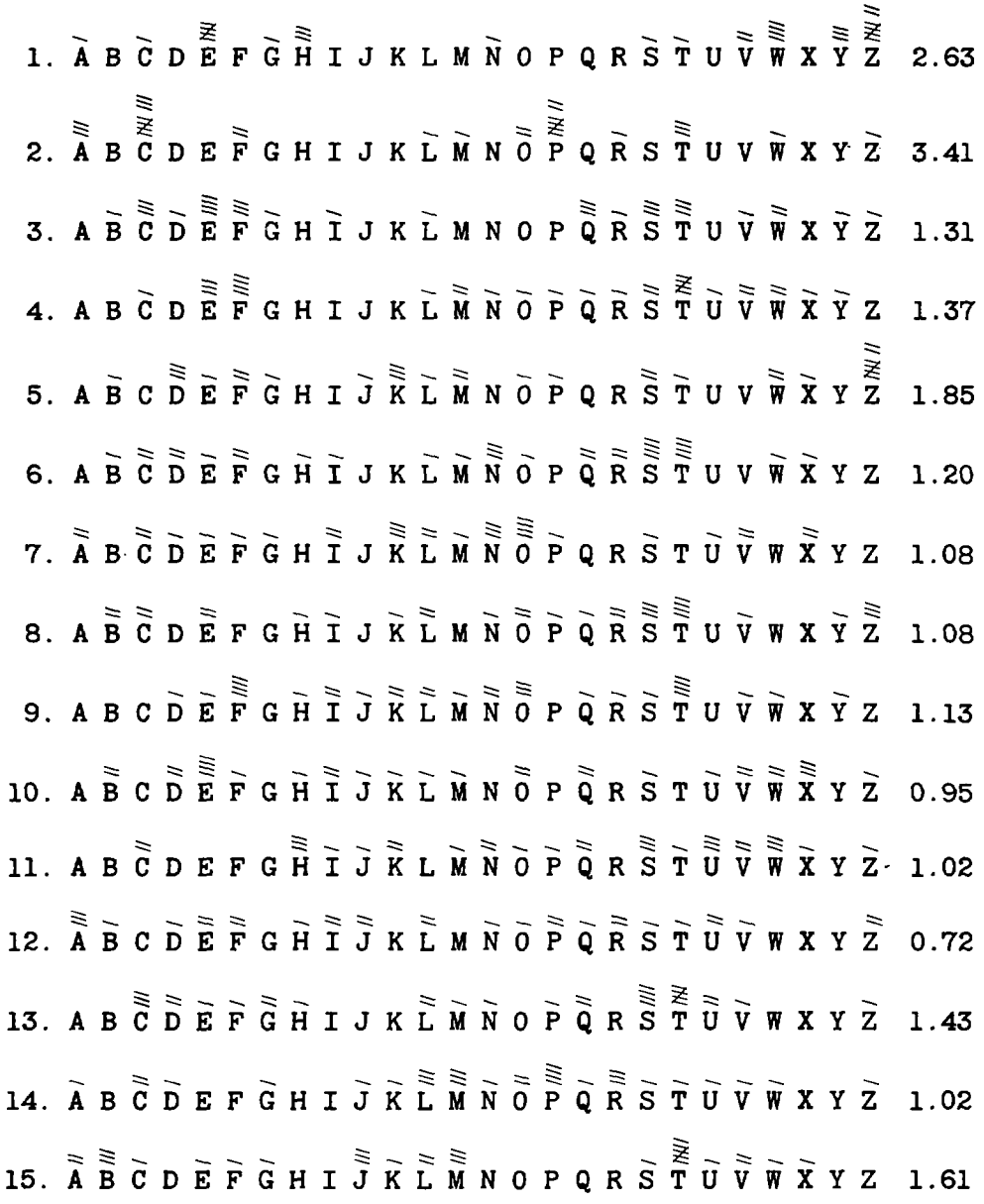


FIGURE 16

c. The first two columns are certainly monoalphabetic; after that, there is a rapid falling off in monoalphabeticity, with the exceptions of cols. 5, 13 and 15 which could be due to chance. We note the digraph ZC, which occurs 6 times in cols. 1 and 2; this could well be the equivalent of RE_p, and HC_c in cols. 1 and 2 could stand for SE_p. On this basis, ZCFFD in Messages 10 and 23 could represent REFER, and HCQE in Messages 11 and 13 could be SEND. We then note

23. $Z \overset{5}{C} \overset{10}{F} \overset{15}{F} D \underline{T} N P F D H D T P F . . .$
 R E F E R

6. $Z C G M W \underline{T} N B I M K U S N L . . .$
 R E

which could represent REFERENCE and REGIMENT. We now turn our attention to the following four message beginnings:

28. N O F ⁵ T Z N L H Q U T J H Z A . . .
 F R
20. Z C T T Z W C T T I K H Q U T . . .
 R E R
21. Z C C T S N E S K O U B M P T . . .
 R E
12. C L C T Z I K S O E O Z C T T . . .
 R

If we assume that T_e in col. 4 represents O_p, then in No. 28—FOR . . . becomes INFORM(ATION), in No. 20 RE-OR- becomes REPORT, in No. 21 RE-O . . . becomes RECOMMEND, and in No. 12—COR--N- becomes ACCORDING.

d. The plain-cipher equivalencies from the foregoing assumptions are entered into a sequence reconstruction matrix, as shown below:

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
1	C										N										Z	H				
2		L	C												O											
3		C		F	G										Q	T										
4			(E)	F							(M)															
5																										
6				I	T																					
7	L			E							K															
8		P																								
9			(K)	F		O					(Q)															
10																										
11																										

Conflicts are noted in lines 5 and 8, and between lines 4 and 9; however, possibility of direct symmetry is noted in the top four lines, which indicates that the recoveries in these lines could well be homogeneous, not having been affected by vagaries of the keying. Transferring values among these four lines, we will develop the reconstruction matrix into the following, in which the cipher components are slides of what is patently a keyword-mixed sequence (derived values in lower case):

P:

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
1	C	e	f	g					m	N	o	q	t								Z	H				l
2		L	C	e	f	g						m	n	O	q	t								z	h	
3	l	C	e	F	G							m	n	o	Q	T								z	h	
4		c	E	F	g							M	n	o	q	T								z	h	l

Our work sheet will now look as illustrated in Fig. 17. which includes the values in the first four columns obtained by direct symmetry shown in lower case:

- | | |
|---|---|
| 1. Y F W F M R I Q M X X E L M J . . . | 16. G O E Q B Q V O C F X E S N H . . . |
| h E | e N e m |
| 2. H W W T T E C T D O Z F D O V . . . | 17. W T S R G X M Z T V S J Q L X . . . |
| S O | r |
| 3. T P Y F K S O V W I H F N C J . . . | 18. W T E V F C I B T S P R C A T . . . |
| n E | r e T |
| 4. Y P E P S N L S K Z N V T J B . . . | 19. Z C V Y M B V N Y W Q U Z G U . . . |
| e M M A N D | R E |
| 5. E A Q U Z D V E S K C I U P A . . . | 20. Z C T T Z W C T T I K H Q U T . . . |
| c N R | R E P O R T |
| 6. Z C G M W T N B I M K U S N L . . . | 21. Z C C T S N E S K O U B M P T . . . |
| R E G I M E N T | R E C O M M E N D |
| 7. E P D O Z F D O V B I L V L W . . . | 22. A F E S J O N K T D V E S K C . . . |
| c k R | h e N |
| 8. E P T L E S A C R B M P T P F . . . | 23. Z C F F D T N P F D H D T P F . . . |
| c P z | R E F E R E N C E |
| 9. W M L S O T O Z E E J Z G V K . . . | 24. V Z I E X R X R F F U N T Q E . . . |
| l a E | v D E |
| 10. Z C F F D C F R J W H L P H X . . . | 25. E P S N L S K L O H W P T R G . . . |
| R E F E R | c j I G |
| 11. H C Q E D T P Y I L N R E M V . . . | 26. Y T S V W L S T L E S A C R B . . . |
| S E N D R E | r M |
| 12. C L C T Z I K S O E O Z C T T . . . | 27. W A Z X Z Q A C H Q U T L S T . . . |
| A C C O R D I N G | t R |
| 13. H C Q E F D K I F Q W O C L M . . . | 28. N O F T Z N L H Q U T J H Z A . . . |
| S E N D I E | I N F O R M A T I O N |
| 14. E P T W K S U Z N V V A U C S . . . | 29. V R C W K M O L N X W S D O L . . . |
| c P | C |
| 15. Z A B M Z H G O F X Q I G M M . . . | 30. S P R C P F X E O J C Q F W M . . . |
| R I R E | b G |

FIGURE 17

e. At this point more plain text could be assumed in the messages from the fragments already present; the cipher component would be recovered in its entirety, the basic key determined, and the cause of the key interruptions (as manifested by the apparent garbles) ascertained. Or, as another

approach, we might take an introspective look at the first 5 letters of matched plain and cipher of the following three message beginnings:

```

10. Z C F F D . . .
    R E F E R
20. Z C T T Z . . .
    R E P O R.
28. N O F T Z . . .
    I N F O R

```

We note the $D_c=R_p$ and $Z_c=R_p$ in position 5 of Messages 10 and 20, and observe that, if the system employs a ciphertext interruptor, it may be either F_c or T_c ; but if $TZ_c=OR_p$ in Messages 20 and 28 is causal, F_c and T_c are eliminated and therefore there is *no* ciphertext interruptor in the cryptosystem. We then note the common $F_c=F_p$ between Messages 10 and 28 and the fact that in position 5 of Message 28 $Z_c=R_p$, and we may conclude that, if a plaintext interruptor is present, it must be O_p . We find this to be true, and when we finish the solution of the problem we find the cipher component to be our perennial friend, the HYDRAULIC . . . XZ sequence, and the basic key to be CALIFORNIAGOLDR (USH) .

20. Additional remarks.—*a.* We have seen in the preceding paragraph a demonstration of solution of only one irregularly keyed system involving unknown cipher alphabets. The solution involved a set of very fortunate circumstances indeed, all of which were happily present awaiting rapid exploitation by the cheerful cryptanalyst. Modern cryptanalysis is quite often contingent upon miracles—minor miracles for minor systems, and healthy miracles for some of the complex systems encountered in present-day operations. When we come right down to it, all cryptanalysis is astonishing; it certainly is so to a layman, and it is so even to an expert—if he pauses long enough from his breaking of one system after another to marvel at the phenomenal luck he has had, shuddering at the thought of what would have happened *if* (i.e., *if* the enemy had done this instead of that, if he had used this instead of that, and *if* . . .). On the other hand, all cryptanalysis is quite commonplace:²² after all, messages have been encrypted with certain invariant mathematico-philosophical-procedural elements, and all the cryptanalyst does is to discover and exploit these elements. And, in retrospect, after a problem has been solved, we often shrug our shoulders and say “Well, how else would one have done it?” Many systems of the types treated in this volume could be virtually unsolvable, or might appear to be so, if only a small amount of traffic is available for study, and if little or nothing is known about the nature of the cryptosystem. However, as happens time and again in actual operations, Fortuna smiles and the incredible is shorn of its prefix.

b. Operationally, cryptodilemmas are resolved by the exploitation of contingencies which are by now well-known to the reader: (1) messages in the same or nearly the same keys; (2) depths and partial depths; (3) polygraphic repetitions; (4) cribs; (5) various kinds of cryptographic errors; (6) isologs; (7) matched plain and cipher; (8) isomorphs; (9) indicators. Each problem presents a very special case, and therefore demands its own special requirements for solution.

c. Most of the types of aperiodic substitution discussed in this chapter are rather unsuitable for practical military usage. Encipherment is slow and subject to error. In some cases encipherment can be accomplished only by a single-letter operation. For, in interruptor systems, if the interruptor is a cipher letter the key is interrupted by a letter which cannot be known in advance; if the interruptor is a plaintext letter, while the interruptions can be indicated before encipherment is begun, the irregularities occasioned by the interruptions in keying cause confusion and quite materially retard the enciphering process. In deciphering, the rate of speed would be just as slow in either method. It is obvious that one of the principal disadvantages in all these methods is that if an error in transmission is made, if some letters are omitted, or if anything happens to the interruptor letter, the message becomes difficult or impossible to decipher by the ordinary cipher clerk. In spite of all these objections, plus the fact that the degree of cryptosecurity attainable by most of these methods is not sufficient for military purposes, these systems have been and are still occasionally encountered—which is what makes the cryptologic world go round.

²² It must have been a deep thinker who first uttered the statement that “all problems in cryptanalysis, like mathematics, are either trivial or impossible.”

(b) (1)
(b) (3) -18 USC 798
(b) (3) -50 USC 3024 (i)
(b) (3) -P.L. 86-36

CHAPTER IV
CIPHERTEXT AUTOKEY SYSTEMS

	Paragraph
The cryptography of autokey encipherment.....	21
Solution of ciphertext autokeyed cryptograms when known cipher alphabets are employed.....	22
Principles of solution by frequency analysis.....	23
Example of solution by frequency analysis.....	24
Solution by means of isomorphs.....	25
Solution of isologs involving the same pair of unknown primary components.....	26
	27
Further remarks on ciphertext autokey systems.....	28

21. The cryptography of autokey encipherment.—*a.* The mechanics of autokey encipherment were treated briefly in the preceding volume.¹ In autokey systems there are two possible sources for successive key letters: the cipher text or the plain text of the message itself. In either case, the *initial* key letter or key letters are supplied by prearrangement between the correspondents, or are designated by means of an indicator; after that, the text letters that are to serve as the key are displaced 1, 2, 3 . . . intervals to the right, depending upon the length of the prearranged key.

b. An example of ciphertext autokey encipherment is shown below, wherein the cipher alphabets are direct standard alphabets, and the single letter X is the prearranged initial key:

```

K: X| Q X F W Z Q U A I U Y L E G U G S S F I X L D W I W R Z M
P: T H I R D R E G I M E N T C O M M A N D P O S T M O V I N G . . .
C: Q X F W Z Q U A I U Y L E G U G S S F I X L D W I W R Z M S

```

FIGURE 18a

Instead of having a single letter serve as the initial key, a word or even a long phrase may be used, as in the example below wherein the word FORTUNE is used as the initial key:

```

K: F O R T U N E| Y V Z K X E I E D L O K X K S P X O X A Z G H
P: T H I R D R E G I M E N T C O M M A N D P O S T M O V I N G . . .
C: Y V Z K X E I E D L O K X K S P X O X A Z G H Q A L V H T N

```

FIGURE 18b

Sometimes only the last cipher letter resulting from the use of the prearranged key word is used as the key letter for enciphering the autokeyed portion of the text. Thus, in the preceding example, the plain text beginning GIMENT . . . would be enciphered differently as follows:

```

K: F O R T U N E| I O W I M Z S U I U G G T W L Z R K W K F N A
P: T H I R D R E G I M E N T C O M M A N D P O S T M O V I N G . . .
C: Y V Z K X E I O W I M Z S U I U G G T W L Z R K W K F N A G

```

FIGURE 18c

c. In plaintext autokey encipherment the procedure is quite similar, as is shown in the following example wherein the prearranged initial key is the letter X:

```

K: X| T H I R D R E G I M E N T C O M M A N D P O S T M O V I N
P: T H I R D R E G I M E N T C O M M A N D P O S T M O V I N G . . .
C: Q A P Z U U V K O U Q R G V Q A Y M N Q S D G L F A J D V T

```

FIGURE 19a

¹ Cf. subpar. 99e on pp. 310-311 of *Military Cryptanalytics, Part II*.

If the word FORTUNE were used as the initial key, the plain text would be enciphered as follows:

K: F O R T U N E | T H I R D R E G I M E N T C O M M A N D P O S
P: T H I R D R E G I M E N T C O M M A N D P O S T M O V I N G . . .
C: Y V Z K X E I Z P U V Q K G U U Y E A W R C E F M B Y X B Y

FIGURE 19b

d. In the foregoing examples, direct standard alphabets were used; however, mixed alphabets, either interrelated or independent,² may be used just as readily. Furthermore, instead of the ordinary type of cipher alphabets, the cryptographic process may employ a mathematical process of addition, but the difference between the latter process and the ordinary one using sliding alphabets is more apparent than real. For example, let us consider the following numerical sequence for the 26 letters

H Y D R A U L I C B E F G J K M N O P Q S T V W X Z
1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 0

and let the plaintext message be the same as before. Let us assume that the cryptographic rules prescribe that the first plaintext letter will be self-enciphered,³ and that each cipher letter from that point on is produced in turn by finding the sum (mod 26) of the numerical equivalents of the preceding cipher letter and the plaintext letter to be enciphered; in other words, a type of numerical ciphertext autokey system. This is shown in the diagram below, wherein P' denotes the numerical equivalents of the plain text, C' the sum of the key and the numerical (i.e., intermediate) plain text, and C the conversion into letters of the intermediate cipher text C'.

K : 0 22 23 5 9 12 16 1 14 22 12 23 14 10 19 11 1 17 22 13 16 9 1 22 18 8 0 23 5 22
P : T H I R D R E G I M E N T C O M M A N D P O S T M O V I N G . . .
P' : 22 1 8 4 3 4 11 13 8 16 11 17 22 9 18 16 16 5 17 3 19 18 21 22 16 18 23 8 17 13
C' : 22 23 5 9 12 16 1 14 22 12 23 14 10 19 11 1 17 22 13 16 9 1 22 18 8 0 23 5 22 9
C : T V A C F M H J T F V J B P E H N T G M C H T O I Z V A T C

FIGURE 20a

e. That the difference between the types of encipherment in the preceding subparagraph and the ordinary method of ciphertext autokey encipherment is illusory is demonstrated by the example in Fig. 20b, below:

K: Z T V A C F M H J T F V J B P E H N T G M C H T O I Z V A T
P: T H I R D R E G I M E N T C O M M A N D P O S T M O V I N G . . .
C: T V A C F M H J T F V J B P E H N T G M C H T O I Z V A T C

FIGURE 20b

In this example, the plain and cipher components are keyword-mixed sequences based upon HYDRAULIC, and Z_p is the index letter against which the key letters in the cipher component are set; the cryptographic results are identical to those obtained in Fig. 20a, above.

f. Since the analysis of ciphertext autokey systems is usually easier than the analysis of plaintext autokey systems, the former will be the first to be discussed.

22. Solution of ciphertext autokeyed cryptograms when known cipher alphabets are employed.—a. First of all, it is to be noted that if the cryptanalyst knows the cipher alphabets which were employed in encipherment, the solution hardly presents any problem. It is only necessary to decipher the message beyond the key-letter or key-word portion and the initial part of the plain text enciphered by this key letter or key word can be filled in from the context.

² For instance, an autokey system might incorporate independent, random alphabets such as those illustrated in Fig. 33 on p. 70.

³ This, on a numerical scale, is tantamount to the effect of a key of 0.

(1) For example, let us consider the following beginning of an intercepted message:

Q X F W Z Q U A I U Y L E G U G S S F I . . .

On the assumption of ciphertext autokey involving direct standard alphabets, if we write the cipher text as key letters, displaced one interval to the right, we obtain the following decipherment:

K: Q X F W Z Q U A I U Y L E G U G S S F
C: Q X F W Z Q U A I U Y L E G U G S S F I . . .
P: H I R D R E G I M E N T C O M M A N D

The introductory key letter required to make $Q_c = T_p$ is found to be X_k .

(2) As a second example, let us consider the following beginning of a cryptogram suspected to have been enciphered by ciphertext autokey with direct standard alphabets:

B P A U V N L F J A L Y M L Q N A E L R . . .

Assuming an introductory key of one letter, we obtain the following decipherment:

K: B P A U V N L F J A L Y M L Q N A E L
C: B P A U V N L F J A L Y M L Q N A E L R . . .
P: O L U B S Y U E R L N O Z F X N E H G

Nothing. We now assume that the introductory key consisted of two letters, and we get the following results:

K: B P A U V N L F J A L Y M L Q N A E
C: B P A U V N L F J A L Y M L Q N A E L R . . .
P: Z J V T Q S Y V C Y B N E C K R L N

Still nothing. We make several more trials, and finally, on the assumption of an introductory key of 8 letters, the following is obtained.

K: B P A U V N L F J A L Y
C: B P A U V N L F J A L Y M L Q N A E L R . . .
P: I L L E R Y F I R E A T

It is clear that the introductory key is 8 letters in length. Doing what comes naturally,

K: N U M B P A U V N L F J A L Y
C: B P A U V N L F J A L Y M L Q N A E L R . . .
P: A R T I L L E R Y F I R E A T

shows that the introductory key ends with NUM; now with but little experimentation, either with the letters of the key or with the beginning of the message plain text, we obtain the complete solution:

K: A L U M I N U M B P A U V N L F J A L Y
C: B P A U V N L F J A L Y M L Q N A E L R . . .
P: B E G I N A R T I L L E R Y F I R E A T

(3) In a third case, we will assume that the following is the beginning of an intercepted message:

D I T G C M G T Z B P C V D Q K Y S K P . . .

Again assuming direct standard alphabets, writing the cipher text as key letters displaced one interval to the right and deciphering, we obtain the following:

K: D I T G C M G T Z B P C V D Q K Y S K
 C: D I T G C M G T Z B P C V D Q K Y S K P . . .
 P: F L N W K U N G C O N T I N U O U S F

We note the plain text "CONTINUOUS F . . ." emerging, preceded by the NG which is probably ING; this indicates that ciphertext autokey is involved with an initial key of 7 letters, and that the last letter of the initial key is used to start the autokeyed portion. After a little experimentation with the initial portion of the message text and the key,⁴ we recover the key word and the first word of the message, as follows:⁵

K: M E R C U R Y | G T Z B P C V D Q K Y S K
 C: D I T G C M G T Z B P C V D Q K Y S K P . . .
 P: R E C E I V I N G C O N T I N U O U S F

b. A mechanical method of solution for ciphertext autokeyed cryptograms when the components are known sequences may be of interest. The method involves the use of sliding alphabet strips aligned in such a manner that, as one progresses from left to right across the strips, each key letter is set opposite the letter k on the preceding strip:⁶ the plain text will appear to the left of the pertinent cipher letter on each strip. In other words, what we have is a mechanical method of correlating the letters of the key, cipher, and plain text; the method is best understood by examples.

(1) In Fig. 21 is illustrated the arrangement of standard-alphabet strips for the first 10 letters of putative key, QXFWZQUAIU, for the message beginning given in subpar. a(1), above. If we assume that a one-letter introductory key has been used, the key letters just named were used to key the 2d through 11th cipher letters, XFWZQUAIUY; therefore we search for these cipher letters consecutively across the strips and we note the letters to their immediate left. In this case the plain text HIRDREGIME is manifested and the problem is solved.

⁴ The I of ING gives a key of Y, which should be preceded by a T, A, L, or very few other letters.

⁵ The key word and the first word of the message may be recovered by working backwards from ING_p, or by assuming various initial digraphs for the plain text or the key; a trial of RE_p for the message beginning would yield ME_x, and we could go on from here to read this "depth of one."

⁶ This is under the assumption that A_p is the index letter in the cryptographic equations.

(K): (Q X F W Z Q U A I U) (B P A U V N L F J A) (B P A U V N L F J A)
(C): (X F W Z Q U A I U Y) (P A U V N L F J A L) (J A L Y M L Q N A E)

<u>A</u> QNSONDXXFZ	<u>AB</u> QQKFSDIRR	<u>AB</u> QQKFSDIRR
BROTPOEYYGA	BCRRRLGTEJSS	BCRRRLGTEJSS
CSPUQPFFZZHB	CDSSSMHUFKTT	CDSSSMHUFKTT
DTQVRQGA <u>AA</u> IC	DETTNIVGLUU	DETTNIVGLUU
EURWSR <u>HBB</u> JD	EFUUOJWHMVV	EFUUOJWHMVV
FVSXTSICCKE	FGVVPKXINWW	FGVVPKXINWW
GWTYUTJDDLFL	GHWWQLYJOXX	GHWWQLYJOXX
H <u>X</u> UZVUKEEMG	HIXXRMZKPHY	HIXXRMZKPHY
IYV <u>AW</u> VLFFNH	IJYYS <u>NAL</u> QZZ	IJYYS <u>NAL</u> QZZ
JZWBXWMGGOI	JKZZTOBM <u>RAA</u>	JKZZTOBM <u>RAA</u>
K <u>AX</u> CYXNHHPJ	KL <u>AA</u> UPCNS <u>BB</u>	KL <u>AA</u> UPCNS <u>BB</u>
LBYDZYO <u>II</u> QK	LM <u>BB</u> <u>EV</u> QDOTCC	LM <u>BB</u> <u>EV</u> QDOTCC
MCZEA <u>AZ</u> PJJRL	MNCCWREPUDD	MNCCWREPUDD
ND <u>AF</u> BA <u>Q</u> KKSM	NODDXSFQVEE	NODDXSFQVEE
OEBGCBRLLTN	OPEEYTGRRFF	OPEEYTGRRFF
PFCHDCSMMUO	PQFFZUHSXGG	PQFFZUHSXGG
QGDIEDTNNVP	QRGG <u>AV</u> ITYHH	QRGG <u>AV</u> ITYHH
RHEJFEUOOWQ	RSHHBWJUZZII	RSHHBWJUZZII
S <u>I</u> FKGFVPPXR	STIICXKVA <u>J</u> J	STIICXKVA <u>J</u> J
TJGLHGWQQYS	TUJJ <u>DYL</u> WBKK	TUJJ <u>DYL</u> WBKK
UKHMIHXRRZT	UVKKEZMX <u>CLL</u>	UVKKEZMX <u>CLL</u>
VLINJIYSS <u>SAU</u>	VWLLFAN <u>YDMM</u>	VWLLFAN <u>YDMM</u>
WMJOKJZTTBV	WXMMGBOZEN	WXMMGBOZEN
XNKPLKA <u>U</u> UCW	XYNNHC <u>PAFOO</u>	XYNNHC <u>PAFOO</u>
YOLQMLBVVDX	YZOOIDQBGP	YZOOIDQBGP
ZPMRNM <u>CWWEY</u>	Z <u>APP</u> JERCHQQ	Z <u>APP</u> JERCHQQ

(P): (H I R D R E G I M E) (O L U B S Y U E R L) (I L L E R Y F I R E)

FIGURE 21

FIGURE 22a

FIGURE 22b

(2) The next example in Fig. 22a illustrates the strip arrangement for the first 10 letters of key, BPAUVNLFJA, for the message beginning given in subpar. a(2). If a one-letter introductory key has been used, these key letters apply to the 2d through 11th cipher letters, PAUVNLFJAL; the decipherment of these letters is found to their immediate left, which is OLUBSYUERL, obviously not plain text. On the same diagram we then search for the decipherment of the 3d through 12th letters, assuming that a two-letter introductory key was employed; again this yields no valid plain text. Finally, on the 8th trial, on the assumption that an 8-letter introductory key is involved, we obtain the plain text ILLERY FIRE; this is shown in Fig. 22b.

(3) For the third and final example, there is illustrated in Fig. 23a the strip arrangement for the first 10 letters of assumed key, DITGCMGTZB, for the message beginning given in subpar. a(3).

(K): (D I T G C M G T Z B)
(C): (I T G C M G T Z B P)

(Z B P C V D Q K Y S)
(B P C V D Q K Y S K)

A D L E K M Y E X W X
B E M F L N Z F Y X Y
C F N G M O A G Z Y Z
D G O H N P B H A Z A
E H P I O Q C I B A B
F I Q J P R D J C B C
G J R K Q S E K D C D
H K S L R T F L E D E
I L T M S U G M F E F
J M U N T V H N G F G
K N V O U W I O H G H
L O W P V X J P I H I
M P X Q W Y K Q J I J
N Q Y R X Z L R K J K
O R Z S Y A M S L K L
P S A T Z B N T M L M
Q T B U A C O U N M N
R U C V B D P V O N O
S V D W C E Q W P O P
T W E X D F R X Q P Q
U X F Y E G S Y R Q R
V Y G Z F H T Z S R S
W Z H A G I U A T S T
X A I B H J V B U T U
Y B J C I K W C V U V
Z C K D J L X D W V W

A Z A P R M P F P N F
B A B Q S N Q G Q O G
C B C R T O R H R P H
D C D S U P S I S Q I
E D E T V Q T J T R J
F E F U W R U K U S K
G F G V X S V L V T L
H G H W Y T W M W U M
I H I X Z U X N X V N
J I J Y A V Y O Y W O
K J K Z B W Z P Z X P
L K L A C X A Q A Y Q
M L M B D Y B R B Z R
N M N C E Z C S C A S
O N O D F A D T D B T
P O P E G B E U E C U
Q P Q F H C F V F D V
R Q R G I D G W G E W
S R S H J E H X H F X
T S T I K F I Y I G Y
U T U J L G J Z J H Z
V U V K M H K A K I A
W V W L N I L B L J B
X W X M O J M C M K C
Y X Y N P K N D N L D
Z Y Z O Q L O E O M E

(P): (F L N W K U N G C O)

(C O N T I N U O U S)

FIGURE 23a

FIGURE 23b

Nothing is seen here, so a number of additional trials is made, sliding the assumed key over successive 10-letter segments of the cipher text, all without success. We could now assume that an introductory key word was used, and that the autokeyed portion began with the last letter of cipher text after the end of the introductory key. With this in mind, we take as hypothetical key some text after the beginning of the cryptogram, say the 9th through 18th letters, ZBPCVDQKYS; trying this as key for the 10th through 19th letters, BPCVDQKYSK, we are successful on the first trial as shown in Fig. 23b with the emergence of the plain text CONTINUOUS.⁷

c. The foregoing mechanical method serves in helping to understand the mechanics of solution of ciphertext autokey encipherment involving known components. A simpler approach, however, is the use of the method of searching for the location of a probable word, as illustrated in the previous volume.⁸

⁷ Had we been a little more observant, we could have noticed what appears to be a good plaintext fragment NGCO in the very first trial in Fig. 23a; this was a contrived lapse of observation, the better to illustrate a pedagogical point in Fig. 23b.
⁸ Cf. Subpar. 22d on pp. 41-42 of *Military Cryptanalytics, Part II*.

(1) For example, if we were to test the message beginning given in subpar. a(2), above, for the possibility of ciphertext autokey involving direct standard alphabets and an introductory key of unknown length, we would construct the following diagram:

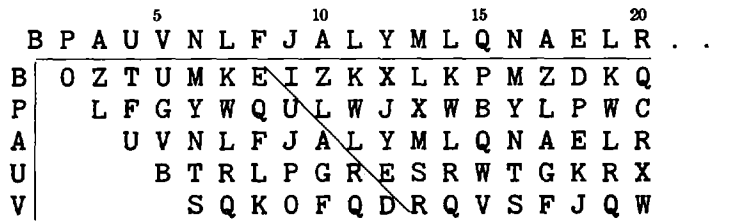


FIGURE 24

In this diagram, the top row contains the cipher letters, and at the left are the first five cipher letters (the putative key); the row just below the line consists of the decipherments of the cipher letters with the first key letter; the second row below the line consists of the decipherments with the second key letter; and so forth. On a diagonal under the 9th cipher letter may be seen the plaintext fragment ILLER, proving that the introductory key was 8 letters in length.

(2) Taking as another example the message beginning given in subpar. a(3), above, we construct the following diagram:

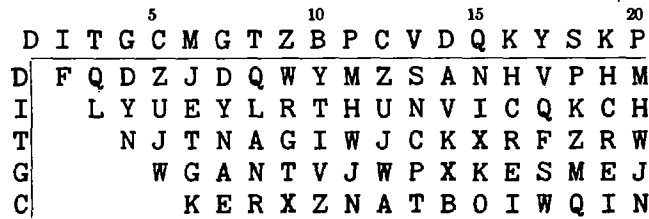


FIGURE 25

Nothing of significance is seen, so, testing the possibility of autokeying from the last letter of a long introductory key, we construct the diagram shown below, in which we have arbitrarily taken as tentative key elements the cipher letters starting at position 11:

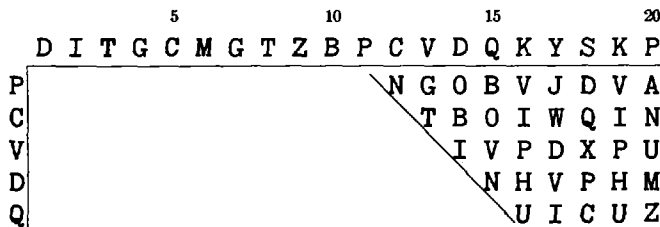


FIGURE 25b

On the very first diagonal, the plain text fragment NTINU manifests itself, showing that the single-letter offset keying begins at least by the 12th cipher letter, if not before (it actually begins at the 8th position, after a 7-letter introductory key, as can be quickly determined).

d. The index letter was A_p in the foregoing examples; if some other letter were used as the index letter, only a slight modification of the general procedure is necessary. Let us study the following example enciphered with direct standard alphabets, with Q_p as the index letter:⁹

K: X|A R J K X Y M C U Q E B E Q O K G Q N A Z X Z C Y W B T Q
P: T H I R D R E G I M E N T C O M M A N D P O S T M O V I N G . . .
C: A R J K X Y M C U Q E B E Q O K G Q N A Z X Z C Y W B T Q G

⁹ Note that, although the plain text and introductory keys are identical with those of the example in Fig. 18a, nevertheless the two cipher texts are not isomorphic, since the change of index letter eliminates any causal isomorphism between the two versions.

If we had only the cipher text, and assumed that it was the result of ciphertext autokey encipherment with direct standard alphabets and a one-letter introductory key, we would perform the following decipherment on the basis of A_p as the index letter:

K : A R J K X Y M C U Q E B E Q O K G Q N
C : A R J K X Y M C U Q E B E Q O K G Q N A . . .
"P": R S B N B O Q S W O X D M Y W W K X N

The "decipherment" does not yield plain text; but if we *complete the plain-component sequence on the result of this decipherment*, we will obtain the true plain text on one of the generatrices, as shown in the diagram below:

R S B N B O Q S W O
S T C O C P R T X P
T U D P D Q S U Y Q
U V E Q E R T V Z R
V W F R F S U W A S
W X G S G T V X B T
X Y H T H U W Y C U
Y Z I U I V X Z D V
Z A J V J W Y A E W
A B K W K X Z B F X
B C L X L Y A C G Y
C D M Y M Z B D H Z
D E N Z N A C E I A
E F O A O B D F J B
F G P B P C E G K C
G H Q C Q D F H L D
*H I R D R E G I M E
I J S E S F H J N F
J K T F T G I K O G
K L U G U H J L P H
L M V H V I K M Q I
M N W I W J L N R J
N O X J X K M O S K
O P Y K Y L N P T L
P Q Z L Z M O Q U M
Q R A M A N P R V N

23. Principles of solution by frequency analysis.—a. It is apparent that repetitions in ciphertext autokey systems will not be nearly as plentiful in the cipher text as they are in the plain text, because in these systems before a repetition can appear two things must happen simultaneously. First, of course, the plaintext sequence must be repeated, and second, one or more ciphertext letters (depending upon the length of the introductory key) immediately before the second appearance of the plaintext sequence must be identical with one or more ciphertext letters immediately before the first appearance of the plaintext sequence. This can happen only as the result of chance. In the following example the introductory key is the single letter X, and the components are direct standard alphabets employed in the usual Vigenère manner:

K: X C K B T M D H N V H L Y K D K S J M D H N V H L Y
P: F I R S T R E G I M E N T T H I R D R E G I M E N T
C: C K B T M D H N V H L Y R K D K S J M D H N V H L Y R

The repeated plaintext word, REGIMENT, has only 8 letters but the repeated ciphertext sequence contains 9, of which only the last 8 letters actually represent the plaintext repetition. In order that the word REGIMENT be enciphered by DHNVHLYR the second time this word appeared in the text, it was necessary that the key letter for its first plaintext letter, R, be M both times; no other key letter will produce the same cipher sequence for the word REGIMENT in this case. Each different key letter for enciphering the first letter of REGIMENT will produce a different encipherment for the word, so that the chance for a repetition in this case is 1 in 26. This is the principal cause for the reduction in repetitions in this system. If an introductory key of two letters were used, it would be necessary that the two cipher letters immediately before the second appearance of the repeated word REGIMENT be identical with the two cipher letters immediately before the first appearance of the word; therefore the chance for a repetition in this case is 1 in 26². In general, then, an n -letter repetition in the cipher text, represents an $(n-k)$ letter repetition in the plain text, where n is the length of the ciphertext repetition and k is the length of the introductory key.

b. There is a second phenomenon of interest in connection with ciphertext autokey systems. Let the letter opposite which the key letter is placed (when using sliding components for encipherment) be termed, for convenience in reference, the "base letter." Normally the base letter is the initial letter of the plain component, but it has been pointed out in the preceding volume that this is only a convention. Now when the introductory key is a single letter, if the base letter occurs as a plaintext letter its cipher equivalent is identical with the immediately preceding cipher letter; that is, there is produced a double letter in the cipher text, no matter what the cipher component is and no matter what the key letter happens to be for that encipherment. For example, using the HYDRAULIC . . . XZ sequence for both primary components, with H (the initial letter of the plain component) as the base letter, and using the introductory key letter X, the following encipherment is produced:

```

K: X|U N F F T T V K U H H M B N
P: I F T H E H Y P O T H E S I S . . .
C: U N F F T T V K U H H M B N E

```

Note the doublets FF, TT, and HH. Each time such a doublet occurs it means that the second letter represents H_p, which is the base letter in this case (the initial letter of the plain component). Now if the base letter happens to be a high-frequency letter in normal plain text, for example the letter E or T, then the cipher text will show a large number of doublets; if it happens to be a low-frequency letter then the cipher text will show very few doublets. In fact, the number of doublets will be directly proportional to the frequency of the base letter in normal plain text. Thus, if the cryptogram contains 1,000 letters there should be about 72 occurrences of doublets if the base letter is A, since in 1,000 letters of plain text there should be about 72 A's. Conversely, if a cryptogram of 1,000 letters shows about 72 doublets, the base letter is likely to be A; if it shows about 90, it is likely to be T, and so on. Furthermore, when a clue to the identity of the base letter has been obtained in this manner, it is possible immediately to insert the corresponding plaintext letter throughout the text of the message. The distribution of this letter may not only serve as a check (if no inconsistencies develop) but may also lead to the assumption of values for other cipher letters.

c. When the introductory key is two letters, then this same phenomenon will produce groups of the formula ABA, where A and B may be any letters, but the first and third must be identical. The occurrence of patterns of this type in this case indicates the encipherment of the base letter.

d. The phenomenon noted above can be used to considerable advantage in the solution of ciphertext autokey cryptograms. For instance, if it is known that the ordinary Vigenère method of encipherment ($\theta_{x/2} = \theta_{1/n}$; $\theta_{p/1} = \theta_{c/2}$) is used, then the initial letter of the plain component is the base letter. If, further, it is known that the plain component is the normal A-Z sequence, then the base letter is A and a word such as BATTALION will be enciphered by a group having the pattern AABCCDEFG. If the plain component is a mixed sequence and happens to start with the letter E, then a word such as ENEMY would be enciphered by a sequence having the pattern AABBCD.¹⁰ Sequences such as these are, of course, idiomorphic and if words yielding such idiomorphisms are frequent in the text there will be produced in the latter several

¹⁰ Six letters are shown because the idiomorphism in this case extends over that many letters.

or many cases of isomorphism. When these are analyzed by the principles of indirect symmetry of position, a quick solution may follow.

e. A final principle underlying the solution of ciphertext autokeyed cryptograms remains to be discussed; it concerns the nature of the frequency distribution required for the analysis of such cryptograms. Consider the message beginning illustrated in Fig. 18a in subpar. 21b. It happens that the letter W_c occurs three times in this short message beginning and, because of the nature of the ciphertext autokeying method, this letter must also appear three times in the key. Now it is obvious that all plaintext letters enciphered by key letter W_k will be in the same cipher alphabet; in other words, if the key text is cipher text offset one letter to the right of the cipher text, *then every cipher letter which immediately follows a W_c in the cryptogram will belong to the same cipher alphabet*, and this alphabet may be designated conveniently as the W cipher alphabet. Now if there were sufficient text, so that there were, say, 30 to 40 W_c 's in it, then a frequency distribution of the letters immediately following the W_c 's will exhibit monoalphabeticity. What has been said of the letters following the W_c 's applies equally well to the letters following all the other letters of the cipher text, the A_c 's, B_c 's, C_c 's, and so on. In short, if 26 distributions are made, one for each letter of the alphabet, showing the cipher letter immediately succeeding each different letter of the cipher text, the text of the cryptograms can be allocated into 26 uniliteral, monoalphabetic frequency distributions which can be solved by frequency analysis, provided that there are sufficient data for this purpose.

(1) The foregoing principle has been described as pertaining to the case when the introductory key is a single letter; that is, when the key text is offset or displaced but one interval to the right of the cipher text. But it applies equally to cases wherein the key text is offset more than one interval, provided that the frequency distributions are based upon the proper interval, as determined by the displacement due to the length of the introductory key. For instance, suppose the introductory key consists of two letters, as in the following example.

K: X Z | M R H F H G F N Q R X O M R M V W E E
P: R E L I A B L E I N F O R M A T I O N . . .
C: M R H F H G F N Q R X O M R M V W E E . . .

The key text in this case is offset two intervals to the right of the cipher text; therefore if we made frequency distributions by taking the cipher letters one interval to the right of a given cipher letter (each time that letter occurs), these distributions will not be monoalphabetic because some letter not related at all to the given cipher letter is the key letter for enciphering the letter one interval to the right of the letter. For example, note the three R_c 's in the foregoing illustration. The first R_c is followed by H_c , representing the encipherment of L_p by M_k ; the second R_c is followed by X_c , representing the encipherment of F_p by Q_k ; the third R_c is followed by M_c , representing the encipherment of A_p by M_k . The three cipher letters H , X , and M are here entirely unrelated and do not belong to the same cipher alphabet because they represent encipherments by three different key letters. On the other hand, the cipher letters *two* intervals to the right of the R_c 's, *viz.*, F , O , and V , are in the same cipher alphabet because these cipher letters are the results of enciphering plaintext letters I , O , and T , respectively, by the *same* key letter, R . It is obvious, then, that when the introductory key consists of two letters and the key text is displaced two intervals to the right of the cipher text, the proper frequency distributions for monoalphabeticity will be based upon the letter at the second interval to the right of each cipher letter. Likewise, if the introductory key consists of three letters and the key text is displaced three intervals to the right of the cipher text, the distributions must be based upon the third interval, and so on, in each case the interval used corresponding to the amount of displacement between key text and cipher text.

(2) Conversely, in solving a problem of this type, when the length of the introductory key and therefore the amount of displacement are not known, the appearance of the frequency distributions based upon various intervals after each different cipher letter will disclose this unknown factor, since only one set of distributions will exhibit monoalphabeticity and the interval corresponding to that set will be the correct interval.

24. Example of solution by frequency analysis.—a. It will be assumed that previous studies have disclosed that the enemy is using ciphertext autokey systems; it will be further assumed that these studies have also disclosed that (1) the introductory key is usually a single letter, (2) the usual Vigenère method of employing sliding primary components is used, and (3) the plain component is usually the normal A-Z sequence, the cipher component a mixed sequence which changes daily. The following cryptograms, all of the same date, have been intercepted:

Message No. 1

I J X W X E E C D A C N Q E T U K N M V D I W P P Q Z S X D
H I F E L N N J J I D I V E Y G T C Z M E H H L M R V C U R
G D I E Q S G T A R J J Q Q Y C A R P H M G L D Y F Y T C D
G Y F K R F K S E T T D I Q K K M L T U R Q G G N K M K I X
J X W K A O K N T B T Z J O Q Y S C D I D G E T X G

Message No. 2

G R V R M Z W K X G W P C K K R M X A N J C C X U R T N J U
A K O B L N L M W K Y Y Z J U C S U H F F H I J A Q B M L T
P U R R S U E Q E V Z E Y G C F F N F I B W N Y S T C E T P
D G T T Z R R Q H Q A O O X D B U Y N K L B W C D G G K

Message No. 3

R W K A O L T C J M Z D K V U J C D D Y B Z E L M M W T Q O
H Q V G X C H O L M W V G R K I B R X D L A Q Y U K I R O Z
T Q Y U

Message No. 4

X J J P M L T Z K X E C A Q Z N T T O C O N D U C T U T C V
G R J P F F D I P P D I X C E S E T W W S U M U J C S L G X
H X M O Z E K A Q I S U A O

Message No. 5

G I S U H W Z H S T T Z O I D D H O O V N B T J G X C T B S
F K I R H M M V Y M I I V U U C Z M J E H A G I E W M E H H
L M W K Y P P D Q Z G B O I W P S F A J U Q Z H Z M T F H Z
M L A C Z R O V D I W P V I B O B C C X N N D G I E S J O C
K B J H Q M U Z E L Y O O V U J W K I E I B B O Z A J I E F
F O R S A J L N Q M B Q

Message No. 6

T B J P A A R Y Y P V H I D I T U X N J M X G S S B D A Q Y
M M T T F U U N M G Q P U X M O V U Y E C E C Z M M W O H C
F O B H V N K A Z C K M

Message No. 7

T B J P A Q A A Z T R X A L X F K K M E I A A B D S F T Q T
C J J G J O V M R G L V W T T J U A W L X U K T X G G B O X
M X D I D S P B S F L Y Z K C F

b. A distribution table is now compiled, the results of which are shown in Fig. 26, below; in originally making the distribution, tallies had been recorded in the appropriate cell in the pertinent horizontal line of the table to indicate the cipher letter which immediately followed each occurrence of the letter to which that line applies. Obviously, the best method of compiling the data is to treat the text biliterally, taking the first and second letters, the second and third letters, and so on, distributing the digraphs as tallies in a digraphic distribution.

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	N	ϕ	I.C.
A	3	1	2				1			3	1	1	1	4		6	3						1		2	29	64	2.05	
B		1	1	2			1			3	1	1	4		1	1	2	2	1		2	2			1	24	26	1.22	
C	2		2	5	3	3	1			2	3		1	1				2	2	1	1		2		4	35	62	1.35	
D	2	1		2			5	2	10	1	1					1		2		1					2	30	120	3.59	
E			4		1	1	3	2	1	3						2		2	5		1	1			2	28	52	1.79	
F	1			1	1	4	2	1	4	1		1	2						1	1					1	21	28	1.73	
G		2	1	1	1		3			3	1	2	1			1	3	1	3			1	3	1		29	32	1.02	
H	1	1			1		2	3		2	2		2		3		1				1	1	1		2	23	22	1.13	
I	1	4		5	5	1				12					1	1	2	1	1		2	3	3			33	70	1.72	
J	1	3		1		2	1	24		1	2	3	4	1							4		1	2		32	56	1.47	
K	4	1	1					5	3	1	4	2	1			2	1	1		1		2	2			31	58	1.62	
L	2	1		1							5	3							4		1		2	2		22	44	2.48	
M		1		3	2		11	1	4	4	2			2		2	2	2	2	5	3		2			37	70	1.37	
N		1	2		1			4	3	1	2	2			2									1		21	28	1.73	
O		3	2				2	2	1	2	1	3	1	1							5		2	3		28	48	1.66	
P	2	1	1	3		1	1			1			3	1		1		2	2							19	18	1.37	
Q	2	1			2	1	1	1	1	2	1	1	1	1	1	1	1	1		1				5	4	26	38	1.52	
R					1	2	1	2	1	2	2	1	2	2	2	2	1		2	1	2	1	2	1			25	18	0.78
S	1	1	1		2	4	1		1	1				1		1	2	5			1					22	36	2.03	
T	1	4	6	1		2		2		1	1	2	3	1	6	4		1	2	4					4	41	110	1.74	
U	3		3	1			2	3	3	1	1			1	4	1	2			2	2	1				30	44	1.31	
V			1	2	1	3	1	1			1	2			1			4		1		1	1			20	22	1.51	
W			1					6	1	1	1	1	4		1	2		1	1	1	1			1		22	44	2.48	
X	2		3	4	2	1	4	1		2		3	2							2		2				28	50	1.72	
Y		1	1		1	2	2				2	1	1	2		2	1	2						2	2	22	16	0.90	
Z	1	1	1	4		1	2	2	2	5	1	1			2	1	2				1					27	42	1.56	
																										705	1218	42.85	

FIGURE 26

c. The individual frequency distributions give every appearance of being monoalphabetic, which confirms the assumption that the enemy is using ciphertext autokey with a *single-letter* introductory key. The average I.C. of the rows of the matrix is $\frac{42.85}{26} = 1.65$, which is fine;¹¹ or, as a better approach, we could calculate the *digraphic* I.C. of the matrix by considering the sum (1218) of the ϕ values of Fig. 26 as the observed value of ϕ and substituting in the formula $\delta = \frac{676 \sum f(f-1)}{N(N-1)} = \frac{676(1218)}{705 \times 704} = 1.66$, again substantiating the same assumption.¹² (This discrepancy between the two figures lies in the round-off errors introduced in obtaining an average I.C.)

¹¹ The arithmetic mean here suffices because the values of N involved are fairly close to one another; since, as has been previously stated, in ciphertext autokey systems the cipher letters are equiprobable (the over-all I.C. of the cipher text in this example is 1.005), a weighted mean is unnecessary.

¹² Ciphertext autokey systems may therefore be identified statistically from the appropriate digraphic distribution (i.e., on the assumption of the correct length of the introductory key) by the fact that the digraphic I.C. will reflect the *monographic* I.C. of the language.

This assumption of AVAILABLE cannot be discarded just yet. Let the values derivable from the assumption be inserted in their proper places in a cipher component, and, using the latter in conjunction with a normal A-Z sequence as the plain component, let an attempt be made to find corroboration for these values. The following placements may be made:¹³

P: A B C D E F G H I J K L M N O P Q R S T U V W X Y Z
C: M F G U N T

The letter M_c appears twice in the cipher sequence and when this partially reconstructed cipher component is tested it is found that the value L_p(N_k) = M_c is corroborated. Having the letters M, F, G, U, N, and T tentatively placed in the cipher component, it is possible to insert certain plaintext values in the text. For example, in the M alphabet, F_c=D_p, G_c=E_p, U_c=O_p, N_c=P_p, and T_c=V_p. In the F alphabet, G_c=B_p, U_c=L_p, N_c=M_p, T_c=S_p, and M_c=X_p. The other letters yield additional values in the appropriate alphabets. The plaintext values thus obtainable are inserted in the cipher text. No inconsistencies appear and, moreover, certain good digraphs are brought to light. For instance, note what is manifested at the end of the third line of Message No. 5:

K: U Q Z H Z M T F H
C: U Q Z H Z M T F H Z
P: V I

Now if the letter H can be placed in the cipher component, several values might be added to this partial decipherment. We note that F and G are sequent in the cipher component; now let us suppose that H follows G therein, and we obtain the following:

K: U Q Z H Z M T F H
C: U Q Z H Z M T F H Z
P: V I C

Suppose the VIC is the beginning of VICINITY. This assumption permits the placement of A, C, L, and Z in the cipher component, as follows:

P: A B C D E F G H I J K L M N O P Q R S T U V W X Y Z
C: M A F G H L Z U N T C

These additional values check in very nicely and presently the entire cipher component is reconstructed. It is found to be as follows:

P: A B C D E F G H I J K L M N O P Q R S T U V W X Y Z
C: M A B F G H J K L Q S V X Z U N D E R W O T Y P I C

The key phrase is clearly based upon UNDERWOOD TYPEWRITER COMPANY. All the messages may now be deciphered with ease. The following gives a letter-for-letter decipherment of the first three groups of each message:¹⁴

Message No. 1 K: KI J X W X E E C D A C N Q E
C: I J X W X E E C D A C N Q E T . . .
P: R I G H T F A I R L Y Q U I E
Message No. 2 K: EG R V R M Z W K X G W P C K
C: G R V R M Z W K X G W P C K K . . .
P: N O T H I N G O F S P E C I A

¹³ Note that, had we not known (or assumed) the plain-component sequence, we would first have entered these values in a 26x26 square rather than in a single strip for the cipher component, and then we would exploit any manifestations of direct or indirect symmetry present.

¹⁴ The introductory keys for these messages are presumed to have been specified by prearrangement, or indicated by the message number, file time, or some other element of the message externals.

Message No. 3 K: R|R W K A O L T C J M Z D K V
 C: R W K A O L T C J M Z D K V U . . .
 P: A B O U T O N E H U N D R E D

Message No. 4 K: J|X J J P M L T Z K X E C A Q
 C: X J J P M L T Z K X E C A Q Z . . .
 P: G U A R D I N S U F F I C I E

Message No. 5 K: E|G I S U H W Z H S T T Z O I
 C: G I S U H W Z H S T T Z O I D . . .
 P: N U M E R O U S F L A S H E S

Message No. 6 K: B|T B J P A A R Y Y P V H I D
 C: T B J P A A R Y Y P V H I D I . . .
 P: T H E R E A R E A B O U T S I

Message No. 7 K: B|T B J P A Q A A Z T R X A L
 C: T B J P A Q A A Z T R X A L X . . .
 P: T H E R E I S A M I X U P H E

f. In the foregoing example the plain component was the normal sequence, so that with the Vigenère method of encipherment the base letter is A. If the plain component is a mixed sequence, the base letter may no longer be A, but in accordance with the principle set forth in subpar. 23b, the frequency of doublets in the cipher text will correspond with the frequency of the base letter as a letter of normal plain text.¹⁵ If a good clue is afforded by the frequency of doublets in the cipher text, the insertion of the corresponding base letter in the plain text will lead to further clues. The solution from there on can be handled along the lines indicated above.

25. Solution by means of isomorphs.—a. It was stated in subpar. 23d that in ciphertext autokey systems the production of isomorphs is a frequent phenomenon and that analysis of these isomorphs may yield a quick solution. An example of this sort will now be studied, using as an illustration the following three messages which are suspected of being in a ciphertext autokey system:

Message No. 1

U S Y P W T R X D I M L E X R K V D B D D Q G S U N S F B O
 B E K V B M A M M O T X X B W E N A X M Q L Z I X D I X G Z
 P M Y U C N E V V J L K Z E K U R C N I F Q F N N Y G S I J
 T C V N I X D D Q Q E K K L R V R F R F X R O C S S J T B V
 E F A A G Z R L F D N D S C D M P B B V D E W R R N Q I C H
 A T N N B O U P I T J L X T C V A O V E Y J J L K D M L E G
 N X Q W H U V E V Y P L Q G W U P V K U B M M L B O A E O T
 T N K K U X L O D L W T H C Z R

Message No. 2

B I I B F G R X L G H O U Z O L L Z N A M H C T Y S C A A T
 X R S C T K V B W K O T G U Q Q F J O C Y Y B V K I X D M T
 K T T C F K V K R O B O E P L Q I G N R I Q O V J Y K I P H
 J O E Y M R P E E W H O T J O C R I I X O Z E T Z N K

Message No. 3

H A L O Z J R R V M M H C V B Y U H A O E O V A C Q V V J L
K Z E K U R F R F X Y B H A L Z O F H M R S J Y L A P G R S
 X A G X D M C U N X X L X G Z J P W U I F D B B Y P V F Z N
 B J N N B I T M L J O O S E A A T K P B Y

¹⁵ If the plain and cipher components had been identical sequences, this fact together with the identity of the base letter could have been determined from the digraphic distribution: one of the rows of the distribution (the row corresponding to the base letter) would reflect an approximation of the normal frequency distribution, i.e., peaks for the letters AEINORST, and blanks or near-blanks for JKQXZ. Furthermore, the reconstruction matrix would have displayed symmetry about the main diagonal (from upper left to lower right); see in this connection subpar. 33e in the next chapter.

b. Frequency distributions are made, based upon the second letters of pairs, as in the preceding example. These distributions are shown in the table in Fig. 27, below. The digraphic I.C. is $\frac{676(500)}{451 \times 450} = 1.67$, confirming ciphertext autokey with a single-letter introductory key. Nevertheless, the data in each distribution are relatively scanty and it would appear that the solution is going to be a rather difficult matter.

2d letter

		A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	N	φ	
1st letter	A	3	1	1	2							2	2	2	1						3				1			18	20	
	B		2	1	1	1		1	2	1			2		4									3	2	3			23	32
	C	1		1	1	1	1								2		1	1	1	2	1	3				1	1	17	8	
	D		2	2	1					2			1	4	1		2		1										16	20
	E	1			1	1	1						4		1	2	1					1	2	2	1	2			20	20
	F	1	1	2			1	1	1	1	1				1		1	2							2		1	15	6	
	G								1						2				1	3		1	1	1			3	13	14	
	H	4	3								1		1	2									1					12	20	
	I		1	1		2	1	2	1	2	1		1		1	1		1	1		2					5		18	26	
	J											1	4	1	4	1		1	2								2	16	28	
	K				1				2		2	1		1	1	1	1	1	4	4							2	20	30	
	L	1	1		2	1	1					1	3	1		2	2	1					1	2		3		22	20	
	M	1		1					2				4	3	1	1	1	2				1				1		18	22	
	N	2	3	1	1				2		2			3		1	1	1								2	1	20	20	
	O	1	2	3	1	3	1		1				1		1					1	4	2	3				2	26	36	
	P		2		1	1	1	1					2	1										2	2			12	8	
	Q					1	2	2	2				1		1	2								1	1			13	8	
	R			1		4		2	1	1	1	2	1		2	3						2		2				22	28	
	S			3	1	1			1	2											1		1			1	1	12	8	
	T		1	3			1	1	2	3		1	2							1	2					2	1	21	20	
	U		1	1			1	1						2	2	1	2	1					1	1	1		1	15	6	
	V	2	3	2	3	1						3	3	1	1				1					2		1		23	30	
	W				1		2						1							1	2	2						9	6	
	X	1	1	5		2							3	1	1	1	3	1	1							2	1	23	36	
	Y		2			1			1	1	1	1				3							2				1	13	10	
	Z				3			1	2					3	2	1	2											14	18	

451 500

FIGURE 27

c. Before becoming discouraged too quickly, however, we make a search throughout the text to see if any isomorphs are present. Fortunately, there appear to be several of them. Note the following:

- Message No. 1 (1) . . . D B D D Q G S U N S F B O B E K . . .
- (2) . . . N E V V J L K Z E K U R C N I F . . .
- (3) . . . T N K K U X L O D L W T H C Z R]
- Message No. 2 (4) . . . C R I I X O Z E T Z N K]
- Message No. 3 (5) . . . C Q V V J L K Z E K U R F R F X . . .

First, it is necessary to delimit the length of the isomorphs. Isomorph (2) shows that the isomorphism begins with the doubled letters; for there is an E before VV in that case and also an E within the isomorph. If the phenomenon included the E, then the letter immediately before the DD in the case of isomorph (1) would have to be an N, to match its homolog, E, in isomorph (2), which it is not. Corroborating data are

given by isomorphs (3), (4), and (5) in this respect. Hence, we may take it as established that the isomorphism begins with the doubled letters. As for the end of the isomorphism, the fact that isomorphs (2) and (5) consist of the same set of 10 letters seems to indicate that this number defines the length of the isomorphism. The fact that Message No. 2 ends 2 letters after the last tie-in letter, Z, corroborates this assumption. It is at least certain that the isomorphism does not extend beyond 11 letters because the recurrence of R in isomorph (5) is not matched by the recurrence of R in isomorph (2), nor by the recurrence of T in isomorph (3). Hence it may be assumed that the isomorphic sequence is probably 10 letters in length, possibly 11. But to be on safe ground it is best to proceed on the 10-letter basis.

d. By applying the principles of indirect symmetry to the superimposed isomorphs, partial chains may be constructed, as shown below:

```

(1-2) D V   Q J   G L   S K   F U Z   N E   B R
(1-3) N D K   Q U O   G X   S L   F W   B T
(1-4) D I   Q X   G O   S Z   U E   F N T   B K
(2-3) V K L X   J U W   Z O   E D   R T
(2-4) V I   J X   L O   R K Z E T   U N
(3-4) D T K I   U X O E   L Z   W N

```

These partial chains may be amalgamated into the following sequence:

L O D J X B S U N . G W . Q . . . F V I . R K Z E T

Noting the J K at an interval of -7, and also W X Z at the same interval, we conclude that a keyword-mixed sequence is involved, and we derive the original sequence as

W X Z . . D R . U L I . B E F G J K . N O . Q S T V ,

whereupon we recognize our perennial friend HYDRAULIC and fill in the missing six letters.

e. We now have the cipher component, and the plain component remains to be reconstructed. The simplest and most foolproof solution ordinarily is a reduction to monoalphabetic terms, using the recovered cipher component and the known offset of the cipher text against itself as key.¹⁶ However, the probable word method, if the probable words are at all probable, may be used to good advantage. A good crib to assume for the 10-letter repetition found in Message Nos. 1 and 3 is ARTILLERY (especially since the doublet rate of the distribution in Fig. 27 is $\frac{33}{451} = 7.3\%$, which is just right for a base letter of A_p to represent the doublet in the repetition). This single assumption is sufficient to place 7 letters in the plain component, thus:

```

K:   V V J L K Z E K U R
C:   V V J L K Z E K U R
P:   A R T I L L E R Y

```

A . . . E . . . I . . L R . T Y .

These few letters (few, but how beautifully spaced!) are sufficient to suggest that the plain component is in all probability the normal sequence. A few moments' testing proves this to be true. The two components are therefore:

```

P: A B C D E F G H I J K L M N O P Q R S T U V W X Y Z
C: H Y D R A U L I C B E F G J K M N O P Q S T V W X Z

```

¹⁶ Note that if the LODJX . . . sequence in subpar. d, above, had not been of systematic construction to enable us to analyze its derivation and thus fill in the missing 6 letters, we still could have converted most of the cipher text to monoalphabetic terms, solved the text, and recovered both components.

f. With the two components at hand, the decipherment of the message is a low-order triviality. Since a single-letter introductory key is known to have been used,¹⁷ we decipher the first five groups of Message No. 1 as follows:

K: ? U S Y P W T R X D I M L E X R K V D B D D Q G S
C: U S Y P W T R X D I M L E X R K V D B D D Q G S U
P: ? P H R F Y I V E F I R E O F L I G H T A R T I L

The mangled beginning is the result either of garbles, or of specialized keying procedure wherein the *last* letter of an introductory key was used as the introductory key letter for enciphering the subsequent autokeyed portion of the text (see Fig. 18c in subpar. 21b). If we assume that the IVE before the word FIRE is the ending of the first word of the plain text, and that this word is INTENSIVE, the introductory key word is found to be WICKER. Thus:

K: W I C K E R | T R X D I M L E X R K V D B D D Q G S
C: U S Y P W T R X D I M L E X R K V D B D D Q G S U
P: I N T E N S I V E F I R E O F L I G H T A R T I L

The beginnings of the other two messages are recoverable in the same way and are found to be as follows:

K: P R O M I S E | R X L G H O U Z
C: B I I B F G R X L G H O U Z O
P: R E Q U E S T V I G O R O U S
K: C H A R G E D | R R V M M H C V
C: H A L O Z J R R V M M H C V B
P: S E C O N D B A T T A L I O N

g. The example solved in the foregoing subparagraphs offers an important lesson to the student, insofar as it teaches him that *he should not immediately feel discouraged when confronted with a problem presenting only a small quantity of text and therefore affording what seems at first glance to be an insufficient quantity of data for solution.* For in this example, while it is true that there are insufficient data for analysis by simple principles of frequency, it turned out that solution was achieved *without any recourse to the principles of frequency of occurrence.* Here, then, is one of those interesting cases of substitution ciphers of rather complex construction which are solvable without any study whatsoever of frequency distributions. Indeed, it will be found to be true that in more than a few instances the solution of quite complicated cipher systems may be accomplished not by the application of the principles of frequency, but by recourse to inductive and deductive reasoning based upon other considerations, even though the latter may often appear to be very tenuous and to rest upon quite flimsy supports.

26. **Solution of isologs involving the same pair of unknown primary components.**—a. Two messages containing identical plain text encrypted in a ciphertext autokey system with two different single-letter introductory keys may be solved in a manner identical to that described in the last paragraph, since what we really have is a pair of long isomorphs one letter shorter than the length of the messages. Even if the introductory keys are words of different lengths and compositions, if the key usage is similar to that illustrated in Fig. 18c in subpar. 21b the message can be solved very rapidly by reconstructing the primary components, since the cryptographic texts of such messages will be isomorphic after the initial keyword portions.

¹⁷ We know this from (a) statistical evidence of the digraphic distribution at an offset of 1, (b) the indications of the correct plain component emerging from a tentative decipherment of the 10-letter repetition, and (c) the unlikelihood that with three rather short messages a long ciphertext repetition would have manifested itself if the offset were more than 1 letter. We knew that the three messages were autokeyed at the same offset, otherwise the isomorphs would have not appeared among all three messages.

(1) Note the two following superimposed messages, in which isomorphism between the two cryptograms is both obvious and consistent after their 6th letters:

```

Msg "A": T S B J S K B N L O C F H A Z L W J A M B N F N S
Msg "B": B K K M J X Y C X B H R P V O X M U V I Y C R C G
Msg "A": M V J R E H F P R X C P C R R E H F M U H R A X C
Msg "B": I K U T D P R E T N H E H T T D P R I W P T V N H
Msg "A": N F D U B A T F Q R
Msg "B": C R S W Y V J R F T

```

Starting with any pair of superimposed letters (after the 6th pair), the following chains are derived:

```

      1 2 3 4 5 6 7 8 9 10 11 12 13 14
(1) Z O B Y . . . .
(2) L X N C H P E D S G . . . .
(3) Q F R T J U W M I . . . .
(4) A V K . . . .

```

The foregoing fragments either are part of two 13-letter chains, or they are parts of a complete 26-letter sequence. If the former is the case, then the two 13-letter chains must be (Z O B Y Q F R T J U W M I) and (L X N C H P E D S G A V K); and, a few moments later, noting phenomena associated with keyword-mixed sequences in the two chains, we superimpose them in the diagram ¹⁸

```

Z O B Y Q F R T J U W M I
H P E D S G A V K L X N C
Y Q F R T J U W M I Z O B

```

from which we speedily obtain the HYDRAULIC . . . XZ sequence.¹⁹

(2) Only the cipher component has been recovered thus far. If we assume that the plain component is the same as the cipher, the initial key words and the message plain texts are at once deciphered; it will be found that the initial key word for Message "A" is PENCE, and that for Message "B" is LATERAL.²⁰ If the plain component had not been guessed in this case, we could have "deciphered" the message text using an arbitrary plain component (say, the A-Z sequence), resulting in a conversion of the complex cipher text into monoalphabetic terms which can then speedily be solved.

(3) The foregoing solution affords a clue to the solution of cases in which the texts of two or more messages are not completely identical but are in part identical because they happen to have similar beginnings or endings, or contain nearly similar information or instructions. The progress in such cases is not so rapid as in the case of messages with wholly identical texts because much care must be exercised in blocking out the isomorphic sequences upon which the reconstruction of the primary components will be based.

b. In the preceding example the autokeyed portions of the texts started with the last letters of the introductory keys. If full autokeying (i.e., the method shown in Fig. 18b), had been employed the solution would hardly be more difficult.

¹⁸ See subpar. 44i on pp. 89-90 of *Military Cryptanalytics, Part II*.

¹⁹ If the four fragments (1), (2), (3), and (4) had been parts of a complete 26-letter sequence, there would have been only 6 ways to permute them, viz., 1-2-3-4, 1-2-4-3, 1-3-2-4, 1-3-4-2, 1-4-2-3, and 1-4-3-2; therefore the problem would still be solvable without too much effort, even if the cipher component has been a random sequence.

²⁰ The reason that the cryptographic texts are isomorphic after the initial keyword portions is, of course, that since the text beyond the key word is enciphered autokey fashion by the preceding cipher letter, the letters before the last letter of the key have no effect upon the encipherment at all. Hence two messages having identical plain text cannot be other than isomorphic after the initial keyword portions.

(1) In order to illustrate such a case, let the same plain texts used in the preceding example be enciphered by introductory key words of the same lengths but different compositions: PENCE and LATER. Thus:

Message "A"

K: PENCE | T S B J S M M N R U L P U I H J B T X F I N N R M
P: R E Q U E S T I N F O R M A T I O N O F S I T U A T I O N I
C: T S B J S M M N R U L P U I H J B T X F I N N R M D W I Q V

K: D W I Q V P C K A O D P A Z O B C M R I A F N W O G L I H T
P: N F I F T E E N T H I N F A N T R Y S E C T O R A T O N C E
C: P C K A O D P A Z O B C M R I A F N W O G L I H T I W W C U

Message "B"

K: LATER | B K K M J R B T U X S G E B Q Y R H H A T E T U C
P: R E Q U E S T I N F O R M A T I O N O F S I T U A T I O N I
C: B K K M J R B T U X S G E B Q Y R H H A T E T U C N O G T M

K: N O G T M L D Q L E N G B Y E W D S U H P U T Z E H H G D K
P: N F I F T E E N T H I N F A N T R Y S E C T O R A T O N C E
C: L D Q L E N G B Y E W D S U H P U T Z E H H G D K T O D E X

(2) Now let the cipher texts be superimposed and isomorphisms be sought. They are shown underlined below:

Msg A: T S B J S M M N R U L P U I H J B T X F I N N R M D W I Q V
Msg B: B K K M J R B T U X S G E B Q Y R H H A T E T U C N O G T M

Msg A: P C K A O D P A Z O B C M R I A F N W O G L I H T I W W C U
Msg B: L D Q L E N G B Y E W D S U H P U T Z E H H G D K T O D E X

It will be noted that the intervals between identical vertical pairs show a constant factor of 5, indicating that the messages have been enciphered with 5-letter introductory key words.

(3) The vertical pairs beyond the first five letters of the messages are now distributed in a reconstruction matrix according to their position based upon this interval of 5, similar to the treatment of vertical pairs in periodic-cipher isologs arising from the use of repeating keys of the same lengths.²¹ This is shown below:

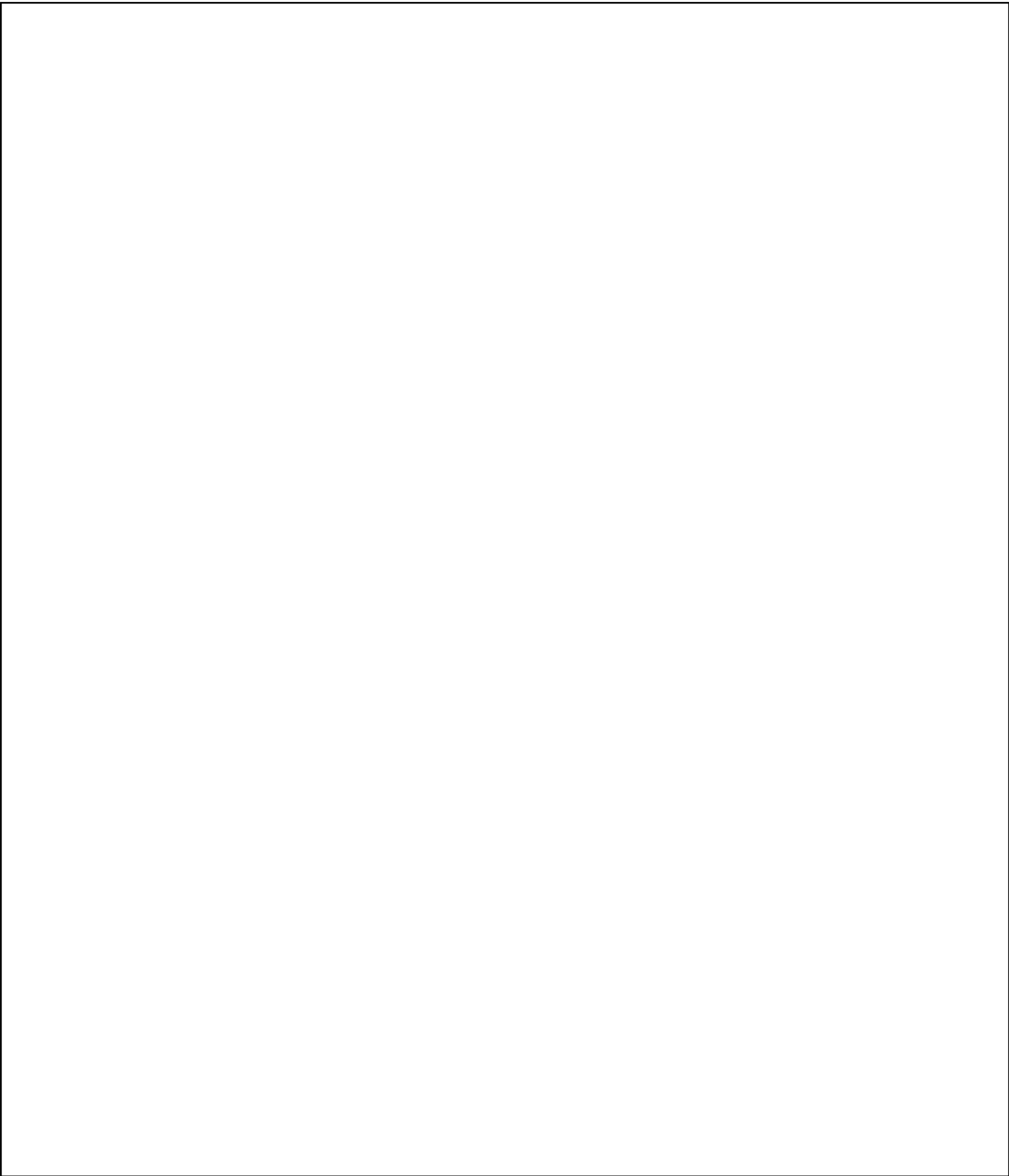
∅	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
1	P	W	N		H		T	Y		S	R		L													
2		R	D		U						H	B	E		G									O		
3	B							G		Q		S	T								H	E		D		
4	L	E						D	B								T	U					Z	H	Y	
5					A		Q	H				C	E								K	X	M			

From the values in this matrix the original cipher component, the HYDRAULIC . . . XZ sequence, may quickly be recovered, because the ∅ line may be included in the chaining.

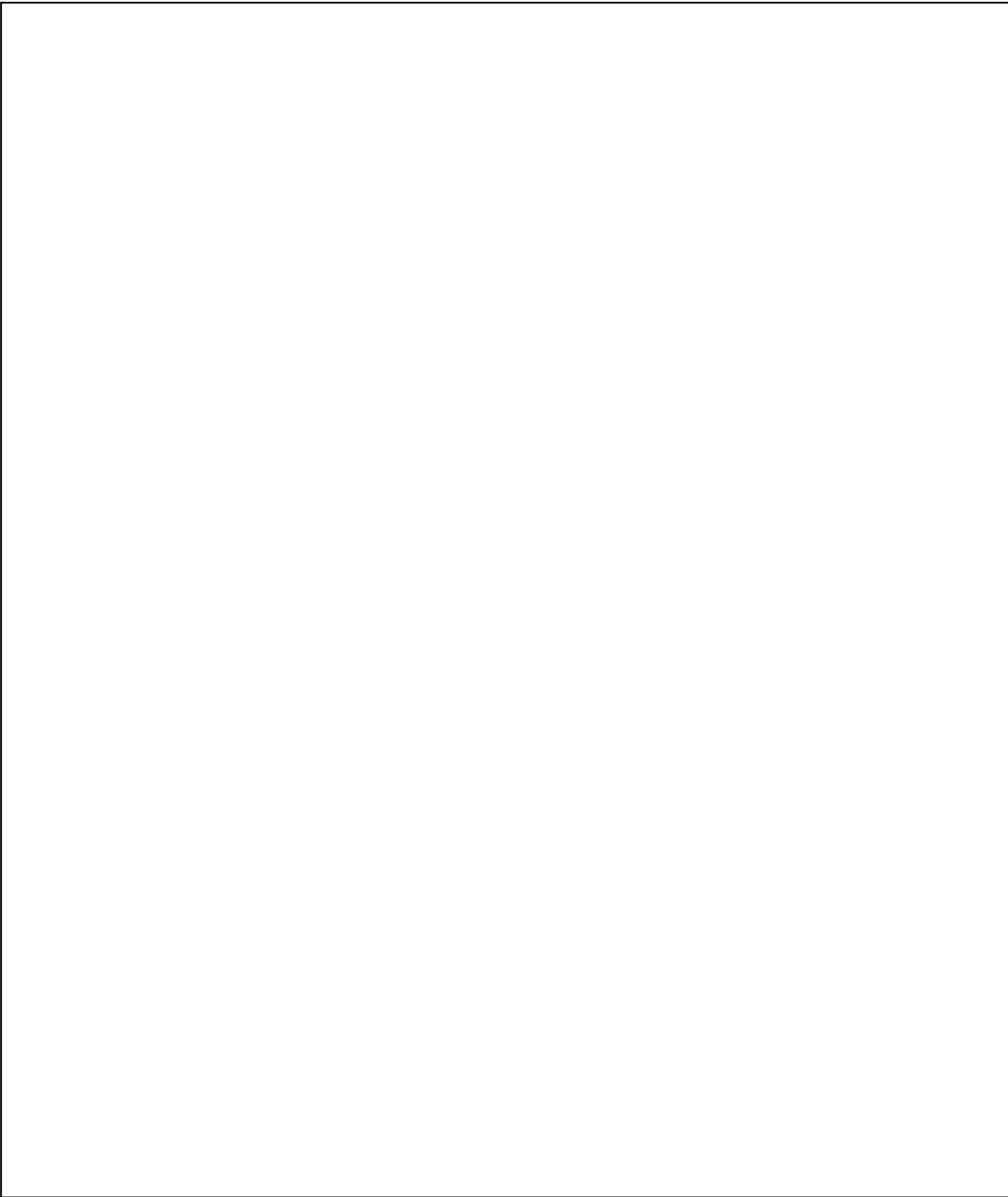


²¹ Cf. subpar. 60f, *Military Cryptanalytics, Part II*.

(b) (1)
(b) (3) -18 USC 798
(b) (3) -50 USC 3024(i)
(b) (3) -P.L. 86-36

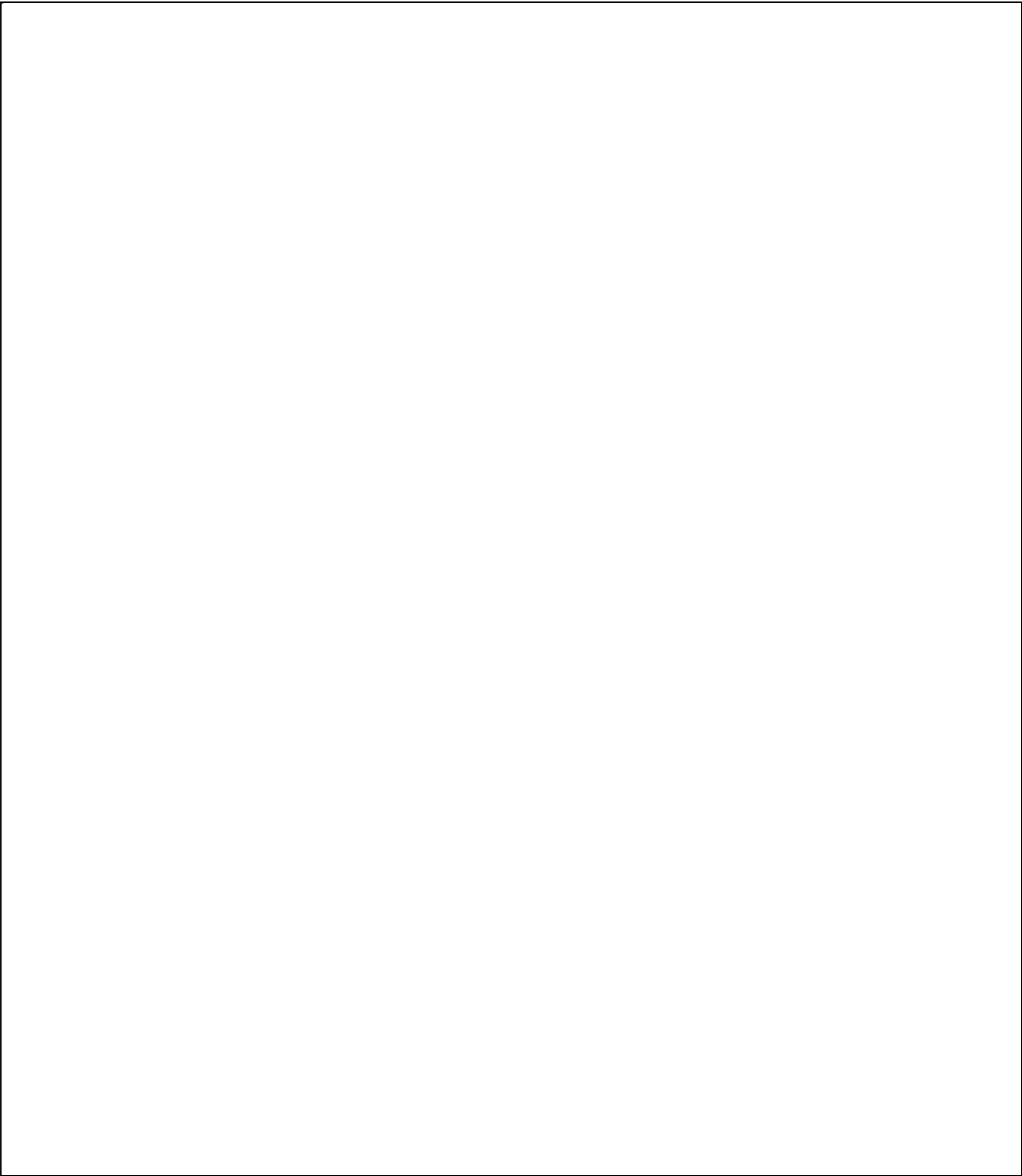


(b) (1)
(b) (3) -18 USC 798
(b) (3) -50 USC 3024 (i)
(b) (3) -P.L. 86-36

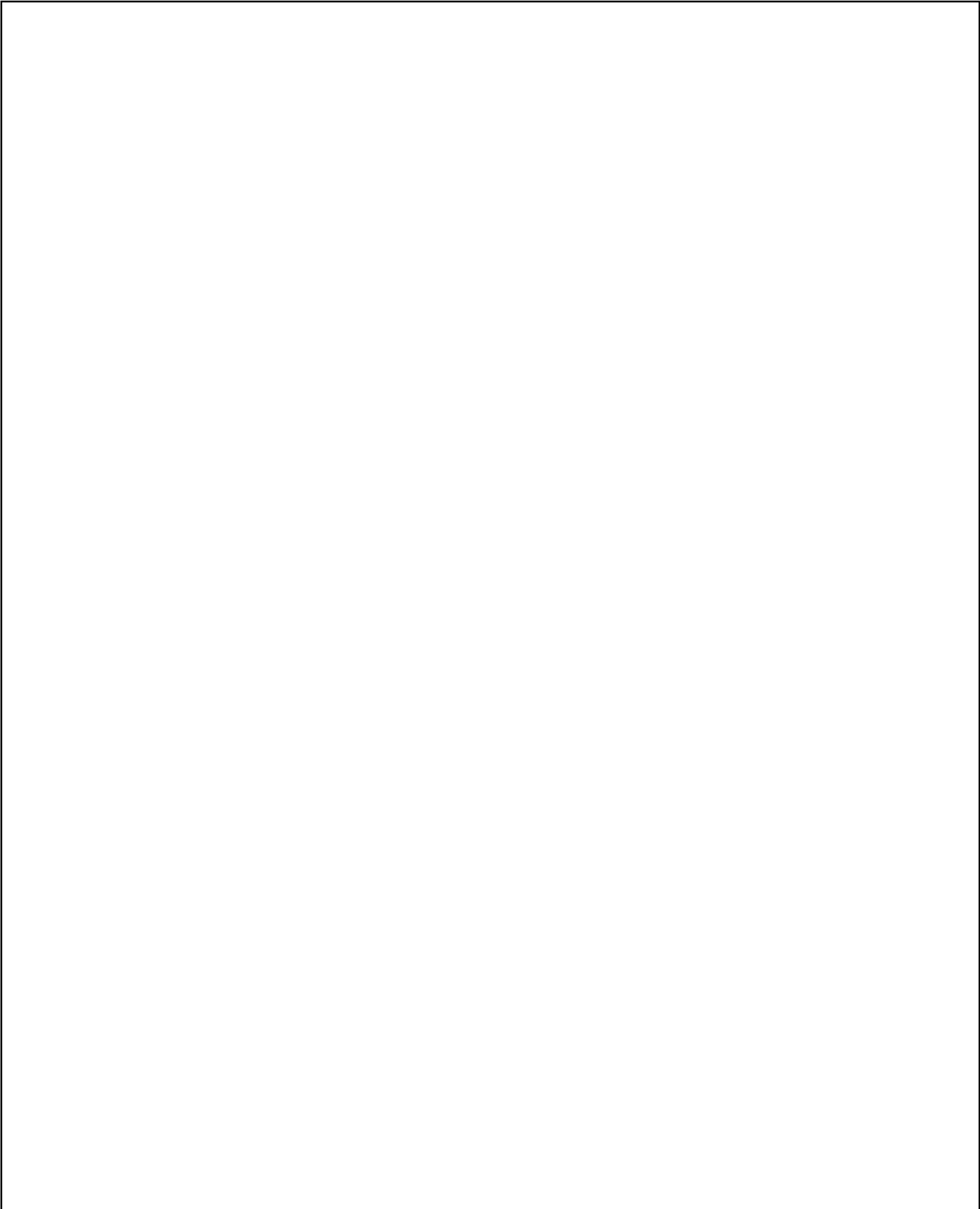


(b) (1)
(b) (3)-18 USC 798
(b) (3)-50 USC 3024 (i)
(b) (3)-P.L. 86-36

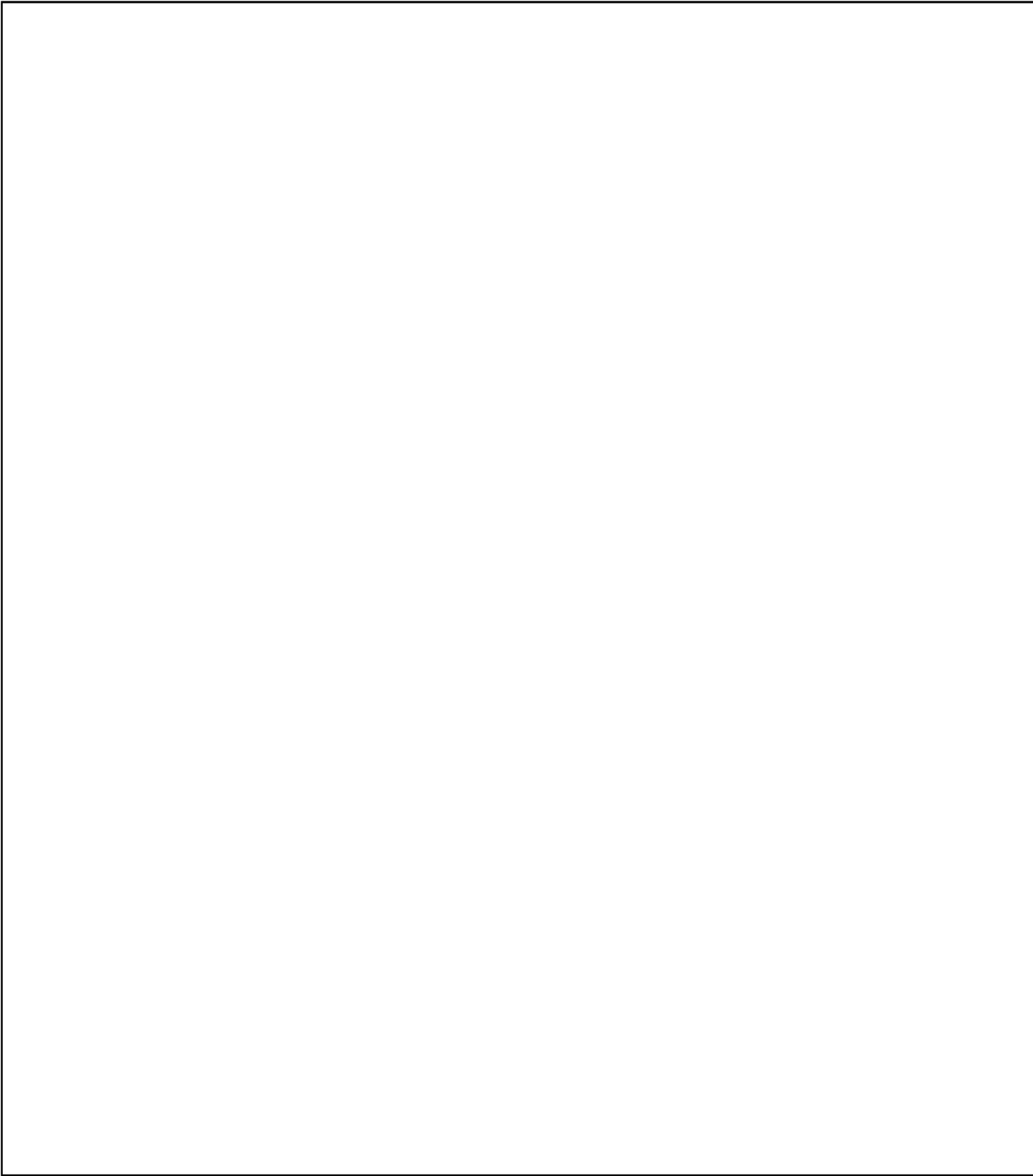
(b) (1)
(b) (3)-18 USC 798
(b) (3)-50 USC 3024 (i)
(b) (3)-P.L. 86-36



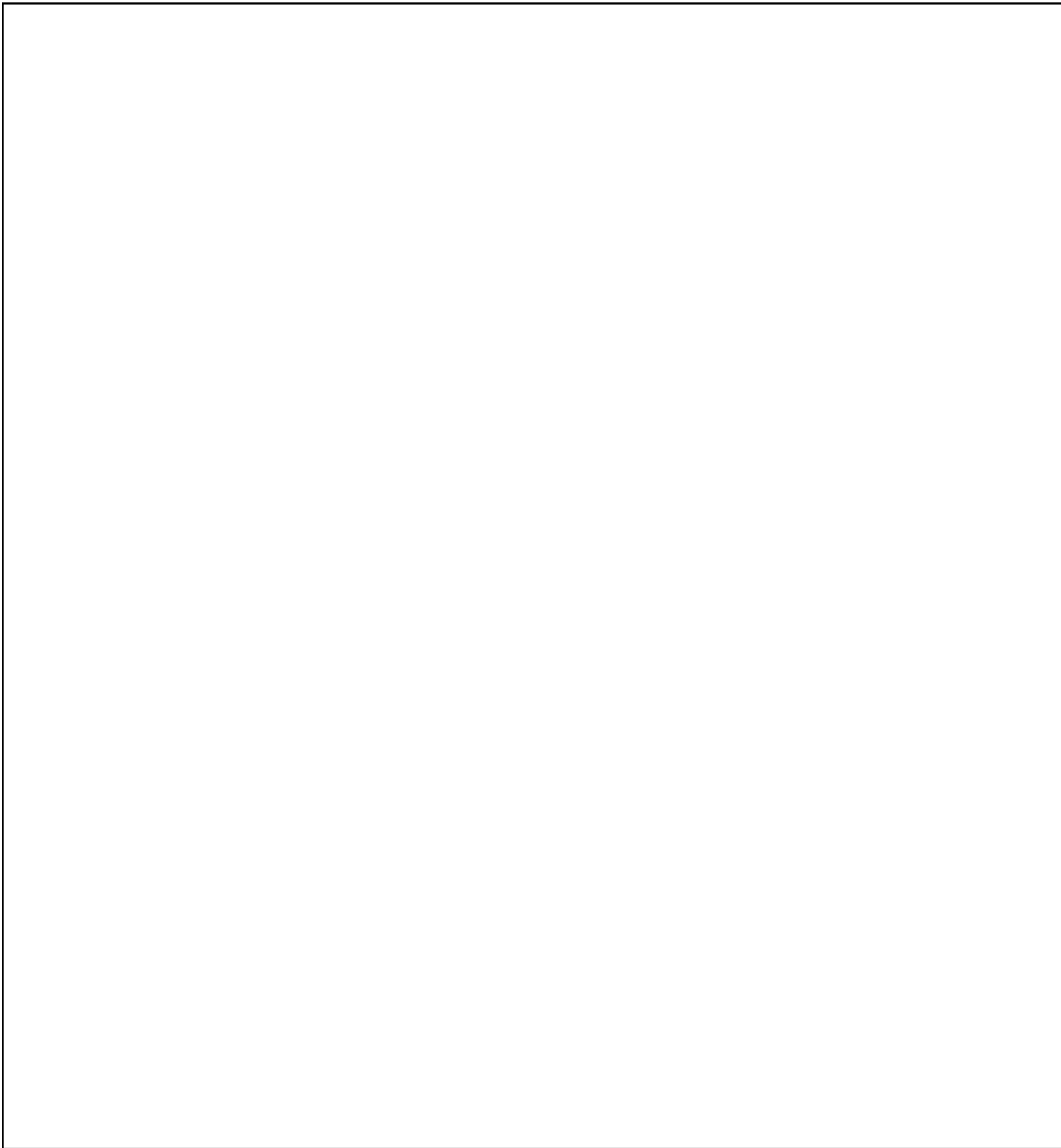
(b) (1)
(b) (3)-18 USC 798
(b) (3)-50 USC 3024(i)
(b) (3)-P.L. 86-36



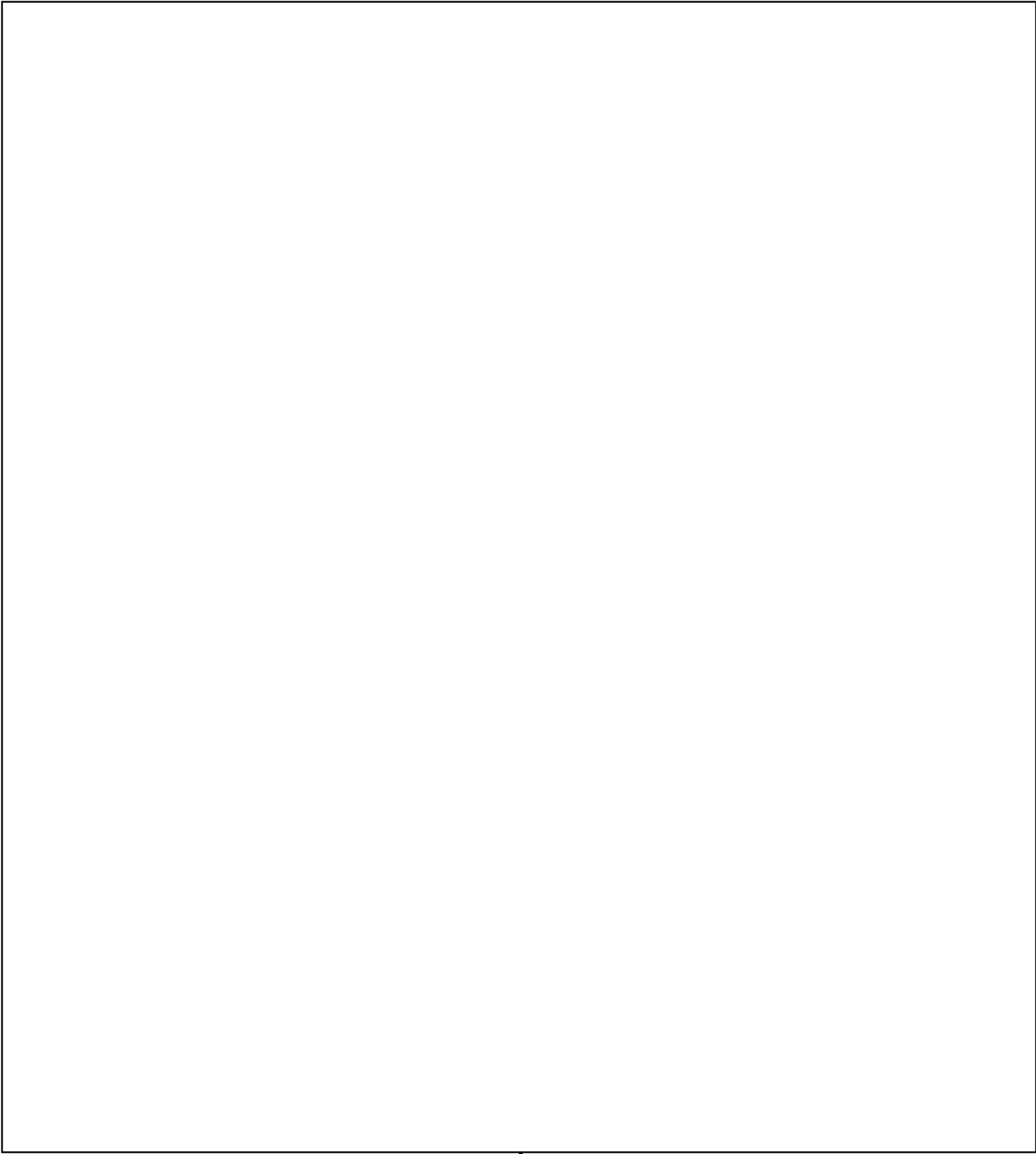
(b) (1)
(b) (3)-18 USC 798
(b) (3)-50 USC 3024(i)
(b) (3)-P.L. 86-36



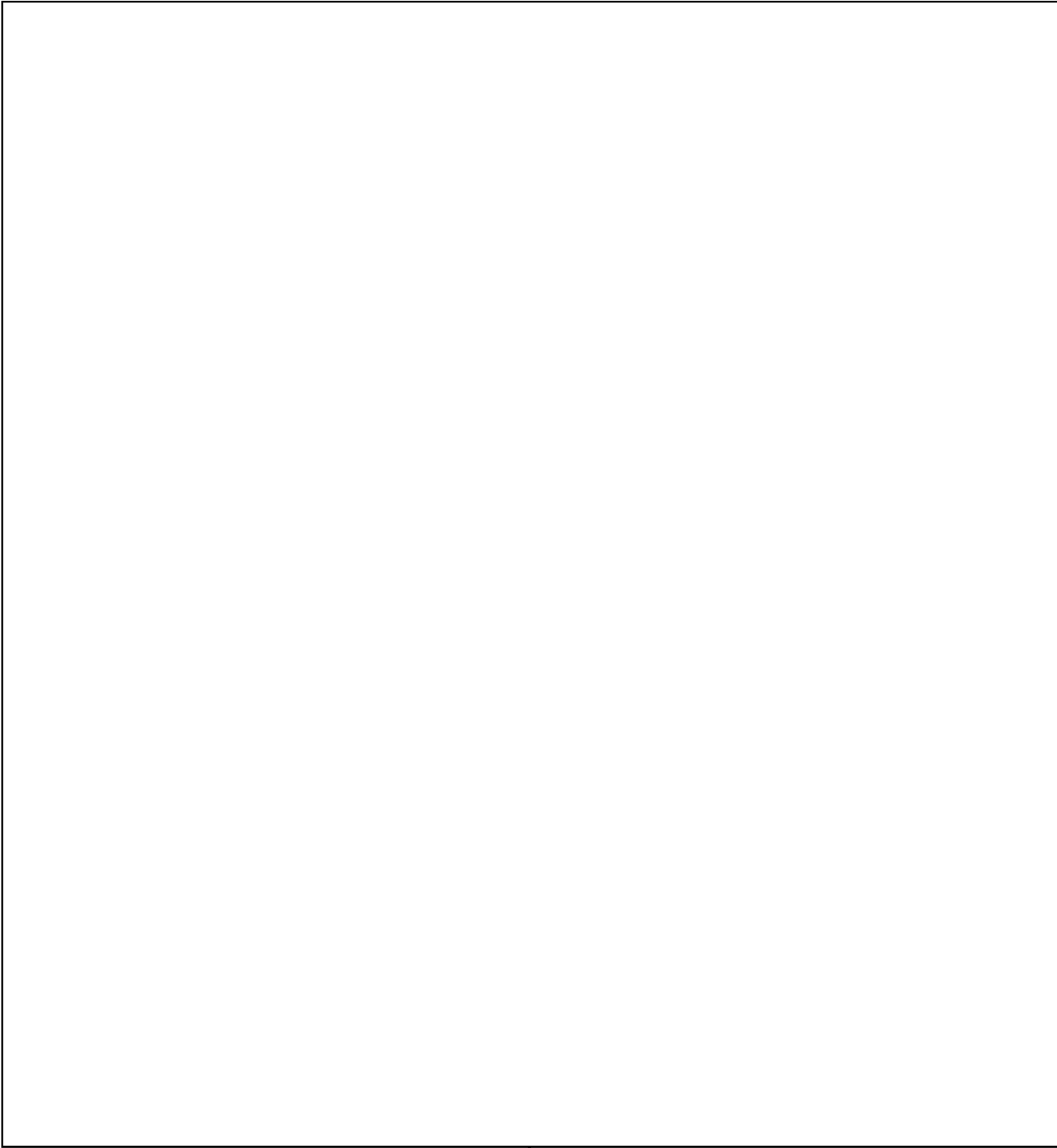
(b) (1)
(b) (3) -18 USC 798
(b) (3) -50 USC 3024 (i)
(b) (3) -P.L. 86-36



(b) (1)
(b) (3)-18 USC 798
(b) (3)-50 USC 3024(i)
(b) (3)-P.L. 86-36



(b) (1)
(b) (3)-18 USC 798
(b) (3)-50 USC 3024(i)
(b) (3)-P.L. 86-36



(b) (1)
(b) (3) -18 USC 798
(b) (3) -50 USC 3024 (i)
(b) (3) -P.L. 86-36

28. Further remarks on ciphertext autokey systems.—a. All of the discussion on ciphertext autokey systems thus far has been limited to alphabetical systems employing sliding primary components (or the equivalent form of a square table). There is no reason, of course, why a set of 26 unrelated random sequences in a table such as that in Fig. 33, below, could not be used for the cipher alphabets. In such

		Plain																									
		A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Key	A	T	O	K	Z	B	L	R	X	S	P	W	N	A	Q	C	E	I	G	D	J	F	V	U	Y	M	H
	B	S	B	A	C	D	E	H	F	I	J	K	T	L	M	O	U	V	Y	G	Z	N	P	Q	X	R	W
	C	Y	Q	R	T	V	W	L	A	D	K	O	M	J	U	B	G	E	P	H	S	C	Z	I	N	X	F
	D	Z	S	A	E	D	C	B	I	F	G	J	H	L	K	M	R	U	O	Q	V	P	T	N	W	Y	X
	E	S	L	W	E	M	Z	V	X	G	A	F	N	Q	U	K	D	O	P	I	T	J	B	R	H	C	Y
	F	G	P	O	C	I	X	L	U	R	N	D	Y	Z	H	W	B	J	S	Q	F	K	V	M	E	T	A
	G	W	A	H	X	J	E	Z	B	N	I	K	P	V	R	O	G	S	Y	D	U	L	C	F	M	Q	T
	H	G	T	D	X	A	I	H	P	J	O	B	W	K	C	V	F	Z	L	Q	E	R	Y	N	S	U	M
	I	A	J	D	S	K	Q	O	I	V	T	Z	E	F	H	G	Y	U	N	L	P	M	B	X	W	C	R
	J	J	G	H	O	N	M	T	P	R	Q	S	V	Z	U	X	Y	W	I	C	A	K	E	L	B	D	F
	K	V	Q	P	N	O	H	U	W	D	I	Z	Y	C	G	K	R	F	B	E	J	A	L	T	M	S	X
	L	E	W	O	A	M	N	F	L	H	Q	G	C	U	J	T	B	Y	P	Z	K	X	I	S	R	D	V
	M	D	H	B	M	K	G	X	U	Z	T	S	W	Q	Y	V	O	R	P	F	E	A	N	C	J	I	L
	N	D	W	P	K	J	V	I	U	Q	H	Z	C	T	X	B	L	E	G	N	Y	R	S	M	F	A	O
	O	S	G	U	E	N	T	C	X	O	W	F	Q	D	R	L	J	Z	M	A	P	B	V	H	I	Y	K
	P	X	C	S	H	D	E	O	K	F	P	Y	A	Q	J	N	U	B	T	G	I	M	W	Z	R	V	L
	Q	N	V	A	R	M	Y	O	F	T	H	E	U	S	Z	J	X	D	P	C	W	G	Q	I	B	K	L
	R	O	Z	P	L	G	V	J	R	K	Y	T	F	U	I	W	X	H	A	S	D	M	C	N	E	Q	B
	S	T	O	J	Y	L	F	X	N	G	W	H	V	C	M	I	R	B	S	E	K	U	P	D	Z	Q	A
	T	Z	X	Q	L	Y	I	O	V	B	P	E	S	N	H	J	W	M	D	G	F	C	K	A	U	T	R
	U	E	Y	B	F	S	J	M	U	D	Q	C	L	Z	W	T	I	P	A	V	N	K	H	R	G	O	X
	V	X	P	U	C	O	T	Y	A	W	V	S	F	D	L	I	E	B	H	K	N	R	J	Q	Z	G	M
	W	E	V	D	T	U	F	O	Y	H	M	L	S	I	Q	N	J	C	P	G	B	Z	A	X	K	W	R
	X	M	V	K	B	Q	W	U	G	L	O	S	T	E	C	H	N	Z	F	R	I	D	A	Y	J	P	X
	Y	W	J	L	V	G	R	C	Q	M	P	S	O	E	X	T	K	I	A	Z	D	N	B	U	H	Y	F
	Z	T	B	R	E	M	X	Z	P	V	Q	Y	U	O	G	A	I	K	L	F	S	W	H	D	C	N	J

FIGURE 33

cases, the general methods treated in par. 22 still apply, with necessary modifications, as also do the methods in pars. 23 and 24, except that it is obvious that (a) there will be no determinable base letter, and (b) there will be no causal isomorphs. For that matter, even with a matrix such as that of Fig. 34 below, in which the key letters are designated by *arbitrary* letters to the left of the square (instead of

		Plain																									
		H	Y	D	R	A	U	L	I	C	B	E	F	G	J	K	M	N	O	P	Q	S	T	V	W	X	Z
Key	A	H	Y	D	R	A	U	L	I	C	B	E	F	G	J	K	M	N	O	P	Q	S	T	V	W	X	Z
	B	Y	D	R	A	U	L	I	C	B	E	F	G	J	K	M	N	O	P	Q	S	T	V	W	X	Z	H
	C	D	R	A	U	L	I	C	B	E	F	G	J	K	M	N	O	P	Q	S	T	V	W	X	Z	H	Y
	D	R	A	U	L	I	C	B	E	F	G	J	K	M	N	O	P	Q	S	T	V	W	X	Z	H	Y	D
	E	A	U	L	I	C	B	E	F	G	J	K	M	N	O	P	Q	S	T	V	W	X	Z	H	Y	D	R
	F	U	L	I	C	B	E	F	G	J	K	M	N	O	P	Q	S	T	V	W	X	Z	H	Y	D	R	A
	G	L	I	C	B	E	F	G	J	K	M	N	O	P	Q	S	T	V	W	X	Z	H	Y	D	R	A	U
	H	I	C	B	E	F	G	J	K	M	N	O	P	Q	S	T	V	W	X	Z	H	Y	D	R	A	U	L
	I	C	B	E	F	G	J	K	M	N	O	P	Q	S	T	V	W	X	Z	H	Y	D	R	A	U	L	I
	J	B	E	F	G	J	K	M	N	O	P	Q	S	T	V	W	X	Z	H	Y	D	R	A	U	L	I	C
	K	E	F	G	J	K	M	N	O	P	Q	S	T	V	W	X	Z	H	Y	D	R	A	U	L	I	C	B
	L	F	G	J	K	M	N	O	P	Q	S	T	V	W	X	Z	H	Y	D	R	A	U	L	I	C	B	E
	M	G	J	K	M	N	O	P	Q	S	T	V	W	X	Z	H	Y	D	R	A	U	L	I	C	B	E	F
	N	J	K	M	N	O	P	Q	S	T	V	W	X	Z	H	Y	D	R	A	U	L	I	C	B	E	F	G
	O	K	M	N	O	P	Q	S	T	V	W	X	Z	H	Y	D	R	A	U	L	I	C	B	E	F	G	J
	P	M	N	O	P	Q	S	T	V	W	X	Z	H	Y	D	R	A	U	L	I	C	B	E	F	G	J	K
	Q	N	O	P	Q	S	T	V	W	X	Z	H	Y	D	R	A	U	L	I	C	B	E	F	G	J	K	M
	R	O	P	Q	S	T	V	W	X	Z	H	Y	D	R	A	U	L	I	C	B	E	F	G	J	K	M	N
	S	P	Q	S	T	V	W	X	Z	H	Y	D	R	A	U	L	I	C	B	E	F	G	J	K	M	N	O
	T	Q	S	T	V	W	X	Z	H	Y	D	R	A	U	L	I	C	B	E	F	G	J	K	M	N	O	P
	U	S	T	V	W	X	Z	H	Y	D	R	A	U	L	I	C	B	E	F	G	J	K	M	N	O	P	Q
	V	T	V	W	X	Z	H	Y	D	R	A	U	L	I	C	B	E	F	G	J	K	M	N	O	P	Q	S
	W	V	W	X	Z	H	Y	D	R	A	U	L	I	C	B	E	F	G	J	K	M	N	O	P	Q	S	T
	X	W	X	Z	H	Y	D	R	A	U	L	I	C	B	E	F	G	J	K	M	N	O	P	Q	S	T	V
	Y	X	Z	H	Y	D	R	A	U	L	I	C	B	E	F	G	J	K	M	N	O	P	Q	S	T	V	W
	Z	Z	H	Y	D	R	A	U	L	I	C	B	E	F	G	J	K	M	N	O	P	Q	S	T	V	W	X

FIGURE 34

the letters in a column under a particular plaintext letter—the base letter), there is likewise no determinable base letter and no causal isomorphs can be produced, as can be shown by the following isologous message beginnings:

Message "A"

K: X P M Q Q P P Z F G T R I R Z N D P Q L J Y M L L H X Q W G
P: T H I R D R E G I M E N T C O M M A N D P O S T M O V I N G . . .
C: P M Q Q P P Z F G T R I R Z N D P Q L J Y M L L H X Q W G P

Message "B"

K: Y Q N S T T V U L P A E S J O U B N O A D T E X P A O E F T
P: T H I R D R E G I M E N T C O M M A N D P O S T M O V I N G . . .
C: Q N S T T V U L P A E S J O U B N O A D T E X P A O E F T U

The ciphertext doublets are the result of chance. Note in this example that, since the plain and cipher components are identical sequences, one of the distributions of the letters immediately following a particular cipher letter (in this case, A_c) will fit the normal, since the plaintext letters enciphered by this key letter will be self-enciphered; the distributions of the letters following the other cipher letters will of course be monoalphabetic.

b. The general principles of ciphertext autokeying apply equally well to digital systems, and for that matter to Baudot systems. The modulus in digital systems is the usual mod-10 arithmetic,²⁶ so that in effect the cipher component is a *known* sequence—thus a reduction to monoalphabetic terms suggests itself at once, if not sooner.

c. As an example, let us study the following message, suspected of having been enciphered in a ciphertext autokey system with the additive method of encipherment ($P+K=C$).²⁷

```

1 5 6 3 5 9 2 0 0 1 1 3 7 5 6 9 4 0 9 3 0 5 1 5 1 4 0 0 9 4
2 2 1 2 3 3 0 4 7 6 6 9 7 2 0 3 9 4 9 8 7 9 9 2 9 5 8 1 1 2
7 6 1 1 1 4 9 3 6 9 2 8 0 7 2 4 8 3 0 1 9 0 0 7 4 4 5 5 4 8
4 0 5 4 4 3 1 5 8 9 1 2 9 4 3 5 0 5 2 9 5 2 8 1 4 7 4 5 1 6
7 1 9 3 2 4 0 5 0 6 1 1 6 8 2 0 5 7 9 3 1 0 6 4 9 2 5 6 9 5
1 9 6 8 9 9 9 6 6 1

```

If a single-digit introductory key has been used, the cipher text is offset against itself at an interval of 1 and a decipherment obtained, the beginning of which is shown below:²⁸

```

K:  1 5 6 3 5 9 2 0 0 1 1 3 7 5 6 9 4 0 9 3 0 5 1 5
C: 1 5 6 3 5 9 2 0 0 1 1 3 7 5 6 9 4 0 9 3 0 5 1 5 1 . . .
P:  4 1 7 2 4 3 8 0 1 0 2 4 8 1 3 5 6 9 4 7 5 6 4 6

```

The I.C. of the entire deciphered message is 0.99, so the length of the introductory key was probably not 1. The cipher text is then offset against itself at intervals of 2, 3, 4 . . . , up to an interval of 9: the I.C.'s obtained from the resulting decipherments are all unsatisfactory, as may be seen from the following table:

Offset	I.C.	Offset	I.C.	Offset	I.C.
1	0.99	4	0.97	7	0.99
2	1.02	5	0.96	8	0.98
3	1.02	6	0.96	9	0.97

²⁶ If other than mod-10 arithmetic is used, say an arbitrary conversion-square encipherment with a square such as the following,

		Plain									
		0	1	2	3	4	5	6	7	8	9
Key	0	3	1	6	7	5	8	2	4	9	0
	1	1	2	3	5	4	6	8	9	0	7
	2	6	4	0	2	8	1	5	3	7	9
	3	7	3	2	9	0	5	6	1	8	4
	4	5	8	4	0	9	2	3	7	1	6
	5	8	5	1	6	7	9	0	2	4	3
	6	2	9	8	1	3	7	4	0	6	5
	7	4	6	9	8	2	0	7	5	3	1
	8	9	0	7	3	6	4	1	8	5	2
	9	0	7	5	4	1	3	9	6	2	8

the problem must be solved as a general case of ciphertext autokey as treated earlier in this chapter. (The conversion square shown here is a *Latin square*, with ten unique digits in each of the rows and in each of the columns; other conversion squares may have columns containing repeated digits.)

²⁷ As regards the effect of the use of different encipherment conventions, see subpars. 35g and h (on pp. 117-120).

²⁸ We have assumed that the enciphering procedure was the *additive* method (i.e., wherein $P+K=C$); see also the remarks in subpar. 35h in the next chapter if subtractive or minuend methods had been involved.

(b) (1)
(b) (3) -18 USC 798
(b) (3) -50 USC 3024 (i)
(b) (3) -P.L. 86-36

CHAPTER V

PLAINTEXT AUTOKEY SYSTEMS

	Paragraph
Preliminary remarks on plaintext autokeying.....	29
Solution of plaintext autokey systems when known cipher alphabets are employed and the introductory key consists of a single letter.....	30
Solution of plaintext autokey systems involving known cipher alphabets when the introductory key consists of several letters.....	31
Analysis of a case involving unknown components.....	32
<div style="border: 1px solid black; width: 450px; height: 15px; display: inline-block;"></div>	33
Analysis of digital plaintext autokey systems.....	34
Concluding remarks on autokey systems.....	35

29. Preliminary remarks on plaintext autokeying.—*a.* If the cipher alphabets are unknown mixed sequences, plaintext autokeying gives rise to cryptograms of more intricate character than does ciphertext autokeying, as has already been intimated in the preceding chapter. As a cryptographic principle, it is very commonly encountered as a new and remarkable “invention” of tyros in the cryptographic art. It apparently gives rise to the type of reasoning to which attention has been directed once before, and which was then shown to be a popular delusion of the uninitiated. The novice to whom the plaintext autokey principle comes as a brilliant flash of the imagination sees only the apparent impossibility of penetrating a secret which enfolds another secret. His reasoning runs about as follows: “In order to read the cryptogram, the would-be solver must, of course, first know the key; but the key does not become known to the would-be solver until he has read the cryptogram and has thus found the plain text. Since this is reasoning around a circle, the system is indecipherable.” How unwarranted such reasoning really is in this case, and how readily the problem is solved, will soon be demonstrated.

b. A consideration of the mechanics of the plaintext autokey method discloses that a repetition of n letters in the plain text will produce a repetition of $(n-k)$ letters in the cipher text, where n represents the length of the repetition and k the length of the introductory key. Therefore, when the introductory key consists of a single letter, there will be as many polygraphic repetitions in the cipher text as there are in the plain text, except for repetitions of digraphs only, which of course disappear. But on the other hand some accidental (i.e., noncausal) digraphic repetitions are to be expected, since it can happen that two different plaintext pairs, enciphered by different key letters, will produce identical cipher equivalents. Such accidental repetitions will happen less frequently, of course, in the case of longer polygraphs, so that when repetitions of four or more letters are found in the cipher text they may be taken to be true or causal repetitions. It is obvious that in studying repetitions in a cryptogram of this type, when the introductory key is a single letter, a 5-letter repetition in the cipher text, for example, represents a 6-letter word or sequence repeated in the plain text. When the introductory key is k letters in length then an n -letter repetition represents a repetition in the plain text of length $(n+k)$ letters.

c. The discussion in this chapter will, as usual, be divided into two principal cases: (1) those in which the cipher alphabets are known, and (2) those in which they are unknown. Under each case the introductory key may consist of a single letter, a word, or a short phrase. Furthermore, in the solution of plaintext autokey systems there are important differences whether the components are identical sequences progressing in the same direction, or running against each other in opposite directions, or whether the components are two different sequences. In addition, complications in solution are introduced when the wrong base letter is assumed, as will presently be demonstrated.

30. Solution of plaintext autokey systems when known cipher alphabets are employed and the introductory key consists of a single letter.—*a.* Note the following plaintext autokeyed encipherment, wherein the introductory key is a single letter, of such commonly encountered words as COMMANDING,

BATTALION, DIVISION, and CAPTAIN, using two identical primary components (in this case direct standard alphabets), with base letter A:

K: . B A T T A L I O N
(1) P: B A T T A L I O N .
C: . B T M T L T W B .

K: . D I V I S I O N
(2) P: D I V I S I O N .
C: . L D D A A W B .

K: . C O M M A N D I N G
(3) P: C O M M A N D I N G .
C: . Q A Y M N Q L V T .

K: . C A P T A I N
(4) P: C A P T A I N .
C: . C P I T I V .

The following characteristics may be noted:¹

(1) The cipher equivalent of A_p is the plaintext letter which immediately precedes A_p (see the two A's in BATTALION, in example 1 above). When the key is A, a plaintext letter is self-enciphered (see the first T_c and the L_c in example 1).

(2) A plaintext sequence of the pattern ABA yields a doublet as the cipher equivalent of the final two letters (see IVI and ISI in DIVISION, in the second example).

(3) Every plaintext trigraph having A_p as its central letter yields a cipher equivalent the last two letters of which are identical with the initial and final letters of the plaintext trigraph (see MAN in COMMANDING, in the third example).

(4) Every plaintext tetragraph having A_p as the initial and the final letter yields a cipher equivalent the second and fourth letters of which are identical with the second and third letters of the plaintext tetragraph (see APTA in CAPTAIN, in the fourth example; also ATTA in BATTALION, in the first example).

b. (1) From the foregoing characteristics and the fact that a repetition of a sequence of n plaintext letters will yield, in the case of a one-letter introductory key, a repetition of a sequence of $n-1$ cipher letters, it is obvious that an easy method of solving this type of cipher is that of the probable word. Indeed, if the system were used for regular traffic it would not be long before the solution would consist merely in referring to lists of cipher equivalents of commonly used words (as found from previous messages) and searching through the traffic for these sequences, aided by their idiomorphic patterns.

(2) Note how easily the following message can be solved:

B E C J I B T M T L T W B P Q A Y M N Q H V N E T W A A L C . . .

We take note of the sequence BTMTLTWB, which is in the list of equivalents in subpar. a, above, and we insert the word BATTALION in the proper position. Thus:

K: B A T T A L I O N
C: B E C J I B T M T L T W B P Q . . .
P: B A T T A L I O N

With this as a start, the decipherment may proceed forward or backward with ease, as shown below:

 5 10 15 20 25 30
K: E A C H B A T T A L I O N C O M M A N D E R W I L L P L A
C: B E C J I B T M T L T W B P Q A Y M N Q H V N E T W A A L C . . .
P: E A C H B A T T A L I O N C O M M A N D E R W I L L P L A C

c. The foregoing example is based upon the normal Vigenère method of encipherment ($\theta_{k/2}=\theta_{1/1}$; $\theta_{p/1}=\theta_{c/2}$). If in encipherment the plaintext letter is sought in the second (i.e., lower) component, and its equivalent taken in the first (i.e., upper) component ($\theta_{k/2}=\theta_{1/1}$; $\theta_{p/2}=\theta_{c/1}$), the steps in solution are identical, except that the list of cipher equivalents of probable words must be modified accordingly.

¹ The reader is cautioned that the characteristics noted apply only to the case where two identical components are used, with the base letter A.

For instance if the components are direct standard sequences the word BATTALION will now be enciphered as BATTALION.

ZTAHLXGZ

d. If reversed standard alphabets are used, the word BATTALION will be enciphered as BATTALION
BHATPDUB

which also presents idiomorphic characteristics leading to the easy recognition of the word in the cipher texts of messages.

e. All of the foregoing phenomena are based upon standard alphabets, but when mixed cipher alphabets are used and these have been reconstructed, similar observations may be recorded and the results employed in the solution of additional messages enciphered by the same components.

f. (1) Let us again consider the case of known components wherein two identical sequences progress in the same direction; for the sake of illustration, let both of these sequences be normal sequences. Let it also be known that plaintext autokey with a single-letter introductory key is involved, and that the enciphering equations are those of the normal Vigenère method.

(2) A message beginning QVGLB TPJTF . . . is intercepted; the only unknown factor is the initial key letter. Of course, one could try to decipher the message using each key letter in turn, beginning with A and continuing until the correct key letter is tried, whereupon plain text will be obtained. But it seems logical to think that all 26 possible "decipherments" might be derived from the first one, so that the process might be much simplified; this is true, as will now be shown. If we take the two cipher groups under consideration and decipher them with initial key letter A, we obtain the following:

K: A Q F B K R C N W X
C: Q V G L B T P J T F . . .
P: Q F B K R C N W X I

The deciphered text is certainly not plain text. But if one completes the sequences initiated by these letters, using the direct standard sequence for the even columns, the reversed standard for the odd columns, the plain text HOSTILE FOR(CE) will appear in one generatrix. From this it is clear that instead of going through the labor of making 26 successive trials, which would consume considerable time, all that is necessary is to have a set of strips bearing the normal direct sequence and another set bearing the reversed normal sequence, and to align the strips, alternatively direct and reversed, to the first "decipherment." The plain text will now reappear on one generatrix of the completion diagram, as shown in Fig. 35, below:

Initial	1	2	3	4	5	6	7	8	9	10
key ltr.	<u>Q</u>	<u>V</u>	<u>G</u>	<u>L</u>	<u>B</u>	<u>T</u>	<u>P</u>	<u>J</u>	<u>T</u>	<u>F</u>
A	Q	F	B	K	R	C	N	W	X	I
B	P	G	A	L	Q	D	M	X	W	J
C	O	H	Z	M	P	E	L	Y	V	K
D	N	I	Y	N	O	F	K	Z	U	L
E	M	J	X	O	N	G	J	A	T	M
F	L	K	W	P	M	H	I	B	S	N
G	K	L	V	Q	L	I	H	C	R	O
H	J	M	U	R	K	J	G	D	Q	P
I	I	N	T	S	J	K	F	E	P	Q
J	*H	O	S	T	I	L	E	F	O	R
K	G	P	R	U	H	M	D	G	N	S
L	F	Q	Q	V	G	N	C	H	M	T
M	E	R	P	W	F	O	B	I	L	U
N	D	S	O	X	E	P	A	J	K	V
O	C	T	N	Y	D	Q	Z	K	J	W
P	B	U	M	Z	C	R	Y	L	I	X
Q	A	V	L	A	B	S	X	M	H	Y
R	Z	W	K	B	A	T	W	N	G	Z
S	Y	X	J	C	Z	U	V	O	F	A
T	X	Y	I	D	Y	V	U	P	E	B
U	W	Z	H	E	X	W	T	Q	D	C
V	V	A	G	F	W	X	S	R	C	D
W	U	B	F	G	V	Y	R	S	B	E
X	T	C	E	H	U	Z	Q	T	A	F
Y	S	D	D	I	T	A	P	U	Z	G
Z	R	E	C	J	S	B	O	V	Y	H

FIGURE 35

g. The peculiar nature of the phenomenon just observed, viz., a completion diagram with the vertical sequences in adjacent columns progressing in opposite directions, those in alternate columns in the same direction, calls for an explanation. Although the matter might seem a bit mysterious, it is not hard to understand. First, it is clear why the letters in column 1 of Fig. 35 form the descending sequence QPO . . . these letters are merely the ones resulting from the successive "decipherment" of Q_c by the successive key letters A, B, C . . . , as shown below:

Initial key A:	Initial key B:	Initial key C:
K: A Q F B K R C N W X	K: B P G A L Q D M X W	K: C O H Z M P L E Y V
C: <u>Q V G L B T P J T F</u>	C: <u>Q V G L B T P J T F</u>	C: <u>Q V G L B T P J T F</u>
P: Q F B K R C N W X I	P: P G A L Q D M X W J	P: O H Z M P E L Y V K

Now since the decipherment obtained from the 1st cipher letter in any row in Fig. 35 becomes the key letter for deciphering the 2d cipher letter in the same row, it is apparent that as the letters in the 1st column progress in a reversed normal (i.e., descending) order, the letters in the 2d column must progress in a direct normal (i.e., ascending) order. The matter may perhaps become more clear if encipherment

When we make our initial "decipherments" of the foregoing cipher texts, assuming erroneously that the base letter is A, we have the following:

K: A P F A K Q C M W W
C: P U F K A S O I S E
P: P F A K Q C M W W I

FIGURE 37a

K: A O F Z K P C L W V
C: O T E J Z R N H R D
P: O F Z K P C L W V I

FIGURE 37b

K: A N F Y K O C K W U
C: N S D I Y Q M G Q C
P: N F Y K O C K W U I

FIGURE 37c

Note that the even letters FK CWI of these three decipherments match. When we make generatrix diagrams from these decipherments, it may be seen in Figs. 38a-c, below, that the true plain text appears on two generatrices, and that the interval between these generatrices reflects the identity of the particular base letter involved. This phenomenon holds true only for those cases in which the plain and cipher components are identical sequences running in the same direction.

P U F K A S O I S E
P F A K Q C M W W I
Q E B J R B N V X H
R D C I S A O U Y G
S C D H T Z P T Z F
T B E G U Y Q S A E
U A F F V X R R B D
V Z G E W W S Q C C
W Y H D X V T P D B
X X I C Y U U O E A
Y W J B Z T V N F Z
Z V K A A S W M G Y
A U L Z B R X L H X
B T M Y C Q Y K I W
C S N X D P Z J J V
D R O W E O A I K U
E Q P V F N B H L T
F P Q U G M C G M S
G[ⓐ]R[ⓑ]H[Ⓒ]L[Ⓓ]D[Ⓔ]N[ⓓ]
H[ⓔ]N[ⓕ]S[ⓖ]I[ⓗ]K[ⓙ]E[ⓓ]Q[ⓔ]
I M T R J J F D P P
J L U Q K I G C Q O
K K V P L H H B R N
L J W O M G I A S M
M I X N N F J Z T L
N H Y M O E K Y U K
O G Z L P D L X V J

FIGURE 38a

O T E J Z R N H R D
O F Z K P C L W V I
P E A J Q B M V W H
Q D B I R A N U X G
R C C H S Z O T Y F
S B D G T Y P S Z E
T A E F U X Q R A D
U Z F E V W R Q B C
V Y G D W V S P C B
W X H C X U T O D A
X W I B Y T U N E Z
Y V J A Z S V M F Y
Z U K Z A R W L G X
A T L Y B Q X K H W
B S M X C P Y J I V
C R N W D O Z I J U
D Q O V E N A H K T
E P P U F M B G L S
F[ⓐ]Q[ⓑ]T[Ⓒ]G[Ⓓ]L[Ⓔ]C[ⓓ]F[ⓔ]M[ⓕ]
G[ⓖ]N[ⓗ]R[ⓙ]S[ⓓ]H[ⓔ]K[ⓕ]D[ⓖ]E[ⓗ]N[ⓙ]Q[ⓓ]
H[ⓔ]M[ⓕ]S[ⓖ]R[ⓙ]I[ⓗ]J[ⓙ]E[ⓓ]D[ⓔ]P[ⓕ]
I L T Q J I F C P O
J K U P K H G B Q N
K J V O L G H A R M
L I W N M F I Z S L
M H X M N E J Y T K
N G Y L O D K X U J

FIGURE 38b

N S D I Y Q M G Q C
N F Y K O C K W U I
O E Z J P B L V V H
P D A I Q A M U W G
Q C B H R Z N T X F
R B C G S Y O S Y E
S A D F T X P R Z D
T Z E E U W Q Q A C
U Y F D V V R P B B
V X G C W U S O C A
W W H B X T T N D Z
X V I A Y S U M E Y
Y U J Z Z R V L F X
Z T K Y A Q W K G W
A S L X B P X J H V
B R M W C O Y I I U
C Q N V D N Z H J T
D P O U E M A G K S
E[ⓐ]P[ⓑ]T[Ⓒ]F[Ⓓ]L[Ⓔ]B[ⓓ]F[ⓔ]L[ⓕ]
F[ⓖ]N[ⓗ]Q[ⓙ]S[ⓓ]G[ⓔ]K[ⓕ]C[ⓖ]E[ⓗ]M[ⓙ]Q[ⓓ]
G[ⓔ]M[ⓕ]R[ⓙ]R[ⓙ]H[ⓙ]J[ⓙ]D[ⓔ]N[ⓕ]P[ⓕ]
H[ⓔ]L[ⓕ]S[ⓖ]Q[ⓙ]I[ⓗ]E[ⓓ]C[ⓔ]O[ⓕ]
I K T P J H F B P N
J J U O K G G A Q M
K I V N L F H Z R L
L H W M M E I Y S K
M G X L N D J X T J

FIGURE 38c

i. When the method of encipherment based upon enciphering equations $\theta_{k/2} = \theta_{1/1}$; $\theta_{p/2} = \theta_{c/1}$ is used instead of that based upon the usual Vigenère equations, the process indicated above is simplified by the fact that no alteration in the direction of the sequences in the completion diagram is required. For example, if the first two groups of a cipher message were YHEBP DTBJD the "decipherments" with key letters A and B, respectively, are shown below:

K: A Y F J K Z C V W F
C: Y H E B P D T B J D
P: Y F J K Z C V W F I

K: B Z G K L A D W X G
C: Y H E B P D T B J D . . .
P: Z G K L A D W X G J

The entire completion diagram would therefore be as follows:

Initial	1	2	3	4	5	6	7	8	9	10
key ltr.	Y	H	E	B	P	D	T	B	J	D
A	Y	F	J	K	Z	C	V	W	F	I
B	Z	G	K	L	A	D	W	X	G	J
C	A	H	L	M	B	E	X	Y	H	K
D	B	I	M	N	C	F	Y	Z	I	L
E	C	J	N	O	D	G	Z	A	J	M
F	D	K	O	P	E	H	A	B	K	N
G	E	L	P	Q	F	I	B	C	L	O
H	F	M	Q	R	G	J	C	D	M	P
I	G	N	R	S	H	K	D	E	N	Q
J	*H	O	S	T	I	L	E	F	O	R
K	I	P	T	U	J	M	F	G	P	S
L	J	Q	U	V	K	N	G	H	Q	T
M	K	R	V	W	L	O	H	I	R	U
N	L	S	W	X	M	P	I	J	S	V
O	M	T	X	Y	N	Q	J	K	T	W
P	N	U	Y	Z	O	R	K	L	U	X
Q	O	V	Z	A	P	S	L	M	V	Y
R	P	W	A	B	Q	T	M	N	W	Z
S	Q	X	B	C	R	U	N	O	X	A
T	R	Y	C	D	S	V	O	P	Y	B
U	S	Z	D	E	T	W	P	Q	Z	C
V	T	A	E	F	U	X	Q	R	A	D
W	U	B	F	G	V	Y	R	S	B	E
X	V	C	G	H	W	Z	S	T	C	F
Y	W	D	H	I	X	A	T	U	D	G
Z	X	E	I	J	Y	B	U	V	E	H

FIGURE 39

j. (1) In the foregoing examples the primary components were normal sequences, but the case of identical mixed components may be handled in a similar manner. Note the following example, based upon

H Y D R A U L I C B E F G J K M N O P Q S T V W X Z

the primary component which we have reconstructed from previous work. Let the first two groups of an intercepted message be XOFMD JNTDS . . .

(2) First, the message is "deciphered" with the initial key letter A and base letter H_p, and then a completion diagram is made, using sliding strips bearing the mixed primary component, alternate strips bearing the same sequence in reverse. Note Fig. 40, in which the plain text HOSTILE FOR(CE) reappears on a single generatrix.

K: A S W K Y Y G A O F
 C: X O F M D J N T D S
 P: S W K Y Y G A O F B
 T V M H D F U N G C
 V T N Z R E L M J I
 W S O X A B I K K L
 X Q P W U C C J M U
 Z P Q V L I B G N A
 *H O S T I L E F O R
 Y N T S C U F E P D
 D M V Q B A G B Q Y
 R K W P E R J C S H
 A J X O F D K I T Z
 U G Z N G Y M L V X
 L F H M J H N U W W
 I E Y K K Z O A X V
 C B D J M X P R Z T
 B C R G N W Q D H S
 E I A F O V S Y Y Q
 F L U E P T T H D P
 G U L B Q S V Z R O
 J A I C S Q W X A N
 K R C I T P X W U M
 M D B L V O Z V L K
 N Y E U W N H T I J
 O H F A X M Y S C G
 P Z G R Z K D Q B F
 Q X J D H J R P E E

FIGURE 40

K: A D K O P E H A B K
 C: X T W Z L X H Z R X
 P: D K O P E H A B K N
 E L P Q F I B C L O
 F M Q R G J C D M P
 G N R S H K D E N Q
 *H O S T I L E F O R
 I P T U J M F G P S
 J Q U V K N G H Q T
 K R V W L O H I R U
 L S W X M P I J S V
 M T X Y N Q J K T W
 N U Y Z O R K L U X
 O V Z A P S L M V Y
 P W A B Q T M N W Z
 Q X B C R U N O X A
 R Y C D S V O P Y B
 S Z D E T W P Q Z C
 T A E F U X Q R A D
 U B F G V Y R S B E
 V C G H W Z S T C F
 W D H I X A T U D G
 X E I J Y B U V E H
 Y F J K Z C V W F I
 Z G K L A D W X G J
 A H L M B E X Y H K
 B I M N C F Y Z I L
 C J N O D G Z A J M

FIGURE 41

K: A L W H Y J G N O W
 C: X B W Z K Y V Z S K
 P: L W H Y J G N O W B
 I X Y D K J O P X E
 C Z D R M K P Q Z F
 B H R A N M Q S H G
 E Y A U O N S T Y J
 F D U L P O T V D K
 G R L I Q P V W R M
 J A I C S Q W X A N
 K U C B T S X Z U O
 M L B E V T Z H L P
 N I E F W V H Y I Q
 O C F G X W Y D C S
 P B G J Z X D R B T
 Q E J K H Z R A E V
 S F K M Y H A U F W
 T G M N D Y U L G X
 V J N O R D L I J Z
 W K O P A R I C K H
 X M P Q U A C B M Y
 Z N Q S L U B E N D
 *H O S T I L E F O R
 Y P T V C I F G P A
 D Q V W B C G J Q U
 R S W X E B J K S L
 A T X Z F E K M T I
 U V Z H G F M N V C

FIGURE 42

k. (1) Next to be considered is the case in which the two primary components progress in opposite directions. Let us assume that XTWZL XHZRX . . . are the first two groups of a message known to have been enciphered by plaintext autokeying with a single letter introductory key and reversed standard alphabets. The procedure in this case is exactly the same as before, except that it is not necessary to have any alternation in direction of the completion sequences; note the solution in Fig. 41. Let the student ascertain why the alternation of the completion sequences is not necessary in this case.

(2) In the foregoing case the alphabets were reversed standard, produced by the sliding of the normal sequence against its reverse. But the underlying principle of solution is the same even if a mixed sequence were used instead of the normal; so long as the sequence is known, the procedure to be followed is exactly the same as demonstrated in subpar. (1), above. For example, let the reconstructed primary components be

P: H Y D R A U L I C B E F G J K M N O P Q S T V W X Z
 C: Z X W V T S Q P O N M K J G F E B C I L U A R D Y H

and let the first two groups of an intercepted message be XBWZK YVZSK Referring to Fig. 42, we may note that the primary mixed sequence is used for the completion sequence and that the plain text, HOSTILE FOR(CE), comes out on one generatrix. It is immaterial whether the direct or reversed mixed component is used for the completion sequence, so long as all the sequences in the diagram progress in the same direction.

l. When the enciphering alphabets are identical sequences but running against each other in opposite directions, an incorrectly assumed base letter has an effect on the same manner of reading the generatrix diagrams. In Fig. 41, above, we assumed correctly that the base letter was A_p, and the plain text reappeared on a single generatrix. If, however, we had assumed the base letter to be B_p, our generatrix diagram would have been that of Fig. 43a, below; and if we had assumed a base letter of C_p, the generatrix diagram would have been that of Fig. 43b. Note that the plain text in Fig. 43a progresses upward on a simple diagonal, while that in Fig. 43b progresses upward on a steeper diagonal, two rows apart. The diagonal for an assumed base letter of D_p would have been three rows apart, and that for an assumed base letter of E_p would have been four rows apart, and so on: this shows that the angle of reading the diagonal, then, depends upon the distance between the true base letter from the assumed base letter, as measured on the component.

K: A E M R T J N H J T
 C: X T W Z L X H Z R X
 P: E M R ^(T) J N H J T X
 F N ^(S) U K O I K U Y
 G ^(O) T V L P J L V Z
^(H) P U W M Q K M W A
 I Q V X N R L N X B
 J R W Y O S M O Y C
 K S X Z P T N P Z D
 L T Y A Q U O Q A E
 M U Z B R V P R B F
 N V A C S W Q S C G
 O W B D T X R T D H
 P X C E U Y S U E I
 Q Y D F V Z T V F J
 R Z E G W A U W G K
 S A F H X B V X H L
 T B G I Y C W Y I M
 U C H J Z D X Z J N
 V D I K A E Y A K O
 W E J L B F Z B L P
 X F K M C G A C M Q
 Y G L N D H B D N ^(R)
 Z H M O E I C E ^(O) S
 A I N P F J D ^(F) P T
 B J O Q G K ^(E) G Q U
 C K P R H ^(L) F H R V
 D L Q S ^(I) M G I S W

FIGURE 43a

K: A F O U X O T O R C
 C: X T W Z L X H Z R X
 P: F ^(O) U X O T O R C H
 G P V Y P U P S D I
^(H) Q W Z Q V Q T E J
 I R X A R W R U F K
 J S Y B S X S V G L
 K T Z C T Y T W H M
 L U A D U Z U X I N
 M V B E V A V Y J O
 N W C F W B W Z K P
 O X D G X C X A L Q
 P Y E H Y D Y B M ^(R)
 Q Z F I Z E Z C N S
 R A G J A F A D ^(O) T
 S B H K B G B E P U
 T C I L C H C ^(F) Q V
 U D J M D I D G R W
 V E K N E J ^(E) H S X
 W F L O F K F I T Y
 X G M P G ^(L) G J U Z
 Y H N Q H M H K V A
 Z I O R ^(I) N I L W B
 A J P S J O J M X C
 B K Q ^(T) K P K N Y D
 C L R U L Q L O Z E
 D M ^(S) V M R M P A F
 E N T W N S N Q B G

FIGURE 43b

m. (1) There remains now to be considered only the case in which the two components are different mixed sequences. Let the two components be

P: H Y D R A U L I C B E F G J K M N O P Q S T V W X Z
 C: Q U E S T I O N A B L Y C D F G H J K M P R V W X Z

and let us examine the cipher text resulting from the following encipherment:

K: X H O S T I L E F O
 P: H O S T I L E F O R
 C: X N Q X Y Y P D I B

(2) First "decipher" the message in plaintext autokey fashion with any arbitrarily selected initial key letter, say A, assuming the base letter to be H_p , the initial letter of the plain component. Now in the first column, under the first decipherment, complete any arbitrary 26-letter sequence (in this example, the normal sequence), as shown in Fig. 44a, below.

K: A N H E V M P H W C
 C: X N Q X Y Y P D I B
 P: N H E V M P H W C W

O
P
Q
R
S
T
U
V
W
X
Y
Z
A
B
C
D
E
F
G
H
I
J
K
L
M

FIGURE 44a

K: A N H E V M P H W C
 C: X N Q X Y Y P D I B
 P: N H E V M P H W C W

O Y
P J
Q I
R G
S A
T R
U L
V F
W E
X B
Y V
Z C
A Z
B X
C T
D S
E U
F Q
G P
H O
I D
J N
K M
L W
M K

FIGURE 44b

K: A N H E V M P H W C
 C: X N Q X Y Y P D I B
 P: N H E V M P H W C W

O Y M U
P J B M
Q I T S
R G F E
S A P A
T R U W
U L N O
V F G B
W E X H
X B O P
Y V A N
Z C K L
A Z Y J
B X D F
C T V D
D S W Y
E U Z Z
F Q H C
G P L K
*H O S T
I D J I
J N Q X
K M I Q
L W R R
M K C G

FIGURE 44c

Then prepare a strip bearing the cipher component *reversed*, and set it below the plain component so that $H_p=N_c$, a setting given by the first two letters of NHEVMPHCW, the spurious plain text obtained by the arbitrary decipherment with the key letter A. Thus:

P: (H) Y D R A U L I C B E F G J K M N O P Q S T V W X Z
 C: (N) O I T S E U Q Z X W V R P M K J H G F D C Y L B A

(3) Now opposite each letter of the completion sequence in column 1, write in column 2 its plain-component equivalent, as given by the juxtaposed sequences above. This gives what is shown in Fig. 44b. Then reset the two sequences so that $E_p=H_c$ (to correspond with the 2d and 3d letters of the spurious

P: H Y D R A U L I C B (E) F G J K M N O P Q S T V W X Z
 C: Q Z X W V R P M K J (H) G F D C Y L B A N O I T S E U

plain text); write down the plain-component equivalents of the letters in column 2, forming column 3. Continue this process, scanning the generatrices from time to time, resetting the two components and finding equivalents from column to column, until it becomes evident on what generatrix the plain text is reappearing. In Fig. 44c it is seen that the plaintext generatrix is the one beginning HOST; from this point on, the solution may be obtained directly, by using the two primary components.

n. When two different components are involved, if the base letter is incorrectly assumed there is nothing much that can be done about it except tedious trial and error. There are no shortcut procedures such as those exemplified in subpars. h or l: successive base letters with their corresponding generatrix diagrams must be tried in turn, until a solution is forthcoming.

o. Another "mechanical" solution for the foregoing cases will now be described because it presents rather interesting cryptanalytic sidelights. Let us take the message "REFERENCE HIS PREFERENCE IN REFERENCE BOOKS AND REFERENCE CHARTS . . ." and encipher it by plaintext autokey, with direct standard alphabets, A_p as the base letter, and the single-letter initial key A_p=G_c. Then note the underscored repetitions:

		5		10		15		20		25		30																																
K:	G	R	E	F	E	R	E	N	C	E	H	I	S	P	R	E	F	E	R	E	N	C	E	I	N	R	E	F	E	R	E	N	C											
P:	R	E	F	E	R	E	N	C	E	H	I	S	P	R	E	F	E	R	E	N	C	E	I	N	R	E	F	E	R	E	N	C	E	I	N	R	E	F	E	R	E	N	C	E
C:	X	<u>V</u>	<u>J</u>	<u>J</u>	<u>V</u>	<u>V</u>	<u>R</u>	<u>P</u>	<u>G</u>	L	P	A	H	G	<u>V</u>	<u>J</u>	<u>J</u>	<u>V</u>	<u>V</u>	<u>R</u>	<u>P</u>	<u>G</u>	M	V	E	<u>V</u>	<u>J</u>	<u>J</u>	<u>V</u>	<u>V</u>	<u>R</u>	<u>P</u>	<u>G</u>											
		35		40		45		50		55																																		
K:	E	B	O	O	K	S	A	N	D	R	E	F	E	R	E	N	C	E	C	H	A	R	T																					
P:	B	O	O	K	S	A	N	D	R	E	F	E	R	E	N	C	E	C	H	A	R	T	S	.	.	.																		
C:	F	P	C	Y	C	S	N	Q	<u>U</u>	<u>V</u>	<u>J</u>	<u>J</u>	<u>V</u>	<u>V</u>	<u>R</u>	<u>P</u>	<u>G</u>	G	J	H	R	K	L																					

Now suppose the message has been intercepted and is to be solved, assuming that the only unknown factor is the initial key letter. Let the message be "deciphered" by means of any initial key letter,³ say A_x, and then note the underscored repetitions in the spurious plain text:

		5		10		15		20		25		30																					
K:	A	X	Y	L	Y	X	Y	T	W	K	B	O	M	V	L	K	Z	K	L	K	H	I	Y	O	H	X	Y	L	Y	X	Y	T	W
C:	X	<u>V</u>	<u>J</u>	<u>J</u>	<u>V</u>	<u>V</u>	<u>R</u>	<u>P</u>	<u>G</u>	L	P	A	H	G	<u>V</u>	<u>J</u>	<u>J</u>	<u>V</u>	<u>V</u>	<u>R</u>	<u>P</u>	<u>G</u>	M	V	E	<u>V</u>	<u>J</u>	<u>J</u>	<u>V</u>	<u>V</u>	<u>R</u>	<u>P</u>	<u>G</u>
P:	<u>X</u>	<u>Y</u>	<u>L</u>	<u>Y</u>	<u>X</u>	<u>Y</u>	<u>T</u>	<u>W</u>	<u>K</u>	<u>B</u>	<u>O</u>	<u>M</u>	<u>V</u>	<u>L</u>	<u>K</u>	<u>Z</u>	<u>K</u>	<u>L</u>	<u>K</u>	<u>H</u>	<u>I</u>	<u>Y</u>	<u>O</u>	<u>H</u>	<u>X</u>	<u>Y</u>	<u>L</u>	<u>Y</u>	<u>X</u>	<u>Y</u>	<u>T</u>	<u>W</u>	<u>K</u>
		35		40		45		50		55																							
K:	K	V	U	I	Q	M	G	H	J	L	K	Z	K	L	K	H	I	Y	I	B	G	L	Z										
C:	F	P	C	Y	C	S	N	Q	<u>U</u>	<u>V</u>	<u>J</u>	<u>J</u>	<u>V</u>	<u>V</u>	<u>R</u>	<u>P</u>	<u>G</u>	G	J	H	R	K	L										
P:	V	U	I	Q	M	G	H	J	<u>L</u>	<u>K</u>	<u>Z</u>	<u>K</u>	<u>L</u>	<u>K</u>	<u>H</u>	<u>I</u>	<u>Y</u>	<u>I</u>	<u>B</u>	<u>G</u>	<u>L</u>	<u>Z</u>	<u>M</u>										

The original four 8-letter repetitions now turn out to be two different sets of 9-letter repetitions. This calls for an explanation. Let the spurious plain text, together with its real plain text, be transcribed as though we were dealing with a periodic cipher involving two alphabets, as shown in Fig. 45, below:

1 2	1 2	1 2	1 2	1 2	1 2	1 2	1 2	1 2	1 2	1 2	1 2	1 2	1 2
XY	LY	XY	TW	KB	OM	VL	KZ	KL	KH	IY	OH	XY	LY
RE	FE	RE	NC	EH	IS	PR	EF	ER	EN	CE	IN	RE	FE
XY	TW	KV	UI	QM	GH	JL	KZ	KL	KH	IY	IB	GL	ZM . . .
RE	NC	EB	OO	KS	AN	DR	EF	ER	EN	CE	CH	AR	TS

FIGURE 45

It will here be seen that the letters in column 1 have been monoalphabetically enciphered, as have been those in column 2. In other words, an autokey cipher, which is an aperiodic polyalphabetic substitution, has been converted into a 2-alphabet periodic polyalphabetic substitution. The two repetitions of XYLYXYTWK represent encipherments of the word REFERENCE, in alphabets 1-2-1-2-1-2-1-2-1; the two repetitions of LKZKLKHIY likewise represent encipherments of the same word but in alphabets 2-1-2-1-2-1-2-1-2. Later on it will be seen how this method of converting an autokey cipher into a periodic cipher may be applied to the case where an introductory key word is used as the initial keying element instead of a single letter, as in the present case.

³ Except the actual key letter or a letter 13 intervals from it. If the actual key letter is used, we will of course obtain plain text; if we use the letter 13 intervals away from the actual key letter, the cipher text will be converted to monoalphabetic terms. (See subpar. r, below.)

p. The student has probably already noted that the phenomena observed in the preceding subparagraph are the same as those observed in subpar. g, in which it was seen that the direction of the sequences in alternate columns had to be reversed in order to bring out the plain text on one generatrix. If this reversal is not done, then obviously the plain text would appear on *two* generatrices, which is equivalent to having the plain text reduced to two monoalphabets.

q. When reciprocal components are employed, the spurious plain text obtained by "decipherment" with a key setting other than the actual one will be monoalphabetic throughout. Note the following encipherment (with initial key $A_p = G_c$, using reversed standard alphabets) and its "decipherment" by setting the two components at $A_p = A_c$.

P : R E F E R E N C E H I S P R E F E R E N C E
C : P N Z B N N R L Y X Z Q D Y N Z B N N R L Y
"P" : L Y Z Y L Y H W Y B C M J L Y Z Y L Y H W Y

Here the spurious plain text is wholly monoalphabetic.

r. The reason for the exception noted in footnote 3 in subpar. o now becomes clear. For if the actual initial key letter (G) were used, of course the decipherment yields the correct plain text; if a letter 13 intervals removed from G is used as the key letter, the cipher alphabet selected for the first "decipherment" is the reciprocal of the actual initial cipher alphabet and thereafter all alternate cipher alphabets are reciprocal. Hence the spurious plain text obtained from such a "decipherment" must be monoalphabetic.

s. In the example illustrated in subpar. o, the primary components were identical normal sequences progressing in the same direction. If they were mixed sequences, the phenomena observed above would still hold true, and, so long as the sequences are known, the indicated method of solution may be applied. When the two primary components are known but differently mixed sequences, this method of solution is too involved to be practical. It is more expedient to try successive initial key letters, noting the plain text each time and resetting the strips until the correct setting has been ascertained, as will be evidenced by obtaining intelligible plain text.

31. Solution of plaintext autokey systems involving known cipher alphabets when the introductory key consists of several letters.—a. In the foregoing discussion of plaintext autokeying, the introductory key was assumed to consist of a single letter, so that the subsequent key letters are displaced one letter to the right with respect to the text of the message itself. But sometimes a word or phrase may serve this function, in which case the subsequent key is displaced as many letters to the right of the initial plaintext letter of the message as there are letters in the introductory key. This will not, as a rule, interfere in any way with the application of the general principles of solution set forth to that part of the cryptogram subsequent to the introductory key, and a solution by the probable-word method and the study of repetitions can be reached. However, it may happen that trial of this method is not successful in certain cryptograms because of the paucity of repetitions, or because of failure to find a probable word in the text. When the cipher alphabets are known, there is another point of attack which is useful and interesting. The method consists of finding the length of the introductory key and then solving by frequency principles; this method will be described in the subparagraphs below.

7
;

b. Suppose that the introductory key word is the 10-letter word PARLIAMENT, that the plaintext message is as below, and that identical primary components progressing in the same direction are used to encipher the message, with the normal Vigenère enciphering convention. Let the components be the normal sequence. The encipherment, shown here written out on a width of 20 (i.e., twice the length of the introductory key) is as follows:

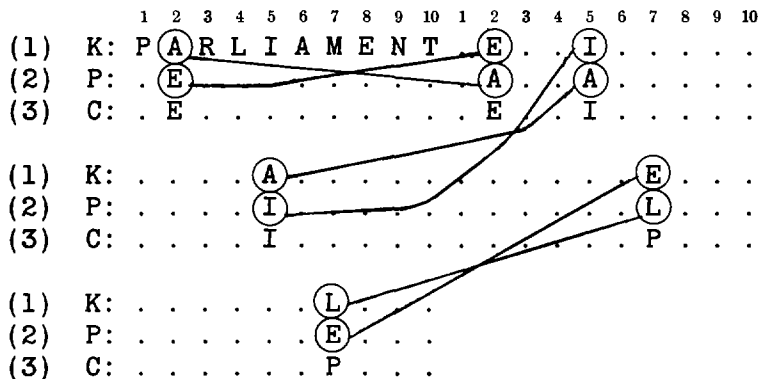
	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
K:	P	A	R	L	I	A	M	E	N	T	R	E	C	E	I	V	I	N	G	H
P:	R	E	C	E	I	V	I	N	G	H	E	A	V	Y	A	R	T	I	L	L
C:	G	E	T	P	Q	V	U	R	T	A	V	E	X	C	I	M	B	V	R	S
K:	E	A	V	Y	A	R	T	I	L	L	E	R	Y	F	I	R	E	O	N	M
P:	E	R	Y	F	I	R	E	O	N	M	Y	L	E	F	T	F	L	A	N	K
C:	I	R	T	D	I	I	X	W	Y	X	C	C	C	K	B	W	P	O	A	W
K:	Y	L	E	F	T	F	L	A	N	K	S	T	O	P	E	N	E	M	Y	I
P:	S	T	O	P	E	N	E	M	Y	I	S	M	A	S	S	I	N	G	H	I
C:	Q	E	S	U	X	S	P	M	L	S	K	F	O	H	W	V	R	S	F	Q
K:	S	M	A	S	S	I	N	G	H	I	S	T	R	O	O	P	S	T	O	L
P:	S	T	R	O	O	P	S	T	O	L	E	F	T	F	R	O	N	T	A	N
C:	K	F	R	G	G	X	F	Z	V	T	W	Y	K	T	F	D	F	M	O	Y
K:	E	F	T	F	R	O	N	T	A	N	D	C	O	N	C	E	N	T	R	A
P:	D	C	O	N	C	E	N	T	R	A	T	I	N	G	A	R	T	I	L	L
C:	H	H	S	T	S	A	M	R	N	W	K	B	T	C	V	G	B	C	L	
K:	T	I	N	G	A	R	T	I	L	L	E	R	Y	T	H	E	R	E	S	T
P:	E	R	Y	T	H	E	R	E	S	T	O	P	R	E	I	N	F	O	R	C
C:	X	Z	L	Z	H	V	K	M	D	E	S	G	P	X	P	R	W	S	J	V
K:	O	P	R	E	I	N	F	O	R	C	E	M	E	N	T	S	I	M	P	E
P:	E	M	E	N	T	S	I	M	P	E	R	A	T	I	V	E	T	O	H	O
C:	S	B	V	R	B	F	N	A	G	G	V	M	X	V	O	W	B	A	W	S
K:	R	A	T	I	V	E	T	O	H	O										
P:	L	D	P	O	S	I	T	I	O	N										
C:	C	D	I	W	N	M	M	W	V	B										

It will now be noted that, since the introductory key consists of 10 letters, the 11th letter of the message is enciphered by the 1st letter of the plain text, the 12th by the 2d, and so on. Likewise, the 21st letter is enciphered by the 11th, the 22d by the 12th, and so on. An important step in the solution of a message of this kind would therefore involve ascertaining the length of the introductory key. This step will now be explained.

c. Since the plain text itself constitutes the key letters in this system (after the introductory key), these key letters will occur with their normal frequencies, and this means that there will be many occurrences of E, T, N, R, O, A, I, S, enciphered by E_k ; there will be many occurrences of these same high-frequency letters enciphered by T_k , by N_k , by R_k , and so on. In fact, the number of times each of these combinations will occur may be calculated statistically. With the enciphering conditions set forth under subpar. b, above, if E_p is enciphered by T_k , for example, it will yield the same cipher equivalent as T_p enciphered by E_k ; in other words, two encipherments of any pair of letters of which either may serve as the key for enciphering the other must yield the same cipher resultant.⁴ It is the cryptographic effect

⁴ It is important to note that this observation applies only to cases in which the two components are *identical sequences progressing in the same direction*; if this is not the case, the entire reasoning is inapplicable.

of these two phenomena working together which permits ascertaining the length of the introductory key in such a case. For every time a given letter, θ_p , occurs in the plain text, it will occur n letters later as a key letter, θ_k , where n equals the length of the introductory key. Note the following illustration:



It may be seen that the key-plain combination $A_k(E_p) = E_c$, yields the same cipher resultant 10 positions later as the combination $E_k(A_p) = E_c$; likewise, $I_k(A_p) = I_c$, and 10 positions away, $A_k(I_p) = I_c$; also, $E_k(L_p) = P_c$, and 10 positions later we have the same cipher resultant from $L_k(E_p) = P_c$. Two identical cipher letters at an interval equal to the length of the introductory key is a function of the key-plain reversibility just demonstrated. But not every pair of identical letters in the cipher text represents a case of this type. For in this system, identity in two cipher letters may be the result of the following three conditions each having a statistically ascertainable probability of occurrence:

- (1) A given plaintext letter is enciphered by the same key letter two different times, at an interval which is purely accidental; the cipher equivalents are identical, but could not be used to give any information about the length of the introductory key.
- (2) Two different plaintext letters are enciphered by two different key letters; the cipher equivalents are fortuitously identical.
- (3) A given plaintext letter is enciphered by a given key letter, and later on the same plaintext letter serves to encipher another plaintext letter which is identical with the first key letter; the cipher equivalents are *causally* identical.

d. It can be proved that the probability for identities of the third type, for that interval which corresponds with the length of the introductory key, is greater than that for identities of either or both 1st and 2d types; that is, if a tabulation is made of the intervals between identical letters in such a system as the one being studied, the interval which occurs most frequently should coincide with the length of the introductory key. In a random case, i.e., cases (1) and (2), above, the probability of a ciphertext identity is for all intents and purposes 1/26 or .0385, whereas in the causal case (case 3, above) the probability is the kappa plain of the language, which for English is .0667 or 1/15. As a practical demonstration of this point, let us transcribe the cipher text of the message in subpar. b on trial widths; those for widths of 7, 8, 9, and 10 are shown in Fig. 46, below:

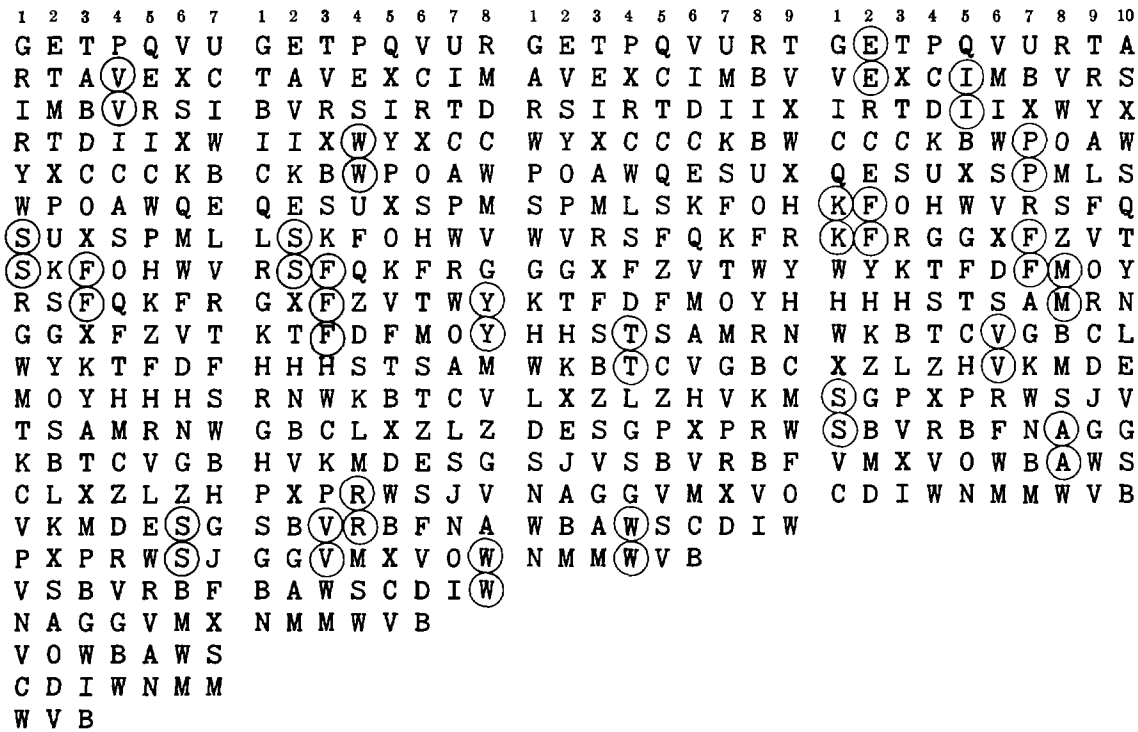


FIGURE 46

In each transcription, every pair of superimposed letters is noted and the number of identities is indicated by circling the letters involved, as shown above. In the diagram below, *w* is the trial width, *C* the number of comparisons, *r* the random expectation (obtained by dividing *C* by 26), *p* the expectation if the width is correct (obtained by dividing *C* by 15), and *i* is the observed number of identities. It is obvious that the width of 10 is probably the correct width.

<i>w</i>	<i>C</i>	<i>r</i>	<i>p</i>	<i>i</i>
7	143	5.5	9.5	4
8	142	5.5	9.5	8
9	141	5.4	9.4	2
10	140	5.4	9.3	10

e. Once we have found the length of the introductory key, two lines of attack are possible if the enciphering alphabets are known: (1) completion of the plain-component sequence on the columns of the correct write-out, or (2) conversion of the aperiodic cipher text to periodic terms and its solution as a repeating-key cipher. The first line of attack will be discussed first, using the cipher message of subpar. b as an example.

f. The cipher letters of column 1 and column 2 (of the write-out on a width of 10) are written in a row, and the key of A is arbitrarily chosen to start an autokey decipherment of the letters. Then, from these decipherments, the plain-component sequence is completed on the assumption of direct standard alphabets, running alternate columns in the reverse direction, as shown in Figs. 47a and b, below:⁵

Column 1

K: A G P T J H D H P S E T Z T C
C: G V I C Q K K W H W X S S V C
P: G P T J H D H P S E T Z T C A

6 G P T J H D H P S E T Z T C A
6 H O U I I C I O T D U Y U B B
~~I N V H J B J N U C V X V A C~~
~~J M W G K A K M V B W W W Z D~~
~~K L X F L Z L L W A X V X Y E~~
~~L K Y E M Y M K X Z Y U Y X F~~
~~M J Z D N X N J Y Y Z T Z W G~~
9 N I A C O W O I Z X A S A V H
4 O H B B P V P H A W B R B U I
~~P G C A Q U Q C B V C Q C T J~~
~~Q F D Z R T R F C U D P D S K~~
12 R E E Y S S S E D T E O E R L
7 S D F X T R T D E S F N F Q M
3 T C G W U Q U C F R G M G P N
2 U B H V V P V B G Q H L H O O
7 V A I U W O W A H P I K I N P
~~W Z J T X N X Z I O J J J M Q~~
~~X Y K S Y M Y Y J N K I K L R~~
~~Y X L R Z L Z X K M L H L K S~~
~~Z W M Q A K A W L L M G M J T~~
5 A V N P B J B V M K N F N I U
7 B U O O C I C U N J O E O H V
5 C T P N D H D T O I P D P G W
~~D S Q M E G E S P H Q C Q F X~~
7 E R R L F F F R Q G R B R E Y
~~F Q S K G E G Q R F S A S D Z~~

FIGURE 47a

Column 2

K: A E A R L T M T F C I R P M A
C: E E R C E F F Y H K Z G B M D
P: E A R L T M T F C I R P M A D

8 E A R L T M T F C I R P M A D
~~F Z S K U L U E D H S O N Z E~~
5 G Y T J V K V D E G T N O Y F
~~H X U I W J W C F F U M P X G~~
~~I W V H X I X B G E V L Q W H~~
3 J V W G Y H Y A H D W K R V I
~~K U X F Z G Z Z I C X J S U J~~
7 L T Y E A F A Y J B Y I T T K
~~M S Z D B E B X K A Z H U S L~~
5 N R A C C D C W L Z A G V R M
2 O Q B B D C D V M Y B F W Q N
6 P P C A E B E U N X C E X P O
5 Q O D Z F A F T O W D D Y O P
~~R N E Y G Z G S P V E C Z N Q~~
4 S M F X H Y H R Q U F B A M R
7 T L G W I X I Q R T G A B L S
~~U K H V J W J P S S H Z C K T~~
~~V J I U K V K O T R I Y D J U~~
~~W I J T L U L N U Q J X E I V~~
~~X H K S M T M M V P K W F H W~~
5 Y G L R N S N L W O L V G G X
~~Z F M Q O R O K X N M U H F Y~~
~~A E N P P Q P J Y M N T I E Z~~
~~B D O O Q P Q I Z L O S J D A~~
6 C C P N R O R H A K P R K C B
~~D B Q M S N S G B J Q Q L B C~~

FIGURE 47b

⁵ Generatrices with three or more of the letters JKQXZ have been eliminated.

The R generatrix of the letters of column 1 (with a two-category score of 12), and the E generatrix of column 2 (with a score of 8) are clearly the correct ones, and the solution is off to a flying start.

g. In the decipherment step of the preceding subparagraph, the base letter was correctly assumed to be A_p. Had we assumed an incorrect base letter, for example D_p, our steps would have been those shown below:

Column 1

K: A J P W J K D K P V E W Z W C
 C: G V I C Q K K W H W X S S V C
 P: J P W J K D K P V E W Z W C D

~~J P W J K D K P V E W Z W C D~~
~~K O X I L C L O W D X Y X B E~~
 3 L N Y H M B M N X C Y X Y A F 0 3
~~M M Z G N A N M Y B Z W Z Z G~~
 7 N L A F O Z O L Z A A V A Y H 6 1
~~O K B E P Y P K A Z B U B X I~~
~~P J C D Q X Q J B Y C T C W J~~
~~Q I D C R W R I C X D S D V K~~
 7 (R)H(E)B(S)V(S)H(D)W(E)R(E)U(L) 6 1
 6 S G F A T U T G E V F Q F T M 4 2
 4 T F G Z U T U F F U G P G S N 2 2
 7 U(E)H(Y)V(S)V(E)G(T)H(O)H(R) 0 1 6
 6 V D I X W R W D H S I N I Q P 3 3
~~W C J W X Q X C I R J M J P Q~~
~~X B K V Y P Y B J Q K L K O R~~
~~Y A L U Z O Z A K P L K L N S~~
~~Z Z M T A N A Z L O M J M M T~~
 7 A Y N S B M B Y M N N I N L U 4 3
~~B X O R C L C X N M O H O K V~~
~~C W P Q D K D W O L P C P J W~~
~~D V Q P E J E V P K Q F Q I X~~
~~E U R O F I F U Q J R E R H Y~~
 8 F T S N G H G T R I S D S G Z 4 4
 7 G S T M H G H S S H T C T F A 5 2
 6 H R U L I F I R T G U B U E B 3 3
~~I Q V K J E J Q U F V A V D C~~

FIGURE 48a

Column 2

K: A H A U L W M W F F I U P P A
 C: E E R C E F F Y H K Z G B M D
 P: H A U L W M W F F I U P P A G

3 H(A)U(L)W(M)W(F)F(I)U(P)P(A)G 0 3
~~I Z V K X L X E G H V O Q Z H~~
~~J Y W J Y K Y D H G W N R Y I~~
~~K X X I Z J Z C I F X M S X J~~
 5 L W Y H A I A B J E Y L T W K 3 2
~~M V Z G B H B A K D Z K U V L~~
 3 N U A F C G C Z L C A J V U M 3 0
 6 O T B E D F D Y M B B I W T N 2 4
 8 P S C D E E E X N A C H X S O 4 4
 3 Q R D C F D F W O Z D G Y R P 1 2
~~R Q E B C G G V P Y E F Z Q Q~~
 5 S P F A H B H U Q X F E A P R 3 2
 9 T O G Z I A I T R W G D B O S 5 4
~~U N H Y J Z J S S V H C C N T~~
~~V M I X K Y K R T U I B D M U~~
~~W L J W L X L Q U T J A E L V~~
~~X K K V M W M P V S K Z F K W~~
~~Y J L U N V N O W R L Y G J X~~
~~Z I M T O U O N X Q M X H I Y~~
 6 A H N S P T P M Y P N W I H Z 4 2
~~B G O R Q S Q L Z O O V J C A~~
~~C F P Q R R R K A N P U K F B~~
~~D E Q P S Q S J B M Q T L E C~~
 8 (E)D(R)O(T)P(T)I(C)L(R)S(M)D(D) 5 3
 7 F C S N U O U H D K S R N C E 4 3
 5 G B T M V N V G E J T Q O B F 4 1

FIGURE 48b

The numbers to the left of the generatrices give the two-category score for the generatrix as a whole, while the numbers to the right give the two-category scores for the odd and even letters, respectively. It may be seen that the correct generatrices are those with the ringed letters, and that from the intervals between them the base letter must have been not D_p, but three letters earlier, or A_p.

h. If the message in subpar. *b* had been enciphered with the same introductory key, PARLIAMENT, but with reciprocal alphabets (e.g., reversed standard), the only way we could have arrived at the length of the introductory key is by trial and error, since the technique demonstrated in subpar. *d* does not apply. We would have had to make generatrix diagrams for the first several columns of trial widths, until a solution was reached. In Fig. 49a, below, is the autokey decipherment of the letters of column 1 obtained from a write-out of the cipher text on a width of 10, together with the appertaining generatrix diagram, on the assumption of reversed standard alphabets; the correct plain text comes out on a generatrix which has been underlined. In Fig. 49b we have the decipherment of the letters of column 1, under the incorrect assumption of the base letter as D_p. Note that the correct letters are those ringed, in an ascending diagonal pattern. This demonstrates the messiness of the case of plaintext autokey encipherment with reversed sequences, an unknown length of introductory key, and an unknown base letter.

K: A C P P J D D D P O E P Z P C
 C: Y N A G G A A O B K P Q K N G
 P: C P P J D D D P O E P Z P C W

K: A F V Y V S V Y N P I W J C S
 C: Y N A G G A A O B K P Q K N G
 P: F V Y V S V Y N P I W J C S P

C P P J D D D P O E P Z P C W
 D Q Q K E E E Q P F Q A Q D X
 E R R L F F F R Q G R B R E Y
 F S S M G G G S R H S C S F Z
 G T T N H H H T S I T D T G A
 H U U O I I I U T J U E U H B
 I V V P J J J V U K V F V I C
 J W W Q K K K W V L W G W J D
 K X X R L L L X W M X H X K E
 L Y Y S M M M Y X N Y I Y L F
 M Z Z T N N N Z Y O Z J Z M G
 N A A U O O O A Z P A K A N H
 O B B V P P P B A Q B L B O I
 P C C W Q Q Q C B R C M C P J
 Q D D X R R R D C S D N D Q K
R E E Y S S S E D T E O E R L
 S F F Z T T T F E U F P F S M
 T G G A U U U G F V G Q G T N
 U H H B V V V H G W H R H U O
 V I I C W W W I H X I S I V P
 W J J D X X X J I Y J T J W Q
 X K K E Y Y Y K J Z K U K X R
 Y L L F Z Z Z L K A L V L Y S
 Z M M G A A A M L B M W M Z T
 A N N H B B B N M C N X N A U
 B O O I C C C O N D O Y O B V

FIGURE 49a

F V Y V [Ⓢ] V Y N P I W J C S P
 G W Z W T W Z O Q J X K D T Q
 H X A X U X A P R K Y L [Ⓢ] U R
 I Y B [Ⓢ] V Y B Q S L Z M F V S
 J Z C Z W Z C R T M A N G W T
 K A D A X A D S U N B [Ⓢ] H X U
 L B [Ⓢ] B Y B E T V O C P I Y V
 M C F C Z C F U W P D Q J Z W
 N D G D A D G V X Q [Ⓢ] R K A X
 O [Ⓢ] H E B E H W Y R F S L B Y
 P F I F C F I X Z S G T M C Z
 Q G J G D G J Y A [Ⓢ] H U N D A
[Ⓢ] H K H E H K Z B U I V O E B
 S I L I F I L A C V J W P F C
 T J M J G J M B [Ⓢ] W K X Q G D
 U K N K H K N C E X L Y R H E
 V L O L I L O D F Y M Z S I F
 W M P M J M P [Ⓢ] G Z N A T J G
 X N Q N K N Q F H A O B U K H
 Y O R O L O R G I B P C V L I
 Z P S P M P [Ⓢ] H J C Q D W M J
 A Q T Q N Q T I K D R E X N K
 B R U R O R U J L E S F Y O [Ⓢ]
 C S V S P [Ⓢ] V K M F T G Z P M
 D T W T Q T W L N G U H A Q N
 E U X U R U X M O H V I B [Ⓢ] O

FIGURE 49b

i. When the plain and cipher components are two different sequences, not only must we arrive at the correct length of the introductory key by trial and error, but each base letter must be laboriously assumed in turn for the specialized generatrix diagrams (cf. those in subpar. 30m) pertaining to each assumption of introductory key length, since the correct plaintext letters cannot be determined from any sort of systematic pattern from the generatrix diagram predicated on an incorrect assumption of the base letter.

j. In subpar. *e* it was stated that the aperiodic substitution resulting from plaintext autokey encipherment can be converted to periodic terms and solved as though it were a repeating-key cipher, provided that the primary components are known sequences. As a demonstration, we shall use as an

method, using direct standard alphabets which we have just proved to have been employed by the enciphering cryptographer.

k. The mystery of the conversion of a plaintext autokey encipherment to periodic terms will now be explained. First, let the key word PARLIAMENT be enciphered by the following alphabet:

∅	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	
P:	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
C:	A	Z	Y	X	W	V	U	T	S	R	Q	P	O	N	M	L	K	J	I	H	G	F	E	D	C	B

P: P A R L I A M E N T
 C: L A J P S A O W N H

Then let the message RECEIVING HEAVY ARTILLERY FIRE . . . be enciphered by direct standard alphabets as before, but for the key add the monoalphabetic equivalents of PARLIAMENT (i.e., LAJPSAOWNH) to the key itself; that is, use the 20-letter key sequence PARLIAMENTLAJPSAOWNH in a repeating-key manner, as shown in the figure below:

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	
K:	<u>P</u>	<u>A</u>	<u>R</u>	<u>L</u>	<u>I</u>	<u>A</u>	<u>M</u>	<u>E</u>	<u>N</u>	<u>T</u>	<u>L</u>	<u>A</u>	<u>J</u>	<u>P</u>	<u>S</u>	<u>A</u>	<u>O</u>	<u>W</u>	<u>N</u>	<u>H</u>	
P:	R	E	C	E	I	V	I	N	G	H	E	A	V	Y	A	R	T	I	L	L	
C:	G	E	T	P	Q	V	U	R	T	A	P	A	E	N	S	R	H	E	Y	S	
P:	E	R	Y	F	I	R	E	O	N	M	Y	L	E	F	T	F	L	A	N	K	. . .
C:	T	R	P	Q	Q	R	Q	S	A	F	J	L	N	U	L	F	Z	W	A	R	

FIGURE 53

The cipher resultants of this process of *enciphering* a message coincide exactly with those obtained from the *deciphering* operation that gave rise to Fig. 52a. How does this happen?

(1) First, let it be noted that the sequence LAJPSAOWNH which forms the second half of the key for enciphering the text in Fig. 53 may be described as the standard-alphabet *complement* of the sequence PARLIAMENT which forms the first half of the key. Arithmetically, the sum of a letter of the first half and its corresponding letter in the second half is ∅, mod 26. Thus:

$$\begin{aligned}
 P + L &= 15 + 11 = 26 = \emptyset \\
 A + A &= \emptyset + \emptyset = \emptyset \\
 R + J &= 17 + 9 = 26 = \emptyset \\
 L + P &= 11 + 15 = 26 = \emptyset \\
 I + S &= 8 + 18 = 26 = \emptyset
 \end{aligned}$$

In other words, the LAJPSAOWNH sequence is, by cryptographic arithmetic, equivalent to "minus PARLIAMENT." Therefore, in Fig. 53, *enciphering* the second half of each line by the key letters LAJPSAOWNH (i.e., adding 11, ∅, 9, 15, 18 . . .) is the same as *deciphering* by the key letters PARLIAMENT (i.e., subtracting 15, ∅, 17, 11, 8 . . .). For example, at position 11 of Fig. 53, $E_p(L_k) = 4 + 11 = 15 = P_c$, but if we use the key letter at position 1 and subtract it from E_p , we have $E_p(-P_k) = 4 - 15 = 4 - 15 + (26) = 15 = P_c$, the same cipher resultant.

(2) Refer now to Fig. 52a. The letters in the first half of line 1, beginning GETPQ . . ., are identical with those in the first half of line 1 of Fig. 53. They must be identical because they are produced from identical elements. The letters in the second half of this same line in Fig. 52a, beginning PAENS . . ., were produced by *deciphering* the letters in the second line of Fig. 50 (VEXCI . . .). Thus (taking for illustrative purposes only the first five letters in each case):

$$\begin{aligned}
 \text{PAENS} &= \text{VEXCI} - \text{GETPQ}. \\
 \text{But VEXCI} &= \text{EAVYA} + \text{RECEI} \\
 \text{and GETPQ} &= \text{RECEI} + \text{PARLI}. \\
 \text{Hence, PAENS} &= (\text{EAVYA} + \text{RECEI}) - (\text{RECEI} + \text{PARLI}), \\
 \text{or PAENS} &= \text{EAVYA} - \text{PARLI}.
 \end{aligned}$$

[I]

As for the letters in the second half of line 1 of Fig. 53, also beginning PAENS . . . , these letters were the result of enciphering EAVYA by LAJPS. Thus:

$$PAENS = EAVYA + LAJPS.$$

But it has been shown in subpar. (1), above, that

$$\begin{aligned} LAJPS &= - PARLI. \\ \text{Hence, } PAENS &= EAVYA + (-PARLI), \\ \text{or } PAENS &= EAVYA - PARLI. \end{aligned} \tag{II}$$

Thus, equations [I] and [II] turn out to be identical but arise from what appear to be quite diverse sources.

(3) What has been demonstrated in connection with the letters in line 1 of Figs. 52a and 53 also holds true for the letters in the other lines of those two figures, and it is not necessary to repeat the explanation. The steps show that the originally aperiodic, autokey cipher has been converted, through a knowledge of the primary components, into a repeating-key cipher with a period *twice the length of the introductory key*. The message may now be solved as an ordinary repeating-key cipher.

l. The procedure just described (in subpars. j and k) has the advantage over the generatrix methods of subpars. g and h in that it is not necessary to assume the correct base letter for the procedure to work.

m. The foregoing case is based upon encipherment by the normal Vigenère equations $\theta_{x/2} = \theta_{1/1}$; $\theta_{p/1} = \theta_{c/2}$. When encipherment has been accomplished by the equations $\theta_{x/2} = \theta_{1/1}$; $\theta_{p/2} = \theta_{c/1}$, the conversion of a plaintext autokeyed cipher yields a repeating-key cipher with a period *equal to the length of the introductory key*. In this conversion the equations $\theta_{x/2} = \theta_{1/1}$; $\theta_{p/1} = \theta_{c/2}$ are used in finding equivalents. As an example, note the plaintext autokey encipherment of the following message by equations $\theta_{x/2} = \theta_{1/1}$; $\theta_{p/2} = \theta_{c/1}$:

K: T U E S D A Y I N F O R M A T I O N F R O M R E L I A B L E S O U R C
P: I N F O R M A T I O N F R O M R E L I A B L E S O U R C E S I N D I C . . .
C: P T B W O M C L V J Z O F O T J Q Y D J N Z N O D M R B T O Q Z J R A

If the cipher text is written out in lines corresponding to the length of the introductory key, and each line is enciphered by the one directly above it, using the normal Vigenère equations in finding equivalents, the results are shown in Fig. 54b. But if the same is enciphered by equations $\theta_{x/2} = \theta_{1/1}$; $\theta_{p/2} = \theta_{c/1}$, using the word TUESDAY as a repeating key, the cipher text (Fig. 54c) is identical with that obtained in Fig. 54b by enciphering each successive line with the line above.

Original cipher text	Original cipher and converted text	Repeating key encipherment
		<u>T U E S D A Y</u>
		I N F O R M A
P T B W O M C ←————→	P T B W O M C ←————→	P T B W O M C
L V J Z O F O ←————→	<u>L V J Z O F O</u>	
	a o k v c r q ←————→	T I O N F R O
T J Q Y D J N ←————→	<u>T J Q Y D J N</u>	A O K V C R Q
	t x a t f a d ←————→	M R E L I A B
Z N O D M R B ←————→	<u>Z N O D M R B</u>	T X A T F A D
	s k o w r r e ←————→	L E S O U R C
T O Q Z J R A ←————→	<u>T O Q Z J R A</u>	S K O W R R E
	l y e v a i e ←————→	E S I N D I C
		L Y E V A I E
(a)	(b)	(c)

FIGURE 54

Now note that the sequences joined by the arrows in Figs. 54b and c are identical; since it is certain that Fig. 54c is periodic in form because it was enciphered by the repeating-key method, it follows that Fig. 54b is now also in periodic form, and in that form the message could be solved as though it were a repeating-key cipher.

n. In the case of primary components consisting of reversed standard alphabets, the process of converting the plaintext autokeyed text to periodic terms is accomplished by using a *direct standard* alphabet and "deciphering" each line of the text (as transcribed in period-lengths) by the line above it. For example, here is a message enciphered by reversed standard alphabets, with the initial key word TUESDAY:

K: T U E S D A Y I N F O R M A T I O N F R O M R E L I A B L E S O U R C
P: I N F O R M A T I O N F R O M R E L I A B L E S O U R C E S I N D I C . . .
C: L H Z E M O Y P F R B M V M H R K C X R N B N M X O J Z H M K B R J A

The cipher text is transcribed in periods equal to the length of the initial key word (7 letters) and the 2d line is "deciphered" with key letters of the 1st line, using the normal Vigenère equations $\theta_{k/2} = \theta_{1/1}$; $\theta_{p/1} = \theta_{c/2}$. The resultant letters are then used as key letters to "decipher" the 3d line of text, and so on. The results are as seen in Fig. 55b below. Now let the original message be enciphered as a *repeating-key cipher* by reversed standard alphabets with the key word TUESDAY; the result is shown in Fig. 55c. Note that the odd or alternate lines of Fig. 55b and c are identical, showing that the autokeyed text has been converted into repeating-key cipher text.

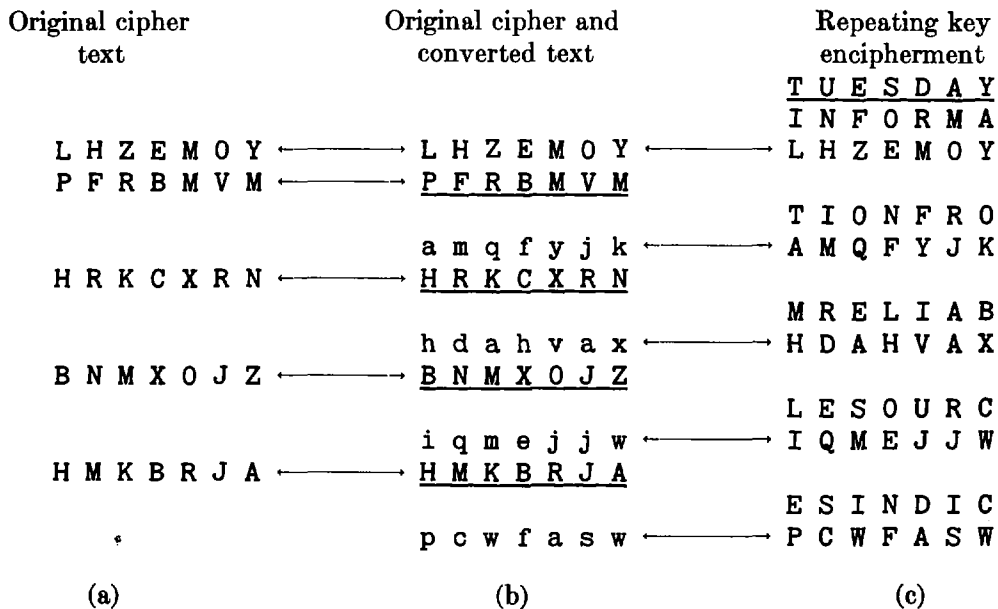


FIGURE 55

o. The foregoing procedures indicate a simple method of solving plaintext autokey ciphers when the primary components or the secondary cipher alphabets are known. It consists in assuming introductory keys of various lengths, converting the cipher text into repeating-key form, and then examining the resulting diagrams for repetitions. When a correct key length is assumed, repetitions will be as numerous as should be expected in ciphers of the repeating-key class; incorrect assumptions for key length will not show so many repetitions.⁷ All of the foregoing presupposes a knowledge of the cipher alphabets involved. When these are unknown, recourse must be had to first principles, and the messages

⁷ These repetitions need not be polygraphic repetitions in order to prove the key length. In the write-outs on the correct width, the average I.C. of the entire array of columns should be near 1.73, with acceptable deviations. See in this connection subpars. 18e et seq. in *Military Cryptanalytics, Part II*.

must be solved purely upon the bases of probable words and repetitions; the general approaches will be demonstrated.

32. Analysis of a case involving unknown components.—a. When the primary components in a plaintext autokey system are unknown, the observations noted under the preceding paragraphs are, of course, not applicable; nevertheless, solution is not difficult. Let us assume that we have available the following three cryptograms, all intercepted on the same day, and therefore suspected of being related.

Message No. 1

H U F I I O C Q J J I V Z O Z V P D G O V V V K W U E W H U
U Q H U M R Z V Q R U A K V D N N E Z V G J P G H A Y J D R
U W N G R Y S K B L Q V U X N P H D P R S V K Z P P P K G S
L L P R V R B H A K W U A V W Y U E Z Q X A P Q Y G P S V S
F N R A K C I F G Z U V C C P D K C W V X T W F M R F K B V
R O Q O J D R U W N G R Y S K B L

Message No. 2

J U F I I O C Q J J I V Z O Z I B F E J S U B R J S P K T S
R Z V X T W F M R F Q H H F O R F J P D G O V V V K W U H E
N D B D D R H W U N K C M P D G O V Z S E N D B D D R H W U
N P P K P E Q O Y

Message No. 3

F J U H F F K D E N A L U P Z K Q M V B J W V P K E U B D D
R H W U M R H V G P D N C U J C D Z C Y R H U J U F Z P Q P
Y Q C Y H O E Q Z V X K C Q F T V H N S V C C E J P E A M P
A P O E P B H M V J U N M H H W K C V G D S W J U E Q Z B O
F F Y U E Z Q X A P Q Y G P A R P Z V X C F N R A K C I F G
Z U V C C P D K C O G J W Z H A P U F Z F V H A V X M H F F
K M Y H S T B S K C V R Q I J Y C P Z H U H C B M T H O F H

b. There are many repetitions within and between the messages, attesting to their cryptographic homogeneity. The intervals between repetitions show no common factor, and the δ I.C. of the composite uniliteral frequency distribution is 1.12; these manifestations admit of the possibility of a plaintext autokey system. Furthermore, the appearance of the repetitions in the first line of Message No. 1, with the isolated 1st and 16th letters, suggests a 1-letter introductory key.

c. The simplest assumption to make is that Vigenère encipherment with standard alphabets is involved; however, the trials both for direct standard and reversed standard alphabets are unsuccessful.⁸ We next assume that the plain component is the normal sequence, the cipher component a mixed sequence. The various repetitions are studied intensively, in particular the 13-letter repetition JDRUWNGRYSKBL and the 10-letter repetition PDGOVVVKWU, which, on the hypothesis of a 1-letter introductory key, must represent 14-letter and 11-letter plaintext sequences or words.

d. If the normal Vigenère method of encipherment is in effect, then the base letter is probably A_p, in which case a good word to fit the 13-letter repetition is

K: . R E C O N N A I S S A N C E
P: R E C O N N A I S S A N C E
C: J D R U W N G R Y S K B L

⁸ The theoretical I.C. for plaintext autokey systems involving either direct or reversed standard alphabets has been computed and found to be 1.035; this then would tend to disprove the assumption of standard alphabets in the case under examination.

and a good word to fit the 10-letter repetition (note the corroborative vertical trigraph ONU with the preceding crib) is

K: . O B S E R V A T I O N
 P: O B S E R V A T I O N
 C: P D G O V V V K W U

e. The values from these two assumptions are inserted in a reconstruction matrix, yielding the following:

Plain

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A							G				K										V					
B																					D					
C				L														R								
D																										
E				D																	O					
F																										
G																										
H																										
I																										
J																										
K																										
L																										
M																										
N	N	B																								
O																										
P				P																						
Q																										
R																										
S	S				J																					
T				G																						
U																										
V	V																									
W																										
X																										
Y																										
Z																										

FIGURE 56a

On the hypothesis of direct symmetry of position, we are able to amalgamate the values in the square into a nearly complete sequence, as shown by the fragmentary matrix below (the derived letters are in lower case):

		Plain																										
		A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	
Key	A	a	d	j	u	s		t	i	n	G	b	c		K	l		o	p	V	w	y	r	e				
	B	b	c					l	o	p		v	w					r	e	D	j	u		i	n			
	C	c			L				o	p		v	w				R	e		d	j	u			i	n		b
	D	d																										
	E	e	D																		o							
	F	f																										
	G	g																										
	H	h														W					R							
	I	i																										
	J	j																										
	K	k																										
	L	l																										
	M	m																										
	N	n	B													W												
	O	o	P													U												
	P	p																										
	Q	q																										
	R	r				J																			V			
	S	s				G															Y							
	T	t									K																	
	U	u																										
	V	v																										
	W	w																										
	X	x																										
	Y	y																										
	Z	z																										

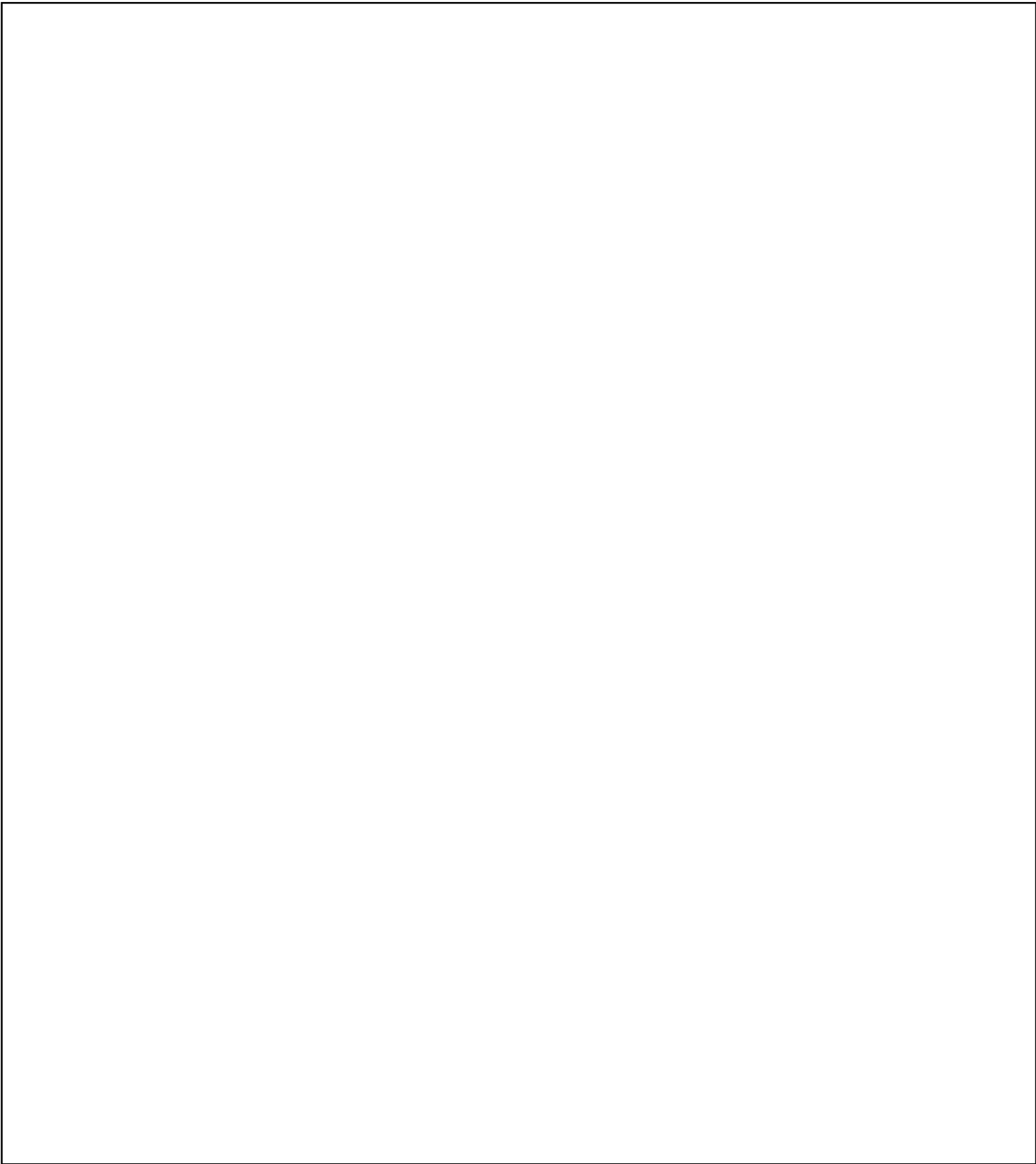
FIGURE 56b

The keyword-mixed sequence is apparent, and the original components must be the following:

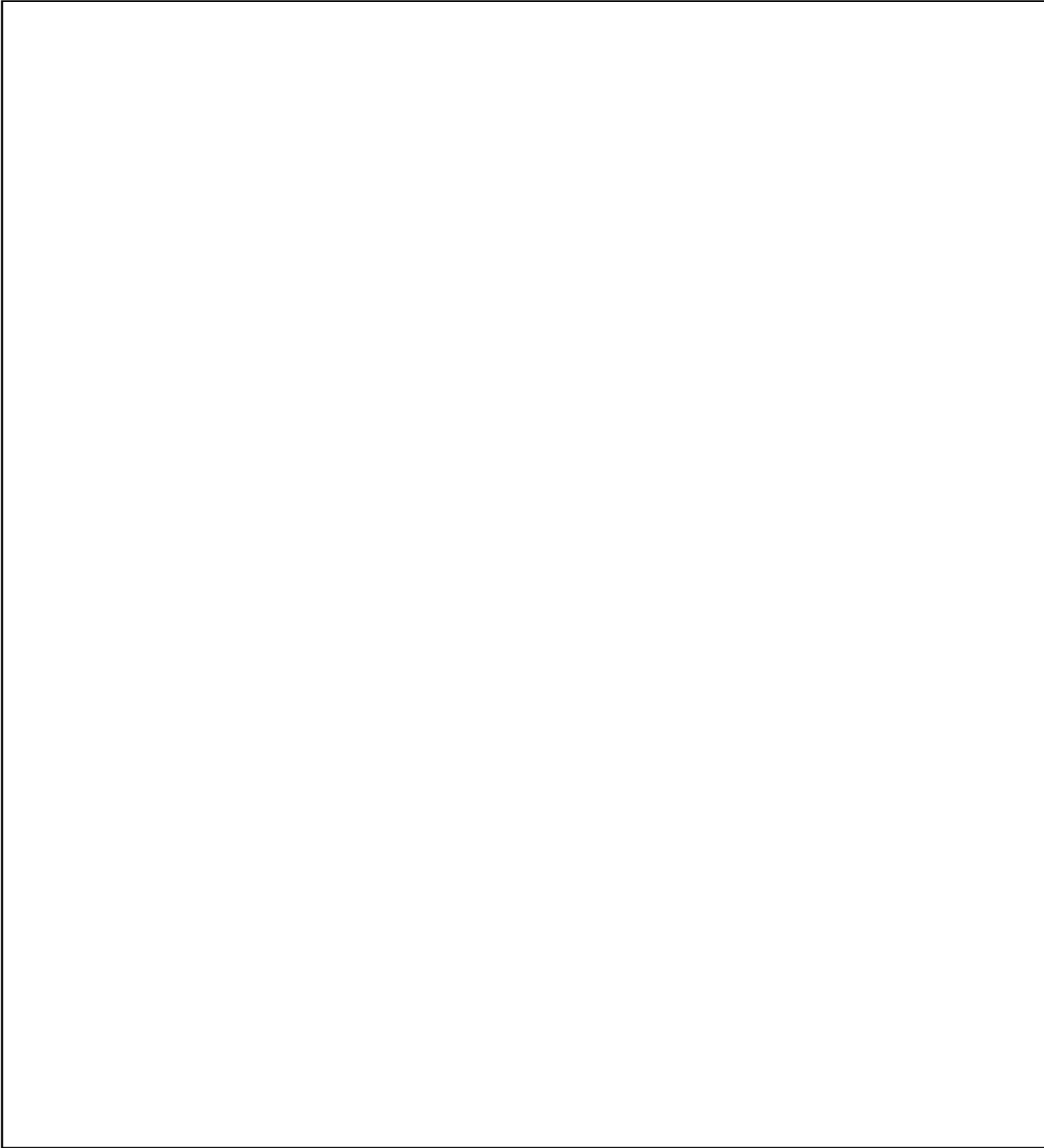
P: A B C D E F G H I J K L M N O P Q R S T U V W X Y Z
 C: R E A D J U S T I N G B C F H K L M O P Q V W X Y Z

With the primary components at hand, solution of the messages is now a trivial matter. The messages are found to have initial keys of R, L, and W, respectively.

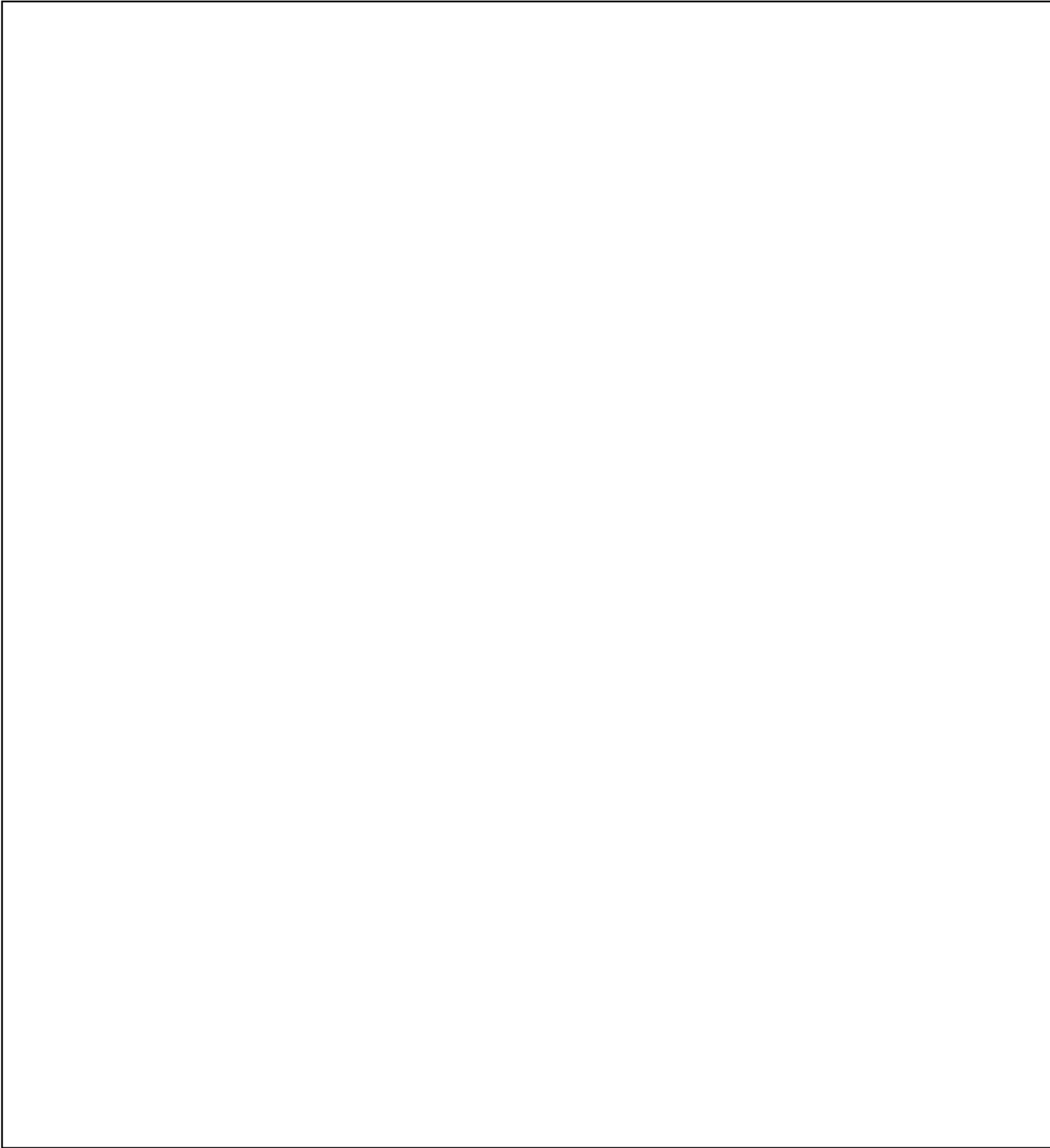
f. The foregoing example used an unknown mixed cipher component sliding against what was first assumed (and later proved) to be the normal sequence. When both primary components are unknown mixed sequences but are identical, solution is more difficult, naturally, because the results of assuming values for repetitions cannot be proved and established so quickly as in the foregoing example; if the primary components are two different unknown mixed sequences, the problem becomes even more difficult. Nevertheless, the general method indicated, and the application of the principles of indirect symmetry of position will lead to solution, if there is an adequate amount of text available for study. When the introductory key consists of several letters, repetitions are much reduced and the difficulty of solution is considerable but by no means insurmountable. Under operational conditions, the inevitable cribs, collateral information, isologs, and compromised plain text, make analysis even of difficult plain-text autokey systems practicable.



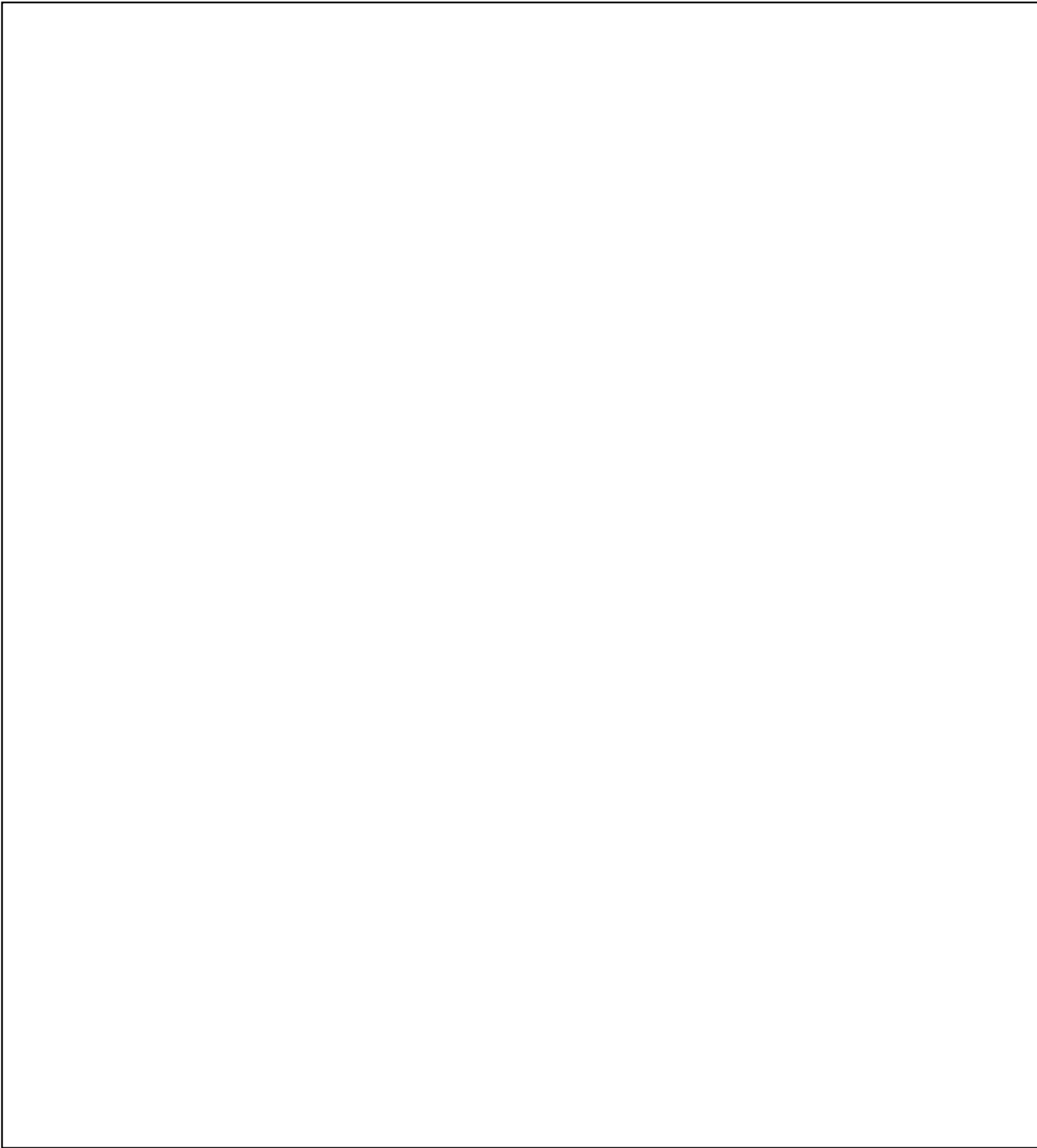
(b) (1)
(b) (3)-18 USC 798
(b) (3)-50 USC 3024(i)
(b) (3)-P.L. 86-36



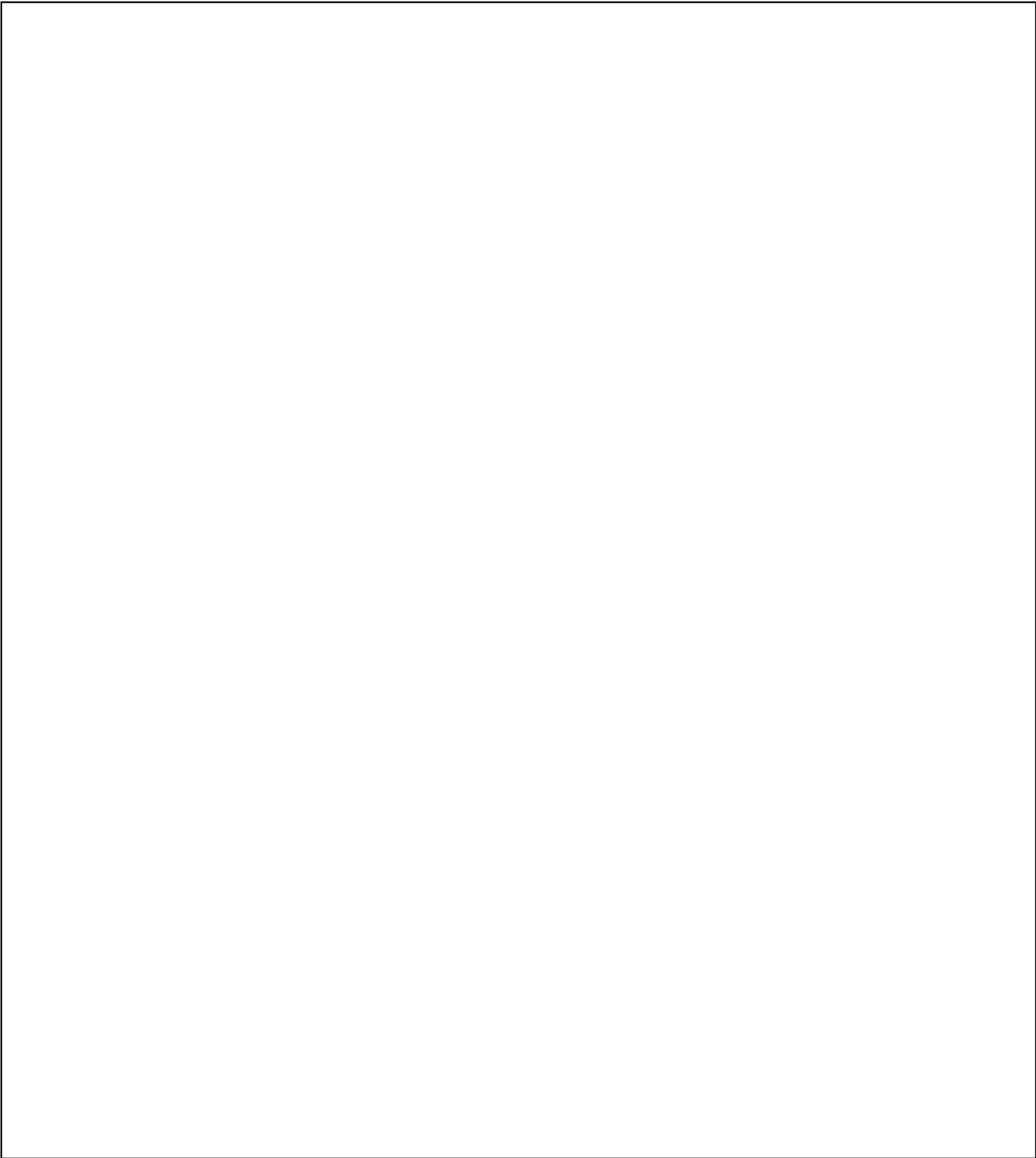
(b) (1)
(b) (3) -18 USC 798
(b) (3) -50 USC 3024 (i)
(b) (3) -P.L. 86-36



(b) (1)
(b) (3)-18 USC 798
(b) (3)-50 USC 3024(i)
(b) (3)-P.L. 86-36



(b) (1)
(b) (3)-18 USC 798
(b) (3)-50 USC 3024(i)
(b) (3)-P.L. 86-36



(b) (1)
(b) (3)-18 USC 798
(b) (3)-50 USC 3024(i)
(b) (3)-P.L. 86-36

(b) (1)
(b) (3)-18 USC 798
(b) (3)-50 USC 3024 (i)
(b) (3)-P.L. 86-36

34. Analysis of digital plaintext autokey systems.—a. In digital plaintext autokey systems wherein the nature of the intermediate text is known, the methods of solution are identical with those of literal plaintext autokey systems involving known components. As an illustration, let us assume that it is known that the enemy is using plaintext autokey systems with one-digit introductory keys, in conjunction with the following variant matrix for producing the intermediate text:

		6	7	8	9	0
		1	2	3	4	5
6	1	A	B	C	D	E
7	2	F	G	H	I	K
8	3	L	M	N	O	P
9	4	Q	R	S	T	U
0	5	V	W	X	Y	Z

The encipherment of the word REGIMENTAL, for example, could then take on the following form:

R E G I M E N T A L
47 15 22 79 82 60 33 94 16 81

This intermediate text, when subjected to additive encipherment by the plaintext autokey method with the introductory key 4, would yield the following cipher text:

K: 4 4 7 1 5 2 2 7 9 8 2 6 0 3 3 9 4 1 6 8
P: 4 7 1 5 2 2 7 9 8 2 6 0 3 3 9 4 1 6 8 1
C: 8 1 8 6 7 4 9 6 7 0 8 6 3 6 2 3 5 7 4 9

Now if a message beginning with the groups 81867 49670 86362 35749 . . . were intercepted, the simplest procedure would be to make a trial "decipherment," and then complete the plain-component sequence down the columns in alternate directions. First, the "decipherment" with an arbitrary key of \emptyset :

K: 0 8 3 5 1 6 8 1 5 2 8 0 6 7 9 3 0 5 2 2
C: 8 1 8 6 7 4 9 6 7 0 8 6 3 6 2 3 5 7 4 9 . . .
8 3 5 1 6 8 1 5 2 8 0 6 7 9 3 0 5 2 2 7

Next, in Fig. 59, below, we show this decipherment, together with the generatrices formed from this first decipherment by running down the normal numerical sequence in the odd columns, and down the reversed normal sequence in the even columns;¹² the generatrix marked with an asterisk is the original plain text, which will decipher as "REGIMENTAL" with the known matrix.

K: 0 8 3 5 1 6 8 1 5 2 8 0 6 7 9 3 0 5 2 2
C: 8 1 8 6 7 4 9 6 7 0 8 6 3 6 2 3 5 7 4 9 . . .
P: 8 3 5 1 6 8 1 5 2 8 0 6 7 9 3 0 5 2 2 7
9 2 6 0 7 7 2 4 3 7 1 5 8 8 4 9 6 1 3 6
0 1 7 9 8 6 3 3 4 6 2 4 9 7 5 8 7 0 4 5
1 0 8 8 9 5 4 2 5 5 3 3 0 6 6 7 8 9 5 4
2 9 9 7 0 4 5 1 6 4 4 2 1 5 7 6 9 8 6 3
3 8 0 6 1 3 6 0 7 3 5 1 2 4 8 5 0 7 7 2
*4 7 1 5 2 2 7 9 8 2 6 0 3 3 9 4 1 6 8 1
5 6 2 4 3 1 8 8 9 1 7 9 4 2 0 3 2 5 9 0
6 5 3 3 4 0 9 7 0 0 8 8 5 1 1 2 3 4 0 9
7 4 4 2 5 9 0 6 1 9 9 7 6 0 2 1 4 3 1 8

FIGURE 59

¹² Since additive encipherment is really a digital Vigenère system with direct standard (numerical) alphabets, the cryptanalytic treatment must be identical to that of its literal counterpart. (See also subpar. 35g on subtractive and minuend methods.)

b. If the general nature of the intermediate text is known but the introductory key consists of an unknown number of digits, generatrix diagrams (similar to those employed in the analysis of literal plaintext autokey systems) for the various possibilities of key lengths would enable the cryptanalyst

	9	4	8	1	2	7	6	5	0	3
-	R	E	P	U	B	L	I	C		
0	A	D	F	G	H	J	K	M	N	O
3	Q	S	T	V	W	X	Y	Z		

to effect a speedy solution. As an example, let us suppose we know that the enemy is using the monome-dinome matrix shown above for his intermediate text, in conjunction with additive-enciphered plaintext autokey and introductory keys of varying lengths, and that the following cryptogram is at hand:

```

0 4 1 6 6 9 4 5 0 3 9 6 3 4 3 3 6 2 4 3 9 4 7 7 0 4 4 8 1 3
3 5 0 7 3 4 8 8 9 0 0 4 2 6 5 6 4 8 3 9 2 3 7 3 4 9 4 3 3 3
4 8 9 3 4 0 8 3 0 1 2 5 0 7 7 7 4 0 0 5 4 6 2 8 8 9 2 1 3 4
8 4 3 1 1 5 5 0 3 5

```

Assumptions of introductory key-lengths of 1, 2, 3, and 4 are tried, without success. On assuming a trial length of 5, we take every fifth digit of the cipher text, starting with the first, and subject these digits to a plaintext autokey decipherment with, say, an arbitrary initial key digit of \emptyset . From these "decipherments" we complete the plain-component sequence down the columns in alternate directions, as shown in Fig. 60a, below:

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
K:	0	0	9	0	3	6	8	5	9	1	5	7	2	2	8	4	3	1	8	0
C:	0	9	9	3	9	4	3	4	0	6	2	9	4	0	2	7	4	9	8	5
P:	0	9	0	3	6	8	5	9	1	5	7	2	2	8	4	3	1	8	0	5
	1	8	1	2	7	7	6	8	2	4	8	1	3	7	5	2	2	7	1	4
	2	7	2	1	8	6	7	7	3	3	9	0	4	6	6	1	3	6	2	3
	3	6	3	0	9	5	8	6	4	2	0	9	5	5	7	0	4	5	3	2
	4	5	4	9	0	4	9	5	5	1	1	8	6	4	8	9	5	4	4	1
	5	4	5	8	1	3	0	4	6	0	2	7	7	3	9	8	6	3	5	0
	6	3	6	7	2	2	1	3	7	9	3	6	8	2	0	7	7	2	6	9
	7	2	7	6	3	1	2	2	8	8	4	5	9	1	1	6	8	1	7	8
	8	1	8	5	4	0	3	1	9	7	5	4	0	0	2	5	9	0	8	7
	9	0	9	4	5	9	4	0	0	6	6	3	1	9	3	4	0	9	9	6

FIGURE 60a

Since it is difficult to recognize "plain text" when we have it, we shall have to resort to statistical recognition and weight the generatrices, using the following log weights computed for the intermediate text produced by this particular monome-dinome matrix:¹³

Plaintext digit: 0 1 2 3 4 5 6 7 8 9
Log weight: 9 1 1 8 7 1 3 0 5 5

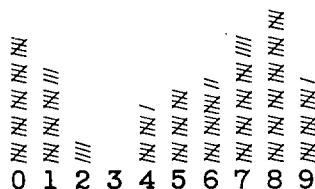
¹³ The computation of these log weights is shown in subpars. 87b and c (on pp. 246-248) of *Military Cryptanalytics, Part II*.

The δ I.C. is $\frac{10(4726)}{160 \times 159} = 1.89$, a high figure, certainly,¹⁴ but one which must be compared with the I.C.'s of the other possible decipherments in order to be able to evaluate its significance.

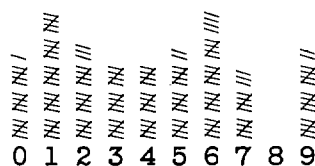
d. The first 30 digits of the next four decipherments, on the basis of plaintext 1, 2, 3, and 4 for the first cipher digit, are shown in Fig. 61, below,¹⁵ followed by their appertaining distributions:

K:	1 6 8 8	8 6 0 7 0	6 8 7 1 5	8 8 9 5 9	7 0 5 8 8	0 6 1 7 2	
C:	4 7 4 6 6	4 6 7 7 6	4 5 8 6 3	6 7 4 4 6	7 5 3 6 8	6 7 8 9 7	...
P:	① 6 8 8 8	6 0 7 0 6	8 7 1 5 8	8 9 5 9 7	0 5 8 8 0	6 1 7 2 5	
			* * * * *				
K:	2 5 9 7	9 5 1 6 1	5 9 6 2 4	9 7 0 4 0	6 1 4 9 7	1 5 2 6 3	
C:	4 7 4 6 6	4 6 7 7 6	4 5 8 6 3	6 7 4 4 6	7 5 3 6 8	6 7 8 9 7	...
P:	② 5 9 7 9	5 1 6 1 5	9 6 2 4 9	7 0 4 0 6	1 4 9 7 1	5 2 6 3 4	
			* * * * *				
K:	3 4 0 6	0 4 2 5 2	4 0 5 3 3	0 6 1 3 1	5 2 3 0 6	2 4 3 5 4	
C:	4 7 4 6 6	4 6 7 7 6	4 5 8 6 3	6 7 4 4 6	7 5 3 6 8	6 7 8 9 7	...
P:	③ 4 0 6 0	4 2 5 2 4	0 5 3 3 0	6 1 3 1 5	2 3 0 6 2	4 3 5 4 3	
			* * * * *				
K:	4 3 1 5	1 3 3 4 3	3 1 4 4 2	1 5 2 2 2	4 3 2 1 5	3 3 4 4 5	
C:	4 7 4 6 6	4 6 7 7 6	4 5 8 6 3	6 7 4 4 6	7 5 3 6 8	6 7 8 9 7	...
P:	④ 3 1 5 1	3 3 4 3 3	1 4 4 2 1	5 2 2 2 4	3 2 1 5 3	3 4 4 5 2	

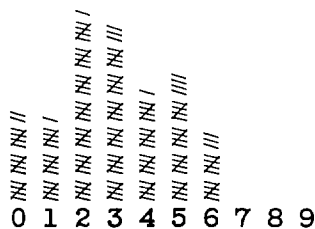
FIGURE 61



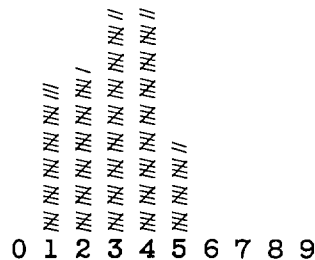
Base 1 $\delta=1.25$



Base 2 $\delta=1.11$



Base 3 $\delta=1.56$

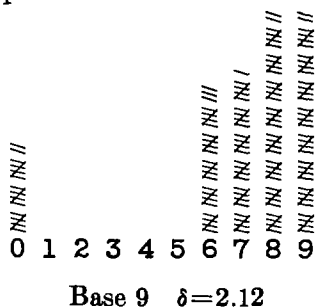
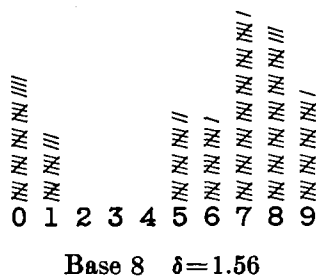
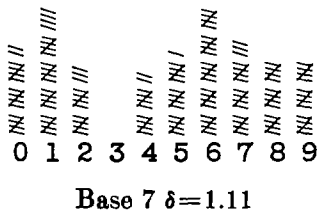
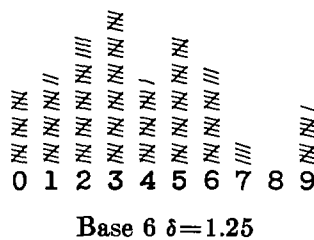
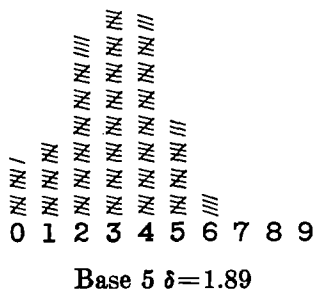


Base 4 $\delta=2.12$

¹⁴ If we had bothered to take an I.C. of the over-all cipher text, we would have found it to be 1.81; therefore the figure of 1.89 hardly reflects anything rougher than the original ciphertext population.

¹⁵ Note that it would be simpler to generate the next four decipherments by means of a generatrix diagram such as that shown in Fig. 59; the example here is for the purpose of pedagogical clarity.

e. If we had made five more decipherments on the basis of plaintext digits 5, 6, 7, 8, and 9 as the equivalents for the first cipher digit, we would have obtained the following distributions:

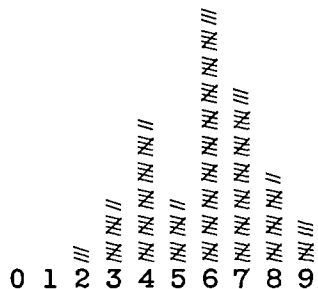


Note that the distribution for base 5 is identical with that of base 0, except for a slide of 5; the distribution for base 6 is identical with that of base 1 (except for the slide of 5), and so on to the distribution for base 9 which is identical with that of base 4, with a slide of 5.¹⁶ This means that we may dispense with the last 5 decipherments, since we can derive their distributions artificially from the first 5 distributions.

f. The greatest roughness is displayed by the distributions based on 4 or 9 as the initial plaintext digit; the problem may now be solved on either base, but the initial plaintext 4 seems, from the limitation of the span of digits 1-5, the more likely base. A dinomic distribution is made of the intermediate text, and it is quickly discovered that it is produced by a 5 x 5 square containing the normal sequence (I=J), with the digits 1 through 5 in normal order as the coordinates;¹⁷ the first two words are found to read "SECOND REGIMENT."

¹⁶ This phenomenon is a result of the mod-10 arithmetic involved; the explanation can be seen more clearly upon examination of rows five apart in Fig. 59.

¹⁷ This is the square employed in the classic Nihilist system (cf. par. 81 of *Military Cryptanalytics, Part II*); the fact that we were faced with a Nihilist system could have been surmised from the distributional appearance of the original cipher text:



g. For the last example we shall consider the case of an unknown type of intermediate text coupled with an unknown length of introductory key.¹⁸ The message under study is given below:

```

1 8 4 4 5 7 3 4 4 9 9 7 0 1 6 4 4 8 0 1 9 8 8 6 6 7 0 8 8 2
9 0 8 4 8 8 3 6 1 5 2 2 4 3 0 4 0 0 1 7 4 3 0 6 7 7 8 0 6 0
3 6 4 0 7 8 3 9 9 5 4 1 4 6 1 1 7 1 4 5 2 4 3 1 1 1 3 6 0 5
0 3 3 9 6 2 4 8 0 1 9 8 8 8 3 8 3 1 1 4 2 1 4 6 2 0 8 4 1 6
2 0 2 1 7 7 8 0 7 0 5 7 6 8 4 3 8 7 2 1 8 9 3 7 6 3 1 0 0 3
0 3 2 7 8 0 2 3 2 3 6 0 3 9 7 4 8 0 4 0 0 1 7 4 6 3 2 4 4 6
7 2 1 7 6 2 8 4 5 9 2 4 7 8 0 2 3 7 3 4 0 2 3 7 0 3 1 8 3 7
3 5 1 9 8 3 6 5 4 6 1 8 9 3 7 6 3 1 0 0 2 9 4 6 8 4 4 0 3 7
4 8 5 0 9 5 0 3 6 9 0 4 4 2 4 8 0 6 7 7 1 2 6 5 0 8 7 4 6 6
7 9 7 6 5 4 3 6 3 6 8 8 7 0 0 9 6 6 7 7 0 8 8 8 9 1 4 2 3 0
9 1 3 7 4 0 3 8 7 4 9 9 5 4 8 5 7 9 5 7 8 8 8 3 2 9 5 0 4 2
1 5 3 0 1 3 9 8 9 1 1 5 9 3 7 8 0 4 0 0 1 7 4 6 3 2 0 5 4 5
8 6 3 1 8 6 6 0 0 7 8 3 3 6 3 8 3 3 6 4 3 7 1 4 4 7 4 3 9 0
4 8 7 6 6 0 6 6 9 6 5 0 1

```

As in the previous example, we begin by assuming an arbitrary plaintext \emptyset for the first cipher digit, at an offset of 1; the decipherment of the first 30 digits and the distribution for the entire decipherment are shown below:

```

K: 0 8 6 8 7 0 3 1 3 6 3 4 6 5 1 3 1 7 3 8 1 7 1 5 1 6 4 4 4
C: 1 8 4 4 5 7 3 4 4 9 9 7 0 1 6 4 4 8 0 1 9 8 8 6 6 7 0 8 8 2 . . .
P: 0 8 6 8 7 0 3 1 3 6 3 4 6 5 1 3 1 7 3 8 1 7 1 5 1 6 4 4 4 8

```

```

      /
     //
    ///
   ////
  /////
 ////
///
//
/
0 1 2 3 4 5 6 7 8 9

```

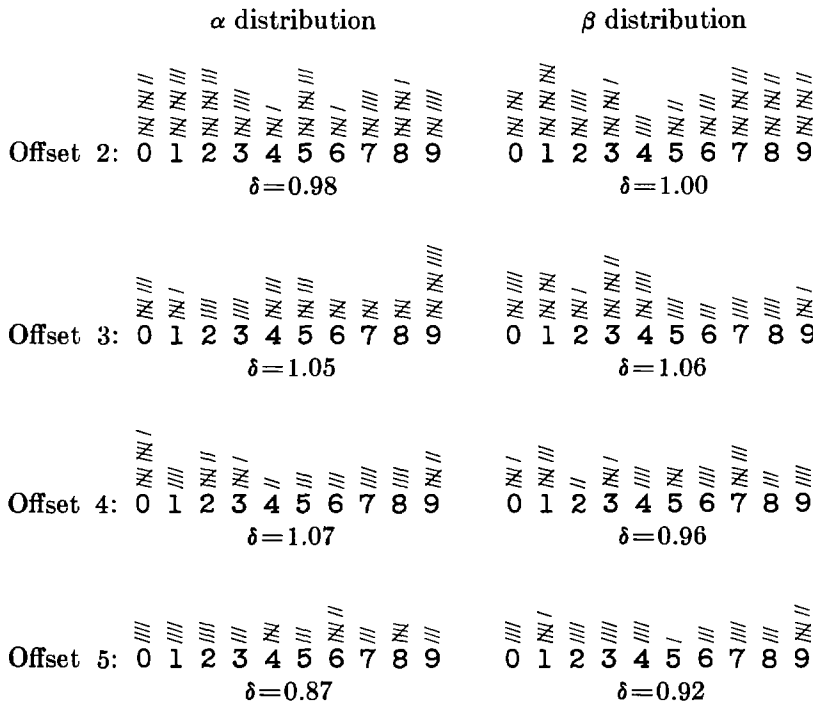
¹⁸ The analysis of digital plaintext autokey systems when the length of the introductory key and the properties of the underlying plain text are unknown, previously considered impossible, was first published in an article ("The Analysis of Digital Plaintext Autokey Systems") by the author in the *NSA Technical Journal*, Vol. XIV, No. 2 (Spring 1969).

h. The δ I.C. is $\frac{10(16,330)}{403 \times 402} = 1.01$ when \emptyset is taken as the equivalent of the first cipher digit; assumptions of 1, 2, 3, and 4 also give I.C.'s hovering near the random expectancy of 1.00. The conjecture is made that, at an incorrect offset, the deciphered text will display the I.C. of random, regardless of the base of the decipherment. Decipherments on a base of \emptyset for offsets of 2, 3, 4, and 5 are now made; Fig. 62, below, shows the "1st alphabet" of these decipherments:

K:	0	4	1	2	2	7	3	3	1	9	0	8	8	2
C: 1 8	4 4	5 7	3 4	4 9	9 7	0 1	6 4	4 8	0 1	9 8	8 6	6 7	0 8	8 2 . . .
P: 0	4	1	2	2	7	3	3	1	9	0	8	8	2	6
	* * * * *													
K:	0	4	9	0	0	4	6	2	4					
C: 1 8 4	4 5 7	3 4 4	9 9 7	0 1 6	4 4 8	0 1 9	8 8 6	6 7 0	8 8 2					
P: 0	4	9	0	0	4	6	2	4	4					
	* * * * *													
K:	0	5	9	1	3	6	0							
C: 1 8 4 4	5 7 3 4	4 9 9 7	0 1 6 4	4 8 0 1	9 8 8 6	6 7 0 8	8 2 . . .							
P: 0	5	9	1	3	6	0	8							
	* * * * *													
K:	0	7	2	2	7									
C: 1 8 4 4 5	7 3 4 4 9	9 7 0 1 6	4 4 8 0 1	9 8 8 6 6	7 0 8 8 2									
P: 0	7	2	2	7	0									

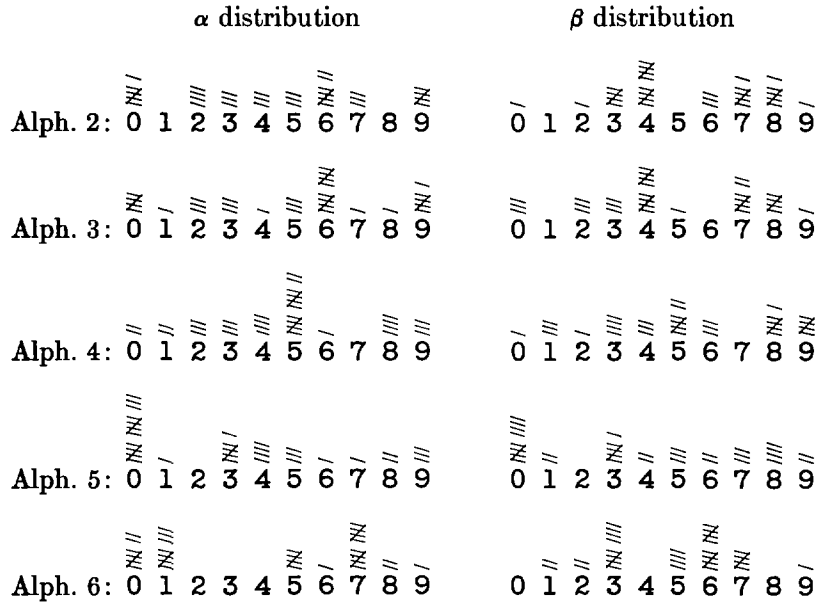
FIGURE 62

The digits of these decipherments are allocated into two distributions, α for the digits in the odd positions, and β for the digits in the even positions; thus, for offset 2, above, the digits 01231 . . . are tallied into the α distribution, while the digits 42739 . . . are tallied into the β distribution.¹⁹ These distributions, together with their I.C.'s are shown below:



¹⁹ Two distributions, rather than amalgamation into one, are necessary to compensate for the mechanics of the system, and to facilitate the establishment of the correct base.

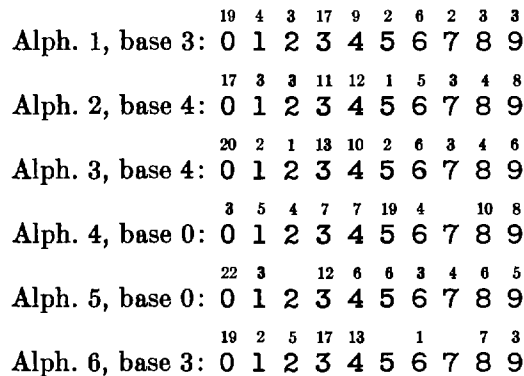
j. Since we know the correct offset, 6, we now make the α and β distributions for the remaining "alphabets" on a base of 0, as are shown below:



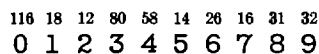
The ξ I.C.'s of these distributions on the various bases are shown in the diagram below:

	Base 0	Base 1	Base 2	Base 3	Base 4
Alph. 2:	0.88	1.05	1.27	0.62	1.41
Alph. 3:	0.57	1.12	1.17	0.69	1.69
Alph. 4:	1.43	0.63	1.16	1.01	0.90
Alph. 5:	1.70	0.63	0.87	0.91	0.91
Alph. 6:	0.86	1.10	0.62	1.91	1.05

From these data it may be inferred that the correct bases for alphabets 2-6 are 4, 4, 0, 0, and 3, respectively. We can thereupon combine the α and β distributions for the correct offsets for each alphabet, as displayed below:



It is now also clear that the distribution for alph. 4 should be shifted 5 positions to be on base 5 (which is congruent to 0, mod 5), in order to make it match with the other distributions. When this is done, the cumulative total distribution is as follows:



The I.C. of the combined distributions is $\frac{10(26,398)}{403 \cdot 402} = 1.63$, which, for this size of sample, would reflect fairly accurately the theoretical I.C. of the underlying intermediate text.²⁰

k. The first six plaintext digits are 344503 (which we have determined from the bases for the six alphabets), so we can reduce the cipher text to monoalphabetic terms, as shown in the beginning fragment below:

	5	10	15	20	25	30																								
K:	8	4	0	9	5	4	3	4	4	5	0	3	0	0	4	9	4	0	1	6	0	5	4	0	0	3	8	3	2	
C:	1	8	4	4	5	7	3	4	4	9	9	7	0	1	6	4	4	8	0	1	9	8	8	6	6	7	0	8	8	2
P:	3	4	4	5	0	3	0	0	0	4	9	4	0	1	6	0	5	4	0	0	3	8	3	2	6	7	7	0	5	0

When the entire text has been reduced to monoalphabetic terms, it is easily diagnosed as a monome-dinome cipher, and solution proceeds with alacrity and celerity. The opening words are "SECOND REGIMENT" and the monome-dinome matrix is reconstructed as the following:

	9	4	8	1	2	7	6	5	0	3	
-	R	E	P	U	B	L	I	C			
0	A	D	F	G	H	J	K	M	N	O	
3	Q	S	T	V	W	X	Y	Z			

As the final step in the solution, the initial key digits 840954 are subjected to scrutiny, and it is discovered that the introductory key is based upon the key word PEACE enciphered through the matrix.

l. The foregoing problem involved what at first blush appeared to be a very complex situation: a six-digit introductory key happened to have been used, and it could have been reasoned that, since there are 10⁶ different 6-digit numbers, a maximum of 1,000,000 trials²¹ with the aid of a computer might be necessary in order to establish the correct introductory key (if the key length were *known*). Instead of these million trials, however, we had to make only 6 trials to arrive at the correct key-length, and 5 more trials to establish the bases for alphabets 2-6.

35. **Concluding remarks on autokey systems.**—a. The plaintext autokey systems treated in this chapter involved those employing sliding primary components, and therefore having related secondary alphabets. As with ciphertext autokey systems, there is no reason why a table of 26 random, unrelated alphabets could not be used, such as that illustrated in Fig. 33 on p. 70. The problem of cryptanalysis in such a case becomes considerably more difficult, naturally, since we do not have the advantage of the exploitation of symmetry of position; nevertheless, as indicated in subpar. 32f, under operational conditions the inevitable cribs, collateral information, isologs, and compromised plain text make analysis even of difficult plaintext autokey systems practicable.

b. Ciphertext and plaintext autokey systems display characteristics which permit their diagnosis. Both cases will show repetitions in the cipher text. In ciphertext autokey systems there will be far fewer repetitions than in the original plain text, especially when introductory keys of more than one letter in length are employed; in plaintext autokey systems there will be nearly as many repetitions in the cipher text as in the original plain text unless long introductory keys are used. In either system the repetitions will show no constancy as regards intervals between them. Ciphertext autokey systems may be distinguished from plaintext autokey by the appearance of the frequency distribution of the second member of sets of two letters separated by the length of the introductory key (see subpar. 23e)—in the case of ciphertext autokey these frequency distributions will be monoalphabetic; in plaintext autokey systems such frequency distributions will not show monoalphabetic characteristics. Ciphertext autokey traffic should be replete with isomorphs; on the other hand, causal isomorphs cannot occur in plaintext autokey systems.

²⁰ The theoretical γ I.C. is in fact 1.63. (See also subpar. 89b on pp. 261-262 of *Military Cryptanalytics, Part II.*)

²¹ Actually, only 999,990 trials, since we exclude the ten trivial cases wherein all the key digits are identical. This results in cutting down the work by a factor of one one-hundred-thousandth.

c. Whereas the expected I.C. of ciphertext autokey traffic is 1.00 (i.e., random), the I.C. of plaintext autokey will show a measurable departure from random. The "bulge" (i.e., the excess over 1.00) of the over-all I.C. may be calculated by the formula $\beta_c = \frac{\beta_k \times \beta_p}{c-1}$, where β_c is the bulge of the cipher text, β_p the bulge of the plain text (= .73), β_k the bulge of the key (which, since the key text is plain text, is also .73), and c is the number of categories (in this case, 26). Thus the expected bulge of plaintext autokey traffic, without regard to the identity of the components involved, is $\frac{.73 \times .73}{25} = .0213$, so the I.C. is 1.02 in the general case.

d. Where the components are known sequences, it is possible to establish the theoretical distribution for the ciphertext letters as well as the I.C. of the specific case. For example, in the case of direct standard alphabets, we would first construct a *deciphering* square (shown in fragmentary form in Fig. 63b, below) from the normal enciphering form (Fig. 63a) of the Vigenère square; we then replace the key letters and the plaintext letters within the deciphering square by their relative frequencies (per thousand letters) in

Plain	
	A B C D E
A	A B C D E
B	B C D E F
C	C D E F G
D	D E F G H
Key E	E F G H I
~~~~~	
X	X Y Z A B
Y	Y Z A B C
Z	Z A B C D

FIGURE 63a

Cipher	
	A B C D E
A	A B C D E
B	Z A B C D
C	Y Z A B C
D	X Y Z A B
Key E	W X Y Z A
~~~~~	
X	D E F G H
Y	C D E F G
Z	B C D E F

FIGURE 63b

Cipher		A	B	C	D	E
A	74	74	10	31	42	130
B	10	1	74	10	31	42
C	31	19	1	74	10	31
D	42	5	19	1	74	10
Key E	130	16	5	19	1	74
~~~~~						
X	5	42	130	28	16	34
Y	19	31	42	130	28	16
Z	1	10	31	42	130	28

FIGURE 63c

English plain text ²² (Fig. 63c), and we multiply the entries in each row by the key-letter value for that row. ²³ Since the square is a deciphering square, the sum of the entries in each column will represent the relative frequencies of the *cipher* letters associated with the columns. For example, it will be found that the sum of the cross-multiplied values in the "A" column is 40,467, and that of the "B" column, 35,314; these of course represent frequencies per 1000² or 1,000,000 letters. The relative frequencies, reduced to a base of 1000 letters, are shown below:

A	40.5	G	45.9	L	41.4	Q	30.9	V	51.7
B	35.3	H	41.8	M	43.5	R	47.2	W	47.3
C	31.6	I	50.5	N	30.1	S	42.2	X	40.8
D	25.0	J	30.1	O	28.0	T	41.4	Y	31.5
E	47.5	K	35.8	P	34.3	U	30.4	Z	35.4
F	39.2								999.3

²² Since the relative frequencies shown are frequencies per thousand, what we have in effect are the probabilities of the letters to three decimals. For reference, the probabilities of English plaintext letters to four decimals are as follows:

A	.0737	G	.0164	L	.0364	Q	.0035	V	.0153
B	.0097	H	.0339	M	.0247	R	.0758	W	.0156
C	.0307	I	.0735	N	.0795	S	.0612	X	.0046
D	.0424	J	.0016	O	.0753	T	.0919	Y	.0193
E	.1300	K	.0030	P	.0267	U	.0260	Z	.0010
F	.0283								1.0000

²³ In the actual computation, a pair of strips bearing the letter frequencies was used, as an equivalent of the bulkier table.

The sum of the squares of the probabilities of these cipher letters is found to be .0398; therefore the theoretical I.C. of plaintext autokey cipher with direct standard alphabets is  $26(.0398) = 1.0348$ .

e. By a similar process, the theoretical ciphertext distribution and the I.C. of plaintext autokey using reversed standard alphabets may be determined. The distribution, expressed in frequencies per 1000, is found to be as follows:²⁴

A	66.9	G	34.8	L	45.4	Q	37.7	V	34.4
B	39.9	H	33.9	M	37.3	R	38.1	W	44.1
C	34.1	I	31.3	N	46.7	S	31.3	X	32.1
D	32.1	J	38.1	O	37.3	T	33.9	Y	34.1
E	44.1	K	37.7	P	45.4	U	34.8	Z	39.9
F	34.4								999.8

The sum of the squares of the probabilities here too is .0398, so the I.C. of reversed standard alphabets is the same as that for direct standard alphabets, namely, 1.0348.

f. The foregoing theoretical ciphertext distributions may be used in matching operations for testing samples of cipher text for possibility of encipherment by plaintext autokey with direct or reversed standard alphabets. For a quick test to determine whether a plaintext autokey system involves direct standard alphabets, we note (in subpar. d, above) that the cumulative frequencies of the highest four cipher letters, VIER, sum to 197, and that the cumulative frequencies of the lowest four letters, JNOD, sum to 113; the ratio of 197 to 113, or 1.7, compared with the random expectancy of 1.0, is indicative that direct standard alphabets may have been used. Similarly, for a quick test to determine whether a plaintext autokey system involves reversed standard alphabets, we observe (in subpar. e) that the frequencies of the four highest letters, ANLP, sum to 204, and that the frequencies of the four lowest, DXIS, sum to 127; the ratio of 204 to 127, or 1.6, compared with the expectancy for random of 1.0, may be employed to establish the use of reversed standard alphabets. (Note that the indices 1.7 and 1.6 will obtain in these situations, regardless of the lengths of the introductory keys, or whether the traffic consists of messages in the same introductory key or in many different keys.)

g. The digital plaintext autokey systems illustrated in par. 36 all involved the *additive* method in their encipherment, wherein  $P+K=C$ . It was stated in the preceding volume²⁵ that an additive system may also be solved as a *subtractive* system (i.e., wherein  $P-K=C$ ) or as a *minuend* system (i.e., wherein  $K-P=C$ ), and that any one of these may be solved as either of the other two. Although this is true in the general cases of numerical polyalphabetic substitution, it is not true in the case of plaintext autokey systems: here an additive system can only be solved as an additive system, but a subtractive system may be solved as a minuend system, and a minuend system solved as a subtractive system, as is about to be demonstrated.

(1) Let us consider three different encipherments of the same intermediate plain text by plaintext autokey and with the same 1-digit introductory key, first by the additive method (Fig. 64a), then by the subtractive method (Fig. 64b), and finally by the minuend method (Fig. 64c):

<i>Additive encipherment</i>	<i>Subtractive encipherment</i>	<i>Minuend encipherment</i>
K: 0 4 3 1 5 1 3 3 4 3	K: 0 4 3 1 5 1 3 3 4 3	K: 0 4 3 1 5 1 3 3 4 3
P: <u>4 3 1 5 1 3 3 4 3 3</u>	P: <u>4 3 1 5 1 3 3 4 3 3</u>	P: <u>4 3 1 5 1 3 3 4 3 3</u>
C: 4 7 4 6 6 4 6 7 7 6	C: 4 9 8 4 6 2 0 1 9 0	C: 6 1 2 6 4 8 0 9 1 0

FIGURE 64a

FIGURE 64b

FIGURE 64c

It will be noted that the subtractive and minuend encipherments are complementary. Now let us see what happens when the cipher text of each type of encipherment is assumed to have been produced by the additive, subtractive, and minuend methods in turn, from the standpoint of their particular generatrix diagrams.

²⁴ Note the symmetry of the distribution about A_n and N_n: the frequencies of M and O are identical, as are L and P, K and Q, etc.

²⁵ Cf. subpar. 84b on p. 238 of *Military Cryptanalytics, Part II*.

(2) First, the cipher text of Fig. 64a (the true additive encipherment), under the assumption of encipherment by the three methods, with an arbitrary  $\theta$  as the first plaintext digit:

<i>Additive trial</i>	<i>Subtractive trial</i>	<i>Minuend trial</i>
K: 0 7 7 9 7 7 9 8 9	K: 0 7 1 7 3 7 3 0 7	K: 0 3 9 3 7 3 7 0 3
C: <u>4 7 4 6 6 4 6 7 7 6</u>	C: <u>4 7 4 6 6 4 6 7 7 6</u>	C: <u>4 7 4 6 6 4 6 7 7 6</u>
P: 0 7 7 9 7 7 9 8 9 7	P: 0 7 1 7 3 7 3 0 7 3	P: 0 3 9 3 7 3 7 0 3 7
0 7 7 9 7 7 9 8 9 7	0 7 1 7 3 7 3 0 7 3	0 3 9 3 7 3 7 0 3 7
1 6 8 8 8 6 0 7 0 6	1 8 2 8 4 8 4 1 8 4	1 4 0 4 8 4 8 1 4 8
2 5 9 7 9 5 1 6 1 5	2 9 3 9 5 9 5 2 9 5	2 5 1 5 9 5 9 2 5 9
3 4 0 6 0 4 2 5 2 4	3 0 4 0 6 0 6 3 0 6	3 6 2 6 0 6 0 3 6 0
<u>4 3 1 5 1 3 3 4 3 3</u>	4 1 5 1 7 1 7 4 1 7	4 7 3 7 1 7 1 4 7 1
5 2 2 4 2 2 4 3 4 2	5 2 6 2 8 2 8 5 2 8	5 8 4 8 2 8 2 5 8 2
6 1 3 3 3 1 5 2 5 1	6 3 7 3 9 3 9 6 3 9	6 9 5 9 3 9 3 6 9 3
7 0 4 2 4 0 6 1 6 0	7 4 8 4 0 4 0 7 4 0	7 0 6 0 4 0 4 7 0 4
8 9 5 1 5 9 7 0 7 9	8 5 9 5 1 5 1 8 5 1	8 1 7 1 5 1 5 8 1 5
9 8 6 0 6 8 8 9 8 8	9 6 0 6 2 6 2 9 6 2	9 2 8 2 6 2 6 9 2 6

FIGURE 65a

FIGURE 65b

FIGURE 65c

The original plain text of course will appear on one of the generatrices of Fig. 65a, but no evidence of either it or its complement in Figs. 65b or c. Next, the cipher text of Fig. 64b (the true subtractive encipherment), under the assumption of encipherment by the three methods:

<i>Additive trial</i>	<i>Subtractive trial</i>	<i>Minuend trial</i>
K: 0 9 9 5 1 1 9 2 7	K: 0 9 7 1 7 9 9 0 9	K: 0 1 3 9 3 1 1 0 1
C: <u>4 9 8 4 6 2 0 1 9 0</u>	C: <u>4 9 8 4 6 2 0 1 9 0</u>	C: <u>4 9 8 4 6 2 0 1 9 0</u>
P: 0 9 9 5 1 1 9 2 7 3	P: 0 9 7 1 7 9 9 0 9 9	P: 0 1 3 9 3 1 1 0 1 1
0 9 9 5 1 1 9 2 7 3	0 9 7 1 7 9 9 0 9 9	0 1 3 9 3 1 1 0 1 1
1 8 0 4 2 0 0 1 8 2	1 0 8 2 8 0 0 1 0 0	1 2 4 0 4 2 2 1 2 2
2 7 1 3 3 9 1 0 9 1	2 1 9 3 9 1 1 2 1 1	2 3 5 1 5 3 3 2 3 3
3 6 2 2 4 8 2 9 0 0	3 2 0 4 0 2 2 3 2 2	3 4 6 2 6 4 4 3 4 4
4 5 3 1 5 7 3 8 1 9	<u>4 3 1 5 1 3 3 4 3 3</u>	4 5 7 3 7 5 5 4 5 5
5 4 4 0 6 6 4 7 2 8	5 4 2 6 2 4 4 5 4 4	5 6 8 4 8 6 6 5 6 6
6 3 5 9 7 5 5 6 3 7	6 5 3 7 3 5 5 6 5 5	<u>6 7 9 5 9 7 7 6 7 7</u>
7 2 6 8 8 4 6 5 4 6	7 6 4 8 4 6 6 7 6 6	7 8 0 6 0 8 8 7 8 8
8 1 7 7 9 3 7 4 5 5	8 7 5 9 5 7 7 8 7 7	8 9 1 7 1 9 9 8 9 9
9 0 8 6 0 2 8 3 6 4	9 8 6 0 6 8 8 9 8 8	9 0 2 8 2 0 0 9 0 0

FIGURE 65d

FIGURE 65e

FIGURE 65f

The original plain text will of course appear on one of the generatrices of Fig. 65c, and the complements of the true plain on one of the generatrices of the minuend trial; the additive trial yields nothing. Finally the cipher text of Fig. 64c (the true minuend encipherment), under the assumption of the three enciphering methods:

<i>Additive trial</i>	<i>Subtractive trial</i>	<i>Minuend trial</i>
K: 0 1 1 5 9 9 1 8 3	K: 0 1 3 9 3 1 1 0 1	K: 0 9 7 1 7 9 9 0 9
C: <u>6 1 2 6 4 8 0 9 1 0</u>	C: <u>6 1 2 6 4 8 0 9 1 0</u>	C: <u>6 1 2 6 4 8 0 9 1 0</u>
P: 0 1 1 5 9 9 1 8 3 7	P: 0 1 3 9 3 1 1 0 1 1	P: 0 9 7 1 7 9 9 0 9 9
0 1 1 5 9 9 1 8 3 7	0 1 3 9 3 1 1 0 1 1	0 9 7 1 7 9 9 0 9 9
1 0 2 4 0 8 2 7 4 6	1 2 4 0 4 2 2 1 2 2	1 0 8 2 8 0 0 1 0 0
2 9 3 3 1 7 3 6 5 5	2 3 5 1 5 3 3 2 3 3	2 1 9 3 9 1 1 2 1 1
3 8 4 2 2 6 4 5 6 4	3 4 6 2 6 4 4 3 4 4	3 2 0 4 0 2 2 3 2 2
4 7 5 1 3 5 5 4 7 3	4 5 7 3 7 5 5 4 5 5	<u>4 3 1 5 1 3 3 4 3 3</u>
5 6 6 0 4 4 6 3 8 2	5 6 8 4 8 6 6 5 6 6	5 4 2 6 2 4 4 5 4 4
6 5 7 9 5 3 7 2 9 1	<u>6 7 9 5 9 7 7 6 7 7</u>	6 5 3 7 3 5 5 6 5 5
7 4 8 8 6 2 8 1 0 0	7 8 0 6 0 8 8 7 8 8	7 6 4 8 4 6 6 7 6 6
8 3 9 7 7 1 9 0 1 9	8 9 1 7 1 9 9 8 9 9	8 7 5 9 5 7 7 8 7 7
9 2 0 6 8 0 0 9 2 8	9 0 2 8 2 0 0 9 0 0	9 8 6 0 6 8 8 9 8 8

FIGURE 65g

FIGURE 65h

FIGURE 65i

Here the original plain text will appear on one of the generatrices of Fig. 65i, as expected, while the complements of the true plain appear on one of the generatrices of the subtractive trial, with nothing manifested in the additive trial. In the foregoing cases, the original plain text will yield the reconstructed matrix of Fig. 66a, below, whereas the complementary plain text will yield the equivalent matrix of Fig. 66b.

	1	2	3	4	5
1	A	B	C	D	E
2	F	G	H	I	K
3	L	M	N	O	P
4	Q	R	S	T	U
5	V	W	X	Y	Z

FIGURE 66a

	9	8	7	6	5
9	A	B	C	D	E
8	F	G	H	I	K
7	L	M	N	O	P
6	Q	R	S	T	U
5	V	W	X	Y	Z

FIGURE 66b

h. Digital *ciphertext* autokey systems also have their restrictions in their analysis as regards their type of encipherment: here a subtractive system can only be solved as a subtractive system, but an additive system may be solved as a minuend system, or vice versa. As an example, let us examine three different encipherments of the same plain text by ciphertext autokey, by the additive method (Fig. 67a), the subtractive method (Fig. 67b), and the minuend method (Fig. 67c):

<i>Additive encipherment</i>	<i>Subtractive encipherment</i>	<i>Minuend encipherment</i>
K: 0 4 7 8 3 4 7 0 4 7	K: 0 4 9 2 3 8 5 8 6 7	K: 0 6 3 2 7 6 3 0 6 3
P: <u>4 3 1 5 1 3 3 4 3 3</u>	P: <u>4 3 1 5 1 3 3 4 3 3</u>	P: <u>4 3 1 5 1 3 3 4 3 3</u>
C: 4 7 8 3 4 7 0 4 7 0	C: 4 9 2 3 8 5 8 6 7 6	C: 6 3 2 7 6 3 0 6 3 0

FIGURE 67a

FIGURE 67b

FIGURE 67c

(Here it will be noted that the additive and minuend encipherments are complementary.) Now we shall see what happens when the cipher text of each case is assumed to have been produced by the additive, subtractive, and minuend methods, in turn. First, the cipher text of Fig. 67a (the true additive encipherment), under the assumption of encipherment by the three methods:

<i>Additive trial</i>		<i>Subtractive trial</i>		<i>Minuend trial</i>	
K:	4 7 8 3 4 7 0 4 7	K:	4 7 8 3 4 7 0 4 7	K:	4 7 8 3 4 7 0 4 7
C:	<u>4 7 8 3 4 7 0 4 7 0</u>	C:	<u>4 7 8 3 4 7 0 4 7 0</u>	C:	<u>4 7 8 3 4 7 0 4 7 0</u>
P:	3 1 5 1 3 3 4 3 3	P:	1 5 1 7 1 7 4 1 7	P:	7 9 5 9 7 7 6 7 7

FIGURE 68a

FIGURE 68b

FIGURE 68c

The original plain text appears in the additive trial, its complement in the minuend trial, and nothing in Fig. 68b. Next, the cipher text of Fig. 67b (the true subtractive encipherment), under the assumption of encipherment by the three methods:

<i>Additive trial</i>		<i>Subtractive trial</i>		<i>Minuend trial</i>	
K:	4 9 2 3 8 5 8 6 7	K:	4 9 2 3 8 5 8 6 7	K:	4 9 2 3 8 5 8 6 7
C:	<u>4 9 2 3 8 5 8 6 7 6</u>	C:	<u>4 9 2 3 8 5 8 6 7 6</u>	C:	<u>4 9 2 3 8 5 8 6 7 6</u>
P:	5 3 1 5 7 3 8 1 9	P:	3 1 5 1 3 3 4 3 3	P:	5 7 9 5 3 7 2 9 1

FIGURE 68d

FIGURE 68e

FIGURE 68f

Here the original plain text comes out under the subtractive trial, but nothing in Figs. 68d or f. Finally, the cipher text of Fig. 67c (the true minuend encipherment), under the assumption of encipherment by the three methods:

<i>Additive trial</i>		<i>Subtractive trial</i>		<i>Minuend trial</i>	
K:	6 3 2 7 6 3 0 6 3	K:	6 3 2 7 6 3 0 6 3	K:	6 3 2 7 6 3 0 6 3
C:	<u>6 3 2 7 6 3 0 6 3 0</u>	C:	<u>6 3 2 7 6 3 0 6 3 0</u>	C:	<u>6 3 2 7 6 3 0 6 3 0</u>
P:	7 9 5 9 7 7 6 7 7	P:	9 5 9 3 9 3 6 9 3	P:	3 1 5 1 3 3 4 3 3

FIGURE 68g

FIGURE 68h

FIGURE 68i

The original plain text here comes out under the minuend trial, its complement under the additive trial, and nothing in Fig. 68h. As before, the original plain text will yield the matrix of Fig. 66a, the complementary plain text the matrix of Fig. 66b.

CHAPTER VI

SYSTEMS EMPLOYING LONG OR CONTINUOUS KEYS

(b) (1)  
(b) (3) -18 USC 798  
(b) (3) -50 USC 3024 (i)  
(b) (3) -P.L. 86-36

Preliminary remarks.....	Paragraph 36
Depth and its exploitation.....	37
Solution of a single cryptogram involving known primary components and an unknown plaintext running key.....	38
[Redacted].....	39
[Redacted].....	40
Recovery of plain texts and the unknown primary components from a number of messages in flush depth.....	41
[Redacted].....	42
[Redacted].....	43
Additional remarks.....	44

**36. Preliminary remarks.—a.** In subpar. 1*d* it was stated that two procedures suggest themselves to cryptographers for eliminating the weaknesses introduced by periodicity of the type produced by simple, repeating-key methods. One of these, when studied, embraced some of the very simple methods of suppressing or destroying periodicity, by such devices as interrupting the key and using variable-length groupings of plain text. It was demonstrated that subterfuges of this simple nature are inadequate to eliminate the weaknesses referred to, and must be discarded in any system intended to afford real security. The other alternative alluded to in subpar. 1*d* therefore remains now to be investigated, *viz.*, that of lengthening the keys to a point where there would seem to be an insufficient amount of text to enable the cryptanalyst to solve the traffic. Attempts toward this end usually consist in extending the key to such a length that the enemy cryptanalysts will have only a very limited number of periods to work with. The key may, indeed, be lengthened to a point where it becomes as long as, or longer than, the text to be enciphered, so that the key is used only once in a message.

*b.* It is obvious that one of the simplest methods of lengthening the key to a message is to use a long phrase or even a complete sentence, provided that it is not too long to remember. In addition to the difficulties that would be encountered in practical military cryptography in selecting long mnemonic phrases and sentences which would have to be imparted to many clerks, there is the fact that the probable-word method of solution still remains as a powerful tool in the hands of the cryptanalyst. And if only a word or two of the key can be reconstructed as a result of a fortunate assumption, it might be possible that the cryptanalyst could guess the entire key from a fragment thereof, since any long phrase or sentence which is selected because it can easily be remembered is likely to be well known to many people.

*c.* There are, however, relatively simple ways of employing a short mnemonic key in order to produce a much longer key. Basically, any transposition method applied to a single alphabetic sequence repeated several times will yield a fairly long key, which, moreover, has the advantage of being unintelligible, thus approaching the appearance of a random selection of letters. For example, a numerical key may be derived from a word or a short phrase; this numerical key may then be applied as a columnar-transposition key for a rectangle within which the normal A-Z sequence has been repeated a previously agreed-upon number of times in straight horizontals starting at the upper left-hand corner, or in any other prearranged manner. The letters when transcribed from the transposition rectangle then become the successive letters for enciphering the plain text, using any desired type of primary components. Or, if a single transposition is not thought to be sufficiently secure, a double transposition will yield a still more mixed-up sequence of key letters. Other types of transposition may be employed for the purpose, including various types of geometric figures. Furthermore, some nontransposition methods of lengthening the keying sequence which at the same time introduce an irregularity, such as aperiodic interruption, have already been described (see subpar. 14*b*).

d. Another method of developing a long key from a short mnemonic one is that shown below. Given the key word CHRISTMAS, a numerical sequence is first derived and then the successive sections of this numerical key are written down, these sections terminating with the successive key numbers 1, 2, 3, . . . of the numerical key. Thus:

Mnemonic key: C H R I S T M A S  
Numerical key: 2 3 6 4 7 9 5 1 8

Extended key: C H R I S T M A ¹|²C | ³CH | ⁴CH R I | ⁵CH R I S T M | ⁶CH R | ⁷CH R I S |  
C H R I S T M A S ⁸| ⁹CH R I S T |

Thus the original key of only 9 letters is expanded to one of 45 letters (1+2+3+ . . . +9=45). The longer key is also an interrupted key of the type noted under subpar. 14a, but if the message is long enough to require several repetitions of the expanded key, the encipherment becomes periodic and can be handled by the usual methods employed in solving repeating-key ciphers. If the basic key is fairly long,¹ so that the expanded key becomes a quite lengthy sequence, then the message or messages may be handled in the manner explained in par. 19.

e. One method for producing a rather long sequence of digits for keying purposes from a single key number is to select a number whose reciprocal when converted by actual division into its equivalent decimal yields a long series of digits. For example, the reciprocal of 49, or 1/49, yields a sequence of 42 digits beginning .0204081632 . . . . Such a number, coupled with a key word like CHRISTMAS, could be used for interrupted keying, the successive cipher alphabets being used for enciphering as many letters as are indicated by the successive digits. In the case of the example cited, the first digit is 0; hence the C alphabet would not be used. The next digit is 2; the H alphabet would be used for enciphering the first and second letters. The third digit is again 0; the R alphabet would not be used. The fourth digit is 4; the I alphabet would be used for enciphering the third, fourth, fifth, and sixth letters. And so on.

f. In the case of digital cryptosystems, various methods have been used to produce an expanded key from a shorter one. Several examples will now be cited.

(1) The method in subpar. d, above, may be adapted so that from the key word CHRISTMAS the basic numerical key 236479518 is expanded into the 45-digit sequence 2 3 6 4 7 9 5 1 | 2 | 2 3 | 2 3 6 4 | 2 3 6 4 7 9 5 | 2 3 6 | 2 3 6 4 7 | 2 3 6 4 7 9 5 1 8 | 2 3 6 4 7 9. Or, this 9-digit basic key may be expanded into an 81-digit key by tying together 9 cycles of the basic key, beginning with 1 8 2 3 6 4 7 9 5 | 2 3 6 4 7 9 5 1 8 | 3 6 . . . and ending with | 9 5 1 8 2 3 6 4 7. Or, again, the 9-digit key may be expanded into a 90-digit key by adding 1 to the digits of the basic key at the end of each cycle, so that the final key will be 2 3 6 4 7 9 5 1 8 | 3 4 7 5 8 0 6 2 9 | 4 5 . . . .

(2) Another method for producing digital key is by a "Fibonacci series,"² which is a series or sequence generated by the successive addition (almost invariably mod 10, or, in certain specialized usages mod 2) of pairs or larger combinations of elements (usually adjacent), beginning with a specified initial key number. Thus, in its simplest form, if the initial key is the dinome 01, we can generate the Fibonacci sequence 0112358314 . . . , which has a cycle length of 60. If the initial key is the pentanome 00001 and the rule of combination is a+b=f (i.e., the sum of the first and second elements of the sequence

¹ For example, if the basic sequence were a 26-letter mixed sequence such as HBPYEQDFSRGTAJVKWLMXINZCO based on HYDRAULIC, then the expanded key would read

H B P Y E Q D F S R G T A ¹| ²H B | ³H B P Y E Q . . . C | H B P etc.

The length of the expanded key is the sum of the first n numbers, given by the formula  $\Sigma(n) = 1 + 2 + 3 + \dots + n = \frac{n(n+1)}{2}$ ; since n=26, the total key length is 351. A possible alternative is the construction of a 676-long key by fitting together 26 cycles of the basic sequence, the successive cycles beginning with A, B, C, . . . (or H, Y, D, . . . , or any other scheme for including all 26 letters for the starts of the cycles).

² This series is named after Leonardo of Pisa (ca. 1170-1248), also known as Fibonacci (i.e., "filius Bonacci," or "son of Bonacci"), who first investigated its properties in connection with the proliferative activities of rabbits.

equals the sixth), at the end of the first 50 digits the sequence will read 1542869604 . . . , continuing for a cycle of 16,401 digits; on the other hand, with this same initial pentanome and the rule of combination  $a+c+d+e=f$ , the cycle of 19,344 digits is reached, maximum for this length of initial key.³ The mathematics involved here is related to the mathematics of shift registers (see subpar. 58h); in fact, some shift register feedback rules are called "Fibonacci rules." The shift register cases all involve mod-2 arithmetic; the mod-10 version, as illustrated here, has additional complications.

g. In connection with the subject of extensive or lengthy keys is the cipher system known as the *running-key*, *continuous-key*, or *nonrepeating-key* system, in which the key consists of a sequence of elements which never repeats, no matter how long the message to be enciphered happens to be. Although any continuous text could be used, the most common and most practical source of such a key is that in which the plain text of a previously agreed-upon book serves as the source for successive key letters for encipherment;⁴ or, in a numerical cryptosystem, the key could be obtained from various mathematical tables or even from a telephone directory. Even though in a running-key system the key for an individual message may be as long as the message and never repeats, nevertheless, if a large group of correspondents employ the same key sequence, it may happen that there will be several messages in the same key, and they will all begin at the same position in the keying sequence; or there might be several messages which will overlap one another with respect to the key, even if they begin at different points in the keying sequence. These situations form the basis of solution of systems of this genre.

h. In addition to the foregoing manual methods, there are a great many mechanical methods of producing a long key, such as those employed in mechanical or electrical cipher machines. In most cases these methods depend upon the interaction of two or more short, primary keys which jointly produce a single, much longer, secondary or resultant key (see par. 4). Only brief reference will be made at this point in the cryptanalytic studies to cases of this kind; the matter will be taken up in detail in Chapter IX.

³ The mathematics of Fibonacci cycles involves complicated aspects of algebra and number theory, and there is no short cut to the determination of the cycle length, given any specified initial key and rule of combination. For the interested reader, the table below gives the cycle lengths for all rules of combination (always including the *a* digit) for pentanomic initial keys; the number in parentheses indicates the number of different cycles of that length. (For a stated rule of combination, the initial group 00001 always gives rise to a maximum cycle.)

$a+b=f$	$a+c=f$	$a+d=f$	$a+e=f$	$a+b+c=f$	$a+b+d=f$	$a+b+e=f$	$a+c+d=f$
16,401 (4)	744 (129)	6448 (15)	168 (500)	840 (80)	1560 (60)	6248 (8)	9372 (4)
5,467 (4)	124 (32)	208 (15)	84 (33)	168 (100)	312 (20)	3124 (12)	4686 (4)
2,343 (4)	31 (1)	124 (1)	42 (16)	140 (20)	30 (4)	1562 (4)	3124 (4)
781 (4)	24 (1)	31 (1)	28 (1)	120 (80)	15 (2)	781 (8)	2343 (8)
21 (1)	1 (1)	4 (1)	24 (500)	28 (24)	2 (4)	8 (2)	1562 (4)
7 (1)		1 (1)	21 (1)	24 (100)	1 (2)	4 (3)	781 (8)
3 (1)			12 (33)	20 (20)		2 (1)	12 (1)
1 (1)			7 (1)	14 (1)		1 (2)	6 (1)
			6 (15)	7 (2)			4 (1)
			5 (1)	4 (24)			3 (2)
			4 (1)	2 (1)			2 (1)
			3 (1)	1 (2)			1 (2)
			1 (2)				

$a+c+e=f$	$a+d+e=f$	$a+b+c+d=f$	$a+b+c+e=f$	$a+b+d+e=f$	$a+c+d+e=f$	$a+b+c+d+e=f$
1860 (48)	10,934 (4)	744 (129)	744 (129)	1240 (72)	19,344 (5)	4686 (16)
930 (4)	5,467 (8)	124 (32)	124 (32)	620 (6)	624 (5)	2343 (8)
372 (16)	1,562 (4)	31 (1)	31 (1)	248 (15)	124 (1)	781 (8)
62 (4)	781 (8)	24 (1)	24 (1)	124 (1)	31 (1)	6 (4)
60 (12)	14 (1)	1 (1)	1 (1)	40 (72)	4 (1)	3 (2)
15 (2)	7 (2)			31 (1)	1 (1)	1 (2)
12 (4)	2 (1)			20 (6)		
1 (2)	1 (2)			8 (15)		
				4 (1)		
				1 (1)		

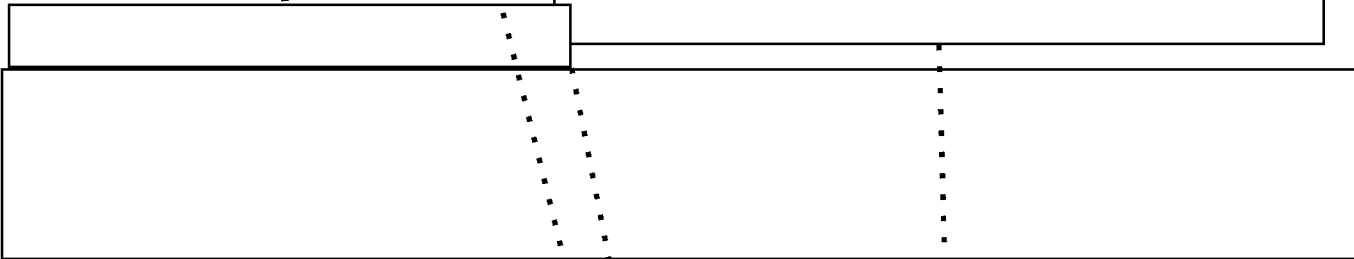
⁴ The key is either the plain text itself as key letters, or a transformation of the plaintext key into digits, say, by enciphering the plain text through a monome-dinome rectangle. See in this connection Appendix "A" (on pp. 250-256) of Alexander Foote's *Handbook for Spies*, New York, 1949.



i. Finally, there must be mentioned certain devices in which, as in encipherment by the autokey method, the text itself serves to produce the variation in cipher equivalents, by controlling the selection of secondary alphabets, or by influencing or determining the sequence in which they will be employed. Naturally, in such cases the key is automatically extended to a point where it coincides in length with that of the text. An excellent example of such a device is the Wheatstone cipher device,⁵ the solution of which will be treated in Chapter VIII.

**37. Depth and its exploitation.**—a. The concept of depth was introduced in the previous text;⁶ it was pointed out that, unless special circumstances are present, the re-use of key, either within a message or among several messages, is a necessary condition to the solution of polyalphabetic ciphers. The sole exception is the case wherein the components are known and the continuous, nonrepeating key is plain text (or has otherwise recognizable systematic or exploitable nonrandom properties); correct cribs in either the plain text or the key will enable a solution to be effected—but this of course in reality is tantamount to a depth of two.

b. The solution of a single message in a periodic polyalphabetic cipher involving unknown primary components rests on the ability of the cryptanalyst to superimpose cycles of the period into a cryptographic depth, i.e., so that all the cipher letters in the individual columns of the depth diagram belong to individual monoalphabetic distributions.



d. We shall now take up the solution of cryptograms involving long or continuous keys under the two general cases: (1) those wherein the primary components are known sequences, and (2) those wherein they are unknown.

**38. Solution of a single cryptogram involving known primary components and an unknown plaintext running key.**—a. This is a trivial case, since what we have is really a depth of two (i.e., the plain text of the message, and the plain text constituting the key); if the primary components are known sequences, a correct assumption of plain text in either the cipher or the key will produce plain text in the other. Furthermore, if a novel or other book is used as key, upon the recovery of sufficient key text the cryptanalyst might be able to identify the particular book that is being used for the key, which would greatly simplify his subsequent efforts.

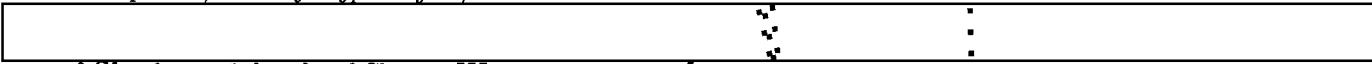
b. As an example, let us suppose that we have at hand the following short cryptogram, assumed to have been enciphered with direct standard alphabets and a plaintext running key:

E U G E M N L L H G B Y D Q V S X P M F A A G Z J B K W A X  
F R H F A Q A A H K G S L I F L X C W V R E K Q D Y W M F  
X K L A C Y D R L L G I C C E X A V O Q H R R H F R P T N L

The procedure here is to try sliding probable words or other plaintext polygraphs through the cipher text, seeing what plausible key fragments are produced thereby, and expanding the placed crib and its

⁵ Some writers classify and treat this method, as well as autokey methods, as forms of the running-key system, but it is preferable to consider the latter as being radically different in principle from the former types, because in the true running-key system the key is wholly external to and independent of the text being enciphered. This is hardly true of autokey systems or of the Wheatstone device.

⁶ Cf. par. 65, *Military Cryptanalytics, Part II*.



⁷ Cf. subpars. 14b and c of Chapter III.

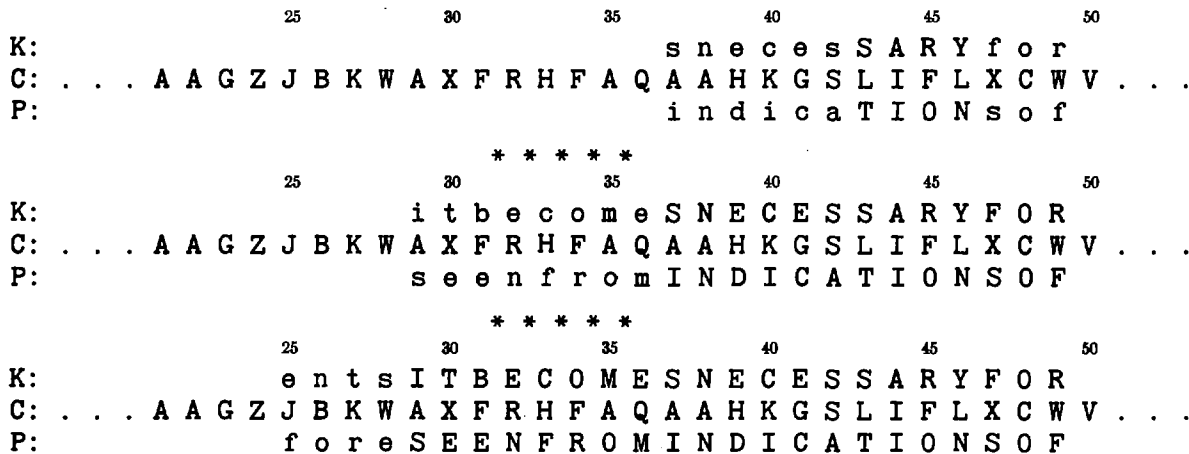
(b) (1)  
(b) (3) -18 USC 798  
(b) (3) -50 USC 3024(i)  
(b) (3) -P.L. 86-36

associated key elements. For instance, if we slide TION through the text, we would construct the diagram shown in Fig. 69, below (under the assumption of A_p as the index letter):⁹

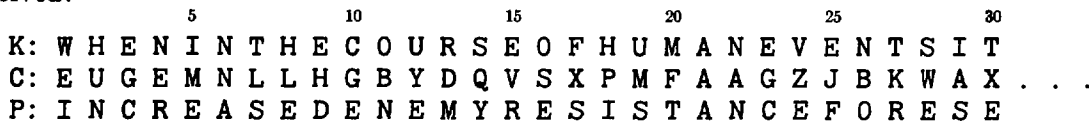


FIGURE 69

Several candidates for plaintext key fragments are noted and are marked in the diagram, the best one perhaps being SARY, as part of the word NECESSARY. Key and plain text are expanded simultaneously, as shown in the following successive steps:

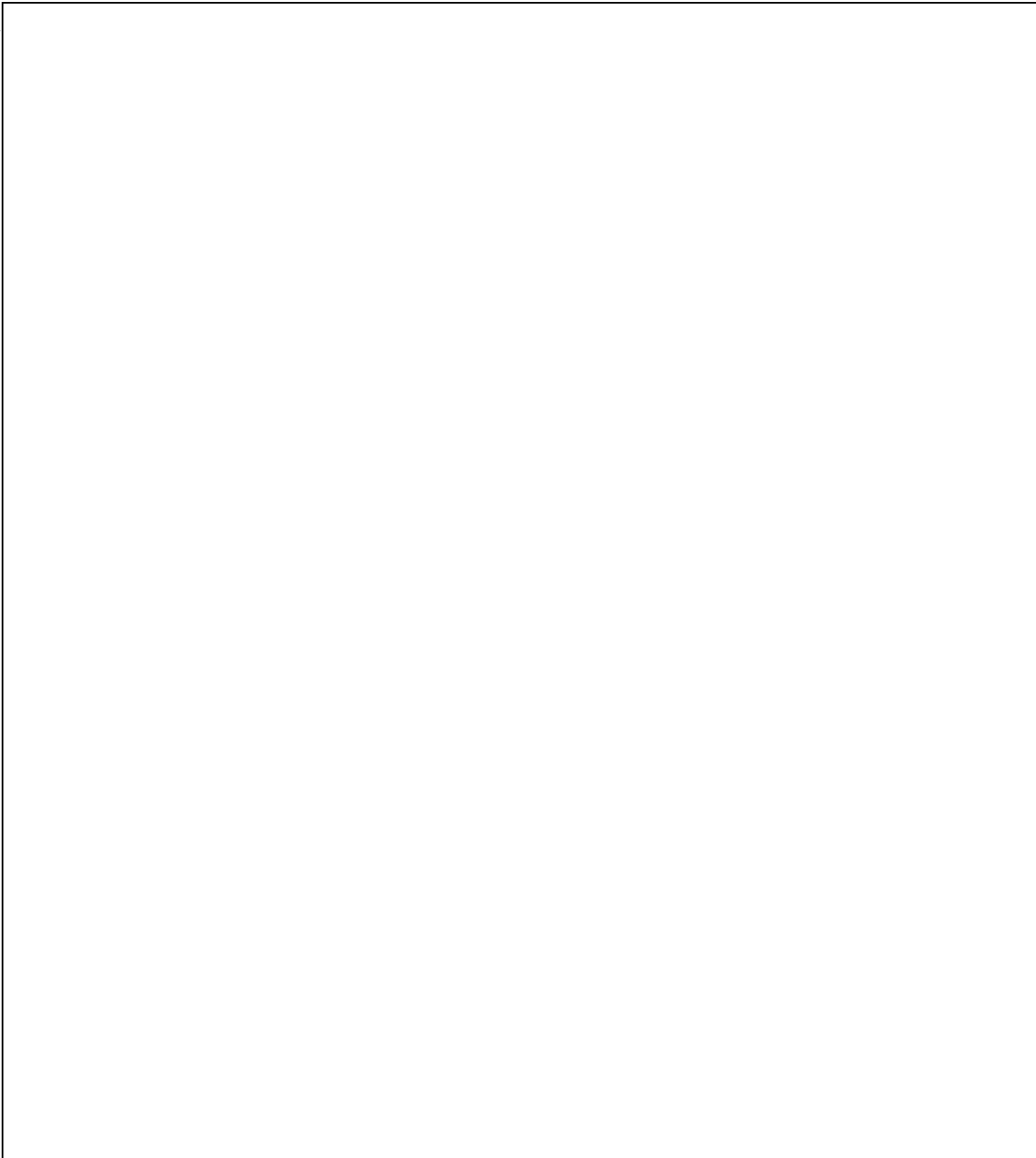


At this point we assume a verb before the word FORESEEN, and we try IS (yielding the key YH), WAS (=EGH_k), ARE (=APV_k), BE (=FV_k), among others. The E_p=V_k looks promising, however, and we suddenly recognize the key text as coming from the Constitution of the United States. The problem is now solved:

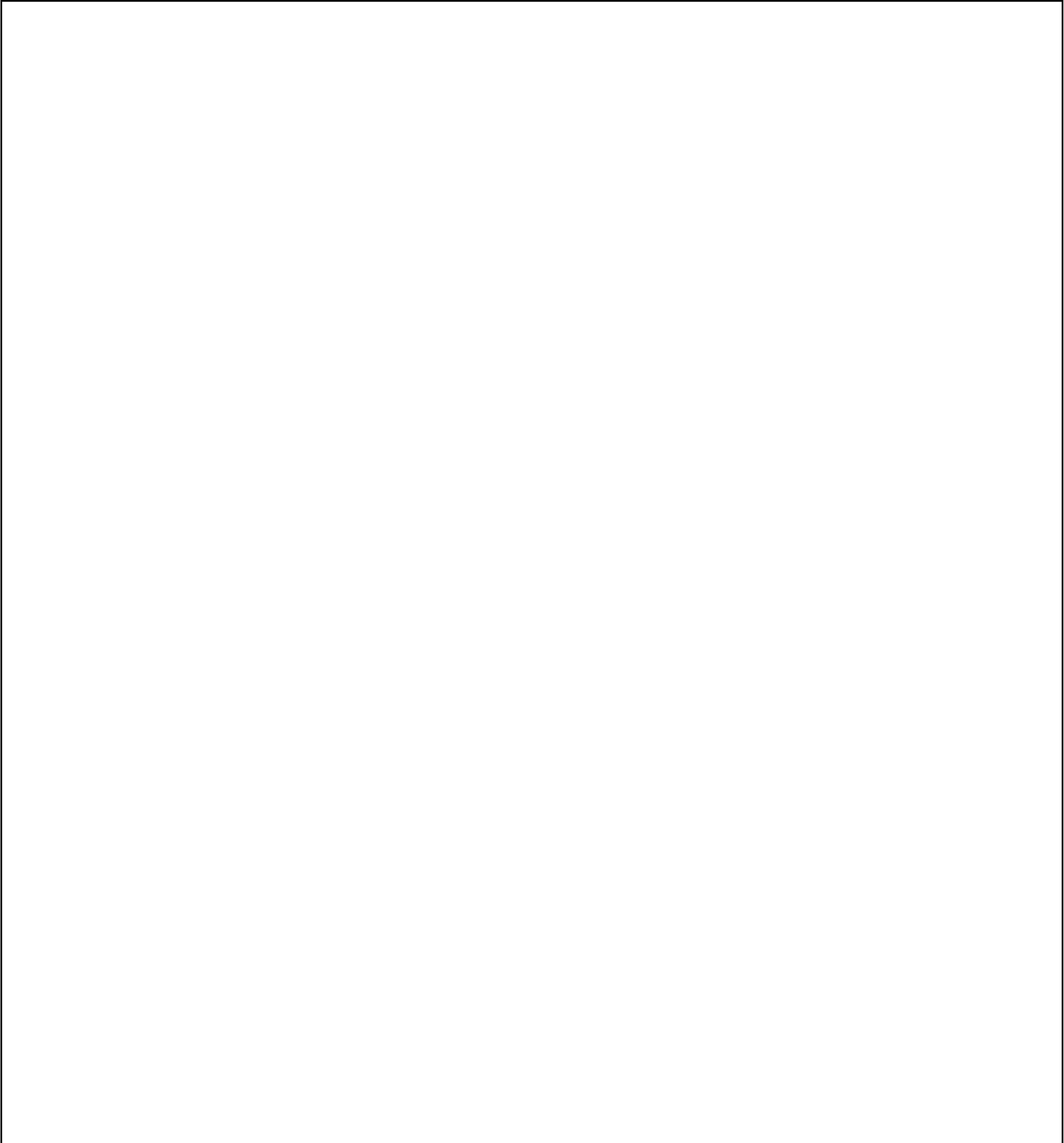


Note that we could also have solved a problem such as this by assuming key text, and seeing what develops in the decipherment of the cipher text.

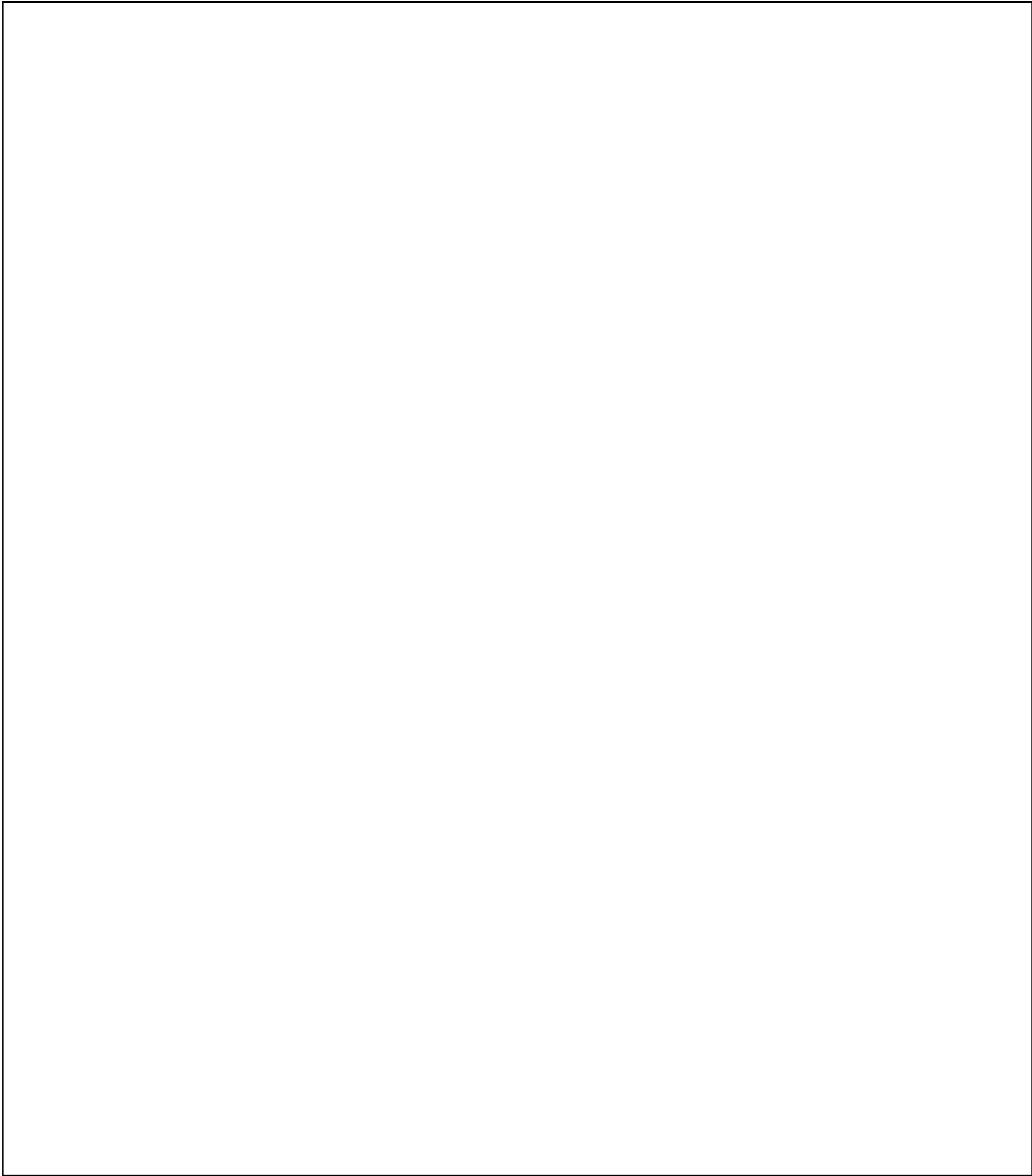
⁹ Cf. subpar. 22d on pp. 41-42 of *Military Cryptanalytics, Part II*.



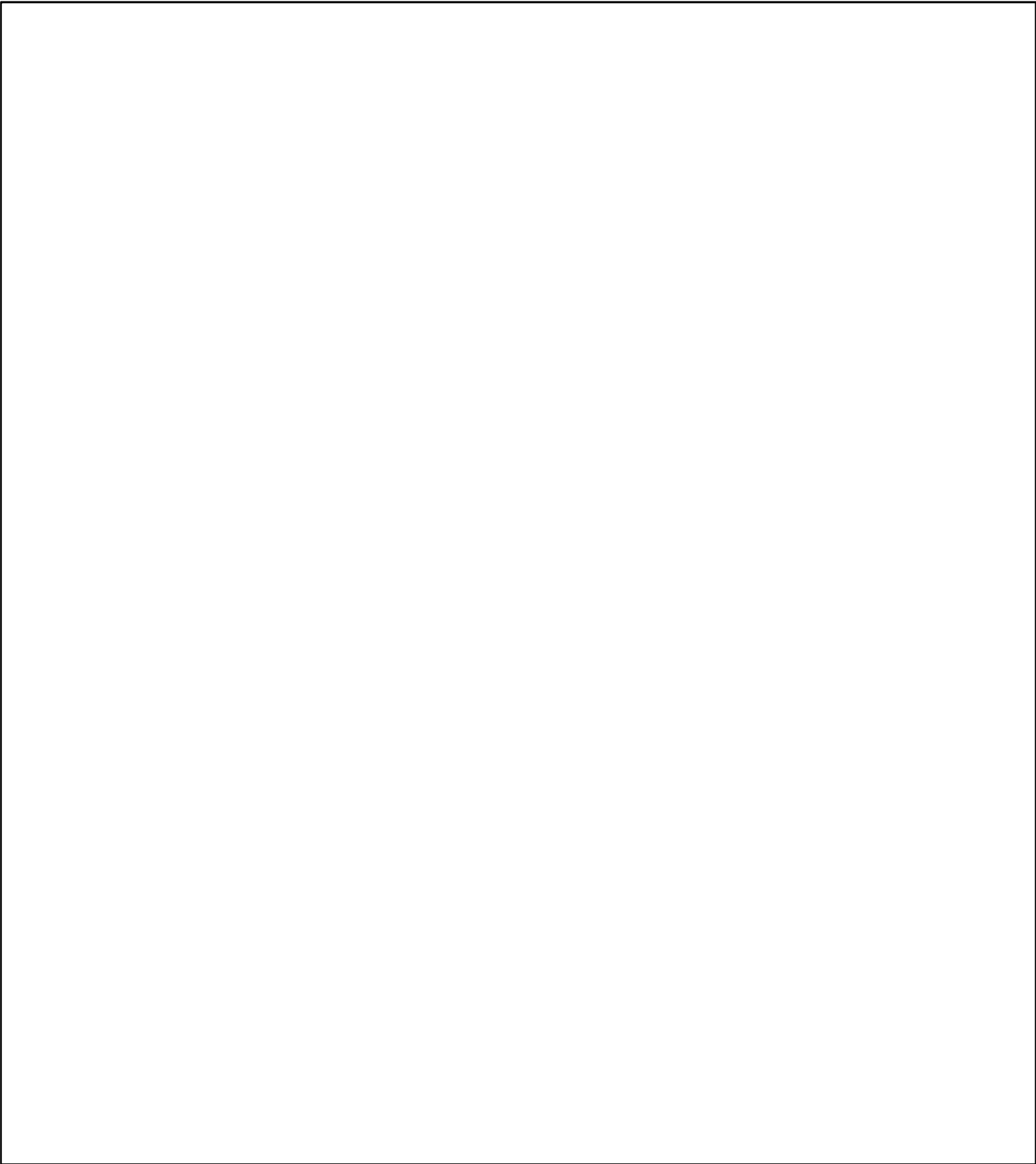
(b) (1)  
(b) (3) -18 USC 798  
(b) (3) -50 USC 3024 (i)  
(b) (3) -P.L. 86-36



(b) (1)  
(b) (3)-18 USC 798  
(b) (3)-50 USC 3024(i)  
(b) (3)-P.L. 86-36



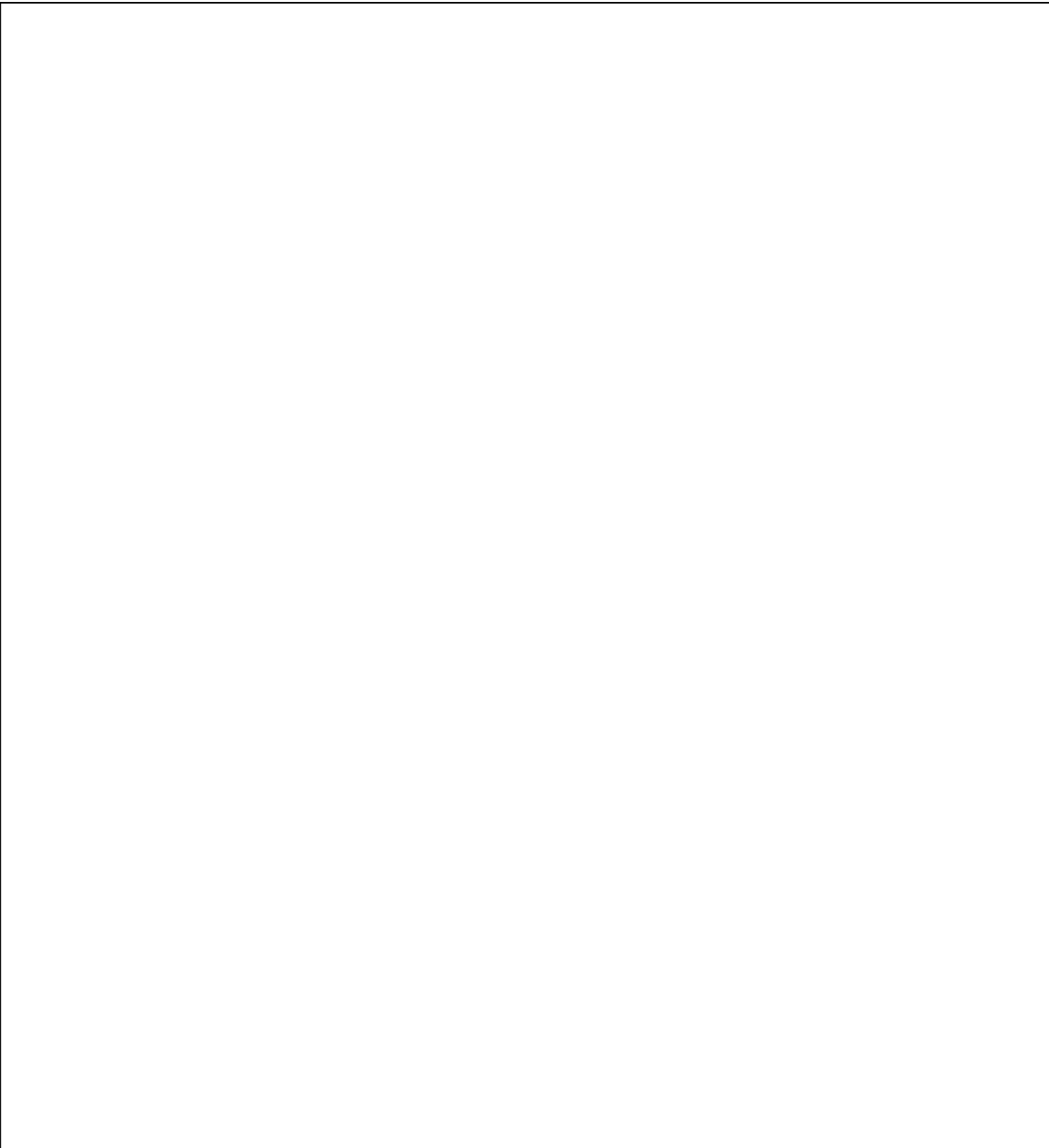
(b) (1)  
(b) (3) -18 USC 798  
(b) (3) -50 USC 3024 (i)  
(b) (3) -P.L. 86-36



(b) (1)  
(b) (3)-18 USC 798  
(b) (3)-50 USC 3024 (i)  
(b) (3)-P.L. 86-36



(b) (1)  
(b) (3)-18 USC 798  
(b) (3)-50 USC 3024(i)  
(b) (3)-P.L. 86-36



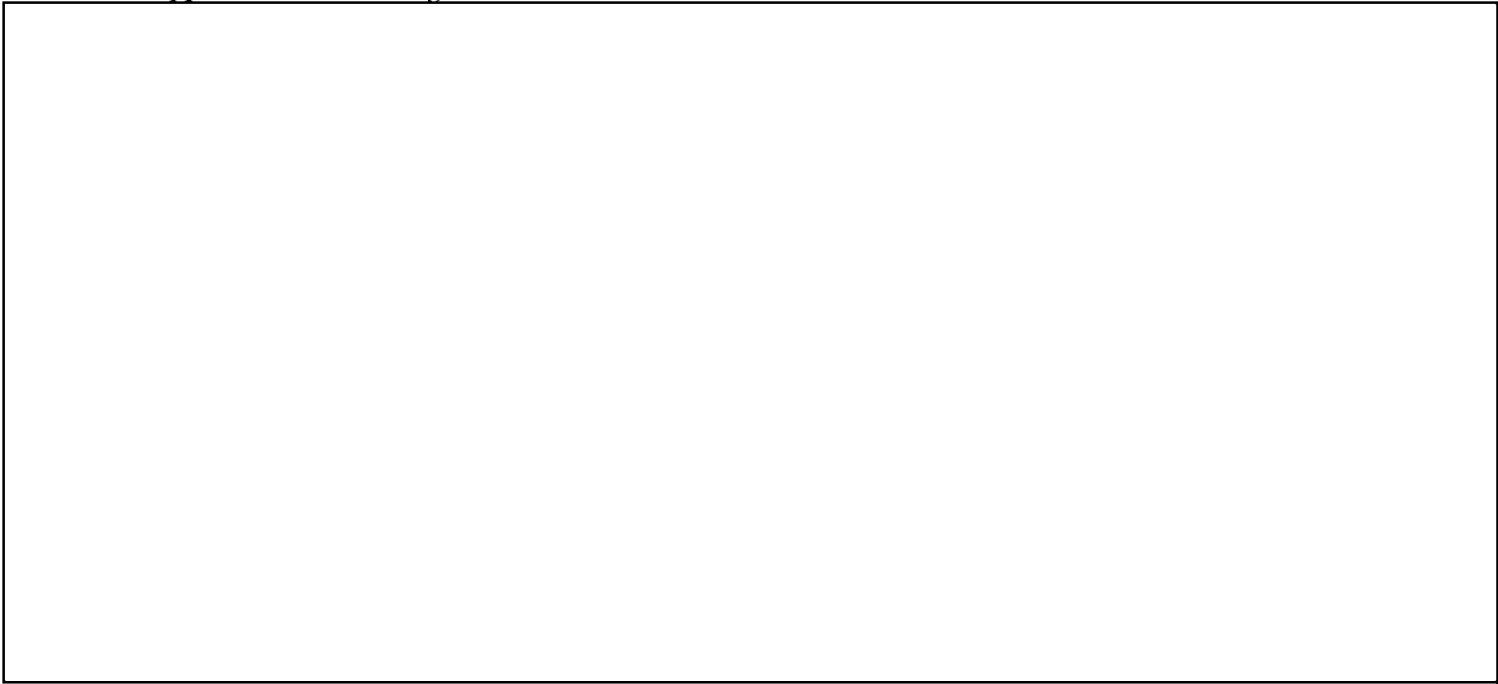
(b) (1)  
(b) (3) -18 USC 798  
(b) (3) -50 USC 3024 (i)  
(b) (3) -P.L. 86-36



(The digraphs obtained from reversals are shown in parentheses.) The cipher component may now be chained out and reconstructed in its original form, and the plain component can be recovered in a few moments by taking advantage of the now-known cipher component. The completion of the solution, including recovery of the key for the messages, is again left to the reader as an exercise.

**41. Recovery of plain texts and the unknown primary components from a number of messages in flush depth.**—*a.* In the previous text ¹¹ it was noted that if there were available a sufficient number of messages (say 25–30, for English) all enciphered beginning at the same point in a long key, the messages would be in flush depth, and the frequency distributions of the columns of the superimposition diagram could be solved, without knowing the length of the key.¹² It was further noted that even if an extremely long key is employed and a series of messages beginning at different initial points is enciphered by such a key, this method of solution by superimposition can be employed, provided that the messages can be superimposed correctly—that is, so that the letters which fall in one column really belong to one cipher alphabet. Messages may be put into depth as a result of the solution of indicators, or by means of long ciphertext repetitions, or by means of the kappa ( $\kappa$ ) test.

*b.* The kappa test has been treated at some length in the previous volume; a review at this time might not be amiss.¹³ The kappa test, or its equivalent form, the kappa I.C., involves nothing more than counting hits between two superimposed messages, and evaluating the result. We know, for instance, that since the repeat rate for English (i.e., the  $\kappa_p$ ) is .0667, if two 1000-letter messages are properly superimposed with respect to their keying sequence (i.e., so that both letters of a vertical pair have been enciphered by the same key letter), we should expect 66 or 67 hits between them if the underlying text is English; and if these same messages are not correctly superimposed, the repeat rate for random ( $\kappa_r = 1/26 = .0385$ ) should prevail, so that the expected number of hits will then be 38 or 39. A demonstration of the application of the kappa test will now be given.



¹¹ Cf. par. 65 (on p. 157) of *Military Cryptanalytics, Part II*.

¹² Prob. 9 (on p. 608) of Section G, Appendix 9, *Military Cryptanalytics, Part II*.

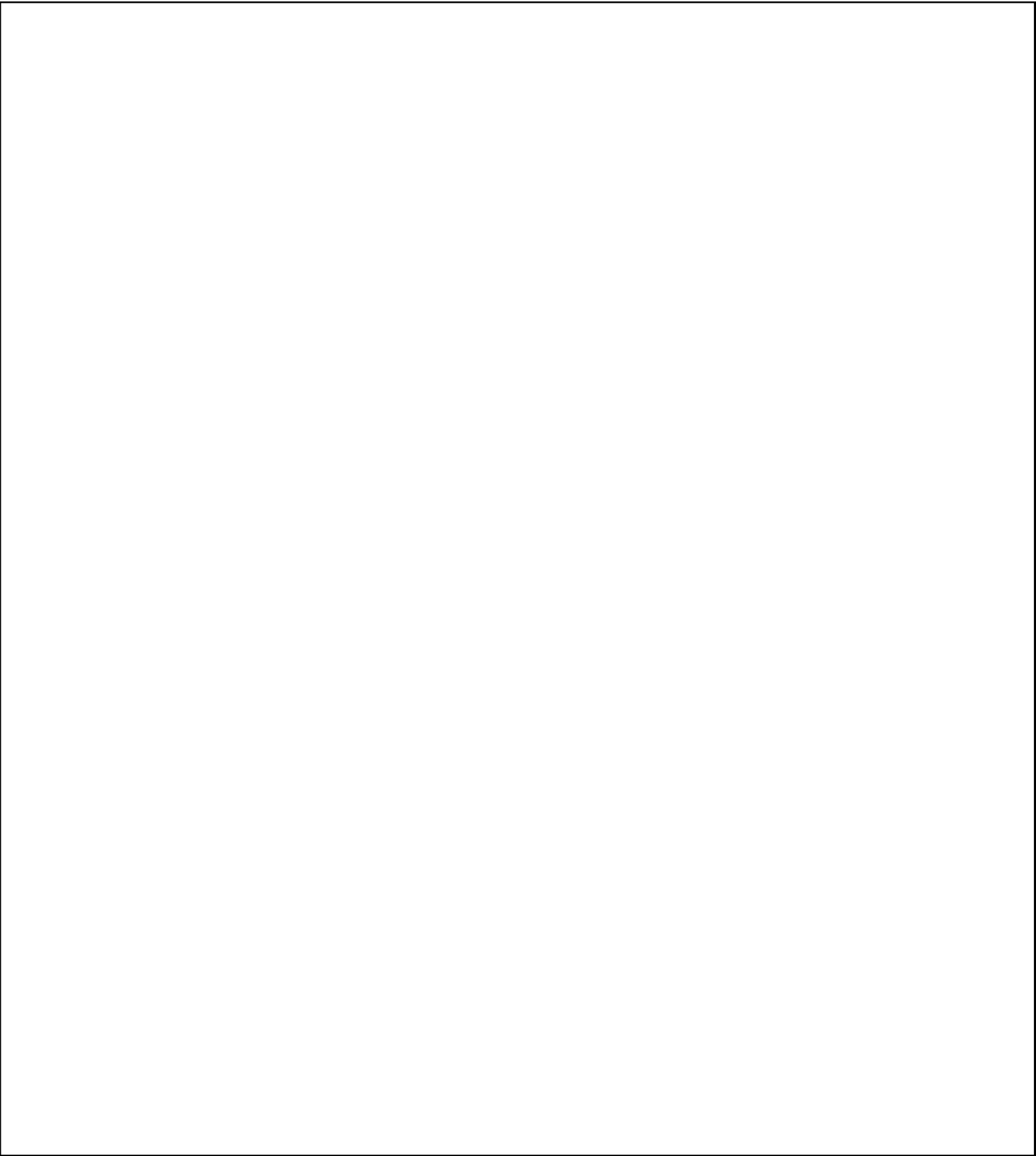
¹³ Cf. par. 98 on pp. 302–308 of *Military Cryptanalytics, Part II*.

(b) (1)  
(b) (3)–18 USC 798  
(b) (3)–50 USC 3024(i)  
(b) (3)–P.L. 86-36

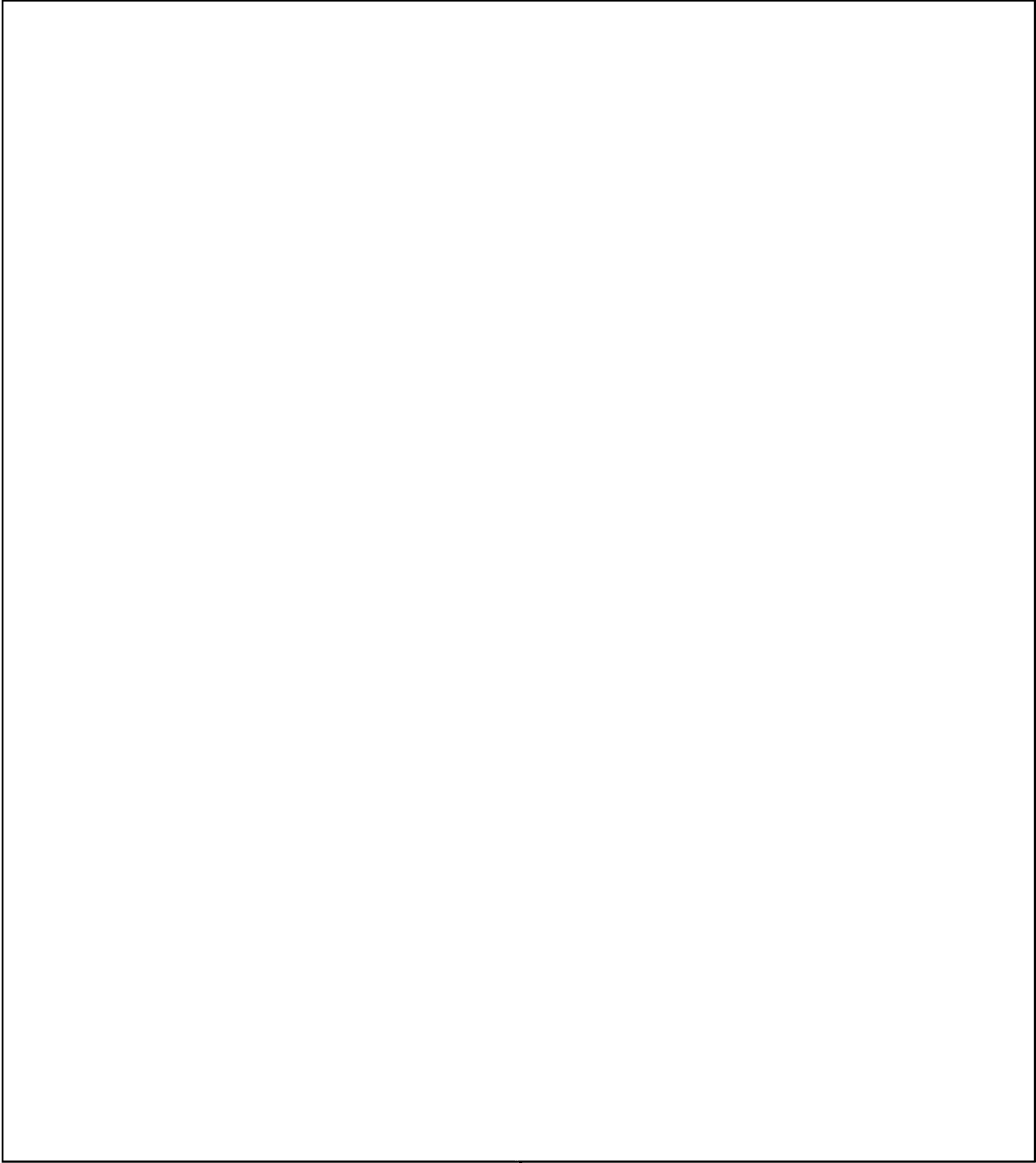
(b) (1)  
(b) (3) -18 USC 798  
(b) (3) -50 USC 3024 (i)  
(b) (3) -P.L. 86-36



(b) (1)  
(b) (3) -18 USC 798  
(b) (3) -50 USC 3024(i)  
(b) (3) -P.L. 86-36

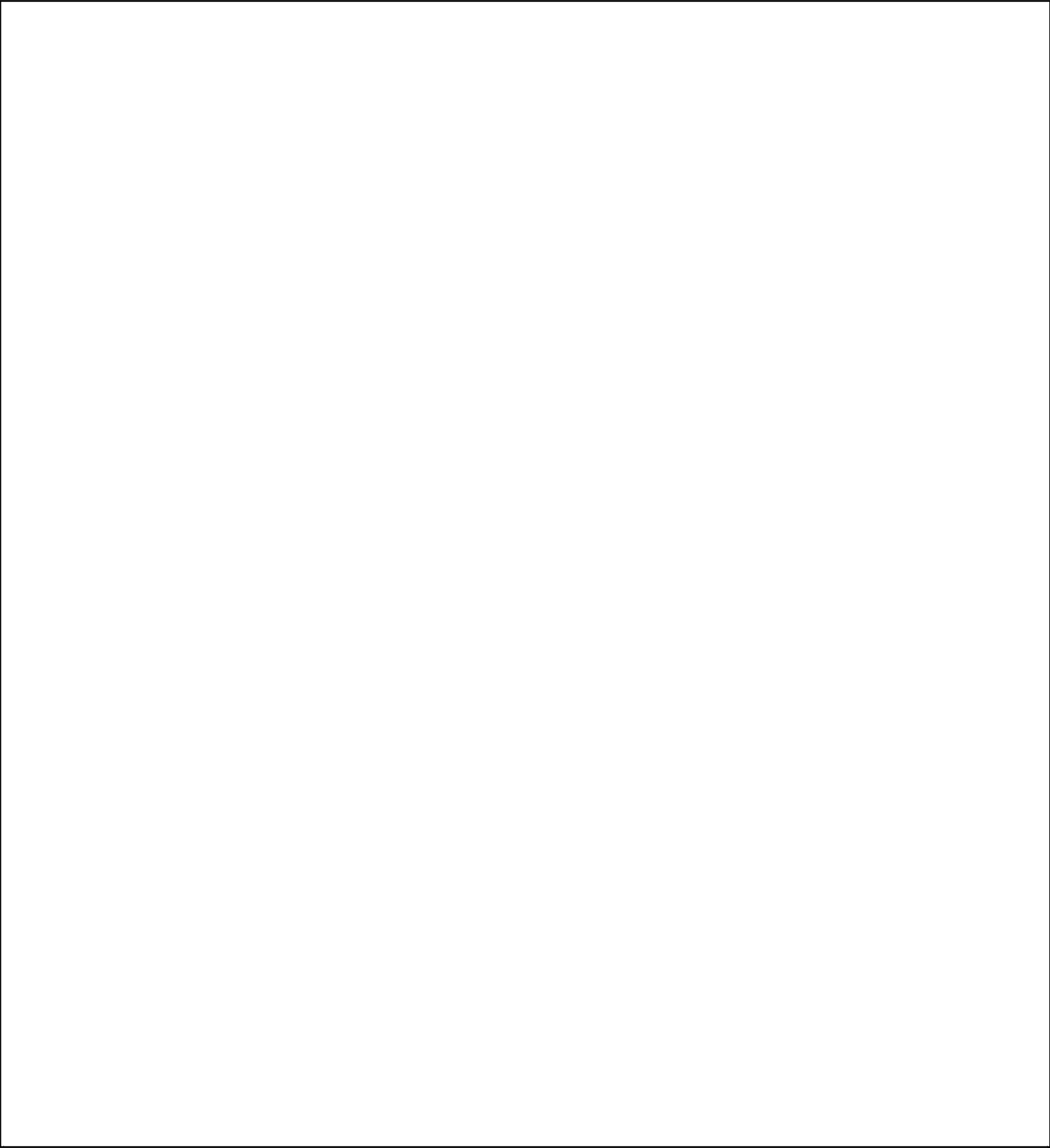


(b) (1)  
(b) (3)-18 USC 798  
(b) (3)-50 USC 3024 (i)  
(b) (3)-P.L. 86-36

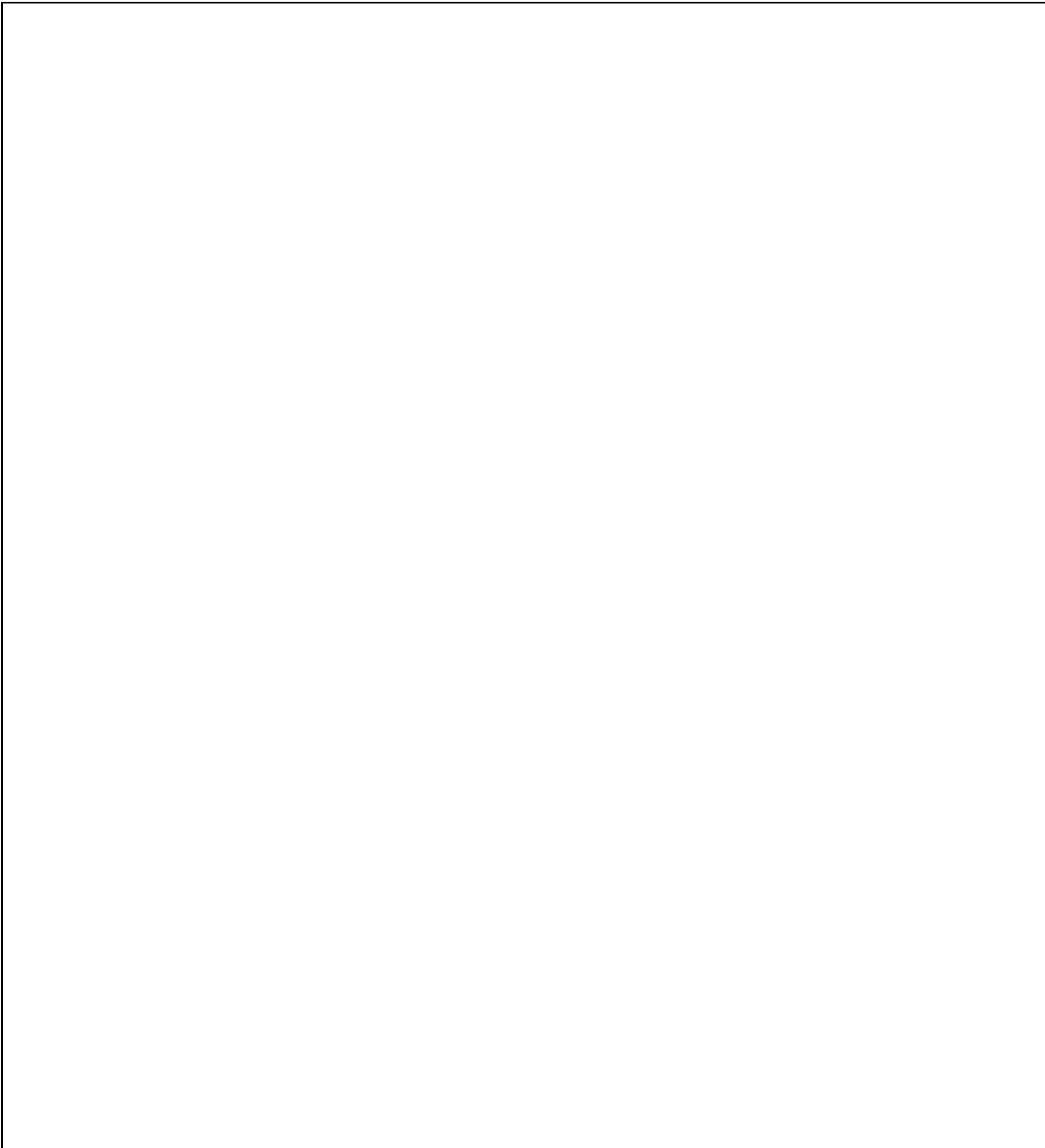


(b) (1)  
(b) (3)-18 USC 798  
(b) (3)-50 USC 3024(i)  
(b) (3)-P.L. 86-36

(b) (1)  
(b) (3)-18 USC 798  
(b) (3)-50 USC 3024(i)  
(b) (3)-P.L. 86-36

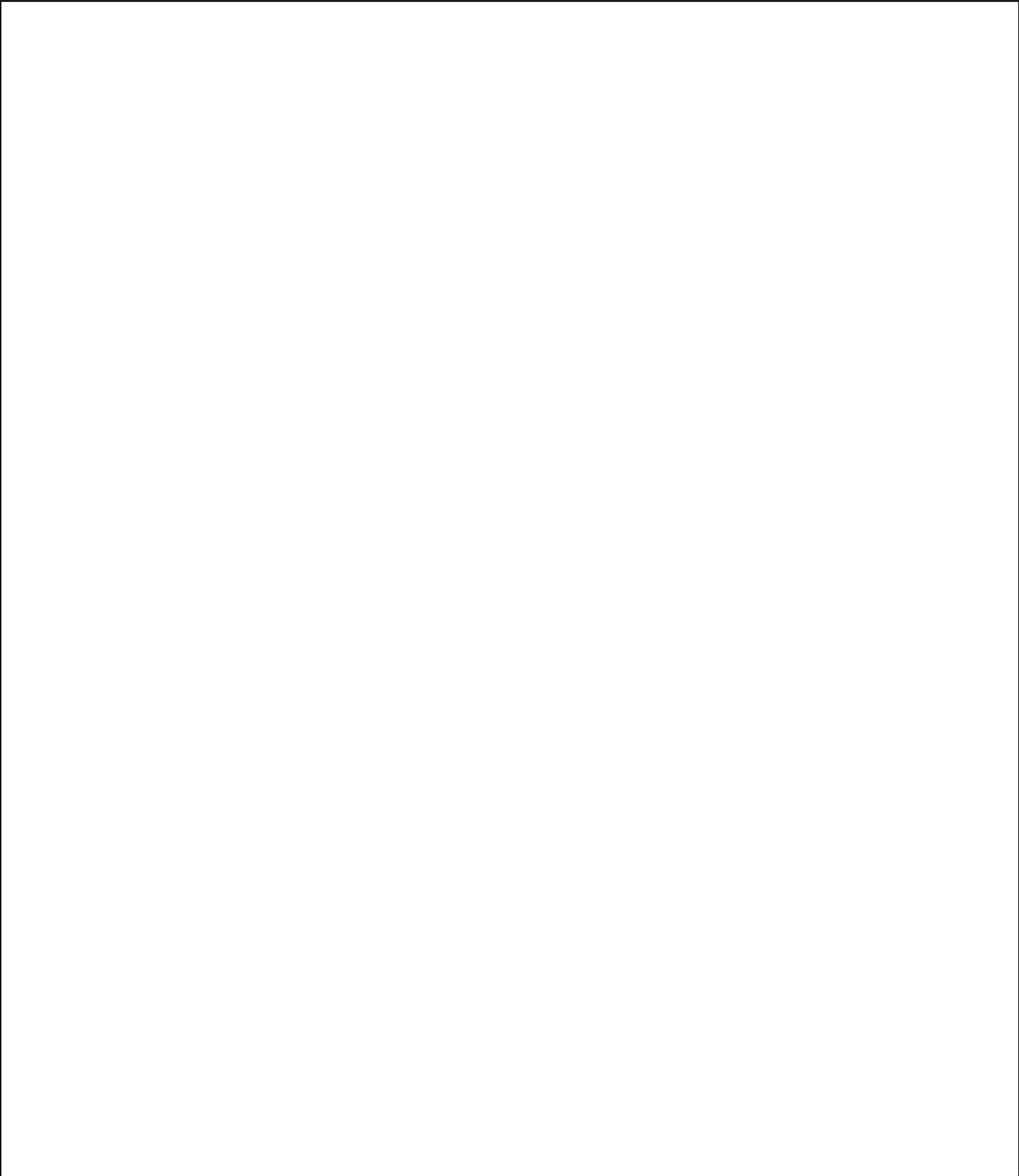


(b) (1)  
(b) (3)-18 USC 798  
(b) (3)-50 USC 3024(i)  
(b) (3)-P.L. 86-36

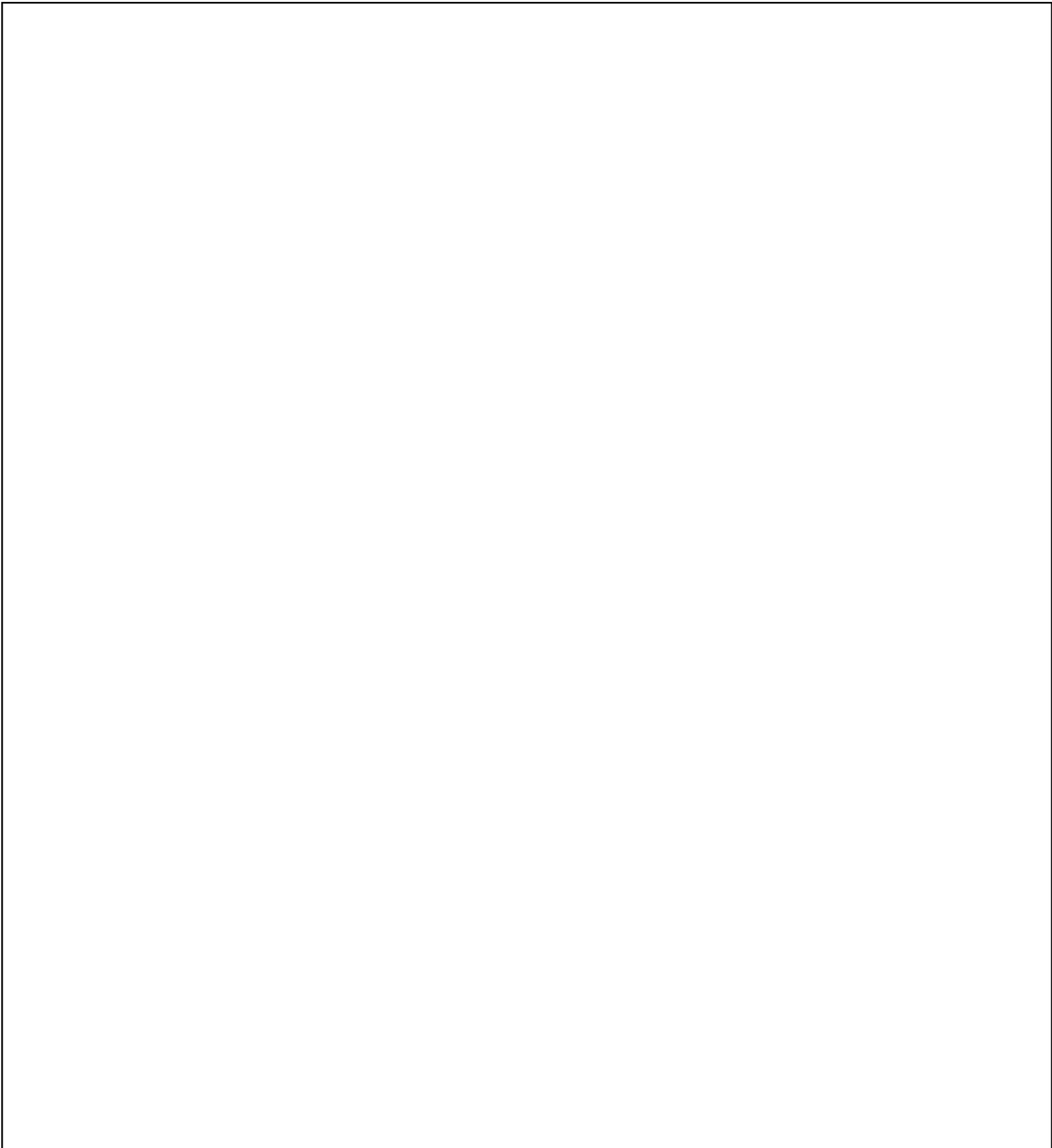


(b) (1)  
(b) (3)-18 USC 798  
(b) (3)-50 USC 3024(i)  
(b) (3)-P.L. 86-36

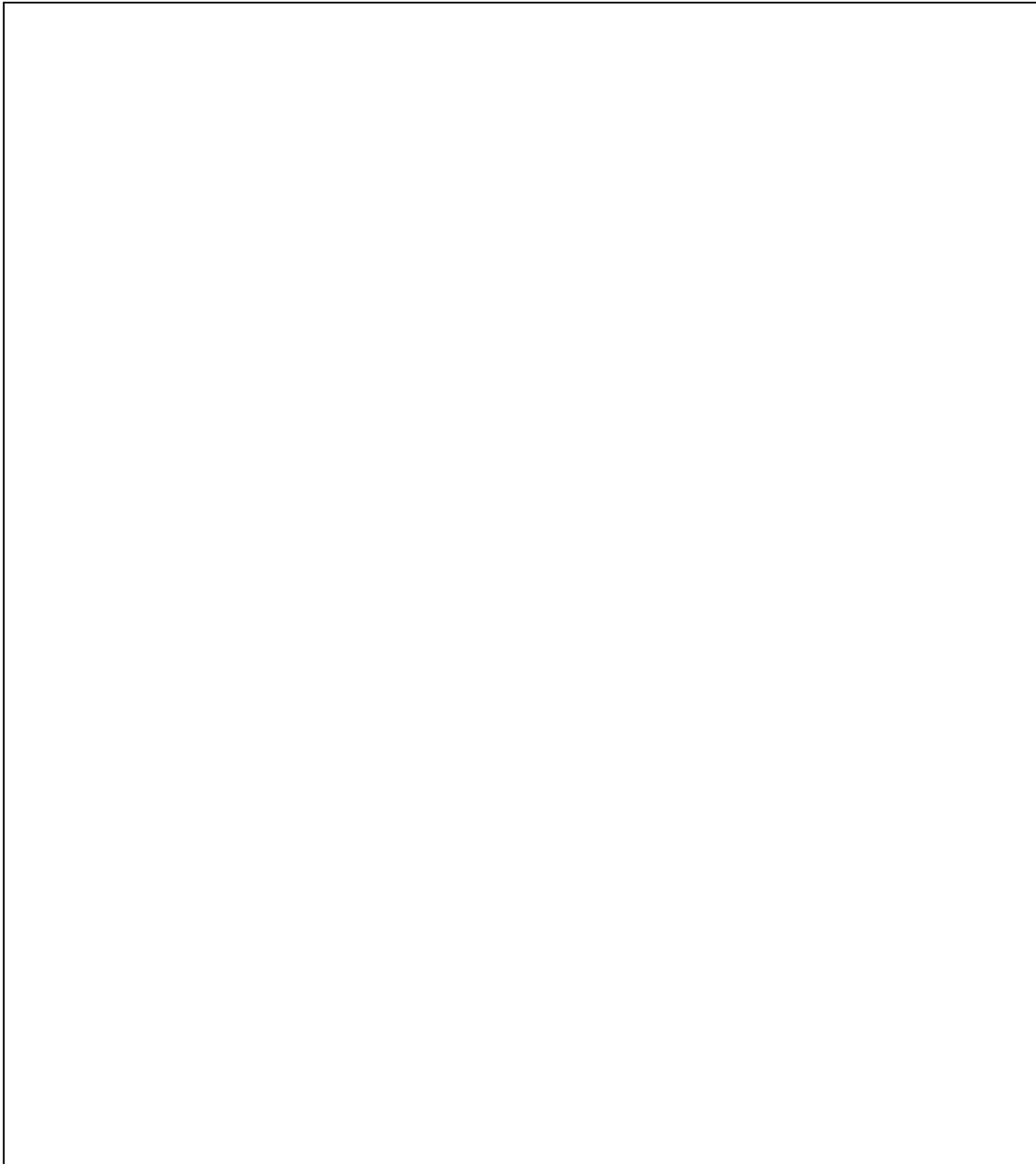




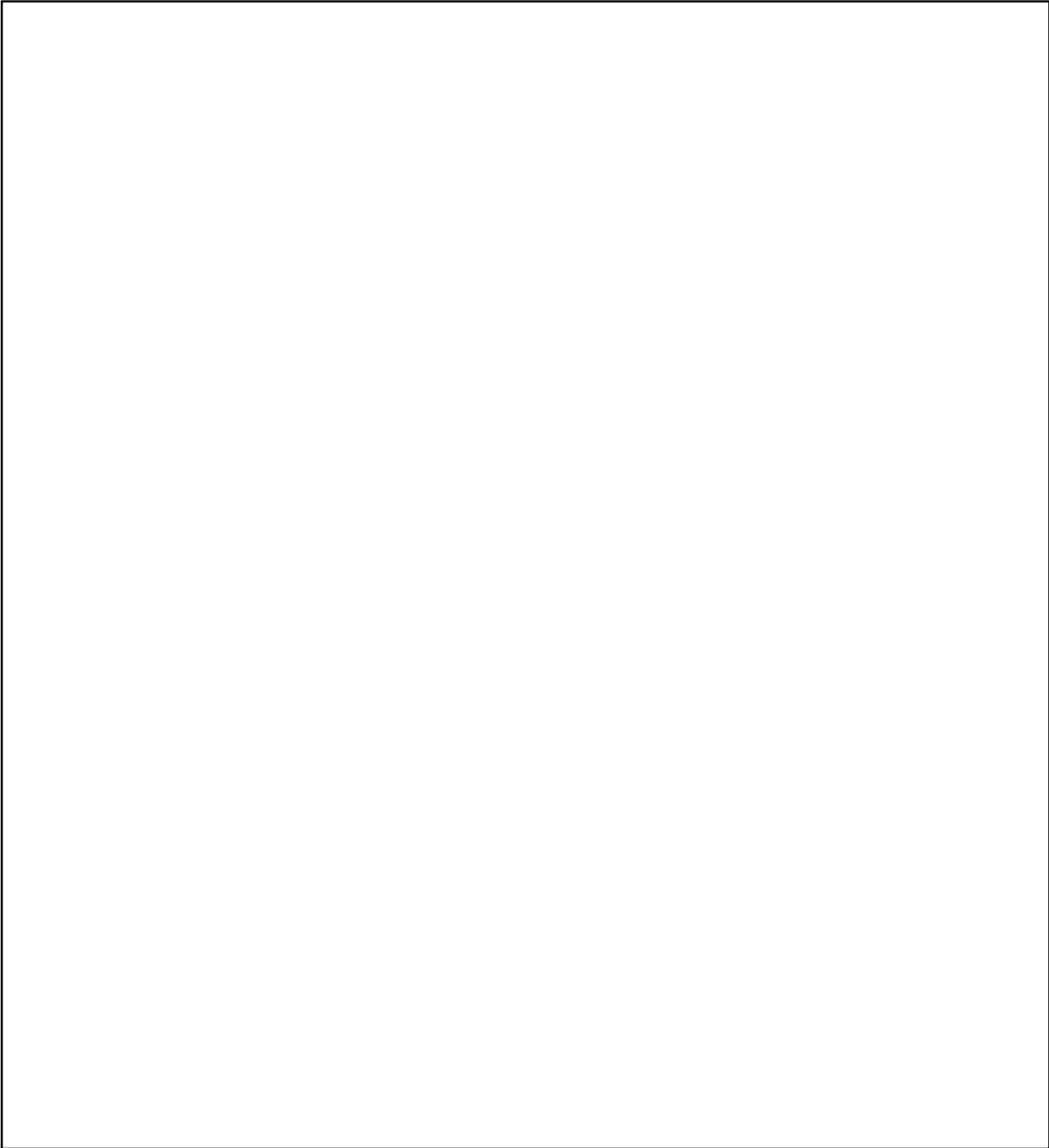
(b) (1)  
(b) (3)-18 USC 798  
(b) (3)-50 USC 3024(i)  
(b) (3)-P.L. 86-36



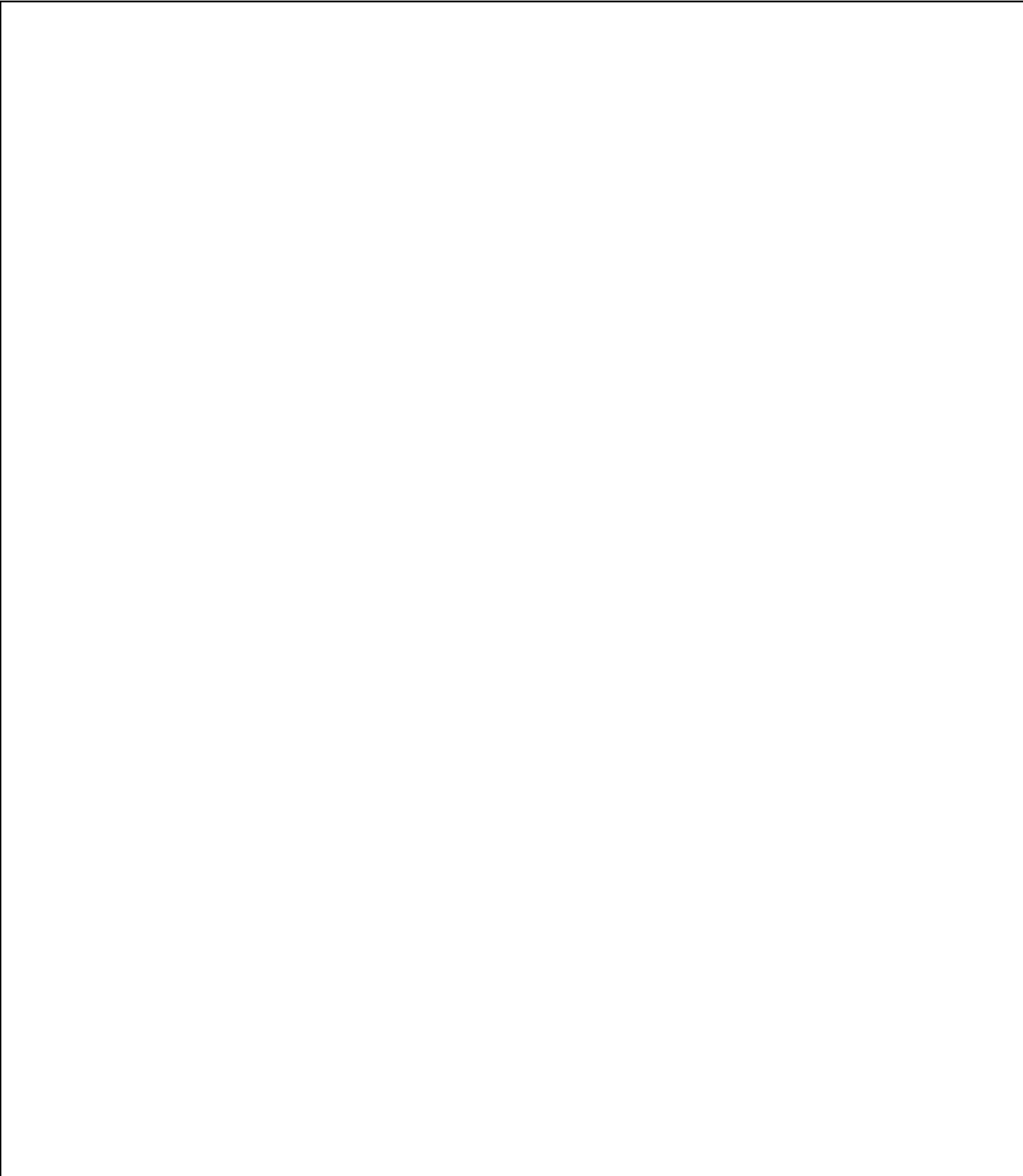
(b) (1)  
(b) (3)-18 USC 798  
(b) (3)-50 USC 3024(i)  
(b) (3)-P.L. 86-36



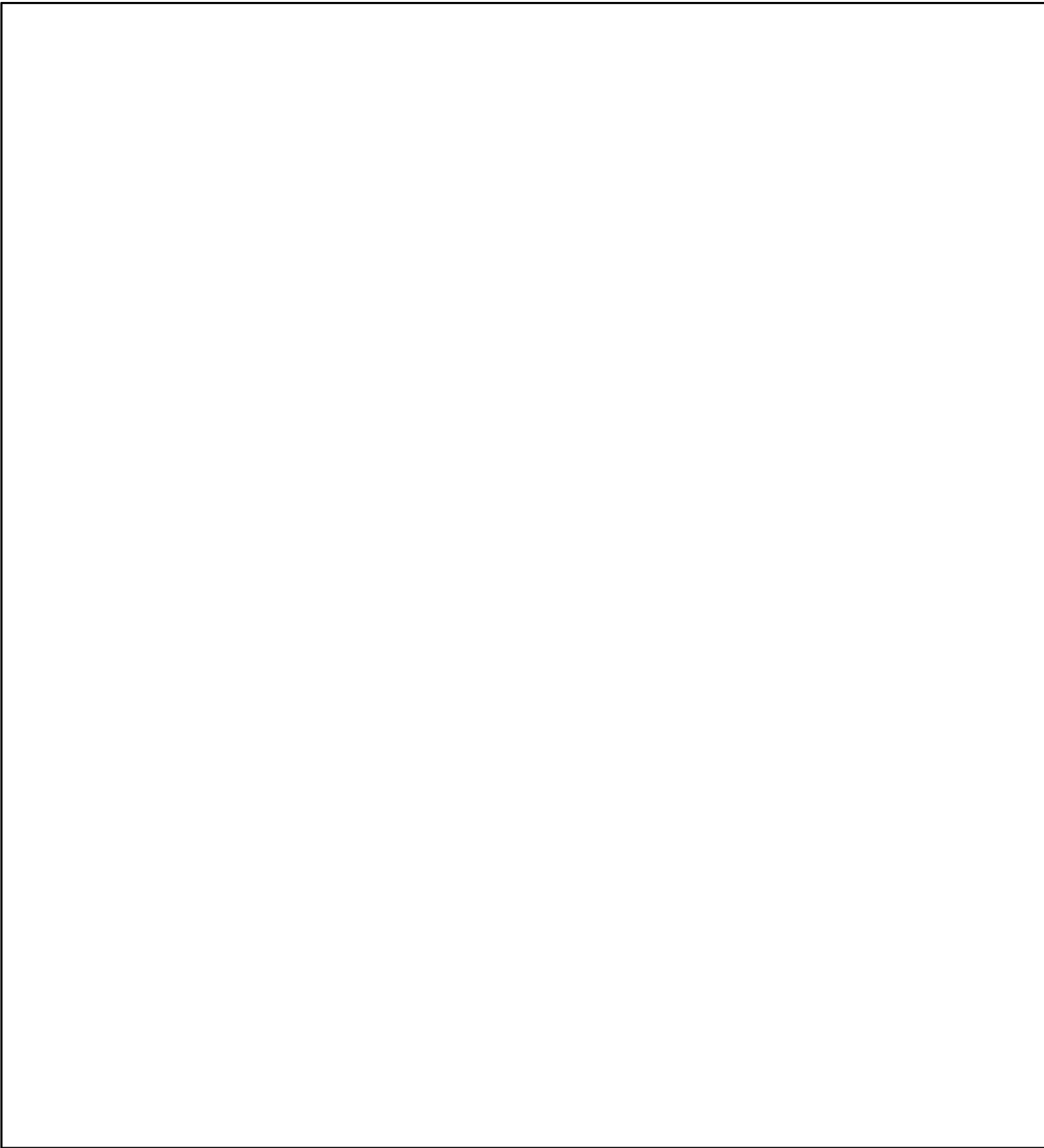
(b) (1)  
(b) (3)-18 USC 798  
(b) (3)-50 USC 3024 (i)  
(b) (3)-P.L. 86-36



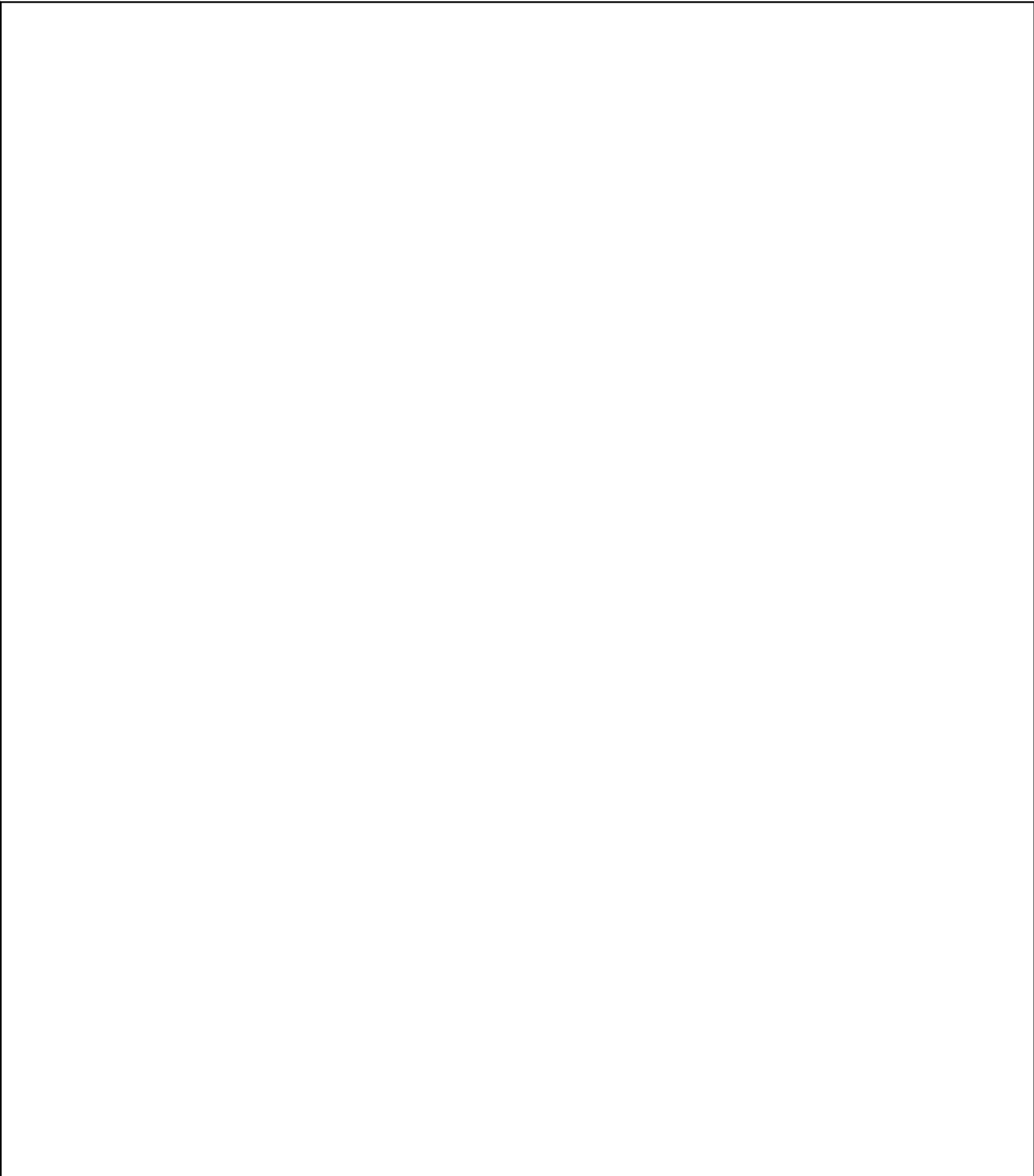
(b) (1)  
(b) (3)-18 USC 798  
(b) (3)-50 USC 3024(i)  
(b) (3)-P.L. 86-36



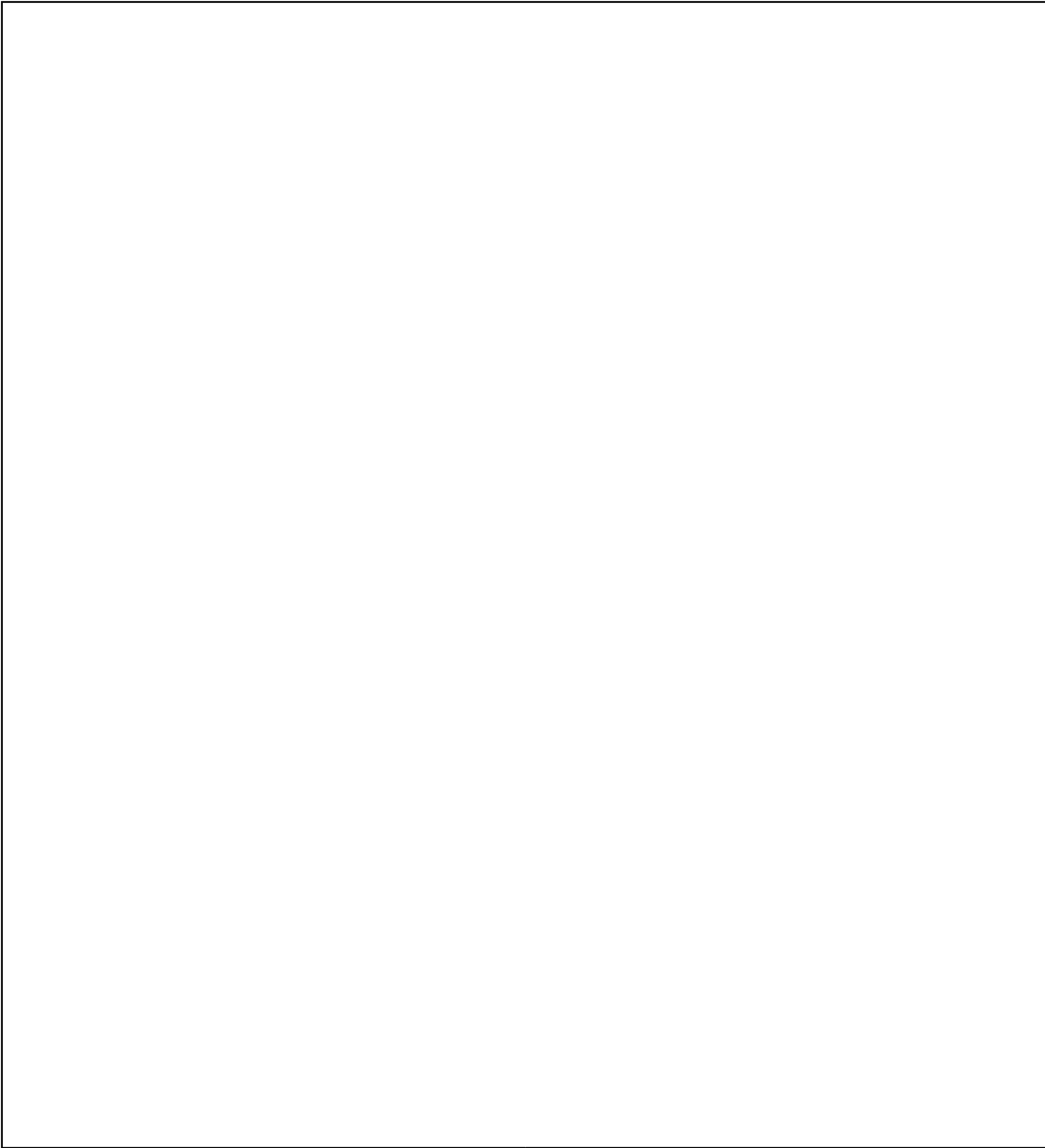
(b) (1)  
(b) (3)-18 USC 798  
(b) (3)-50 USC 3024(i)  
(b) (3)-P.L. 86-36



(b) (1)  
(b) (3)-18 USC 798  
(b) (3)-50 USC 3024(i)  
(b) (3)-P.L. 86-36

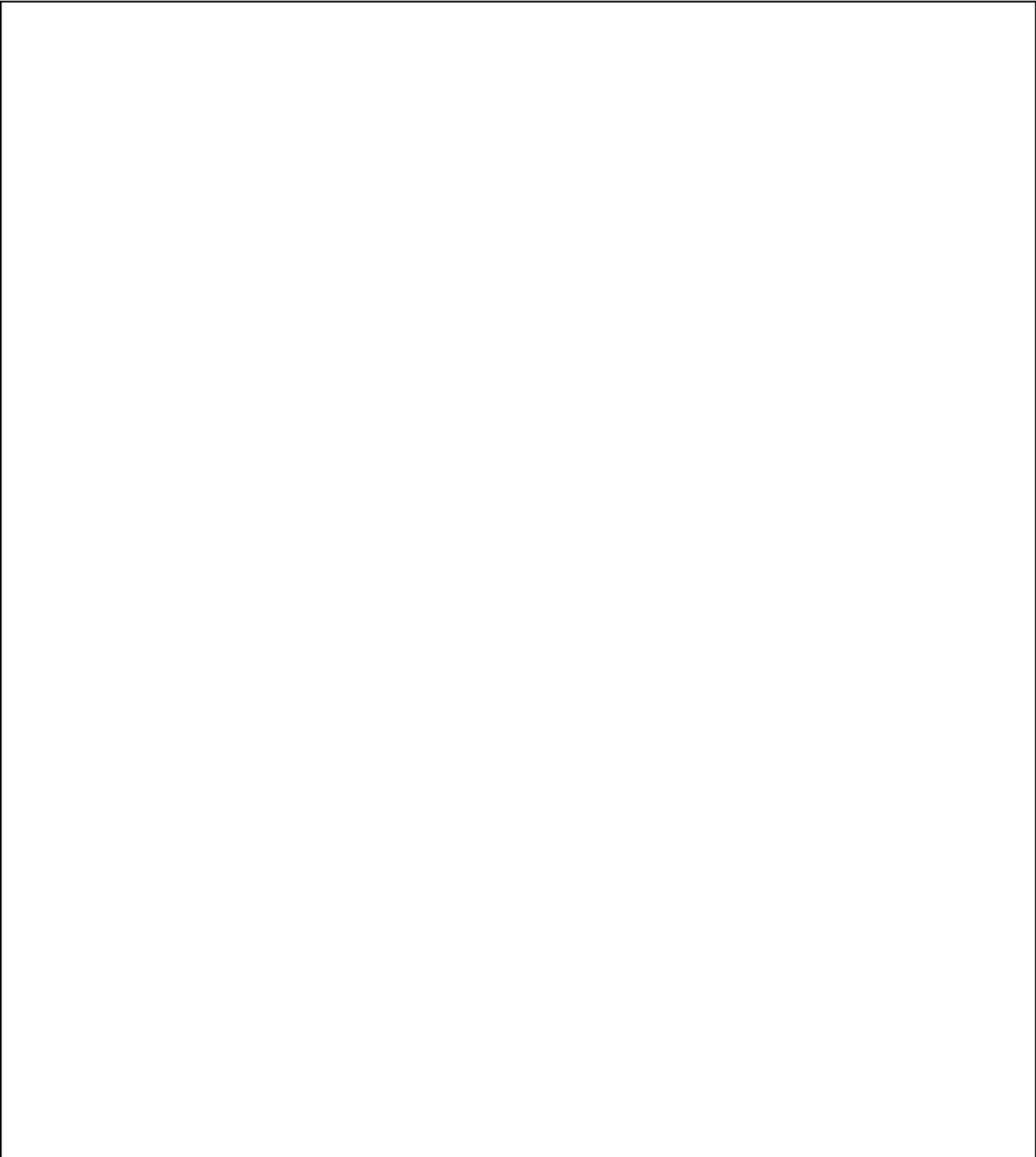


(b) (1)  
(b) (3)-18 USC 798  
(b) (3)-50 USC 3024(i)  
(b) (3)-P.L. 86-36

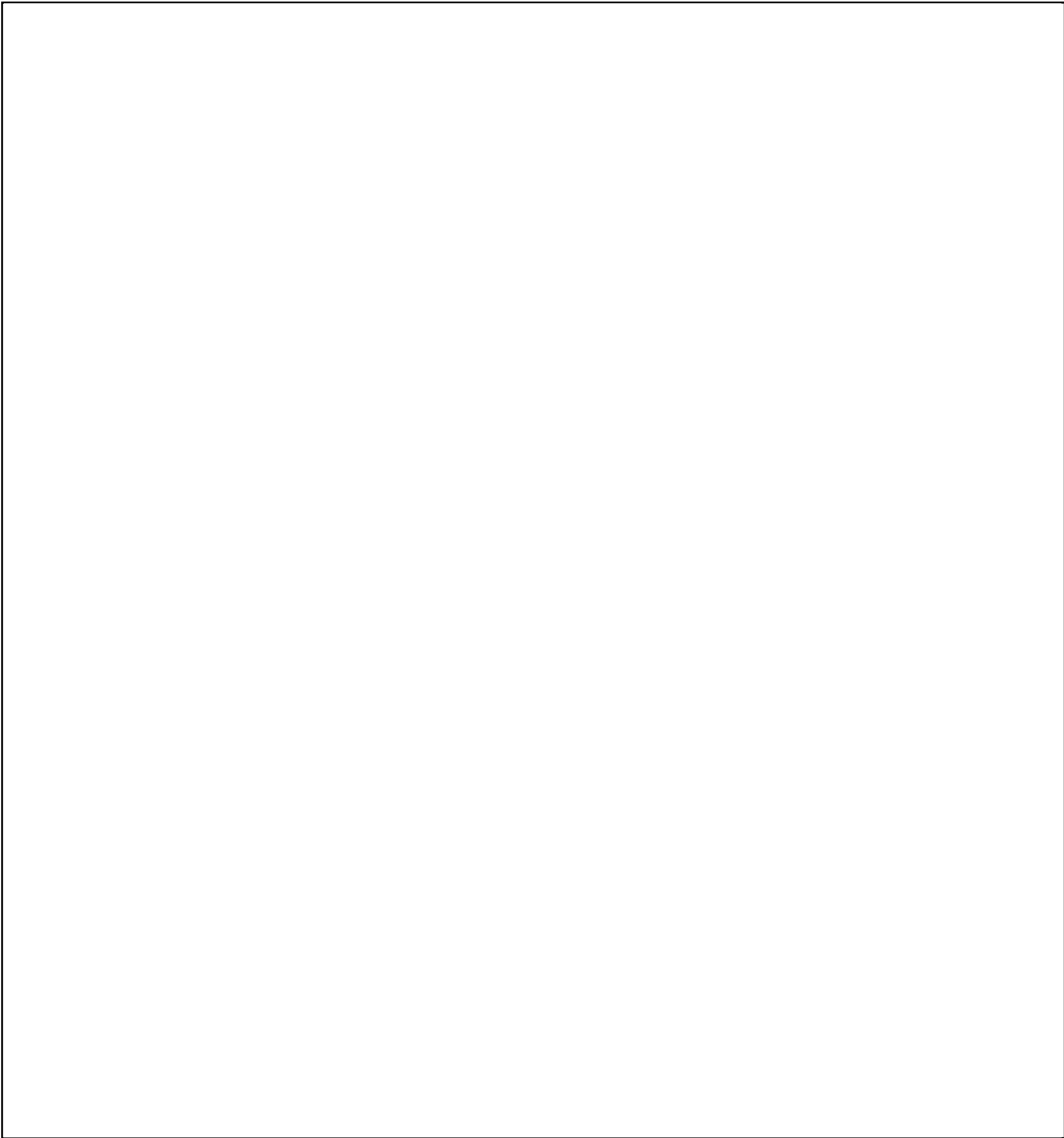


(b) (1)  
(b) (3)-18 USC 798  
(b) (3)-50 USC 3024 (i)  
(b) (3)-P.L. 86-36

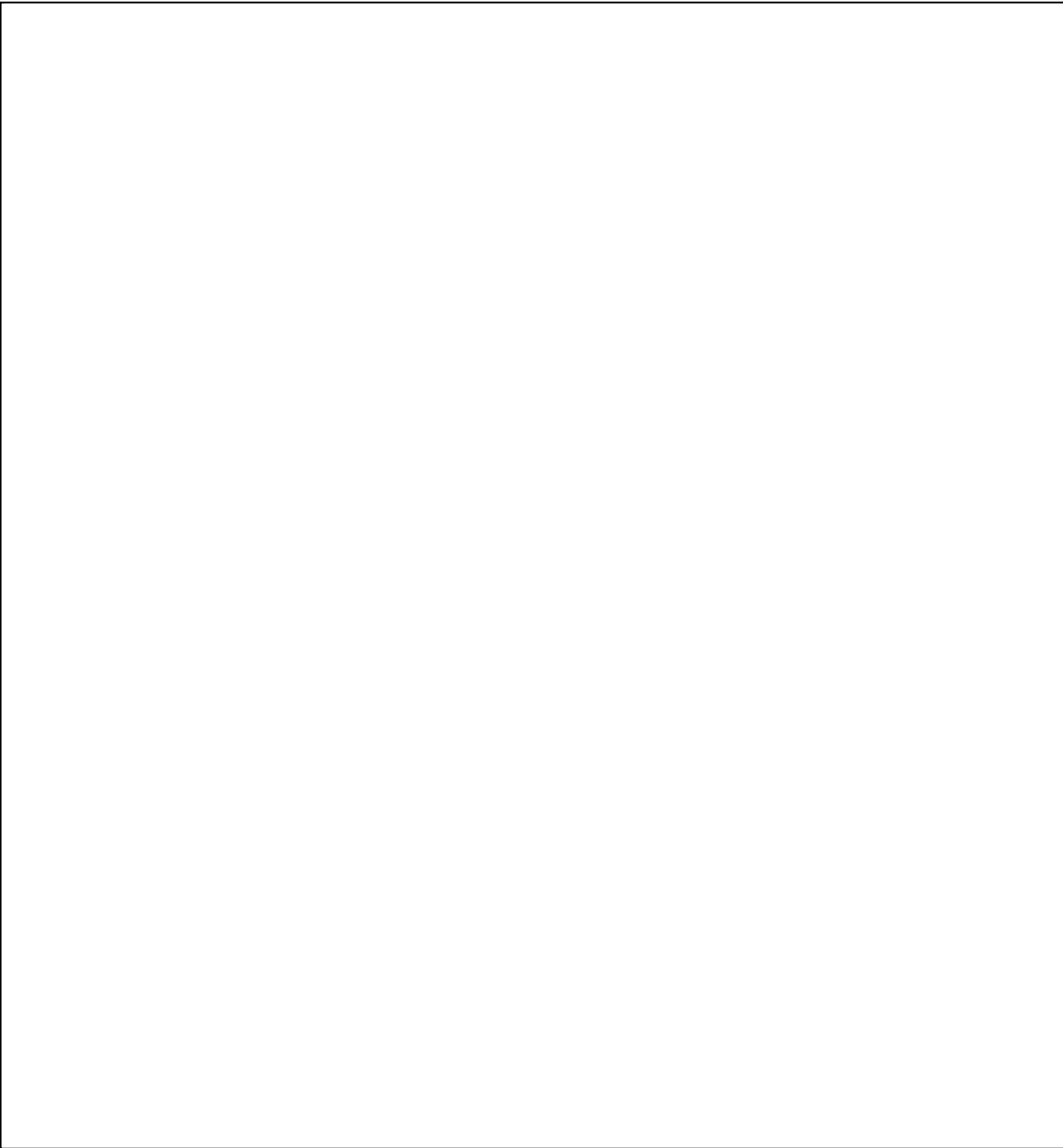




(b) (1)  
(b) (3)-18 USC 798  
(b) (3)-50 USC 3024(i)  
(b) (3)-P.L. 86-36



(b) (1)  
(b) (3)-18 USC 798  
(b) (3)-50 USC 3024(i)  
(b) (3)-P.L. 86-36



(b) (1)  
(b) (3)-18 USC 798  
(b) (3)-50 USC 3024 (i)  
(b) (3)-P.L. 86-36

## CHAPTER VII

## CYLINDRICAL CIPHER DEVICES AND STRIP CIPHER SYSTEMS

	Paragraph
General.....	45
Reconstruction of unknown cipher alphabets.....	46
Analysis of cryptograms involving known alphabets but with unknown keys.....	47
Further remarks.....	48

**45. General.**—*a.* The cryptography of cylindrical cipher devices and strip cipher systems was treated briefly in the previous text.¹ In the first published description of a cylindrical cipher device,² the apparatus consisted of 20 numbered rotatable disks, each bearing a different alphabet engraved on its periphery. The disks were to be arranged in an agreed-upon order on a shaft, and rotated so that the first 20 letters of the message plain text appeared in a row; the cipher text was then formed by arbitrarily taking off *any other row*—thus the basic cryptoprinciple is that of polyalphabetic substitution with the added complication of a *variable generatrix* feature. The remaining letters of the message were to be treated in the same fashion, 20 letters at a time. In decipherment, the disks were first arranged on the shaft according to the agreed-upon order, the first 20 cipher letters set up across one row, and the other rows searched for the one and only one row that contained plain text all the way across; and so on for the rest of the decipherment.

*b.* Credit for the original invention of the cylindrical cipher device belongs to Thomas Jefferson, among whose papers in the Library of Congress (vol. 232, item 41575, Jefferson's Papers) there was found in 1922 a description of a device incorporating 36 disks, on each of which are placed "all the letters of the alphabet, not in their established order, but jumbled & without order so that no two shall be alike." The device was independently invented for the third time by Captain Parker Hitt, U.S. Army, who in 1914 conceived a device of 25 disks, and also a similar apparatus of flat strips, cryptographically equivalent to the disk device. Hitt's alphabets were not very thoroughly mixed and bore many relationships among them so as to enable their reconstruction from memory—for example, there were many repetitions of sequences such as AEIOU, BCDFG, and HNRST. Major Joseph O. Mauborgne (later to become Chief Signal Officer of the U.S. Army) in 1917 noted that, because the alphabets were not thoroughly scrambled, the cryptograms produced by Hitt's device were too easily solved; his modification of the device, prescribing that "each disk have on it 26 letters of the alphabet, nonrepetitive on any disk and as far as possible so arranged that the fewest number of repetitions of pairs of letters . . . would occur," resulted in the adoption by the U.S. Army in 1923 of the cylindrical cipher device known as the M-94.

*c.* A strip cipher system comprises a series of printed, random-alphabet strips to take the place of the disks of a cylindrical cipher device; these strips, bearing identifying numbers, slide freely in the channels of a strip board which may be made of metal, wood, or plastic. The strips are simpler to produce and more economical to replace than metal disks; but, most important of all, with the use of strip cipher systems it is possible to incorporate certain simple modifications of the Jefferson principle (i.e., the variable-generatrix principle) which result in a very considerable augmentation of the security of the system. First of all, in cylindrical cipher devices the number of disks must be limited, for the sake of practicability, and furthermore all  $n$  disks (20 in the Bazeries device, 25 in the M-94) are always used together, so that the latent period is always  $n$ . But with a strip cipher system, it is possible to employ, say, 100 or more strips in the basic system, and then choose, for example, 30 of these strips for a daily key; furthermore, it is possible to employ a variable keying element *for each message*, so that several of the strips are eliminated before encryption begins, avoiding the possibility of the encryption of two messages in exactly the same key, and in general resulting in a latent flexible periodicity. Finally, because of the ease of production of paper strips, it is possible to have different sets of strips for different groups of holders, or for various types of traffic, thus reducing the volume of traffic in any one cryptosystem.

¹ See *Military Cryptanalytics, Part II*, pp. 443-444.

² Etienne Bazeries, *Les chiffres secrets dévoilés*, Paris 1901.

d. The analysis of cylindrical cipher devices and strip cipher systems involves two main aspects: (1) when the alphabets are unknown, and (2) when the alphabets are known, but their specific order is unknown. These cases will be discussed in the succeeding paragraphs.

46. Reconstruction of unknown cipher alphabets.—a. Let us assume that we have at hand the compromised plain text to a long cipher message, known to involve a cylindrical cipher device or strip cipher system of 25 alphabets.³ The matched plain and cipher, written on a width of 25, is shown below:

1.	THEFO	LOWI	NGALT	ERNAT	EPLAN	21.	AGENE	RALLY	PARAL	LELOF	ROADS
	EPWWZ	VIUFT	EVTJB	MCFIH	IBRSP		ZJAKJ	ADJTT	JXULT	BVMEE	WJITJ
2.	SOFDE	FENSE	FORTH	EREGI	MENTA	22.	TOONE	THREE	THREE	THREE	STOPO
	HEETJ	DFCMZ	WKUKR	ZGWAA	GYFKM		QUMWM	AXYFL	MQPGN	GEKKS	JYYXE
3.	LRESE	RVELI	NESAR	EHERE	BYSUB	23.	RDASH	TOEXT	ENDRE	GIMEN	TALDE
	PACCX	ZSSXE	WMVPM	PZZKJ	MSJSF		FGZRN	ZHPZK	UKVQM	OEKXZ	BJWLW
4.	MITTE	DCOLO	NONED	ASHAG	ENERA	24.	FENSI	VELIN	EBYTA	KINGU	PPOSI
	NPEFO	ENNQW	FBZKK	VLLCI	WYQWG		BREPN	WQBAB	YHXVQ	XXXOM	QRRBP
5.	LDEFE	NSEOF	REGIM	ENTAL	RESER	25.	TIONS	INDEF	ENSEO	FNORT	HWEST
	IUQVK	KAANS	VCRGU	BUCHJ	UXXJI		UDLQR	GJUIE	KWXTN	DINVC	AOXUS
6.	VELIN	ESCOM	MAWIT	HDEPL	OYMEN	26.	SLOPE	OFBUC	KHILL	ANDSO	UTHSL
	NPIWL	HZXXE	GKHMV	IOIVF	TQRKS		USXFP	JKUKT	PSQKU	LJRFC	HNXPI
7.	TOFTH	REERI	FLECO	MPANI	ESINL	27.	OPESO	FDIŞC	UMHIL	LSTOP	FOURD
	CAUGN	MUPHM	OIUOH	FYVPF	TGEBI		HVMNN	WRGCU	QVCWW	MFVDY	OMRCT
8.	INESU	PPORT	EDBYC	OMPAN	YHAND	28.	ASHIN	CASEO	FATTE	MPTED	ENEMY
	LJWUW	JWUGE	WJPQV	WWAIX	PYLQM		YTTQR	WVJXX	QTAFI	EACYQ	LOSTP
9.	USING	THERI	FLECO	MPANY	MACHI	29.	PENET	RATIO	NSTHR	OUGHL	EWISV
	VWZTX	EAQCW	RFFZX	IDHXL	JYJCK		TQBPF	ADQCK	AJDDN	RACOC	AMTVN
10.	NEGUN	SFROM	SELEC	TEDPO	SITIO	30.	ALLEY	DASHT	OCOUN	TERAT	TACKF
	YYQAH	CNHLI	ZUWPA	HIVNG	PXJWH		DGJGZ	JBXPZ	ZPNXF	RDIFY	KLXLR
11.	NSFRO	MTHIS	LINES	TOPTW	ODASH	31.	ROMEA	STSLO	PEOFB	UCKHI	LLORF
	LNSGF	JUGJN	RBOZB	ANNUP	VYJQA		EXCLI	GNHJZ	YQIIE	VVAKJ	KQJVM
12.	DEFEN	SEOFR	EGIME	NTALR	ESERV	32.	ROMSO	UTHWE	STSLO	PEOFH	ERRHI
	QODLJ	GOQBI	QKUVI	RPOMB	QNMVE		TIWTF	PUGNY	EHKHU	HMMAV	KIBLS
13.	ELINE	SSTOP	THREE	DASHI	NCASE	33.	LLSTO	PFIVE	DASHI	NCASE	OFATT
	VGRAA	EFPFU	PTCMW	YTQBS	XVVZZ		SUIYT	ITJED	YFYTS	TQMUH	YIWAH
14.	OFATT	EMPTE	DENVE	LOPME	NTOFO	34.	EMPTE	DENVE	LOPME	NTOFO	URLEF
	LIDNJ	TQJZL	IWCIN	XFLIS	KYYRE		UNXAF	SVXYH	PQIKF	WXRCH	TPPIC
15.	URRIG	HTFLA	NKDas	HTOCO	UNTER	35.	TFLAN	KDASH	TOEXT	ENDOU	RDEFE
	EYZZL	LDJEZ	TUEGP	ZVDFR	EDXWY		PVGHJ	CACFV	HCBML	NHPHO	JJMMB
16.	ATTAC	KFROM	VICIN	ITYOF	RJONE	36.	NSELI	NEBYT	AKING	UPPOS	ITION
	NKRSH	FCEQN	XXNVE	GFKTG	HRFHO		KYAEA	GFTOB	YGOHA	OTDEQ	MQTMO
17.	THREE	THREE	THREE	MOVIN	GFROM	37.	ONNOR	THEAS	TSLOP	EOFSY	KESHI
	RLDGA	INGNG	PTCMW	XSFUG	FHFNT		ULGCK	JLWLH	KTPGQ	RKLWA	ZATUM
18.	RESER	VEASS	EMBLY	POSIT	IONWE	38.	LLORB	UTLER	HILLO	ROCO	UNTER
	BLYJE	OVWZI	XCTMT	BZBPI	RFAED		GRISX	FPXWK	BLWWB	PGUQG	NTJPA
19.	STVIA	STONE	WALLC	OMMAS	OUTHW	39.	ATTAC	KFROM	BUTLE	RHILL	ORGEN
	BVKLK	MJVXJ	CHKRQ	AHBLM	FAHIR		QSHOU	NPOBK	UWIJA	QKPKG	WVYVP
20.	ESTVI	ASTON	EWALL	TOROA	DCOMM	40.	ERALL	YALON	GTHEM	ORLAY	TRAIL
	IBVPT	GYDIM	JONEJ	GFKJU	QOYVP		YHGPA	FIMGZ	LSTAK	NUFNN	RUTVS

³ The diagnosis of a strip cipher system was made from the characteristic frequency distribution—made cumulatively on all the traffic—associated with a noncrashing system (see subpar. 48c); the number of strips involved was determined from the factors of intervals between long polygraphic repetitions found within or between messages.

b. Our first step is to make tabulations of the columnar plain-cipher equivalencies, as a prelude to the establishment of related lines of matched plain and cipher. In these tabulations the vertical plain-cipher digraphs have been recorded (under the reference alphabet) as single-letter entries under the earlier letter in the normal alphabetic sequence, so that, in col. 1 for example, TE and SH are recorded in the inverse form as ET and HS, while LP is recorded as LP. The tabulations for the first five columns of the 40 pairs of lines are shown below, where letters that have occurred at least twice in combination with the reference letter are ringed.

Col. 1: A B C D E F G H I J K L M N O P Q R S T U V W X Y Z  
 N R T Q T R L S (L) N P N V U (T) (T) U U V  
 Z S V O (L) N Y (T) (T)  
 Y F (U) O  
 D I S  
 Q R  
 (U)  
 Y

Col. 2: A B C D E F G H I J K L M N O P Q R S T U V W X Y Z  
 R S U (O) I (L) P P N T S N S U V Y W V  
 O G P V J L O U X (T)  
 I V (L) R N Y  
 (O) R (T)  
 L  
 R  
 Q

Col. 3: A B C D E F G H I J K L M N O P Q R S T U V W X Y Z  
 D N E F (W) U Q (T) L L V O O X X Z Y V  
 (E) M R F S L (T) Z W T  
 Z T N R  
 (E) Q S  
 G (W) O  
 N  
 M

Col. 4: A B C D E F G H I J K L M N O P Q R S T U V W X Y Z  
 U S T (L) W T W N P (T) V (S) U Y  
 N (G) T R Z (T) S (S) T  
 S J V O L W  
 T P P Q Q  
 H (G) S  
 O (L)  
 (L)

Col. 5: A B C D E F G H I J K L M N O P Q R S T U V W X Y Z  
 (E) X H (J) (O) X (N) T (N) R N O Z S W Z  
 (E) U X T L (N) N T R T  
 K O (O) (N) (N)  
 (T) K  
 (T) R  
 L (J) M P F

* * * * *

c. The summary of related lines of matched plain and cipher from the foregoing five tabulations is given below:⁴

- |                                                                                                |                                                                                                                        |
|------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------|
| Col. 1: EU 15, $\tilde{34}$<br>PT 29, $\tilde{35}$<br>RT 17, $\tilde{32}$<br>IL 5, $\tilde{8}$ | Col. 4: EL 12, 31, $\tilde{36}$<br>EG 17, 30<br>NT 9, $\tilde{14}$<br>RS 23, $\tilde{38}$                              |
| Col. 2: EO 2, $\tilde{12}$<br>GL 13, 30<br>ST 28, $\tilde{39}$                                 | Col. 5: AE 13, 17<br>AI 31, $\tilde{36}$<br>EJ 2, 21<br>FO 11, 32<br>HN 7, $\tilde{10}$ , 23<br>JN 12, 35<br>* * * * * |
| Col. 3: AE 21, 36<br>EW 1, 8<br>HT 28, $\tilde{39}$                                            |                                                                                                                        |

A family of seven related lines (2,  $\tilde{12}$ , 21, 29,  $\tilde{31}$ ,  $\tilde{35}$ , 36) is evident among the relationships set forth above; and several more families of related lines may also be built up from the foregoing data. If we examine all 40 lines, we will arrive at the following families:

- Family "A": 2,  $\tilde{12}$ , 21, 29,  $\tilde{31}$ ,  $\tilde{35}$ , 36
- Family "B": 1, 5, 8,  $\tilde{28}$ , 39
- Family "C": 7,  $\tilde{10}$ , 23, 26,  $\tilde{38}$
- Family "D": 9, 14,  $\tilde{16}$ , 20, 22
- Family "E":  $\tilde{11}$ , 13, 17, 30,  $\tilde{32}$
- Family "F":  $\tilde{15}$ , 18,  $\tilde{24}$ , 34
- Family "G": 3,  $\tilde{25}$
- Family "H": 19,  $\tilde{27}$
- Family "I": 37,  $\tilde{40}$

Lines 4, 6, and 33 are isolated members of three different families: a maximum of 13 families in all is possible.

d. The relationship among the seven members of Family "A" is made clear when we examine the lines of matched plain and cipher:

2.	S(0)FD(E)	FENSE FORTH EREGI MENTA
	H(E)ET(J)	DFCMZ WKURR ZGWAA GYFKM
(12.)	D(E)F(E)N	SEOFRE GIMENTALR ESERV
	Q(0)D(L)J	GOQB I QKUVDR POMB QNMVE
21.	AG(E)N(E)	RALLY PARAL LELOF ROADS
	ZJ(A)K(J)	ADJTT JXULT BVME E WJITJ
29.	(P)ENET RATIO NSTHR OUGHL EWISV	
	(T)QBPF ADQCK AJDDN RACOC AMTVN	
(31.)	ROM(E)(A)	STSL OPEOFBU CKHILLORF
	EXCL(I)	GNHJZ YQIEE VVAKJ KQJVM
(35.)	(T)FLA(N)	KDASH TOEXT ENDOU RDEF E
	(P)VGH(J)	CACFV HCBML NHPHO JJMMB
36.	NS(E)LY(I)	NEBYT AKING UPPOS ITION
	KY(A)E(A)	GFTOB YGOHA OTDEQ MQTMO

⁴ The tilde (~) over the numbers indicates an inverse relationship between the lines involved; this point is clarified in subpar. d, below.

In this diagram, the identities of encipherment in the first five columns have been marked with a solid oval ring, while the inverse (i.e., reciprocal) relationships have been marked with a dotted oval ring. Thus it may be seen that lines 2, 21, 29, and 36 involve the same plain and cipher generatrices, while lines 12, 31, and 35 involve the same generatrices, but interchanged between plain and cipher. This means that for Family "A" we can establish the following two-letter chains as belonging to col. 1 (i.e., alphabet 1):

2   12   21   29   31   35   36  
SH   QD   AZ   PT   ER   PT   NK

(Note that we have reversed the letters of the digraphs from lines 12, 31, and 35 which bear an inverse relationship to the other four lines.)

e. Since Families "A" through "F" contain the most members, we proceed to make chains for the individual alphabets. Below are given the chains for the first five alphabets, as an illustration:

Family "A"	Family "D"
1. SH QD AZ PT ER NK	1. VU OL NA EI TQ
2. XOEQ GJ VF SY	2. WSB FI KT OU
3. DFEA NB CM GL	3. ZI AD RTV OM
4. DT LEP NK HA	4. TNW SA VP
5. EJN TF IA	5. XG ITJ HC EM
* * * * *	* * * * *
Family "B"	Family "E"
1. TE IL YAQ	1. LN EV TR AD
2. HP UD NJ TS	2. NS HLG IO
3. QEW TH	3. SF IRD LJ WM
4. VFW SU QI AO	4. EGR NA TS
5. OZ KE CUW RN	5. FO EA YZ
* * * * *	* * * * *
Family "C"	Family "F"
1. TC YN RF SU GL	1. EU RBF
2. OA YE RLS DG	2. YREL MN
3. FU QG AZ IOX	3. ZR SY EN PX
4. TG AU SR PF	4. ZI EJ PS TA
5. HN EP XB	5. LG REF NI
* * * * *	* * * * *

We can now begin to amalgamate the chains within each alphabet in order to reconstruct the strips involved. In employing the graphical method of indirect symmetry, we arbitrarily assign to Family "A" the direction ↓, and to Family "D" the horizontal direction →. Thus in the initial reconstruction of the first five alphabets, we shall have the following partial diagrams, among lesser fragments:

Alph. 1	Alph. 2	Alph. 3	Alph. 4	Alph. 5
NA	X	AD	D	EM
KZ	OU	F	TNW	ITJ
	E	E	K	AFN
	Q	A		



Family "F" is tied into the diagrams through the observed relationship of REF in Alphabet 5 which is tied into the EF already in the diagram, establishing the direction of Family "F" as ↙¹2. The other

families are soon tied in; Alphabet 3 is reconstructed in its entirety, while the other four alphabets are recovered with only two or three blanks, after all the relationships present in the columns have been exhausted.⁵

f. The 25 alphabets recoverable from the 40 lines of matched plain and cipher are the following:⁶ (The ringed letters could be recovered from other messages in the same key.)

1. A B C E I G D **(j)** F V U Y M H T Q K Z O L R **(x)** S P **(w)** N
2. A **(c)** D E H F I J K T L M O U V Y G **(z)** N P Q X R W S B
3. A D K O M J U B G E P H S C Z I N X F Y Q R T V W L
4. A E D C **(b)** I F G J H L K **(m)** R U O Q V P T N W Y **(x)** Z S
5. A F N **(q)** U K **(d)** O P I T J B R H C Y S L W E M Z **(v)** X G
6. A G P O C I **(x)** L U R N D Y Z H W **(b)** J S **(q)** F K V M E T
7. A H X J E Z B N I K P V R O G S Y D U L C F M Q T W
8. A I H P J O B W **(k)** C V F **(z)** L Q E R Y N S U M G T D X
9. A J _d S _k Q O I V T Z E F H G Y _u N L P M B X W C R
10. A K E L B D F J G H O N M T P R Q S V Z U X Y W I C
11. A L T M S X V Q P N O H U W D I Z Y C G K R F B E J
12. A M N F L H Q G C U J T B **(y)** P **(z)** K X I S **(r)** D V E W O
13. A N C **(j)** I L D H B **(m)** K G X U Z T S W Q Y V O R P F E
14. A O D W P K J V I U Q H Z C T X **(b)** L E G N Y R _s M F
15. A P B V H I Y K S G U E N T C X O W F Q D R L J Z M
16. A Q **(j)** N U B T G I M W Z R V L X **(c)** **(s)** H D E O K F P Y
17. A R M Y O F T H E U S Z J X D P C W G Q I B K L N V
18. A S D M C N E Q B O Z P L G V J R K Y T F U I W X H
19. A T O J Y L F X N G W H V C M I R B S E K U P **(d)** **(z)** Q
20. A U T R Z X Q L Y I O V B P E S N H J W M D G F C K
21. A V N K H R G O X E Y B F S J M U D Q C L Z W T I P
22. A W V S F D L I E B H **(k)** N R J Q **(z)** G M X P U C O T Y
23. A X **(k)** W R E V **(d)** T U F O Y H M L S I Q N J C P G B **(z)**
24. A **(v)** J P X M V K B Q W U **(g)** L O S T E C H N Z F R I D
25. A Z D N B **(u)** H Y F W J L V G R C **(q)** M P S O E **(x)** T K I

⁵ It would be excellent practice for the reader to reconstruct the first five alphabets—and, for that matter, all 25 of them—following the procedures exemplified in the foregoing subparagraphs.

⁶ These are actually the alphabets of the U.S. Cipher Device, Type M-94, in their original order and at the correct decimation.

47. Analysis of cryptograms involving known alphabets but with unknown keys.—a. After the alphabets have been reconstructed, all messages which are in the same key (i.e., using the same order of the strips as just recovered) can now be read automatically. Subsequent key changes involve a permutation in the order of the strips, and for the analysis of messages in other key periods we must first construct 26 charts called "synoptic tables" which will facilitate our work. These tables are nothing more than generatrix diagrams based on the original recovered strips arranged vertically, in which the top rows of the tables consist of the strips aligned to all A's, all B's, etc., as shown in fragmentary form for the first two tables below:⁷

Synoptic Table for A

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25
0	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A
1	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
2	C	D	K	D	N	P	X	H	D	E	T	N	C	D	B	J	M	D	O	T	N	V	K	J	D
3	E	E	O	C	Q	O	J	P	S	L	M	F	J	W	V	N	Y	M	J	R	K	S	W	P	N
4	I	H	M	B	U	C	E	J	K	B	S	L	I	P	H	U	O	C	Y	Z	H	F	R	X	B
5	G	F	J	I	K	I	Z	O	Q	D	X	H	L	K	I	B	F	N	L	X	R	D	E	M	U
									*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*
23	P	W	V	X	V	M	Q	T	W	W	B	E	P	S	J	F	L	W	D	F	T	O	G	R	T
24	W	S	W	Z	X	E	T	D	C	I	E	W	F	M	Z	P	N	X	Z	C	I	T	B	I	K
25	N	B	L	S	G	T	W	X	R	C	J	O	E	F	M	Y	V	H	Q	K	P	Y	Z	D	I

Synoptic Table for B

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25
0	B	B	B	B	B	B	B	B	B	B	B	B	B	B	B	B	B	B	B	B	B	B	B	B	B
1	C	A	G	I	R	J	N	W	X	D	E	Y	M	L	V	T	K	O	S	P	F	H	Z	Q	U
2	E	C	E	F	H	S	I	K	W	F	J	P	K	E	H	G	L	Z	E	E	S	K	A	W	H
3	I	D	P	G	C	Q	K	C	C	J	A	Z	G	G	I	I	N	P	K	S	J	N	X	U	Y
4	G	E	H	J	Y	F	P	V	R	G	L	K	X	N	Y	M	V	L	U	N	M	R	K	G	F
5	D	H	S	H	S	K	V	F	A	H	T	X	U	Y	K	W	A	G	P	H	U	J	W	L	W
									*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*
23	W	R	M	E	I	Z	J	P	L	K	K	U	L	C	M	J	G	N	M	I	X	L	C	M	Z
24	N	W	J	D	T	H	E	J	P	E	R	J	D	T	A	N	Q	E	I	O	E	I	P	V	D
25	A	S	U	C	J	W	Z	O	M	L	F	T	H	X	P	U	I	Q	R	V	Y	E	G	K	N

(The small numbers on top are the strip numbers, while the large numbers at the side are the generatrix numbers.)

b. Let us now assume that we have at hand the following cryptogram enciphered by a different permutation of the strips that we have recovered, and that the first word of the underlying plain text is DIVISION:

C	T	Y	N	O	J	L	T	D	P	L	R	S	Z	J	Z	U	U	W	H	I	O	W	S	Y
J	Q	J	Z	G	O	Z	T	S	H	E	X	P	E	O	V	D	E	Y	A	I	L	Q	V	M
L	Z	U	I	I	W	D	C	K	W	S	O	J	I	W	Z	G	M	S	Z	R	H	G	Y	D
G	Z	R	V	K	M	Y	S	Z	R	T	P	W	Y	E	Q	Q	C	T	F	F	B	V	L	S

Our first step will be to determine the possible generatrices for the encipherment of DIVISION as CTYNOJLT. If we refer to the synoptic table for the letter D, we can see that D may be enciphered as C on generatrices 1, 2, and 3, but not by 5 through 8, nor by 10, 15, 18, 21, or 24. Similarly, referring to the synoptic table for the letter I, we find that I_p=T_c is possible on all generatrices except 4, 5, 9, and 21.

⁷ The complete synoptic tables are given in Appendix 2.

This process is repeated for all eight plain-cipher equivalencies of the encipherment of the putative crib; the results are shown in Fig. 73, below, wherein the x's indicate the generatrix possibilities for the eight encipherments. It will be seen that the correct generatrix must be either 1, 12, 19, or 25, since all the letters of the encipherment of the initial crib must necessarily come from a single generatrix.

	D I V I S I O N							
	C	T	Y	N	O	J	L	T
1	x	x	x	x	x	x	x	x
2	x	x	x	x		x		x
3	x	x	x		x	x	x	x
4	x		x	x	x	x		x
5			x	x	x		x	x
6		x	x		x		x	x
7		x	x	x		x		
8		x			x		x	x
9	x		x	x		x	x	x
10		x		x	x	x		x
11	x	x	x		x	x	x	
12	x	x	x	x	x	x	x	x
13	x	x		x				x
14	x	x			x	x		x
15		x		x				x
16	x	x	x		x	x	x	
17	x	x	x	x	x		x	x
18		x	x			x		x
19	x	x	x	x	x	x	x	x
20	x	x		x	x	x		x
21			x	x	x	x	x	x
22	x	x	x	x	x		x	x
23	x	x	x	x				x
24		x			x	x	x	
25	x	x	x	x	x	x	x	x

FIGURE 73

c. The next step is to consider each generatrix in turn, and determine which strip or strips can give rise to the particular encipherment on that generatrix. For example, in taking generatrix 1 into consideration, we find from the synoptic tables the following possibilities for strips:

D I V I S I O N							
C	T	Y	N	O	J	L	T
4	5	2	3	25	2	1	15

Generatrix 1 is impossible, because we cannot have strip number 2 in two positions since the permutation of strips does not admit of any repeated elements. Likewise, generatrix 25 is ruled out because of repeated unique strip numbers:

D I V I S I O N							
C	T	Y	N	O	J	L	T
2	21	13	7	24	13	24	4

The strip permutations (with multiple possibilities) for generatrices 12 and 19 are shown below:

D I V I S I O N  
C T Y N O J L T  
 Gen. 12:  $\begin{matrix} 3 & 17 & 16 & 2 & 8 & 6 & 9 & 20 \\ & 19 & 14 & & & & & 22 \end{matrix}$

D I V I S I O N  
C T Y N O J L T  
 Gen. 19:  $\begin{matrix} 6 & 12 & 5 & 10 & 18 & 11 \\ 24 & 20 & 19 & & 16 & 17 \end{matrix}$

Note that in the strip possibilities for generatrix 19 we have crossed out a 5, 10, and 19 from some columns since these numbers are uniquely represented in three other positions.

d. Generatrices 12 and 19 both admit of 8 possibilities of strip arrangements, so we shall try the former first. We first try the strip order 3-17-16-2-8-6-9-20 and, searching in the other three lines of cipher text for plausible plaintext fragments, we arrive at the results shown in Fig. 74a, below. The

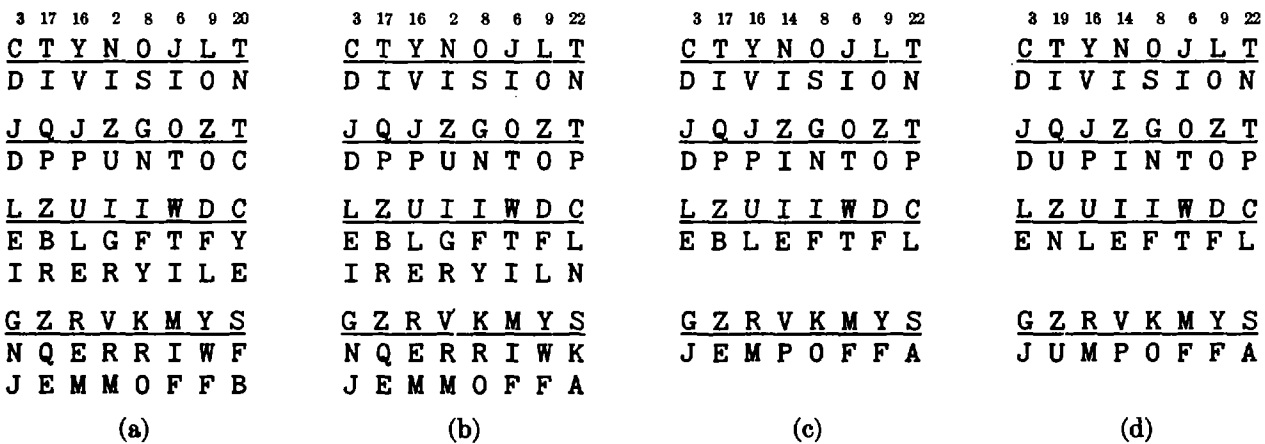


FIGURE 74

cipher JQJZGOZT yields DDPUNTOC as an interesting possibility; the cipher LZUIIWDC yields EBLGFTFY and IRERYILE that contain plausible plaintext fragments, while cipher GZRVKMYS yields NQERRIWF and JEMMOFFB among other generatrices containing fragments of what may be plain text. We now change the strip number 20 in the last position to its other variant, 22, and we see what the strip order 3-17-16-2-8-6-9-22 gives us; the results are shown in Fig. 74b. Changing the fourth strip (number 2) into its variant, 14, improves matters, as shown in Fig. 74c; and finally when we change the strip in the second position (number 17) into its variant, 19, so that the strip order now reads 3-19-16-14-8-6-9-22, we get valid plain text all the way across the generatrices, as shown in Fig. 74d.

e. The continuation of the third row of Fig. 74d seems to be the word FLANK; when this is assumed, the word POSITION emerges in the second row of the cipher text, as is shown in the decryption below:

```

  3 19 16 14 8   6 9 22 1 24   10 4 20 17 15
  C T Y N O   J L T D P   L R S Z J   Z U U W H   I O W S Y
  D I V I S   I O N r e   s e r v e
  J Q J Z G   O Z T S H   E X P E O   V D E Y A   I L Q V M
  D U P I N   T O P o s   i T I O N
  L Z U I I   W D C K W   S O J I W   Z G M S Z   R H G Y D
  E N L E F   T F L A N   K s t o p
  G Z R V K   M Y S Z R   T P W Y E   Q Q C T F   F B V L S
  J U M P O   F F A t n   o o n a s

```

At this point it might be noticed that the key exhibits isomorphism beginning with the 12th element: this is the result of the use of an 11-element basic key (with a literal key probably underlying the key numbers) expanded to the required 25 elements. Thus the complete key may be recovered as in the following diagram:

3 19 16 14 8 6 9 22 1 24 10  
4 20 17 15 11 7 12 23 2 25 13  
5 21 18

When this key is tried, it is found that the entire message can be read. A numerical key of the numbers of the top row of the foregoing diagram is made, and when this simplified basic key of 2-9-8-7-4-3-5-10-1-11-6 is analyzed,⁸ it is found to be based upon the word CONFEDERATE, and the method of key production by the cryptographer was probably the following:

5 10 15 20 25  
C O N F E D E R A T E C O N F E D E R A T E C O N  
3 19 16 14 8 6 9 22 1 24 10 4 20 17 15 11 7 12 23 2 25 13 5 21 18

f. The preceding case exemplified the exploitation of a crib whose position was known or assumed. In the next example we shall assume that the cryptogram below contains the word HEADQUARTERS, but that its position in the message is unknown:

A E N L V D C B J Q J M T F E B J G L P A Q K O T  
Z P C R U J J Z P N V X P T C Z J E F K H S L I L  
W R Z G Q Y I Y S Q R R D H V S C L H Z C W G L W  
Z P R T Q K B L K K N N A I S W E A F Z A O A O A

Our first step is to determine the location of the crib. We could take advantage of the noncrashing properties of a strip cipher system, but there still would be too many possibilities for the placement of the crib; the property of the *limitations* of the cipher equivalents for plaintext letters on each generatrix will therefore be used. Since we do not know the generatrix involved, we shall first assume that it is number 13, and then, if this is unsuccessful, we shall try 14, 12, 15, 11 . . . in turn, until we have determined the correct generatrix.

g. In the alphabets of the M-94 there is a considerable limitation in the cipher equivalents of plaintext letters on all generatrices, except for generatrix numbers 1 and 25.⁹ For example, in the synoptic table for A, we find on the 13th generatrix no occurrence of the letters A, B, D, E, F, I, J, K, M, N, or Q. If we were to make diagrams of the impossible cipher equivalents for the letters in the word HEAD-QUARTERS, on let us say, generatrix numbers 13 and 20, they would be the following:

<i>Generatrix 13</i>	<i>Generatrix 20</i>
<u>H E A D Q U A R T E R S</u>	<u>H E A D Q U A R T E R S</u>
C A A A A C A B G A B C	B B A D C B A A B B A A
H E B B D D B C H E C D	E D B F G C B C C D C C
J I D D G F D H L I H E	H E G G H E G D L E D D
K L E I H G E K N L K F	M F H J I G H J O F J H
N M F N M H F L T M L G	Q G S K M K S K P G K M
P N I P O L I O U N O K	W J T L N L T L T J L P
Q P J Q Q M J R Z P R N	Y N W M Q N W M V N M R
R S K S U O K X S X O	R X O U O X N X R N S
T V M U Z Q M V P	Y Q W S Y Q Z Q X
U Y N T N Y S	Z T T Z R R
X Q U Q	U U U U
X	W Y Y

⁸ For the method of derivation of literal keys from numerical keys, see pp. 427-429 of *Military Cryptanalytics, Part II*.

⁹ These alphabets have been specially constructed so that the smallest number of repetitions of pairs of letters would occur; in the 25 sequences, the only digraphs appearing twice are DE, YA, and UB. Nevertheless, there are manifold occurrences of skip digraphs (A-B, A-B, etc.) at wider intervals.



of the crashing plain and cipher text, nor for the same reason can it begin in 12 other positions in the range specified; thus there are only 20 positions left to try. The first trial, assuming that the crib begins at position 16, is shown in Fig. 75a, below, and it is seen that generatrix numbers 14 and 25 are the

Crib at position 16

	H E A D Q U A R T E R S											
	B	J	G	L	P	A	Q	K	O	T	Z	P
1	x	x	x	x	x		x	x	x	x	x	x
2	x				x	x					x	
3					x			x	x	x	x	
4	x	x			x			x	x	x	x	x
5	x	x	x		x	x	x	x				x
6	x	x	x			x	x		x	x		x
7	x	x	x		x		x	x	x			x
8	x	x	x	x	x	x			x	x	x	x
9	x	x	x	x	x		x	x				x
10		x		x		x	x	x	x			x
11	x	x	x							x	x	
12	x	x	x	x		x		x		x		x
13	x	x	x	x	x	x			x	x	x	
14	x	x	x	x	x	x	x	x	x	x		x
15	x	x		x	x	x	x		x			
16		x	x	x	x	x	x	x	x	x	x	x
17		x	x			x						x
18			x		x	x	x		x	x		x
19		x	x			x					x	x
20				x	x	x			x	x		x
21	x			x		x					x	x
22	x	x	x	x	x	x	x	x	x	x	x	x
23		x		x		x	x	x			x	x
24	x			x	x		x	x	x	x	x	x
25	x	x	x	x	x	x	x	x	x	x	x	x

FIGURE 75a

Crib at position 20

	H E A D Q U A R T E R S											
	P	A	Q	K	O	T	Z	P	C	R	U	J
1	x	x	x	x	x	x		x	x	x	x	x
2		x			x	x	x			x		x
3		x	x	x	x	x			x			x
4					x	x	x		x	x		x
5	x	x	x		x	x		x	x	x	x	x
6	x	x	x	x		x		x		x	x	x
7		x	x			x			x			x
8	x	x		x	x				x		x	x
9	x	x	x	x	x							x
10	x		x	x	x				x	x	x	x
11	x	x			x				x		x	x
12	x	x		x					x	x	x	x
13					x				x	x	x	x
14	x		x						x	x	x	x
15	x	x	x	x	x				x	x	x	x
16	x	x		x	x	x			x	x	x	x
17		x			x	x			x		x	x
18		x	x	x	x	x			x	x	x	x
19	x	x		x	x				x	x		x
20	x	x	x	x	x				x			x
21	x	x		x					x	x		x
22	x	x	x	x	x	x			x		x	x
23	x	x	x	x	x	x			x	x	x	
24	x				x				x	x	x	x
25	x	x	x	x	x	x			x	x	x	x

FIGURE 75b

only ones with x's all the way across to the vertical line marking the end of a line of 25 cipher letters of the message.¹⁰ Fig. 75b shows the second trial, assuming that the crib begins at position 20 with the letters being split 50-50 on two cipher lines; the first six letters could involve generatrix numbers 1, 23, or 25, while the last six letters could involve generatrix numbers 1, 13, 14, 15, or 25. Both of the first two trials come to naught, since the keys derived do not yield plain text in other parts of the message.

¹⁰ As mentioned in the previous footnote, these particular alphabets have been constructed so as to achieve the maximum variety of consecutive digraphs among the 25 sequences, therefore in the M-94 alphabets generatrix numbers 1 and 25 will almost always be present as possible candidates. If the alphabets had been constructed by a truly random process, these generatrices would be present no more frequently than any other generatrix.

(4) After very considerable and laborious experimentation involving several hundred trials, we arrive at the placement of the crib at position 72 as shown in Fig. 75c, below:

	H E A D Q U A R T E R S											
	W	G	L	W	Z	P	R	T	Q	K	B	L
1	x	x	x	x	x	x	x	x	x	x	x	x
2	x	x			x					x	x	
3	x	x	x	x	x	x	x	x	x	x	x	x
4			x	x		x	x	x	x			x
5	x	x	x	x	x	x	x	x	x			
6		x	x			x		x	x			x
7		x	x	x	x			x			x	x
8		x		x	x							
9		x		x	x	x	x					x
10	x	x	x		x	x		x	x	x		
11	x		x	x	x			x	x	x	x	x
12	x	x	x		x	x	x	x			x	x
13	x	x	x	x		x	x	x	x	x		x
14	x		x				x		x	x		x
15			x				x				x	x
16	x	x				x	x	x		x	x	
17	x		x	x		x		x	x			x
18	x	x	x	x	x	x		x			x	x
19	x		x	x	x			x	x	x	x	
20			x			x	x	x	x	x	x	x
21		x		x			x	x				
22			x	x		x	x	x		x	x	x
23		x	x	x	x		x	x	x	x		x
24	x	x		x	x			x	x			x
25	x	x	x	x	x	x	x	x	x	x	x	x

FIGURE 75c

Since the longer fragment **QUARTERS** has been enciphered on one generatrix, at the beginning of the fourth line of the cipher, we shall consider this portion first. The generatrix possibilities are generatrix numbers 1, 3, 20, and 25, so we derive the multiple keys shown below:

	<table border="1"> <thead> <tr><th>Q</th><th>U</th><th>A</th><th>R</th><th>T</th><th>E</th><th>R</th><th>S</th></tr> <tr><th>Z</th><th>P</th><th>R</th><th>T</th><th>Q</th><th>K</th><th>B</th><th>L</th></tr> </thead> <tbody> <tr><td>22</td><td>19</td><td>17</td><td>3</td><td>1</td><td>19</td><td>19</td><td>5</td></tr> </tbody> </table>	Q	U	A	R	T	E	R	S	Z	P	R	T	Q	K	B	L	22	19	17	3	1	19	19	5	<table border="1"> <thead> <tr><th>Q</th><th>U</th><th>A</th><th>R</th><th>T</th><th>E</th><th>R</th><th>S</th></tr> <tr><th>Z</th><th>P</th><th>R</th><th>T</th><th>Q</th><th>K</th><th>B</th><th>L</th></tr> </thead> <tbody> <tr><td>10</td><td>9</td><td>20</td><td>18</td><td>10</td><td>22</td><td>2</td><td>22</td></tr> <tr><td>16</td><td></td><td></td><td></td><td>13</td><td>25</td><td></td><td></td></tr> <tr><td>21</td><td></td><td></td><td></td><td></td><td></td><td></td><td></td></tr> </tbody> </table>	Q	U	A	R	T	E	R	S	Z	P	R	T	Q	K	B	L	10	9	20	18	10	22	2	22	16				13	25			21															
Q	U	A	R	T	E	R	S																																																																			
Z	P	R	T	Q	K	B	L																																																																			
22	19	17	3	1	19	19	5																																																																			
Q	U	A	R	T	E	R	S																																																																			
Z	P	R	T	Q	K	B	L																																																																			
10	9	20	18	10	22	2	22																																																																			
16				13	25																																																																					
21																																																																										
Gen. 1:		Gen. 3:																																																																								
	<table border="1"> <thead> <tr><th>Q</th><th>U</th><th>A</th><th>R</th><th>T</th><th>E</th><th>R</th><th>S</th></tr> <tr><th>Z</th><th>P</th><th>R</th><th>T</th><th>Q</th><th>K</th><th>B</th><th>L</th></tr> </thead> <tbody> <tr><td>3</td><td>8</td><td>1</td><td>1</td><td>6</td><td>21</td><td>7</td><td>8</td></tr> <tr><td>10</td><td>10</td><td>12</td><td>16</td><td></td><td>14</td><td>14</td><td></td></tr> <tr><td>16</td><td></td><td></td><td></td><td></td><td>17</td><td></td><td></td></tr> <tr><td></td><td></td><td></td><td></td><td></td><td>28</td><td></td><td></td></tr> </tbody> </table>	Q	U	A	R	T	E	R	S	Z	P	R	T	Q	K	B	L	3	8	1	1	6	21	7	8	10	10	12	16		14	14		16					17								28			<table border="1"> <thead> <tr><th>Q</th><th>U</th><th>A</th><th>R</th><th>T</th><th>E</th><th>R</th><th>S</th></tr> <tr><th>Z</th><th>P</th><th>R</th><th>T</th><th>Q</th><th>K</th><th>B</th><th>L</th></tr> </thead> <tbody> <tr><td>19</td><td>22</td><td>9</td><td>20</td><td>7</td><td>10</td><td>5</td><td>23</td></tr> </tbody> </table>	Q	U	A	R	T	E	R	S	Z	P	R	T	Q	K	B	L	19	22	9	20	7	10	5	23
Q	U	A	R	T	E	R	S																																																																			
Z	P	R	T	Q	K	B	L																																																																			
3	8	1	1	6	21	7	8																																																																			
10	10	12	16		14	14																																																																				
16					17																																																																					
					28																																																																					
Q	U	A	R	T	E	R	S																																																																			
Z	P	R	T	Q	K	B	L																																																																			
19	22	9	20	7	10	5	23																																																																			
Gen. 20:		Gen. 25:																																																																								

Generatrix 1 is eliminated at once, and the possible strip arrangements for generatrices 3 and 25 do not decipher the text; this leaves generatrix 20 as the sole candidate, albeit in 28 possible strip arrangements.







Generatrices 1 and 25 are eliminated immediately because of repeated unique occurrences of strip numbers, leaving only generatrix 23 to be considered. The solution from here proceeds as in subpars. *d* and *e*, except that instead of only 8 possibilities of strip arrangements, there may be 45 possible trials before the correct arrangement is found.

48. Further remarks.—*a*. The Bazeries device incorporated 20 systematic 25-letter alphabets, including the normal and reversed normal sequences, and 14 keyword-mixed sequences. The alphabets of Hitt's device, as already indicated, bore many interrelationships, constituting a cryptographic weakness. For example, in the synoptic table for A, no generatrix contains more than 10 different letters, and several contain as few as four; moreover, some of the generatrices contain one letter 20 times: all this greatly facilitates crib placement. The M-94 alphabets devised by Mauborgne were intended to be as diverse as possible, but the diversity did not extend beyond digraphs; and since the only digraphs occurring twice are DE, YA, and UB, he originally called his system the DEYAUB cipher.

*b*. In Bazeries' device 24 cipher generatrices were possible, but he prescribed that the first two and last two should not be used; thus there were only 20 generatrices available. In the M-94, which used a guide bar along which to align the plaintext letters, the 1st generatrix was completely hidden, while the 2d generatrix was half hidden, so that these generatrices could not be used; conversely, the 24th and 25th generatrices were not to be used, because these could not be seen when the cipher text was set up along the guide bar. With strip cipher systems, no limitation of generatrices exists—except of course for the 26th generatrix, which is the same as the  $\emptyset$  or plaintext generatrix.

*c*. The cryptograms produced by a cylindrical cipher device or a strip cipher system are non-crashing, i.e., a plaintext letter can never be enciphered by itself. Since the 25 cipher equivalents of any plaintext letter are equiprobable, the theoretical ciphertext frequencies for English underlying text can be computed, resulting in the following distribution:

A	3.70	G	3.94	L	3.86	Q	3.99	V	3.94
B	3.96	H	3.86	M	3.90	R	3.70	W	3.94
C	3.88	I	3.70	N	3.68	S	3.76	X	3.98
D	3.83	J	3.99	O	3.70	T	3.63	Y	3.92
E	3.48	K	3.99	P	3.89	U	3.90	Z	4.00
F	3.88								100.00

The  $\gamma$  I.C. of the cipher text is most easily computed by the formula  $\gamma = 1 + \frac{\beta_p}{(c-1)^2}$ , where  $\beta_p$  is the bulge of the I.C. of the plain text (i.e.,  $\gamma - 1.00$ ) and  $c$  is the number of categories; therefore  $\gamma = 1 + \frac{.73}{(26-1)^2} =$

1.0012. A property of such systems is that, if the distribution of the cipher letters is made in the descending frequency order of the plaintext letters of the language, the slope of frequencies of the ciphertext letters will be that of a gradual ascent; thus:

E	3.48	I	3.70	C	3.88	Y	3.92	X	3.98
T	3.63	S	3.76	F	3.88	G	3.94	Q	3.99
N	3.68	D	3.83	P	3.89	W	3.94	K	3.99
R	3.70	L	3.86	U	3.90	V	3.94	J	3.99
O	3.70	H	3.86	M	3.90	B	3.96	Z	4.00
A	3.70								100.00

The slope is so gradual that usually about 8000 letters are required for a positive determination of a noncrashing system.

*d*. In the example given in subpar. 46*a* the unknown alphabets were reconstructed by means of a long cipher message and its compromised plain text. The alphabets could also be recovered if we had available a long pair of isologs, even if the underlying plain text were unknown—in fact, even if the language were totally unknown! In this case, the cipher of Message "A" could be treated as if it were the plain of Message "B", and solution would proceed as outlined in par. 46.

e. In the absence of either matched plain and cipher or of isologs, the *modus operandi*, albeit very laborious, is as follows: First, lines of cipher text enciphered by the same generatrix must be established, initially on the basis of polygraphic repetitions of at least tetragraphs between them. Second, further lines of cipher are added, on the basis of coincidences between the lines under consideration and the family of lines already established. For example, if we are testing a new line against a homogeneous family of six lines, we should expect  $.0667 \times 25 \times 6 = 9.9$  coincidences if the new line really belongs to that family, as against  $.0385 \times 25 \times 6 = 5.7$  for random. Third, some plain text must be assumed, either for the repetitions or for possible initial stereotypes. Finally, the assumed plain text is tested against the other lines of the same family.

f. The first solution of a cylindrical cipher device was accomplished by the Marquis Gaëtan Henri Léon de Viaris, who in 1893 described his analysis of the Bazeries device in what is one of the most brilliant feats of cryptanalysis in history, in view of the state of the art at the time.¹¹ De Viaris assumed possession of the device, a premise granted by the inventor, and he asked Bazeries for three test situations: (1) a cryptogram with the generatrix numbers indicated for each line of cipher; (2) another cryptogram in which one word of the plain text would be given; and (3) three cryptograms with the only information that they are in the same key. The first test case was academic, since in practice a cryptanalyst would never know the generatrix numbers, and de Viaris solved this easily by means of synoptic tables of which he was the inventor. In the second problem he dragged the crib OFFICIER through the cipher, placing the crib correctly on the basis of ciphertext limitations, testing all 20 possible generatrices, and recovering the order of all the disks.¹² In the third situation he pondered the problem, toying with the idea of dragging possible cribs such as the endings EMENT and ERAIENT through the cipher texts, until he hit upon the thought that perhaps one of the messages began with the definite article LES. When he tried LES at the beginning of the second message, he obtained DES and LAV as the beginnings of the first and third messages. He expanded LAV first into LA VUE and then into LA VITESSE, which yielded DES PARCS A . . . and LES APPROV . . . in the other two messages; he expanded the latter into LES APPROVISIONNEMENTS which yielded DES PARCS AEROSTATIQUES and LA VITESSE D'UNE COLONNE and the problem came to a quick end. De Viaris not only obtained the numerical keys for the three test cases, but he also devised the procedure for recovering the literal keys on which the numerical keys were based.

g. The method of expanding a short key into a longer one was proposed by Bazeries for his device, and this method of key construction was prescribed in the instructions for the use of the M-94. The weakness of such a scheme can be demonstrated in connection with the partial key of eight elements recovered in subpar. 47d: 3-19-16-14-8-6-9-22. If we had encountered difficulties in assuming further plain text, and if an expanded key had been used, we could recover the entire key in the following way. If the basic key length is 9, then key number 1 must of course be in position 9, and we can also insert in the second and third cycles the key numbers shown:

3 19 (16) 14 (8) 6 9 22 1] 4 20 17 15 10 7 11 23 2] 5 21 18 (16) 12 (8) 13

Since conflicts (indicated by the ringed numbers) arise, the key length cannot be 9. If the key length is 10, we know that the digit 1 must be in either position 9 or 10, and we can fill in the following mandatory values:

3 19 (16) 14 8 6 9 22 . . ] 4 20 17 15 . 7 . . . . ] 5 21 18 (16) .

¹¹ Marquis de Viaris, *L'art de chiffrer et déchiffrer les dépêches secrètes*, Paris 1893.  
¹² De Viaris suggests that 20 clerks be employed for the generatrix testing, one for each of the generatrices permissible in the Bazeries device ("Notons en passant que ce travail d'essai pourrait être fait par 20 secrétaires examinant chacun l'hypothèse d'une des 20 génératrices du cylindre"). Actually, if we consider the amount of work we had to do in solving the case given in subpars. 47f and g, this might not be such a bad idea. (The De Viaris suggestion antedates the contemporary "1,000,000 Chinamen" allusion.)

Since there is a conflict between the 16's at positions 3 and 24, we rule out a key length of 10 and try a length of 11, filling in the automatic values:

3 19 16 14 ⁵ 8 6 9 22 . . . ] ¹⁰ 4 20 17 15 . 7 . . . ] ²⁰ 5 21 18 ²⁵

Since no conflicts developed, we can take it that the basic key is probably 11 elements long, and that therefore the first cycle must contain the numbers (1, 10, 23), (1, 10, 24), (1, 12, 23), or (1, 12, 24) in one of their six possible permutations. We could now try the 24 possible keys on the rest of the cipher message to discover which is the correct one, or we could reduce the first cycle of each of the 24 keys to a basic key and recover a key word from the correct one. The only key from which a plausible key word can be derived is

Key: 3 19 16 14 8 6 9 22 1 24 10  
Basic: 2 9 8 7 4 3 5 10 1 11 6

which is found to be based upon the word CONFEDERATE, so the entire key must be

⁵ ¹⁰ ¹⁵ ²⁰ ²⁵  
C O N F E D E R A T E C O N F E D E R A T E C O N  
3 19 16 14 8 6 9 22 1 24 10 4 20 17 15 11 7 12 23 2 25 13 5 21 18

h. In subpar. d, above, it was stated that alphabets could be reconstructed through the use of isologs, even if the underlying text were in a language totally unknown. Furthermore, once we are in possession of the alphabets, even if their order is initially unknown, isologs would make it possible to recover the plain text by establishing the order *in toto* of the strips, following the procedure demonstrated in subpar. 47h. We would then search the generatrices for the one row in each set that gives evidence of being plain text of some kind, either by the distribution of vowels and therefore the pronounceability of the text, or by repetitions or other attributes expected of a language. We shall give below a striking demonstration of this possibility of analysis, involving the encipherment of an intermediate text of unknown composition.

(1) The following two intercepted messages were known to have been enciphered with the M-94:

Message "A"

D I I W Z L E X L U D T F N S L M A U E X G Y X O  
S E L V A I C I J D K K V J Q M K G W V K V I D V  
C A M M Y Q E V E F B I C N D J M K Z H J E G P T  
L W P N C I O C F H V N R Y L F V J G H S H Q G A

Message "B"

G D O S F V V R A S B S F P H W E M F W H O A Y W  
U Y P O D W M Y B D

In the absence of any probable words to try, solution may be very difficult indeed—unless we are lucky and, for example, the messages contain identical beginnings in the underlying text. We observe a hit between the two messages at their 13th positions, so if they do have similar beginnings these could not be more than 12 letters in length.

(2) We first construct a diagram similar to that of Fig. 73 to test for similar beginnings, and we find that this situation is possible on generatrix numbers 7 or 25. We then establish the order of the disks for these two possibilities, as shown below:

D I I W Z L E X L U D T  
Gen. 7: G D O S F V V R A S B S  
3 10 12 16 6 4 7 14 1 23 17 5  
25 15  
19  
21

D I I W Z L E X L U D T  
Gen. 25: G D O S F V V R A S B S  
① ① 9 13 ⑧ 16 12 ① ① ⑧ 10 24

Generatrix 25 is ruled out at once because of conflicts, and we are left with the 8 possibilities of disk orders on generatrix 7. We now run down the generatrices on the beginning of Message "A" for the positions that have unique keys, as shown in Fig. 77a, below:

		3	10	12	16		7	14	1	23	17	5	
		<u>D</u>	<u>I</u>	<u>I</u>	<u>W</u>	<u>Z</u>	<u>L</u>	<u>E</u>	<u>X</u>	<u>L</u>	<u>U</u>	<u>D</u>	<u>T</u>
1	K	C	S	Z			Z	B	R	F	F	J	
2	O	A	R	R			B	L	X	O	C	B	
3	M	K	D	V			N	E	S	Y	W	R	
4	J	E	V	L			I	G	P	H	G	H	
5	U	L	E	X			K	N	W	M	Q	C	
6	B	B	W	C			P	Y	N	L	I	Y	
7	G	D	O	S			V	R	A	S	B	S	
8	E	F	A	H			R	S	B	I	K	L	
9	P	J	M	D			O	M	C	Q	L	W	
10	H	G	N	E			G	F	E	N	N	E	
11	S	H	F	O			S	A	I	J	V	M	
12	C	O	L	K			Y	O	G	C	A	Z	
13	Z	N	H	F			D	D	D	P	R	V	
14	I	M	Q	P			U	W	J	G	M	X	
15	N	T	G	Y			L	P	F	B	Y	G	
16	X	P	C	A			C	K	V	Z	O	A	
17	F	R	U	Q			F	J	U	A	F	F	
18	Y	Q	J	J			M	V	Y	X	T	N	
19	Q	S	T	N			Q	I	M	K	H	Q	
20	R	V	B	U			T	U	H	W	E	U	
21	T	Z	Y	B			W	Q	T	R	U	K	
22	V	U	P	T			A	H	Q	E	S	D	
23	W	X	Z	G			H	Z	K	V	Z	O	
24	L	Y	K	I			X	C	Z	D	J	P	
25	A	W	X	M			J	T	O	T	X	I	

FIGURE 77a

Generatrix numbers 1, 2, 24, and 25 are ruled out as possibilities for Message "A" because of the idiosyncrasies of the M-94, and likewise generatrix numbers 5 through 9 for Message "B". To our astonishment, however, even though we have proved the existence of similar beginnings we are unable to see plain text on any of the generatrices. The "plain text," then, must be some kind of intermediate text. In order to assist our analysis, we make generatrix diagrams for the other four lines of cipher text under the already recovered key; these are shown in Figs. 77b-e on the next page.

(3) In Fig. 77e (the diagram for the last line of Message "B") we note the letters A Q C X . . Y X X X on generatrix 20; if this generatrix is valid, perhaps null X's have been used to complete the last group of five letters, which would then make this message 32 letters in length. This observation, coupled with the length of Message "A" (100 letters) and the length of the similar beginnings (12 letters), leads us to the assumption that the underlying text consists of a 4-letter code. We now note on the 21st generatrix in Fig. 77d (the diagram for the last line of Message "A") the sequence of letters Q)V U P . . I I E)T I V which, on the basis of 4-letter code groups, might indicate the presence of another VUPT which had already occurred on generatrix 22 of Fig. 77a. Of the two key possibilities (6 and 25) for the 5th column, only disk number 6 will produce a T_p out of C_e on the 21st generatrix. One more column of possible decipherments can now be added to each of the diagrams of Figs. 77a-e.

(4) We now take a close look at our diagrams and we examine the putative plain text we have just considered:

- In Fig. 77a, generatrix 22: V U P T)R . AH)Q E S D
- In Fig. 77d, generatrix 21: Q)V U P T) . I I E)T I V
- In Fig. 77e, generatrix 20: A Q C)X I . Y)X X X

	3 10 12 16	7 14 1 23 17 5
	<u>S E L V A I C I J D K K</u>	
1		
2		
3	I D G C	Q H U F V P
4	N F C S	T Z Y O A I
5	X J U H	W C M Y R T
6	F G J D	A T H H M J
7	Y H T E	H X T M Y B
8	Q O B O	X B Q L O R
9	R N Y K	J L K S F H
10	T M P F	E E Z I T C
11	V T Z P	Z G O Q H Y
12	W P K Y	B N L N E S
13	L R X A	N Y R J U L
14	A Q I Q	I R X C S W
15	D S S J	K S S P Z E
16	K V R N	P M P G J M
17	O Z D U	V F W B X Z
18	M U V B	R A N Z D V
19	J X E T	O O A A P X
20	U Y W G	G D B X C G
21	B W O I	S W C K W A
22	G I A M	Y P E W G F
23	E C M W	D K I R Q N
24		
25		

FIGURE 77b

	3 10 12 16	7 14 1 23 17 5
	<u>C A M M Y Q E V E F B I</u>	
1		
2		
3	N L L R	N Q D H N B
4	X B H V	I H J M V R
5	F D Q L	K Z F L A H
6	Y F G X	P C V S R C
7	Q J C C	V T U I M Y
8	R G U S	R X Y Q Y S
9	T H J H	O B M N O L
10	V O T D	G L H J F W
11	W N B E	S E T C T E
12	L M Y O	Y G Q P H M
13	A T P K	D N K G E Z
14	D P Z F	U Y Z B U V
15	K R K P	L R O Z S X
16	O Q X Y	C S L A Z G
17	M S I A	F M R X J A
18	J V S Q	M F X K X F
19	U Z R J	Q A S W D N
20	B U D N	T O P R P Q
21	G X V U	W D W E C U
22	E Y E B	A W N V W K
23	P W W T	H P A D G D
24		
25		

FIGURE 77c

	3 10 12 16	7 14 1 23 17 5
	<u>L W P N C I O C F H V N</u>	
1		
2		
3	K A X T	Y B Y S M K
4	O K I G	D L M I Y D
5	M E S I	U E H Q O O
6	J L R M	L G T N F P
7	U B D W	C N Q J T I
8	B D V Z	F Y K C H T
9	G F E R	M R Z P E J
10	E J W V	Q S O G U B
11	P G O L	T M L B S R
12	H H A X	W F R Z Z H
13	S O M C	A A X A J C
14	C N N S	H O S X X Y
15	Z M F H	X D P K D S
16	I T L D	J W W W P L
17	N P H E	E P N R C W
18	X R Q O	Z K A E W E
19	F Q G K	B J B V G M
20	Y S C F	N V C D Q Z
21	Q V U P	I I E T I V
22	R Z J Y	K U I U B X
23	T U T A	P Q G F K G
24		
25		

FIGURE 77d

	3 10 12 16	7 14 1 23
	<u>U Y P O D W M Y B D</u>	
1		
2		
3	E C X P	W M I F
4	P A I Y	A F G O
5	H K S A	H A D Y
6	S E R Q	X O J H
7	C L D J	J D F M
8	Z B V N	E W V L
9	I D E U	Z P U S
10	N F W B	B K Y I
11	X J O T	N J M Q
12	F G A G	I V H N
13	Y H M I	K I T J
14	Q O N M	P U Q C
15	R N F W	V Q K P
16	T M L Z	R H Z G
17	V T H R	O Z O B
18	W P Q V	G C L Z
19	L R G L	S T R A
20	A Q C X	Y X X X
21	D S U C	D B S K
22	K V J S	U L P W
23	O Z T H	L E W R
24		
25		

FIGURE 77e





B	A E I O U Y
C	- A E I O U Y
D	-- A E I O U Y
F	--- A E O O U Y
G	---- A E I O U Y
H	----- A E I O U Y
J	----- A E I O U Y
K	----- A E I O U Y
L	----- A E I O U Y
M	----- A E I O U Y
N	----- A E I O U Y
P	----- A E I O U Y
Q	----- A E I O U Y
R	----- A E I O U Y
S	----- A E I O U Y
T	----- A E I O U Y
V	----- A E I O U Y
W	----- A E I O U Y
X	----- A E I O U Y
Z	----- A E I O U Y

A	B	C	D	E	F	G	H	I	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	Z
B	C	D	E	F	G	H	I	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	A
C	D	E	F	G	H	I	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	B
D	E	F	G	H	I	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	C
E	F	G	H	I	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	D
F	G	H	I	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	E
G	H	I	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	F
H	I	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	G
I	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	H
K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	I
L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	K	K
M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	K	L	L
N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	K	L	M	M
O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	K	L	M	N	N
P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	K	L	M	N	O	O
Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	K	L	M	N	O	P	P
R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	K	L	M	N	O	P	Q	Q
S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	K	L	M	N	O	P	Q	R	R
T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	K	L	M	N	O	P	Q	R	S	S
U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	K	L	M	N	O	P	Q	R	S	T	T
V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	K	L	M	N	O	P	Q	R	S	T	U	U
W	X	Y	Z	A	B	C	D	E	F	G	H	I	K	L	M	N	O	P	Q	R	S	T	U	V	V
X	Y	Z	A	B	C	D	E	F	G	H	I	K	L	M	N	O	P	Q	R	S	T	U	V	W	W
Y	Z	A	B	C	D	E	F	G	H	I	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	X
Z	A	B	C	D	E	F	G	H	I	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Y

FIGURE 79

(b) (1)  
(b) (3) -18 USC 798  
(b) (3) -50 USC 3024 (i)  
(b) (3) -P.L. 86-36

CHAPTER VIII

SYSTEMS EMPLOYING GEARED DISK CRYPTOMECHANISMS

	Paragraph
Introduction.....	49
The Wheatstone cipher device.....	50
Analysis of the Wheatstone cipher device.....	51
The Kryha cipher machine.....	52
Analysis of the original Kryha machine.....	53
<span style="border: 1px solid black; display: inline-block; width: 250px; height: 15px;"></span> .....	54
Concluding remarks.....	55

**49. Introduction.**—*a.* The earliest cipher devices involved concentric disks rotated by hand in a prearranged manner to achieve a polyalphabetic substitution, usually periodic. In some of these devices the alphabets, usually standard sequences, were unchangeable; in others, the order of the letters in the sequences could be changed at will by the correspondents. At the beginning of this century the hand-operated disk cipher devices were improved by the incorporation of gear mechanisms to accomplish the polyalphabetic substitution automatically.

*b.* The more primitive of these devices produced periodic polyalphabetic substitution—in fact, one device marketed commercially produced cryptograms having a period of three (!). Others yielded the encipherments of progressive alphabet systems, ciphertext autokey systems, and plaintext autokey systems; still others used variable pin wheels to govern the displacement of the components in an irregular (but periodic) manner. The more sophisticated and interesting devices employing geared disk cryptomechanisms are those typified by the Wheatstone cipher device and the Kryha cipher machine, and these deserve extensive treatment.

**50. The Wheatstone cipher device.**—*a.* This device, invented by Sir Charles Wheatstone¹ in 1867, is a little more than four inches in diameter, and consists of a dial with two hands, as shown in Fig. 80, below. The dial is composed of two independent circles of letters. In the outer circle, which constitutes the plain component, the letters progress clockwise in normal alphabetic sequence, but there is an extra character between the Z and the A which is used as a word separator, making a total of 27 characters; furthermore, the digits 1-0 are inscribed together with the letters A-J and also N-W, for enciphering numbers. In the inner circle, which constitutes the cipher component, the letters are arranged in a mixed sequence and are inscribed either on a surface which permits erasure, or on a detachable cardboard circle which can be removed and replaced by another circle bearing a different sequence.

*b.* The two hands are pivoted concentrically, after the fashion of the hour and minute hands of a clock. In a clock, when the minute hand makes a complete revolution, the hour hand makes 1/2 of a complete revolution; the action in the case of this device, however, is somewhat different. The short hand is free to be set independently of the long one, although the motion of the latter affects the former. Since the outer circle has 27 spaces and the inner one only 26, by a simple gear assembly each complete revolution of the long hand causes the short hand to make 1 1/26 revolutions, thus causing the short hand to point one place in advance of where it pointed at the end of the preceding revolution of the long hand. For example in Fig. 80, when the long hand is over B of the outer circle and the short hand points to R of the inner circle, if the long hand is pushed clockwise around the dial, making a complete revolution, the short hand will also make a complete revolution clockwise plus one space, thus pointing to D.

¹ Credit for the conception of the system described here belongs not to Sir Charles Wheatstone, as is commonly thought, but to an American, Decius Wadsworth, who in 1817 constructed a device identical in principle with that described on pp. 342-348 of the *Scientific Papers of Sir Charles Wheatstone*, published by the Physical Society of London in 1879. The Wheatstone device used a 27-element outer alphabet and a 26-element inner alphabet; the Wadsworth device used a 33-element outer alphabet (26 letters and the digits 2-8, inclusive) and a 26-element inner alphabet. Furthermore, whereas in the Wheatstone device only the cipher component could be varied, in the Wadsworth device both components could be varied.

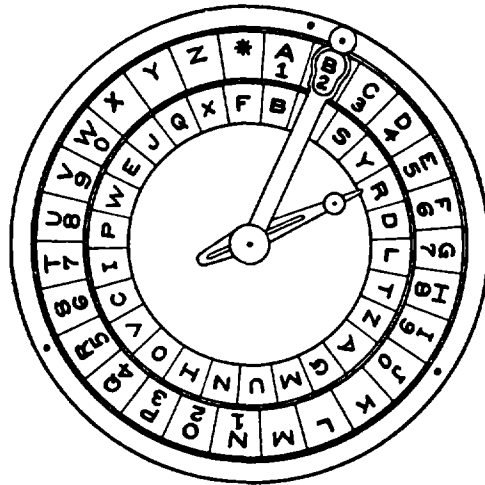


FIGURE 80

c. To encipher a message, the long hand and the short hand are first set to prearranged initial positions, or set according to an indicator procedure; furthermore, by previous agreement, the long hand is invariably to be moved in the same direction, usually clockwise. Suppose the message to be enciphered is SEND AMMUNITION. The long hand is moved clockwise until it is directly over S on the outer sequence; the letter to which the short hand points is the cipher equivalent of S and is written down. Then the long hand is moved clockwise to a position over E, and the letter to which the short hand points is noted and written down; the next two letters are enciphered in the same manner. After the encipherment of each word, the long hand is moved clockwise to the asterisk, and the cipher equivalent of this word separator is recorded; when a doubled letter occurs in the plain text, as in the case of the doubled M of AMMUNITION, some infrequently used letter such as Q_p must be substituted for the second occurrence of the letter, and encipherment proceeds as before. To decipher a message, the hands are first set to their prearranged initial position, and then the long hand is moved clockwise until the short hand points to the first cipher letter; the long hand is then directly over the plaintext equivalent. The process is continued until the message is completely deciphered.

d. The principle of the Wheatstone device can be duplicated with a pair of sliding alphabet strips—a 27-element plain component and a doubled-length cipher component. After the two strips are set to their prearranged initial juxtaposition, the cipher equivalent is found for the first plain-text letter. The cipher component strip is moved one position to the left for succeeding encipherments *whenever a letter in the plain component is located to the left of the immediately preceding plaintext letter of the message.* What makes the Wheatstone device particularly interesting is that the motion of the cipher component is highly irregular and unpredictable, depending as it does upon the particular sequence of the letters of the plain text and upon the particular arrangement of the letters in the plain component. At the time of its invention, the Wheatstone device was of course considered by the cryptologic world as “absolutely indecipherable.”

51. Analysis of the Wheatstone cipher device.—a. In order to understand the mechanics of Wheatstone encipherment, let us study a cipher message with its compromised plain text, as given below:

	5		10		15		20		25		30																		
S	L	Y	Y	I	R	L	M	H	T	Q	W	O	A	X	D	C	B	Z	R	I	I	J	Z	X	F	I	R	I	Q
R	E	F	E	R	Q	I	N	G	*	T	O	*	Y	O	U	R	*	M	E	S	Q	A	G	E	*	N	U	M	B
	35		40		45		50		55		60																		
U	R	K	L	L	I	R	O	T	B	X	M	X	P	V	J	Q	S	I	V	C	I	S	Z	U	V	I	W	W	K
E	R	*	O	N	E	*	E	I	G	H	T	*	T	W	O	*	D	A	T	E	D	*	T	W	O	*	O	N	E
	65		70		75		80		85		90																		
A	V	F	Q	H	H	H	G	F	W	O	I	B	R	J	T	S	B	T	X	Z	U	R	E	E	D	J	B	G	E
*	J	A	N	U	A	R	Y	*	C	O	M	Q	A	*	G	E	N	E	R	A	L	*	L	U	N	S	F	O	R
	95		100		105		110		115		120																		
E	Q	X	B	B	V	S	D	F	T	B	B	Z	F	S	G	X	R	B	F	I	L	C	E	J	H	D	F	X	M
D	*	W	I	L	Q	*	B	E	*	A	R	Q	I	V	I	N	G	*	A	T	*	Y	O	U	R	*	H	E	A
	125		130		135		140		145		150																		
K	B	V	V	V	F	T	X	G	R	Q	J	V	F	F	B	Z	P	Y	W	C	K	E	S	A	M	O	N	F	N
D	Q	U	A	R	T	E	R	S	*	A	T	*	O	N	E	*	S	E	V	E	N	*	H	U	N	D	R	E	D

(The enciphering components used in this example were the following,

	5		10		15		20		25		27																
P:	H	Y	D	R	A	U	L	I	C	B	E	F	G	J	K	M	N	O	P	Q	S	T	V	W	X	Z	*
C:	Q	U	E	S	T	I	O	N	A	B	L	Y	C	D	F	G	H	J	K	M	P	R	V	W	X	Z	

although at this stage we are not supposed to be privy to this information, which is being given for surreptitious reference only.)

(1) We note that whenever there is a ciphertext doublet, the plaintext digraphic equivalent *always* consists of a pair of consecutive letters in the plain component, but in reverse; thus we can establish EF, QS, NO, and DRAULI as chains from the original plain component. We also note that whenever there is an A-A doublet in the plain text, the cipher equivalent will be a pair of consecutive letters (without reversal) in the cipher component; thus we can establish LYC, IO, MP, VW, ST, UE, and FG as chains from the original cipher component.

(2) We now note, at position 5, that  $RQI_p = IRL_c$ ; and since we have determined that the letters DRAULI are in sequence in the plain component, it is obvious that in enciphering the plaintext fragment  $RQI_p$ , the cipher component must have moved just once. If the juxtaposition of the plain and cipher components at this point is  $R_p = I_c$ , then we can arrive at the following graphic representation for the distance between  $I_c$  and  $L_c$  (adding the  $O_c$  and  $Y_c$  from the chains already established in the cipher component):

At pos. 5,  $RQI_p$ ,  $\therefore$  D R A U L I  
 $I R L_c$                     I O . . . L y c

Likewise, at positions 16, 80, and 102 we have the following relationships and recoveries of fragments of the cipher component:

At pos. 16,  $UR_p$ ,  $\therefore$  D R A U L I  
 $DC_c$                     C D

At pos. 80,  $RAL_p$ ,  $\therefore$  D R A U L I  
 $XZU_c$                     X Z . U e

At pos. 102,  $RQI_p$ ,  $\therefore$  D R A U L I  
 $BZF_c$                     B . . . . F g

(3) Now since  $ER_p = YI_c$  (at pos. 4) =  $UR_c$  (31) =  $TX_c$  (79), we can establish (R . . X Z . U E S T) as one of the chains from the cipher component, in addition to (I O . . . L Y C D) and (B . . . . F G) already recovered. Other relationships are exploited, as follows:

$N G_p = X R_c$  (107) =  $M H_c$  (8),  $\therefore$  (H . . M)  
 $N E_p = L I_c$  (35) =  $W K_c$  (59) =  $B T_c$  (78),  $\therefore$  (K . . . . V W)  
 $T *_p = M X_c$  (42),  $\therefore$  (M . . . . X)  
At. pos. 115,  $U R_p$ ,  $\therefore$  D R A U L I; at pos. 147,  $D R_p$ ,  $\therefore$  D R A U L I  
                  J H_c                  H J                  O N_c          O N  
 $G *_p = H T_c$  (9) =  $R B_c$  (108), tying two of our chains together.

At this point the several chains can be amalgamated into one sequence,

H J K M . R V W X Z . U E S T I O N . B L Y C D F G

and the missing values can be recovered from other relationships in the matched plain and cipher.

(4) In reconstructing the plain component, we begin with the fragment (D R A U L I) and add the following relationships:

$S L_c = R E_p$  (1),  $\therefore$  (D R A U L I . . E f)  
 $T B_c = I G_p$  (39) =  $* A_p$  (100),  $\therefore$  (* . . D R A U L I . . E F G)  
 $R I_c = E S_p$  (20) =  $U M_p$  (28),  $\therefore$  (* . . D R A U L I . . E F G . . M . . . . S)

We now add the following relationships:

$F I_c = * N_p$  (26);  $M H_c = N G_p$  (8);  $X D_c = O U_p$  (15);  $X M_c = H T_p$  (41);  
 $A X_c = Y O_p$  (14);  $V F_c = J A_p$  (62);  $S G_c = V I_p$  (105);  $X B_c = W I_p$  (93);  
 $I Q_c = M B_p$  (29);  $F W_c = * C_p$  (69)

These yield the following recoveries in the plain component:

* H Y D R A U L I C B E F G J . M N O . Q S T V W . .

(5) A different method for deriving the cipher component from the foregoing matched plain and cipher will now be demonstrated. First, we make an abridged digraphic distribution of the plain text, as shown in Fig. 81, below, in which repeated letters in the columns (representing repeated plaintext digraphs with the reference letter at the top) have been circled.

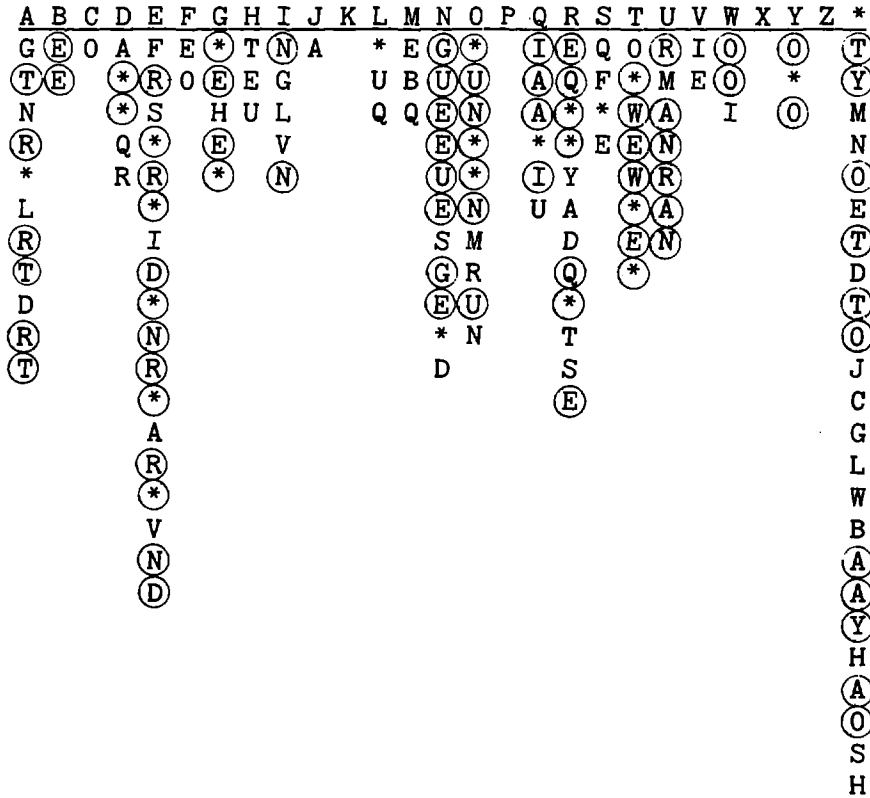


FIGURE 81

Referring to the matched plain and cipher, we make a table of the cipher equivalents of the repeated plaintext digraphs; this is shown in Fig. 82a, below:

1.	AR	HH BB VV	19.	QI	RL ZF
2.	AT	IV FI QJ	20.	RE	SL NF
3.	BE	QU DF	21.	RQ	IR BZ
4.	D*	IS EQ	22.	R*	CB RK HD
5.	ED	CI FN	23.	TE	VC FT
6.	EN	SB CK	24.	TW	PV ZU
7.	ER	YI UR TX	25.	T*	MX IL JV
8.	E*	XF IR KA FT BZ	26.	UA	HH VV
9.	GE	ZX TS	27.	UN	ED AM
10.	G*	HT RB	28.	UR	DC JH
11.	IN	LM GX	29.	WO	VJ UV
12.	NE	LI WK BT FB	30.	YO	AX CE
13.	NG	MH XR	31.	*A	TB BF RQ
14.	NU	IR QH	32.	*H	DF ES
15.	ON	LL WW FF	33.	*O	KL IW VF
16.	OU	XD EJ	34.	*T	TQ XP SZ
17.	O*	WO JQ VI	35.	*Y	OA LC
18.	QA	IJ BR			

FIGURE 82a



On the assumption of direct standard alphabets, we complete the plain component sequence as is shown in Fig. 83a, below, for the first 15 letters:

```

M L Y B A F M Q R Q W D W U H
N M Z C B G N R S R X E X V I
O N A D C H O S T S Y F Y W J
P O B E D I P T U T Z G Z X K
Q P C F E J Q U V U A H A Y L
R Q D G F K R V W V B I B Z M
S R E H G L S W X W C J C A N
T S F I H M T X Y X D K D B O
U T G J I N U Y Z Y E L E C P
V U H K J O V Z A Z F M F D Q
W V I L K P W A B A G N G E R
X W J M L Q X B C B H O H F S
Y X K N M R Y C D C I P I G T
Z Y L O N S Z D E D J Q J H U
A Z M P O T A E F E K R K I V
B A N Q P U B F G F L S L J W
C B O R Q V C G H G M T M K X
D C P S R W D H I H N U N L Y
E D Q T S X E I J I O V O M Z
F E R U T Y F J K J P W P N A
G F S V U Z G K L K Q X Q O B
H G T W V A H L M L R Y R P C
I H U X W B I M N M S Z S Q D
J I V Y X C J N O N T A T R E
K J W Z Y D K O P O U B U S F
L K X A Z E L P Q P V C V T G

```

FIGURE 83a

```

M L Y B A F M Q R Q W D W U H
M K X * Y C J N O M S Z R O A
N L Y A Z D K O P N T * S P B
O M Z B * E L P Q O U A T Q C
P N * C A F M Q R P V B U R D
Q O A D B G N R S Q W C V S E
R P B E C H O S T R X D W T F
S Q C F D I P T U S Y E X U G
T R D G E J Q U V T Z F Y V H
U S E H F K R V W U * G Z W I
V T F I G L S W X V A H * X J
W U G J H M T X Y W B I A Y K
X V H K I N U Y Z X C J B Z L
Y W I L J O V Z * Y D K C * M
Z X J M K P W * A Z E L D A N
* Y K N L Q X A B * F M E B O
A Z L O M R Y B C A G N F C P
B * M P N S Z C D B H O G D Q
C A N Q O T * D E C I P H E R
D B O R P U A E F D J Q I F S
E C P S Q V B F G E K R J G T
F D Q T R W C G H F L S K H U
G E R U S X D H I G M T L I V
H F S V T Y E I J H N U M J W
I G T W U Z F J K I O V N K X
J H U X V * G K L J P W O L Y
K I V Y W A H L M K Q X P M Z
L J W Z X B I M N L R Y Q N *

```

FIGURE 83b

Nothing seems to be in evidence. But we are a little uneasy about our method, so on second thought we first decipher the cipher letters according to the Wheatstone rule of motion, at the setting  $A_p=A_c$ , and we then complete the 27-character plain-component sequence. This is shown in Fig. 83b, wherein the plain text appears on one generatrix. (In referring back to Fig. 83a, we see that we could have spotted the plain text on staggered generatrices, had we not been so hasty.) The generatrix method, then, is the one to use when the components are either known or are assumed—but we should take into consideration the mechanics of the particular cryptography involved if we are to achieve a facile solution.

c. For the next case, let us assume that we have the following cryptogram at hand, known to be in a Wheatstone system with mixed alphabets:

```

G E T E I P L K U C C F G K H H U F Q J R P Y L Y I J M K A
O R O T H E F M Q O O I F V X B E Q O M P A J F E T H K Z U
C J S T T F E L B P S H X H Y W T I R I K Q F D L L R C F T
T D R P N V I U U Q N K I X A F L Y S E Q N O P U L J I F Y
W B F T X L Q Z T T W E J J Y W A S F M M G O S U U F G I Z
C M I N R F J J S Q O T Z P M M W R Z J U B P M A K I N R B
O T P D G R L L E Y

```



(1) In Wheatstone systems, different encipherments of the same underlying plain text will be isomorphic; we therefore search for isomorphs and find the following sets

- a. K U C C F G K H H U F
- b. F D L L R C F T T D R
- c. S F M M G O S U U F G
- d. Q O O I F V X B E Q O M P A J F E
- e. P M M W R Z J U B P M A K I N R B

The chains derived from the foregoing are the following:

- a-b: KFR UD GCL HT
- a-c: KS HUFGO CM
- b-c: DFS LM RG CO TU
- d-e: QPK OMAIW FR VZ XJN EBU

Employing the graphical method of indirect symmetry beginning with the a-b and d-e chains as the horizontal elements and the a-c chains as the vertical, we arrive at the following reconstruction fragments:

```

      HT
      EBUD
    QPKFR          VZ          XJN
      SGCL
      OMAIW

```

There are no tie-ins between these fragments, so we shall have to see whether we can extend the isomorphic passages. We therefore copy the isomorphs together with their five preceding and following letters, as shown below:

```

a. t e i [ p l K U C C F G K H H U F q j r ] [ p y
b. i r i [ k q F D L L R C F T T D R p n v ] [ i u
c. j j y [ w a S F M M G O S U U F G i z c ] [ m i
d. t h e f m [ Q O O I F V X B E Q O M P A J F E t h ] [ k z u
e. s q o t z [ P M M W R Z J U B P M A K I N R B o t ] [ p d g

```

The solid brackets show the outer limits of the isomorphism. No new values are picked up, but the vertical digraph LQ between lines a-b now permits us to establish a long chain,

O M A I W S G C L Q P K F R V Z E B U D . . . . H T,

with only two placements possible for the fragment XJN and the missing letter Y, either XJNY or YXJN. We shall start with the XJNY possibility.

(2) If this is a decimation of a systematically mixed sequence, the original cipher component might be recovered by trial decimations to uncover the method by which it was constructed; otherwise we would be forced to assume decimations of -1, +3, -3, +5 . . . -11, in turn, "deciphering" the cipher text in the Wheatstone fashion, until the  $\delta$  I.C. of the converted text showed us that we had arrived at the correct decimation. For example, using the sequence given above as the cipher component, and the normal sequence followed by a 27th character for the plain component (at the setting  $A_b=O_c$ ), the following is the conversion of the first 60 letters of the text and their frequencies:

```

G E T E I P L K U C C F G K H H U F Q J R P Y L Y I J M K A
G Q Z P B I F I P D C H A F S R K D * L C Z L W K Q H N X N
O R O T H E F M Q O O I F V X B E Q O M P A J F E T H K Z U . . .
K X J H F X S G O E D G P R X T R J * A J A T J N W U G K N
≡ - ≡ ≡ - ≡ ≡ ≡ ≡ ≡ ≡ ≡ ≡ - ≡ ≡ ≡ ≡ ≡ - ≡ ≡
A B C D E F G H I J K L M N O P Q R S T U V W X Y Z *

```

The I.C. of this converted text is  $\frac{27(126)}{60.59} = 0.96$ , somewhat less than miserable; the conversions using the next six decimations of the cipher component, through +7, also give negative results. The -7 decimation of our recovered sequence is the following:

O D F S H B P I N Z L M X R G T U K W Y E Q A J V C

When we use this for the cipher component we arrive at the following conversion of the text and its accompanying distribution:

G E T E I P L K U C C F G K H H U F Q J R P Y L Y I J M K A  
O U O T F D H O M V U X I L Y X I U M O D W I Z H V K Y D I  
O R O T H E F M Q O O I F V X B E Q O M P A J F E T H K Z U . . .  
M Z L * O D L U D I H O I D R J Y Z D O I Y Z D V P D Q H O

A B C D E F G H I J K L M N O P Q R S T U V W X Y Z *

This gives us an I.C. of  $\frac{27(238)}{60.59} = 1.82$ , so we know we have hit the answer.

(3) The entire text can now be converted to monoalphabetic terms and solved. The decipherment of the first 60 letters is shown below, together with the plaintext values of the monoalphabetically converted text:

C: G E T E I P L K U C C F G K H H U F Q J R P Y L Y I J M K A  
"P": O U O T F D H O M V U X I L Y X I U M O D W I Z H V K Y D I  
P: E N E M Y * R E C O N Q A I S Q A N C E * P A T R O L S * A  
C: O R O T H E F M Q O O I F V X B E Q O M P A J F E T H K Z U . . .  
"P": M Z L * O D L U D I H O I D R J Y Z D O I Y Z D V P D Q H O  
P: C T I V E * I N * A R E A * J U S T * E A S T * O F * G R E  
P: * Y R A U L I C E F G J M N O P Q S T V  
"P": A B C D E F G H I J K L M N O P Q R S T U V W X Y Z *

The original plain and cipher components are the following:

P: H Y D R A U L I C B E F G J K M N O P Q S T V W X Z *  
C: A J V C O D F S H B P I N Z L M X R G T U K W Y E Q

The original cipher component, a numerical-key columnar transposition-mixed sequence based upon HYDRAULIC, could have been recovered earlier, but this was glossed over for the sake of the exposition which has just been presented.

d. We have seen in subpar. c, above, that when we know or correctly assume the cipher component, the cipher text can be converted to monoalphabetic terms and solved. When only the plain component is known in a Wheatstone system this is still a useful bit of information, since the placing of cribs is greatly facilitated. For example, if the plain component is the normal A-Z sequence followed by the 27th character for the word separator, the encipherment of the word *ENEMY* will always produce an A-B-BA-idiomorphic pattern, *regardless of the composition of the cipher component*. We can therefore make up idiomorphic lists of frequent words and word combinations to assist us in cribbing, such as the following patterns which are based upon a direct-standard plain component.

*ENEMY*	*CROSSROADS*	*COUNTERATQACK*
A-B-BA-	-A-B-BAC-C	--ABAB---BC-C
*DIVISION*	*ROADJUNCTION*	*COMUNICATION*
-A-----BBA	-----A-BBA	--A-----ABB-
*ARTILQERY*	*HEADQUARTERS*	*RECONQAISQANCE*
-ABC-B-CA-	--A-A-B-B-B-	---ABBCA---C---
*BATQALION*	*INTELQIGENCE*	*REINFORCEMENTS*
-AA-B---BB-	-A-B-C-DAC-DB	-AB-C-BC-ADDB

(1) Let us now suppose that we have available the cryptogram given below, known to have been enciphered in a Wheatstone system involving a normal plain component and a mixed cipher component:

```

      5           10           15           20           25           30
M O L V L   E L X H G   M M S U K   C F D U E   Q Y I I H   P S B E E
      35           40           45           50           55           60
X N J T L   C B S X F   G I P H F   Z K B P G   W E J D P   O E F O I
      65           70           75           80           85           90
O J P M V   O O K G D   T I H Q H   A E I L U   D Q M F W   V V M C Q
      95           100
O W G I V   R U L R P

```

We search through our idiomorph list and find that the word *ROADJUNCTION* will fit at position 75:

```

      75           80           85           90
. . . T I H Q H A E I L U D Q M F W V V M C Q . . .
      * R O A D J U N C T I O N *

```

We set a blank strip against one bearing the normal sequence plus an asterisk, and we enter the cipher values from our crib on the blank strip, moving it to the left one position whenever we have to go to the left on the plain component. This yields the following partial sequence for the cipher component:

H . . I . . L M . . . U . W . E Q A . V . . D F .

Since the three letters to the left of the crib are on our cipher component, they can now be deciphered, and the word NEAR is confirmed by the word separator (D_c) which is correctly deciphered with our

```

      70           75           80           85           90
. . . O O K G D T I H Q H A E I L U D Q M F W V V M C Q . . .
      E A R * R O A D J U N C T I O N *

```

partial component: this adds a T in our sequence immediately to the left of the U.

(2) We now scan the cipher text, taking note of those letters which have already been placed in our cipher component, as shown by the capital letters in the diagram below:

```

      5           10           15           20           25           30
M o L V L E L x H g M M s U k c F D U E Q y I I H p s b E E . . .

```

Since there are two substantial clusters (of five letters each) at positions 3 and 17, we align our components arbitrarily at  $A_p=H_c$ , decipher the cipher according to the Wheatstone rule of motion and complete the plain-component sequence. This is shown in Figs. 84a and b, below:

5

... L V L E L ...

G U F P E  
H V G Q F  
I W H R G  
J X I S H  
K Y J T I  
L Z K U J  
M * L V K  
N A M W L  
O B N X M  
P C O Y N  
Q D P Z O  
R E Q * P  
S F R A Q  
T G S B R  
U H T C S  
V I U D T  
W J V E U  
X K W F V  
Y L X G W  
Z M Y H X  
* N Z I Y  
A O * J Z  
B P A K *  
C Q B L A  
D R C M B  
E S D N C  
F T E O D

FIGURE 84a

20

... F D U E Q ...

Y W K O P  
Z X L P Q  
* Y M Q R  
A Z N R S  
B * O S T  
C A P T U  
D B Q U V  
E C R V W  
F D S W X  
G E T X Y  
H F U Y Z  
I G V Z *  
J H W * A  
K I X A B  
L J Y B C  
M K Z C D  
N L * D E  
O M A E F  
P N B F G  
Q O C G H  
R P D H I  
S Q E I J  
T R F J K  
U S G K L  
V T H L M  
W U I M N  
X V J N O

FIGURE 84b

The plaintext fragments REQ*P and CAPTU suggest THREQ*P and *CAPTURED*, and the beginning of the text is quickly deciphered:

5                    10                    15                    20                    25

M O L V L E L X H G M M S U K C F D U E Q Y I I H . . .  
T H R E Q * P R I S O N E R S * C A P T U R E D *

This adds new values to our cipher component, making 20 recoveries in all:

H . . I . . L M X . G T U K W Y E Q A . V C O D F S

The rest of the cipher text is now deciphered in similar fashion, and the entire cipher component is found to be

H B P I N Z L M X R G T U K W Y E Q A J V C O D F S

52. The Kryha cipher machine.—*a.* This machine, invented by Alexander von Kryha in Germany in 1924, is a spring-operated polyalphabetic cipher machine which has as its principle the irregular displacement of two concentric disks which comprise the plain and cipher components. (Actually, the cipher component is a 52-element disk while the plain component is in the shape of a semicircular frame juxtaposed against the revolving cipher component.) The letters of the two components are printed on small metal tabs which are inserted in slots on the two disks so that the sequence of the letters may be varied according to prearranged keys. The displacement of the alphabets occurring after each encipherment is accomplished through a selector wheel having on its periphery 17 toothed sectors consisting of from one to six teeth each, the sectors being designated by the numbers 1–17. These teeth serve to displace the components a distance equivalent to the number of teeth in the sector; however, owing to the manner of spacing between the toothed portions of the wheel, an additional displacement of four positions is added at each operation of the machine. The selector wheel has the following effective displacements between its 17 numbered positions:

No.:	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	1
Displacement:	7	6	7	5	6	7	6	8	6	10	5	6	5	7	6	5	9	

Since the sum of these displacements is 111 ( $\equiv 7, \text{ mod } 26$ ) it follows that after a complete revolution of the selector wheel the cipher component will be displaced 7 positions to the left from its original juxtaposition; and since this number 7, is prime to 26, there will be 26 series of 17 displacements each, making the period of the machine  $17 \times 26 = 442$ .

*b.* As an illustration of encipherment, let us assume that the components of the machine have been arranged as follows:

P: A B C D E F G H I J K L M N O P Q R S T U V W X Y Z  
 C: H Y D R A U L I C B E F G J K M N O P Q S T V W X Z

If the initial juxtaposition of the components is that shown above (i.e., in the key of H), the first plaintext letter is enciphered in the H alphabet, and a stepping button is pressed to bring the next alphabet into position. If the setting of the selector wheel was at position 1 at the beginning of the encipherment, the next alphabet to be brought into play will be 7 to the right of the first or H alphabet (i.e., the 8th or I alphabet), and the one after that will be 6 places to the right of the I alphabet (i.e., the 14th or J alphabet), and so on. At the end of 17 encipherments the alphabets shall have been displaced 7 positions, mod 26, relative to the initial setting, so that the key series 1, 8, 14 . . . becomes the isomorphic equivalent 8, 15, 21 . . .; in other words, the elements in each succeeding row of 17 letters are 7 more than the corresponding elements in the preceding row. The first five rows of 17 elements of the key are shown in the diagram below:

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	
7	6	7	5	6	7	6	8	6	10	5	6	5	7	6	5	9	
1	8	14	21	26	6	13	19	1	7	17	22	2	7	14	20	25	
8	15	21	2	7	13	20	26	8	14	24	3	9	14	21	1	6	
15	22	2	9	14	20	1	7	15	21	5	10	16	21	2	8	13	
22	3	9	16	21	1	8	14	22	2	12	17	23	2	9	15	20	
3	10	16	23	2	8	15	21	3	9	19	24	4	9	16	22	1	. . .

Translating the foregoing numbers into literal form as 1=A, 2=B, . . . 26=Z for typographic convenience, we obtain the complete key diagram as shown in Fig. 85, below:

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17
<u>7</u>	<u>6</u>	<u>7</u>	<u>5</u>	<u>6</u>	<u>7</u>	<u>6</u>	<u>8</u>	<u>6</u>	<u>10</u>	<u>5</u>	<u>6</u>	<u>5</u>	<u>7</u>	<u>6</u>	<u>5</u>	<u>9</u>
A	H	N	U	Z	F	M	S	A	G	Q	V	B	G	N	T	Y
H	O	U	B	G	M	T	Z	H	N	X	C	I	N	U	A	F
O	V	B	I	N	T	A	G	O	U	E	J	P	U	B	H	M
V	C	I	P	U	A	H	N	V	B	L	Q	W	B	I	O	T
C	J	P	W	B	H	O	U	C	I	S	X	D	I	P	V	A
J	Q	W	D	I	O	V	B	J	P	Z	E	K	P	W	C	H
Q	X	D	K	P	V	C	I	Q	W	G	L	R	W	D	J	O
X	E	K	R	W	C	J	P	X	D	N	S	Y	D	K	Q	V
E	L	R	Y	D	J	Q	W	E	K	U	Z	F	K	R	X	C
L	S	Y	F	K	Q	X	D	L	R	B	G	M	R	Y	E	J
S	Z	F	M	R	X	E	K	S	Y	I	N	T	Y	F	L	Q
Z	G	M	T	Y	E	L	R	Z	F	P	U	A	F	M	S	X
G	N	T	A	F	L	S	Y	G	M	W	B	H	M	T	Z	E
N	U	A	H	M	S	Z	F	N	T	D	I	O	T	A	G	L
U	B	H	O	T	Z	G	M	U	A	K	P	V	A	H	N	S
B	I	O	V	A	G	N	T	B	H	R	W	C	H	O	U	Z
I	P	V	C	H	N	U	A	I	O	Y	D	J	O	V	B	G
P	W	C	J	O	U	B	H	P	V	F	K	Q	V	C	I	N
W	D	J	Q	V	B	I	O	W	C	M	R	X	C	J	P	U
D	K	Q	X	C	I	P	V	D	J	T	Y	E	J	Q	W	B
K	R	X	E	J	P	W	C	K	Q	A	F	L	Q	X	D	I
R	Y	E	L	Q	W	D	J	R	X	H	M	S	X	E	K	P
Y	F	L	S	X	D	K	Q	Y	E	O	T	Z	E	L	R	W
F	M	S	Z	E	K	R	X	F	L	V	A	G	L	S	Y	D
M	T	Z	G	L	R	Y	E	M	S	C	H	N	S	Z	F	K
<u>T</u>	<u>A</u>	<u>G</u>	<u>N</u>	<u>S</u>	<u>Y</u>	<u>F</u>	<u>L</u>	<u>T</u>	<u>Z</u>	<u>J</u>	<u>O</u>	<u>U</u>	<u>Z</u>	<u>G</u>	<u>M</u>	<u>R</u>
A	H	N	U	Z	.	.	.	.	.	.	.	.	.	.	.	.

FIGURE 85

c. Kryha subsequently improved his machine by incorporating a selector wheel with 52 adjustable screws or "stops," each screw having the function of bringing into play a particular displacement, of at least 3, of the alphabets. Any combination of these 52 screws could be used to generate a series of successive displacements which summed to 179 ( $\equiv 23, \text{ mod } 26$ ). Since 23 is prime, the period of the improved Kryha machine is 26 times the number of stops used, and therefore ranges between 26 (for 1 stop, which would raise the devil with the machine mechanically) and 1352 (when all 52 stops are used). Below is given the stepping pattern of the improved model of the Kryha machine:

Screw No.:	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
Skips:	4	3	4	3	3	3	4	3	4	4	3	3	3	3	4	4	3	3	4	3
Screw No.:	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36	37	38	39	40
Skips:	3	4	3	3	4	3	3	4	4	4	3	3	4	3	3	3	4	3	4	3
Screw No.:	41	42	43	44	45	46	47	48	49	50	51	52	1							
Skips:	3	4	5	3	3	3	3	4	3	3	4	5								

d. In the analysis of the Kryha machine we shall first treat the aspects of solution of the original 1924 model and then those applying to the improved model.

53. Analysis of the original Kryha cipher machine.—a. For a demonstration of the general method of solution of the original Kryha machine, we shall use as an example a test message submitted to the U.S. Army Signal Corps in 1933; this is shown in Fig. 86, below:²

X	Y	I	C	P	N	D	E	A	M	A	P	D	T	R	A	X	X	P	Z	X	H	Y	R	Y	T	W	Q	X	F
H	C	D	J	K	A	H	Q	U	R	Z	P	P	P	Z	Q	O	F	U	V	K	F	E	M	N	E	A	O	N	G
T	T	X	S	V	V	U	B	D	G	J	R	E	J	F	H	E	O	K	V	C	Q	H	F	H	R	O	K	U	P
M	Q	P	Q	W	A	C	O	J	C	R	L	M	B	M	E	V	K	R	V	J	D	Y	N	N	S	X	U	D	L
H	N	P	F	W	M	O	C	M	J	F	L	G	P	M	B	K	H	A	U	X	L	I	V	V	Q	S	X	U	N
J	Z	U	K	K	O	B	A	A	E	U	Q	O	Y	J	I	Z	S	Z	U	H	G	W	G	W	A	T	E	J	W
Y	D	I	V	X	P	E	I	K	E	E	C	M	C	I	R	X	X	L	A	Z	L	A	I	N	M	J	Z	X	I
C	I	D	K	Q	L	M	M	T	E	L	L	F	J	T	J	U	B	Q	O	L	J	A	W	M	F	E	H	E	V
S	Y	C	A	S	K	F	O	N	O	Z	U	M	P	A	D	A	P	J	Y	L	P	F	N	T	R	U	I	T	C
B	W	H	J	H	M	O	L	C	V	R	D	E	P	F	Q	A	C	I	U	H	C	Z	C	B	X	T	O	K	C
I	X	G	O	S	G	C	M	R	F	H	J	V	X	S	V	Z	N	M	U	G	J	J	S	O	Q	B	J	Q	H
B	Q	N	L	H	R	T	M	E	L	Y	N	H	K	U	F	X	J	D	M	J	Y	C	P	A	D	P	P	W	Y
M	G	U	W	O	I	A	I	I	G	P	T	S	F	C	S	O	K	I	D	G	G	T	Y	O	A	A	Q	D	R
Q	R	R	M	N	T	S	H	Y	N	E	X	Y	V	F	C	M	J	J	K	N	X	V	T	E	F	X	A	U	T
S	E	Z	Q	S	H	L	U	L	Y	C	Y	G	X	O	N	L	A	W	Q	T	E	J	N	B	S	M	V	T	E
H	S	X	U	Y	N	J	K	X	F	P	E	P	G	F	C	M	M	C	W	Z	R	P	J	Y	G	O	P	Z	U
Q	N	V	X	I	A	X	Z	K	Q	M	J	E	F	W	W	M	R	Q	R	T	E	T	P	X	R	S	U	K	C
D	L	H	E	D	L	L	C	T	J	K	S	Z	M	Q	M	K	N	J	U	V	P	F	L	Y	H	Y	F	Q	R
E	W	N	D	Z	M	B	M	P	B	O	J	X	E	Q	I	Z	A	X	H	N	D	B	Q	Q	W	D	I	X	Q
P	I	F	A	Y	J	G	Q	J	O	F	W	F	C	D	B	X	Y	N	X	Y	T	W	Y	K	E	Q	C	D	P
D	Y	D	O	Z	H	J	F	C	Z	U	E	D	D	J	B	F	X	T	T	V	F	Y	G	H	C	T	B	G	O
F	E	H	B	U	B	Z	D	Q	Q	T	I	G	D	Y	A	I	Y	F	D	F	H	A	B	S	A	H	Y	G	X
I	B	B	L	E	C	Q	O	S	E	M	O	M	Z	V	K	H	Q	S	J	C	M	J	F	F	E	V	V	T	L
W	T	E	S	L	A	Y	W	F	Y	C	K	O	X	P	S	V	N	A	I	G	O	C	Z	Z	K	V	V	V	J
S	O	P	E	N	Y	X	D	D	X	L	D	C	Y	A	X	M	W	W	O	C	W	O	I	I	B	N	X	T	V
T	L	I	V	Q	W	X	U	E	T	P	S	U	H	C	S	O	Y	T	P	V	Y	I	K	Z	N	F	V	I	E
Y	P	H	K	I	N	C	G	G	V	I	K	R	O	O	S	O	V	M	G	H	K	U	N	U	S	U	N	Y	V
C	F	E	L	O	O	W	S	A	I	Y	R	R	E	V	N	E	X	P	E	S	E	G	R	P	Z	N	B	M	M
Y	U	Z	F	G	S	X	R	X	W	M	N	W	T	L	R	H	V	F	H	G	S	X	M	W	V	R	E	A	J
D	G	O	Z	A	G	R	X	K	J	L	D	O	G	Y	P	T	Y	X	N	T	M	W	Q	M	Y	S	Q	W	L
X	H	N	G	Z	Q	D	M	C	W	P	Y	A	T	G	N	Z	F	J	K	W	G	D	K	A	V	S	J	M	H
J	G	W	J	E	C	W	T	D	B	Z	N	M	Y	T	N	A	O	R	V	H	A	R	R	P	D	X	G	C	A
P	H	J	N	Z	K	T	L	Q	R	Q	J	J	A	F	F	Z	G	D	X	L	R	F	F	S	A	W	S	Z	N
G	L	S	A	Q	B	M	C	D	Y	J	F	M	B	L	S	X	E	O	T	L	F	J	G	G	L	G	K	K	R
Y	Y	W	D	A	L	H	H	J	V	C	G	Y	V	R	L	Y	S	P	J	V	P	K	G	W	W	X	H	F	A
C	M	T	R	G	U	J	E	J	W	T	A	F	S	N	Z	X	V	V	W	I	Y	W	O	O	M	T	L	U	F
S	B	C	A	J	R	N	R	M	P	I	Y	L	W	I	K	A	O	K	H	T	M	X	C	N	I	M	W	T	F
G	T	T	D	E	H	T	D	H	M	K	K	C	D	K	E	A	P	H	I	A	X	Z	Y	P					

FIGURE 86

² The interesting circumstances surrounding this case are recorded in an article by the author entitled "Q.E.D.—2 Hours, 41 Minutes," published in the *NSA Technical Journal*, Vol. XVIII, No. 4, Fall 1973.

b. Now it is clear from the key diagram in Fig. 85 that if a message were encrypted starting at, say, position 1 of the selector wheel and "alphabet 1" of the enciphering components, the 1st, 9th, 33d, 41st, and 57th letters, for example, would be enciphered in the key of A, and would therefore belong to one monoalphabetic distribution; this is shown in the key fragment in Fig. 87a, below. It may also be seen that, owing to the isomorphism of the key, even if a different initial alphabet were used (take

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17
<u>7 6 7 5 6 7 6 8 6 10 5 6 5 7 6 5 9</u>																
Ⓐ	H	N	U	Z	F	M	S	Ⓐ	G	Q	V	B	G	N	T	Y
H	O	U	B	G	M	T	Z	H	N	X	C	I	N	U	Ⓐ	F
O	V	B	I	N	T	Ⓐ	G	O	U	E	J	P	U	B	H	M
V	C	I	P	U	Ⓐ	H	N	V	B	L	Q	W	B	I	O	T

FIGURE 87a

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17
<u>7 6 7 5 6 7 6 8 6 10 5 6 5 7 6 5 9</u>																
Ⓑ	I	O	V	A	G	N	T	Ⓑ	H	R	W	C	H	O	U	Z
I	P	V	C	H	N	U	A	I	O	Y	D	J	O	V	Ⓑ	G
P	W	C	J	O	U	Ⓑ	H	P	V	F	K	Q	V	C	I	N
W	D	J	Q	V	Ⓑ	I	O	W	C	M	R	X	C	J	P	U

FIGURE 87b

any other letter in the first column of Fig. 85—for example, B), as long as the selector wheel was set at position 1 the 1st, 9th, 33d, 41st, and 57th letters would still be monoalphabetically distributed, as shown by the key fragment in Fig. 87b, above. Therefore in the course of analysis a total of 17 sets of distributions might have to be made, and the correct initial position of the selector wheel would be that in which *all 26* distributions of one of the 17 sets revealed a close approximation to the expected  $\delta$  I.C. for the language involved.

c. One way of making the distributions is to write out the cipher text in a block consisting of rows of 17 letters, allocating the letters of column 1 into 26 distributions, each succeeding letter in the column being recorded in a distribution 7 away from its predecessor because of the +7 isomorphic progression of the key; thus the letters of column 1 would go into distributions 1, 8, 15, 22, 3. . . . Then the letters of column 2 would likewise be allocated into the same distributions, but starting with the proper distribution for the first letter of column 2 (which depends upon the selector position assumed for the first letter of column 1). For example, with selector position 1 the keying sequence is that shown in line (1) of Fig. 88 below, so the first letter of column 2 would be put into the 8th distribution, the first letter of column 3

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17
	<u>7 6 7 5 6 7 6 8 6 10 5 6 5 7 6 5 9</u>																
(1)	1	8	14	21	26	6	13	19	1	7	17	22	2	7	14	20	25
	8	15	21	2	7	. . .											
(2)		1	7	14	19	25	6	12	20	26	10	15	21	26	7	13	18
	1	8	14	21	26	6	. . .										
							*	*	*	*	*	*	*				
(17)																	1
	10	17	23	4	9	15	22	2	10	16	26	5	11	16	23	3	8
	17	24	4	11	. . .												

FIGURE 88

into the 14th distribution, and so on to the first letter of column 17 which would be placed into the 25th distribution. In testing for initial selector position 2, the keying sequence is that shown in line (2) of Fig. 88, so if the first letter of column 2 would be put into the 7th distribution, the first letter of column 3 into the 14th distribution, and so on to the first letter of the last column which would be placed into the 1st distribution. Finally, in testing for initial selector position 17 with the keying sequence shown in line (17) of Fig. 88, the first letter of column 1 would be put into distribution 1, while the first letter of the last column would go into distribution 3.

d. A much easier and quicker way of making the distributions presents itself, using a grille to be placed over the cipher text which is written out in a block 17 wide. Using the key diagram of Fig. 85 as a guide, we cut holes into our grille at the locations of any arbitrary key letter, say the letter A, as shown in Fig. 89, below. We then complete the grille as illustrated in Fig. 90, with the necessary cyclically offset portion shown in dotted lines, and the grille doubled in length for convenience in use. (The heavy circles show the index or reference position used in designating the placement of the grille over the cipher text.)



1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17  
 7 6 7 5 6 7 6 8 6 10 5 6 5 7 6 5 9

A H N U Z F M S A G Q V B G N T Y  
 H O U B G M T Z H N X C I N U A F  
 O V B I N T A G O U E J P U B H M  
 V C I P U A H N V B L Q W B I O T  
 C J P W B H O U C I S X D I P V A  
 J Q W D I O V B J P Z E K P W C H  
 Q X D K P V C I Q W G L R W D J O  
 X E K R W C J P X D N S Y D K Q V  
 E L R Y D J Q W E K U Z F K R X C  
 L S Y F K Q X D L R B G M R Y E J  
 S Z F M R X E K S Y I N T Y F L Q  
 Z G M T Y E L R Z F P U A F M S X  
 G N T A F L S Y G M W B H M T Z E  
 N U A H M S Z F N T D I O T A G L  
 U B H O T Z G M U A K P V A H N S  
 B I O V A G N T B H R W C H O U Z  
 I P V C H N U A I O Y D J O V B G  
 P W C J O U B H P V F K Q V C I N  
 W D J Q V B I O W C M R X C J P U  
 D K Q X C I P V D J T Y E J Q W B  
 K R X E J P W C K Q A F L Q X D I  
 R Y E L Q W D J R X H M S X E K P  
 Y F L S X D K Q Y E O T Z E L R W  
 F M S Z E K R X F L V A G L S Y D  
 M T Z G L R Y E M S C H N S Z F K  
 T A G N S Y F L T Z J O U Z G M R

A H N U Z . . .

FIGURE 89

e. We now place the grille so that the index position is over the first letter of the cipher text, as illustrated in Fig. 91a (only the top 40 of the 67 lines of cipher are shown here), and we make the following distribution of the letters exposed through the apertures:

/  
 ≡ - = - - = - ≡ = = - = ≡ - - - = = = ≡ ≡  
 A B C D E F G H I J K L M N O P Q R S T U V W X Y Z

This distribution has a  $\delta$  I.C. of 1.18, nothing to write home about. We then slide the grille over one position to the right, so that the index position is over the second letter of the cipher text, and we arrive at a distribution with an I.C. of 0.95. Sliding the grille so that the index position is over the third letter of the cipher, we obtain a distribution with an I.C. of 0.97. When, however, we slide the grille so that the index position is over the fourth letter of the cipher (as illustrated in fragmentary form in Fig. 91b) we obtain the following distribution:

≡ ≡ ≡ - ≡ - = = = / - ≡ ≡ ≡ ≡ ≡  
 A B C D E F G H I J K L M N O P Q R S T U V W X Y Z

The I.C. of this distribution is 1.79 so we know that, barring the touch of a Mephistophelian (or rather, a Bernoullian) finger, the fourth letter of the text was enciphered at position 1 of the selector wheel; therefore the initial setting for the first letter must have been position 15. In any case, we shall prove or disprove this point very quickly.

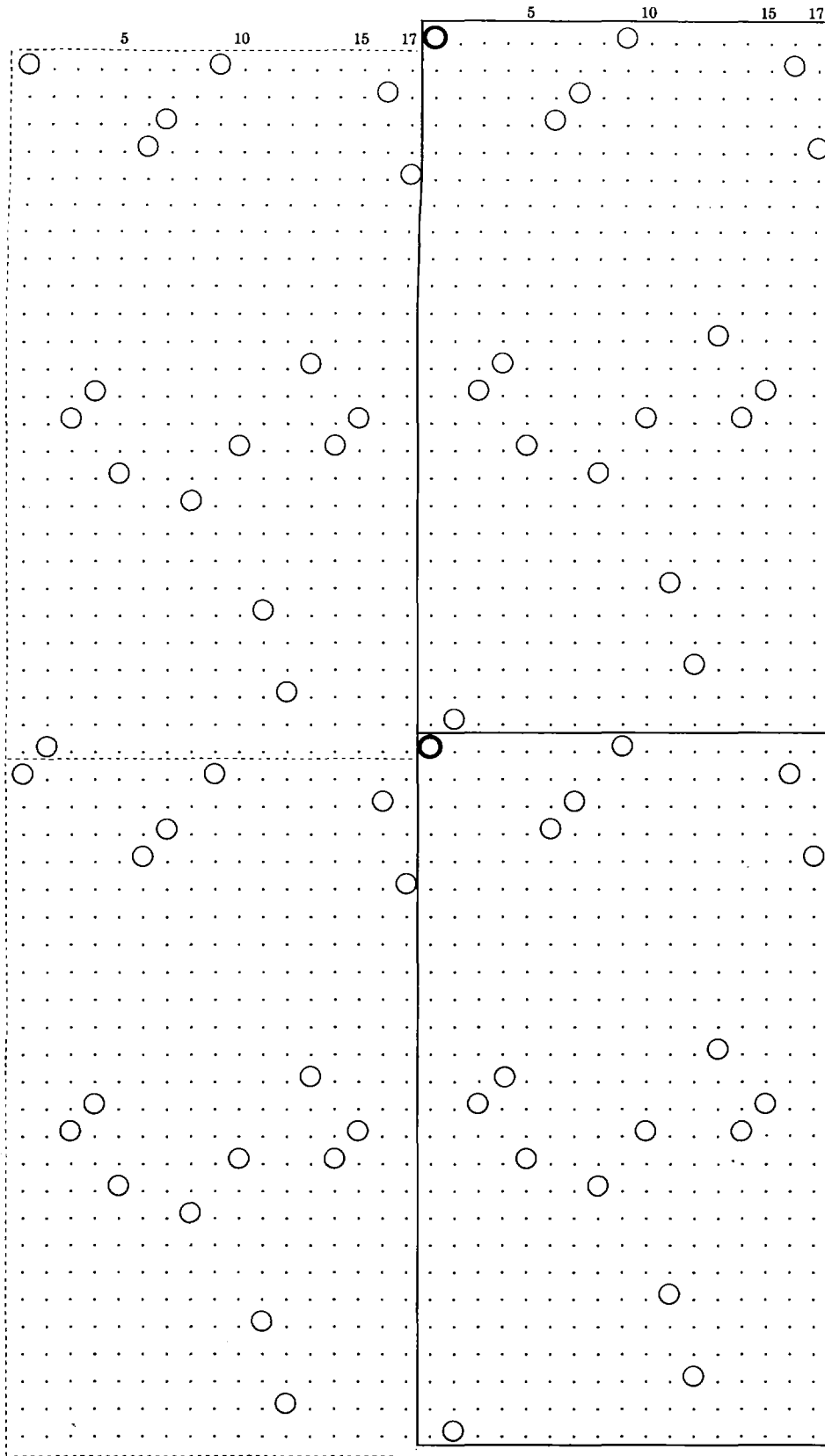


FIGURE 90

f. If this is the correct initial setting of the selector wheel and we drop the grille vertically one position, the letters exposed through the apertures will still be monoalphabetically distributed, but in an alphabet +7 away from that which we have just obtained above; in other words, referring to Fig. 85, if the letters exposed in Fig. 91b belonged to the A or 1st alphabet, then sliding the grille down one position would reveal the letters that belonged to the H or 8th alphabet. Sure enough, the I.C. of the distribution of these letters is 1.92, so we know that we are on the right track. By successively sliding

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	
	ⓧ	Y	I	C	P	N	D	E	Ⓐ	M	A	P	D	T	R	A	X	
	X	P	Z	X	H	Y	R	Y	T	W	Q	X	F	H	C	Ⓓ	J	
	K	A	H	Q	U	R	⓪	P	P	P	Z	Q	O	F	U	V	K	
	F	E	M	N	E	Ⓐ	O	N	G	T	T	X	S	V	V	U	B	
5	D	G	J	R	E	J	F	H	E	O	K	V	C	Q	H	F	Ⓜ	
	R	O	K	U	P	M	Q	P	Q	W	A	C	O	J	C	R	L	
	M	B	M	E	V	K	R	V	J	D	Y	N	N	S	X	U	D	
	L	H	N	P	F	W	M	O	C	M	J	F	L	G	P	M	B	
	K	H	A	U	X	L	I	V	V	Q	S	X	U	N	J	Z	U	
10	K	K	O	B	A	A	E	U	Q	O	Y	J	I	Z	S	Z	U	
	H	G	W	G	W	A	T	E	J	W	Y	D	I	V	X	P	E	
	I	K	E	E	C	M	C	I	R	X	X	L	Ⓐ	Z	L	A	I	
	N	M	J	⓪	X	I	C	I	D	K	Q	L	M	M	T	E	L	
	L	F	J	⓪	T	J	U	B	Q	O	L	J	A	W	M	Ⓜ	E	H
15	E	V	S	Y	C	A	S	K	F	⓪	N	O	Z	⓪	M	P	A	
	D	A	P	J	⓪	L	P	F	N	T	R	U	I	T	C	B	W	
	H	J	H	M	O	L	C	⓪	R	D	E	P	F	Q	A	C	I	
	U	H	C	Z	C	B	X	T	O	K	C	I	X	G	O	S	G	
	C	M	R	F	H	J	V	X	S	V	Z	N	M	U	G	J	J	
20	S	O	Q	B	J	Q	H	B	Q	N	L	H	R	T	M	E	L	
	Y	N	H	K	U	F	X	J	D	M	J	Y	C	Ⓜ	A	D	P	
	P	W	Y	M	G	U	W	O	I	A	I	I	G	P	T	S	F	
	C	S	O	K	I	D	G	G	T	Y	O	A	A	Q	D	R	Q	
	R	M	R	N	T	S	H	Y	N	E	X	Y	V	F	C	M	J	
25	J	K	N	X	V	T	E	F	X	A	U	T	S	E	Z	Q	S	
	H	L	U	L	Y	C	Y	G	X	O	N	L	A	W	Q	T	E	
	⓪	N	B	S	M	V	T	E	Ⓜ	S	X	U	Y	N	J	K	X	
	F	P	E	P	G	F	C	M	M	C	W	Z	R	P	J	Y	G	
	O	P	Z	U	Q	N	V	X	I	Ⓐ	X	Z	K	Q	M	J	E	
30	F	W	W	M	R	⓪	R	T	E	T	P	X	R	S	U	K	C	
	D	L	H	E	D	L	L	C	T	J	K	S	Z	M	Q	M	Ⓜ	
	N	J	U	V	P	F	L	Y	H	Y	F	Q	R	E	W	N	D	
	Z	M	B	M	P	B	O	J	X	E	Q	I	Z	A	X	H	N	
	D	B	Q	Q	W	D	I	X	Q	P	I	F	A	Y	J	G	Q	
35	J	O	F	W	F	C	D	B	X	Y	N	X	Y	T	W	Y	K	
	E	Q	C	D	P	D	Y	D	O	Z	H	J	F	C	Z	U	E	
	D	D	J	B	F	X	T	T	V	F	Y	G	H	C	T	B	G	
	O	F	E	H	B	U	B	Z	D	Q	Q	T	I	G	D	Y	A	
	I	Y	F	Ⓜ	F	H	A	B	S	A	H	Y	G	X	I	B	B	
40	L	E	C	Q	O	S	E	M	O	M	Z	V	K	H	Ⓜ	S	J	

FIGURE 91a

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	
	X	Y	I	Ⓜ	P	N	D	E	A	M	A	Ⓜ	D	T	R	A	X	
	X	P	Z	X	H	Y	R	Y	T	W	Q	X	F	H	C	D	J	
	K	Ⓐ	H	Q	U	R	Z	P	P	Ⓜ	Z	Q	O	F	U	V	K	
	F	E	M	N	E	A	O	N	Ⓜ	T	T	X	S	V	V	U	B	
5	D	G	J	R	E	J	F	H	E	O	K	V	C	Q	H	F	H	
	R	O	Ⓜ	U	P	M	Q	P	Q	W	A	C	O	J	C	R	L	
	M	B	M	E	V	K	R	V	J	D	Y	N	N	S	X	U	D	
	L	H	N	P	F	W	M	O	C	M	J	F	L	G	P	M	B	
	K	H	A	U	X	L	I	V	V	Q	S	X	U	N	J	Z	U	
10	K	K	O	B	A	A	E	U	Q	O	Y	J	I	Z	S	Z	U	
	H	G	W	G	W	A	T	E	J	W	Y	D	I	V	X	P	E	
	I	K	E	E	C	M	C	I	R	X	X	L	A	Z	L	Ⓐ	I	
	N	M	J	Z	X	I	Ⓜ	I	D	K	Q	L	M	M	T	E	L	
	L	F	J	T	J	Ⓜ	B	Q	O	L	J	A	W	M	F	E	H	
15	Ⓜ	V	S	Y	C	A	S	K	F	O	N	O	⓪	U	M	P	Ⓐ	
	D	A	P	J	Y	L	P	Ⓜ	N	T	R	U	I	T	C	B	W	
	H	J	H	M	O	L	C	V	R	D	Ⓜ	P	F	Q	A	C	I	
	U	H	C	Z	C	B	X	T	O	K	C	I	X	G	O	S	G	
	C	M	R	F	H	J	V	X	S	V	Z	N	M	U	G	J	J	
20	S	O	Q	B	J	Q	H	B	Q	N	L	H	R	T	M	E	L	
	Y	N	H	K	U	F	X	J	D	M	J	Y	C	Ⓜ	A	D	P	
	P	W	Y	M	G	U	W	O	I	A	I	I	G	P	T	S	F	
	C	S	O	K	I	D	G	G	T	Y	O	A	A	Q	D	R	Q	
	R	M	R	N	T	S	H	Y	N	E	X	Y	V	F	C	M	J	
25	J	K	N	X	V	T	E	F	X	A	U	T	S	E	Z	Q	S	
	H	L	U	L	Y	C	Y	G	X	O	N	L	A	W	Q	T	E	
	J	N	B	Ⓜ	V	T	E	H	S	X	Ⓜ	Y	N	J	K	X		
	F	P	E	P	G	F	C	M	M	C	W	Z	R	P	J	Y	G	
	O	Ⓜ	Z	U	Q	N	V	X	I	Ⓐ	X	Z	K	Q	M	J	E	
30	F	W	W	M	R	Q	R	T	Ⓜ	T	P	X	R	S	U	K	C	
	D	L	H	E	D	L	L	C	T	J	K	S	Z	M	Q	M	K	
	N	J	Ⓜ	V	P	F	L	Y	H	Y	F	Q	R	E	W	N	D	
	Z	M	B	M	P	B	O	J	X	E	Q	I	Z	A	X	H	N	
	D	B	Q	Q	W	D	I	X	Q	P	I	F	A	Y	J	G	Q	
35	J	O	F	W	F	C	D	B	X	Y	N	X	Y	T	W	Y	K	
	E	Q	C	D	P	D	Y	D	O	Z	H	J	F	C	Z	U	E	
	D	D	J	B	F	X	T	T	V	F	Y	G	H	C	T	B	G	
	O	F	E	H	B	U	B	Z	D	Q	Q	T	I	G	D	Y	A	
	I	Y	F	D	F	H	Ⓐ	B	S	A	H	Y	G	X	I	B	B	
40	L	E	C	Q	O	Ⓜ	S	E	M	O	M	Z	V	K	H	Q	S	J

FIGURE 91b

the grille down one position at a time in Fig. 91b, we obtain the 26 distributions shown in Fig. 92, below, given together with the numerical designations of these alphabets (in parentheses) and their I.C.'s. The average I.C. of these distributions, 1.88, makes us very happy.

Alph.	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	I.C.
1. (21)	5	5	4	1	3			1	2	2			2	6	1	3		3							6	1	1.79
2. (2)	2	3	2	1	6				2			2	1	5					5		1	6	3		5		1.92
3. (9)			1	3	1	4	6	1	1	1	3		1	2	7	1	3	1	1	1	1	1	1		3		1.58
4. (16)	3		4	2	1			1	4		2	1	2	1	2	3	1			2		4	8	1			1.72
5. (23)		6	7	2	4	1			1	4		4	2	1	1	1	3	3	1		1						1.87
6. (4)		1	2	1	1			1	1	7		4	2		2	1	1	2		2	6	4	4				1.78
7. (11)	1	2	4					2	1			2	4	6	3	5		1	1	2	5	1		3			1.64
8. (18)				1	8	7	4	1	3	1				2	5	3				1	2		3	1	1		2.19
9. (25)	1	3	3	2	5	6				1				1	2	1	1		5	6	3	3					1.84
10. (6)	2	1	4	4					5	2		1		1	4	6				5	3	5					1.96
11. (13)	4	1	2	1	4				2	3	5	4	5	1	2	4								2	2	1	1.50
12. (20)	2	1	9	4	1	4		4	2	4	1	1	3	3		3		1	3	3		1					1.95
13. (1)	1	1	4	3	1			2	1	2	6	1	2				4		1	7	7	3					1.96
14. (8)	2			5	3	1		1	1	3	3	2	3	8	6	4	2	1									1.94
15. (15)			4	4	3			5	6	1	1	2	7	1	1	6	1		4								1.73
16. (22)	6	1	10	4	3	2	1	3	1	1	1	1	1	3	2	1	1			3		1					2.10
17. (3)	2	2	3	1	1			4	4			2	5	1		1	6			6	6						2.01
18. (10)	3		2		3	3	6	3	1	3	7	6	2			5				3					3		2.05
19. (17)		4	2	4	1	1		3	3	7	6	2			1	1	1		1	3	3						1.79
20. (24)	3	5	2	3	8	1		1	6	2	1		2	1	2	2	2	2		2							1.90
21. (5)		1	2					3	3		5	4	1	2	5	6	2	8									2.36
22. (12)	2	2	3	4	3	2	1	4	1	2	2		1	1	2	1	4	5		2		1					1.18
23. (19)	3		4	2	1	6	5	5	5	2	2		2				1			3	2						1.63
24. (26)	7	1		1	3	3	6	1	1	2	2	3		2						3	1	5	3				1.76
25. (7)		2			1	1		2	7	4	1	2		3	1	3	3		3	1	1	2					2.96
26. (14)		2	2	3			3	5	2	4	6	2	6	1	2	1	2	4									1.68

FIGURE 92

g. The next step is to rewrite the successive columns of Fig. 92 as rows of a new matrix for convenience in the matching process on which we are about to embark. This new matrix is shown in Fig. 93, below, in which the cipher letters are at the left, and tally totals for each row at the right. The frequencies within each row represent the frequencies of the successive plaintext equivalents of the cipher letter designated at the left, and therefore the method of solution bears a close resemblance to that of the classic progressive alphabet cipher in which we match the cipher-letter rows to obtain a statistical reconstruction of the cipher component, regardless of the identity of the plain component.³

³ Cf. pp. 162-168, *Military Cryptanalytics, Part II*.





h. Since we know both the cipher component and its motion, we are now able to reduce the cipher text to monoalphabetic terms, using an arbitrary A-Z sequence for the plain component at the initial setting as shown below:

P: A B C D E F G H I J K L M N O P Q R S T U V W X Y Z  
C: J N F G H E A C B D W Y X Z V U R S T Q L O I M P K

The first cipher letter of the message,  $X_c$ , is deciphered as  $M_p$ ; the second letter,  $Y_c$ , involves a shift of the cipher component of 6 positions to the left and is therefore deciphered as  $F_p$ ; and so on for the reduction of the rest of the text. The reduction of the first 10 of the 67 lines of 17 letters is shown in Fig. 95, together with the distribution of the monoalphabetically converted text.

	15	16	17	1	2	3	4	5	6	7	8	9	10	11	12	13	14
	<u>6 5 9 7 6 7 5 6 7 6 8 6 10 5 6 5 7</u>																
C:	X	Y	I	C	P	N	D	E	A	M	A	P	D	T	R	A	X
"P":	<u>M</u>	<u>F</u>	<u>L</u>	<u>N</u>	<u>X</u>	<u>U</u>	<u>V</u>	<u>M</u>	<u>H</u>	<u>R</u>	<u>U</u>	<u>E</u>	<u>J</u>	<u>I</u>	<u>B</u>	<u>L</u>	<u>M</u>
C:	X	P	Z	X	H	Y	R	Y	T	W	Q	X	F	H	C	D	J
"P":	<u>F</u>	<u>L</u>	<u>V</u>	<u>L</u>	<u>W</u>	<u>X</u>	<u>V</u>	<u>L</u>	<u>M</u>	<u>X</u>	<u>A</u>	<u>L</u>	<u>V</u>	<u>N</u>	<u>L</u>	<u>H</u>	<u>T</u>
C:	K	A	H	Q	U	R	Z	P	P	P	Z	Q	O	F	U	V	K
"P":	<u>L</u>	<u>M</u>	<u>F</u>	<u>L</u>	<u>A</u>	<u>V</u>	<u>L</u>	<u>R</u>	<u>L</u>	<u>E</u>	<u>N</u>	<u>L</u>	<u>H</u>	<u>E</u>	<u>M</u>	<u>F</u>	<u>L</u>
C:	F	E	M	N	E	A	O	N	G	T	T	X	S	V	V	U	N
"P":	<u>H</u>	<u>E</u>	<u>R</u>	<u>M</u>	<u>J</u>	<u>E</u>	<u>M</u>	<u>N</u>	<u>J</u>	<u>R</u>	<u>L</u>	<u>X</u>	<u>W</u>	<u>J</u>	<u>E</u>	<u>Z</u>	<u>N</u>
C:	D	G	J	R	E	J	F	H	E	O	K	V	C	Q	H	F	H
"P":	<u>H</u>	<u>V</u>	<u>N</u>	<u>U</u>	<u>C</u>	<u>R</u>	<u>M</u>	<u>J</u>	<u>E</u>	<u>N</u>	<u>L</u>	<u>S</u>	<u>F</u>	<u>H</u>	<u>N</u>	<u>F</u>	<u>C</u>
C:	R	O	K	U	P	M	Q	P	Q	W	A	C	O	J	C	R	L
"P":	<u>H</u>	<u>G</u>	<u>F</u>	<u>M</u>	<u>O</u>	<u>H</u>	<u>W</u>	<u>W</u>	<u>L</u>	<u>V</u>	<u>L</u>	<u>E</u>	<u>M</u>	<u>H</u>	<u>J</u>	<u>M</u>	<u>L</u>
C:	M	B	M	E	V	K	R	V	J	D	Y	N	N	S	X	U	D
"P":	<u>H</u>	<u>M</u>	<u>W</u>	<u>V</u>	<u>X</u>	<u>C</u>	<u>M</u>	<u>F</u>	<u>L</u>	<u>N</u>	<u>J</u>	<u>R</u>	<u>L</u>	<u>R</u>	<u>H</u>	<u>E</u>	<u>T</u>
C:	L	H	N	P	F	W	M	O	C	M	J	F	L	G	P	M	B
"P":	<u>X</u>	<u>B</u>	<u>T</u>	<u>H</u>	<u>E</u>	<u>G</u>	<u>M</u>	<u>F</u>	<u>L</u>	<u>U</u>	<u>R</u>	<u>L</u>	<u>X</u>	<u>W</u>	<u>M</u>	<u>F</u>	<u>L</u>
C:	K	H	A	U	X	L	I	V	V	Q	S	X	U	N	J	Z	U
"P":	<u>V</u>	<u>U</u>	<u>R</u>	<u>R</u>	<u>H</u>	<u>J</u>	<u>E</u>	<u>R</u>	<u>L</u>	<u>J</u>	<u>B</u>	<u>O</u>	<u>L</u>	<u>N</u>	<u>H</u>	<u>O</u>	<u>L</u>
C:	K	K	O	B	A	A	E	U	Q	O	Y	J	I	Z	S	Z	U
"P":	<u>O</u>	<u>I</u>	<u>Z</u>	<u>D</u>	<u>U</u>	<u>O</u>	<u>G</u>	<u>L</u>	<u>J</u>	<u>E</u>	<u>O</u>	<u>V</u>	<u>L</u>	<u>S</u>	<u>R</u>	<u>H</u>	<u>E</u>

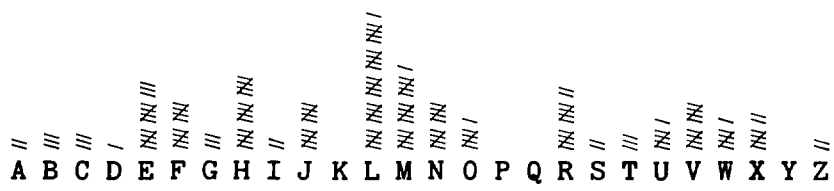


FIGURE 95

The simple substitution is now easily solved, beginning with the identification of L_c of the converted text as E_p, and the initial trigraph MFL_c as THE_p. The decipherment of the first two rows is shown in the fragment below:

	15	16	17	1	2	3	4	5	6	7	8	9	10	11	12	13	14	
	6	5	9	7	6	7	5	6	7	6	8	6	10	5	6	5	7	
C:	X	Y	I	C	P	N	D	E	A	M	A	P	D	T	R	A	X	
"P":	M	F	L	N	X	U	V	M	H	R	U	E	J	I	B	L	M	
P:	T	H	E	C	O	U	R	T	I	S	U	N	A	B	L	E	T	
C:	X	P	Z	X	H	Y	R	Y	T	W	Q	X	F	H	C	D	J	. . .
"P":	F	L	V	L	W	X	V	L	M	X	A	L	V	N	L	H	T	
P:	H	E	R	E	F	O	R	E	T	O	P	E	R	C	E	I	V	

The recovered plain component, set in position against the cipher component for decipherment of the first letter of the text, is as follows:

P: P L M J N H G I B A K E T C D . . S W V U R F O . Y  
 C: J N F G H E A C B D W Y X Z V U R S T Q L O I M P K

Since the sequences were made up at random (but not too thoroughly mixed at that) and since three letters did not occur in the first 170 letters of the plain text, we cannot be certain of the placement of the missing letters in the plain component. (An X_p does occur, however, at the 539th and 647th positions of the text, so this letter could be inserted in its proper place in the plain component, immediately to the left of the S.)

i. In subpar. e we arrived at the correct grille placement by sliding it through successive positions of the cipher until a favorable I.C. was reached. The theoretical I.C. of the cipher letters at an incorrect setting of the grille, however, is not 1.00 as might be supposed. For example, if we place our grille (with the "A" positions cut out) over the key diagram of Fig. 85, we shall expose 17 A's, of course; but if we move the grille one position over to the right, instead of a random assortment of equiprobable key letters we obtain a severely limited distribution of 4 F's, 6 G's, 4 H's, and one each of the letters I, J, and K. The distributions of key letters for the 17 positions of the grille are shown in the diagram below:

Pos.	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	
1.	17																										
2.						4	6	4	1	1	1																
3.											4	2	5	3	1	2											
4.																1	6	1	3	4	1			1			
5.	1	6		2	1																			2	3	2	
6.			2		3	3	3	3	2		1																
7.								1			1	3	5	4	1	1	1										
8.																	1	2	7	1	3	3					
9.	4	6	1	1																					2	3	
10.				1	1	6	4	3	2																		
11.											3	3	1	7	2	1											
12.																	1	1	1	4	5	3	1		1		
13.	3	3	3		2																	1		2	3		
14.			1	2		6	1	2	3	2																	
15.									1		1	4	3	1	6		1										
16.																		2	1	3	5	2	4				
17.	4	6	4																						1	1	1



It may be seen that the number of different key letters in the wrong cases is 6, 7, or 8, with biased distributions which are symmetrically disposed between 2 and 17, 3 and 16, 4 and 15, etc. This may result in situations wherein, if the number of letters in the distribution is too small a sample, a wrong grille position might yield an I.C. even in excess of the expected 1.73; that is why, in subpar. *f*, we reserved judgment until we made additional distributions at our assumed setting to confirm its validity. In order to establish the theoretical I.C. of the cipher text at a particular wrong setting of the grille, we must calculate the bulge of the  $\gamma$  I.C. (i.e.,  $\gamma - 1$ , or the excess over the expected 1.000 for random), which is given by the formula  $\beta_c = \frac{\beta_k \times \beta_p}{c-1}$ , where  $\beta_c$  is the bulge of the cipher text,  $\beta_k$  the bulge of the key,  $\beta_p$  the bulge of the plain text (for English, .73), and  $c$  is the number of categories (in this case, 26). Thus for selector position 2 with a distribution of (4, 6, 4, 1, 1, 1) the  $\gamma$  I.C. of the key⁴ is  $\frac{26[6^2 + 2(4^2) + 3(1^2)]}{17^2} = 6.40$ , the bulge  $\beta_k = 6.40 - 1.00 = 5.40$ , and the bulge of the cipher  $\beta_c = \frac{(5.40)(.73)}{25-1} = 0.16$ ; therefore the expected I.C. of the cipher text is  $1.00 + .16 = 1.16$ . The complete table of values is shown below:

	$\gamma_k$	$\beta_k$	$\beta_c$	Exp. I.C.		$\gamma_k$	$\beta_k$	$\beta_c$	Exp. I.C.
1.	26.00	25.00	0.73	1.73	10.	6.03	5.03	0.15	1.15
2.	6.40	5.40	0.16	1.16	11.	6.58	5.58	0.16	1.16
3.	5.30	4.30	0.13	1.19	12.	4.94	3.94	0.12	1.12
4.	5.85	4.85	0.14	1.14	13.	4.06	3.06	0.09	1.09
5.	5.30	4.30	0.13	1.13	14.	5.30	4.30	0.13	1.13
6.	4.06	3.06	0.09	1.09	15.	5.85	4.85	0.14	1.14
7.	4.94	3.94	0.12	1.12	16.	5.30	4.30	0.13	1.13
8.	6.58	5.58	0.16	1.16	17.	6.40	5.40	0.16	1.16
9.	6.03	5.03	0.15	1.15					

The average of the theoretical I.C.'s for the 16 wrong settings of the grille is 1.14.

*j.* Once we have recovered the components, the solution of additional messages using the same components is a simple matter. For example, let us assume that we have recovered the components as

P: H Y D R A U L I C B E F G J K M N O P Q S T V W X Z  
 C: Q U E S T I O N A B L Y C D F G H J K M P R V W X Z

and that the following message is at hand:

C N C A X V H N Q O J O C R Y I C K O Q J I A F L Q N M O V  
 U A K G O B E U S G B B V F D A R C C O

The simplest procedure here is to prepare a diagram such as that illustrated below, in which the first row of letters represents the "decipherments" of

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21
	1	8	14	21	26	6	13	19	1	7	17	22	2	7	14	20	25	8	15	21	2
C	G	U	Z	P	J	I	H	S	G	L	V	O	F	L	Z	Q	K				
N		H	S	J	C	D	T	M	I	Y	O	G	L	Y	S	K	B	H			
C			Z	P	J	I	H	S	G	L	V	O	F	L	Z	Q	K	U	X		
A				K	B	R	V	N	C	D	P	J	I	D	T	M	E	Y	S	K	
X					Z	Q	G	L	X	P	C	R	W	P	F	U	H	O	E	A	W

⁴ Since we are dealing with the entire key population in the various cases, it is the  $\gamma$  I.C. given by  $\frac{c \sum f^2}{N^2}$  which is involved here and not the  $\delta$  I.C. given by  $\frac{c \sum f(f-1)}{N(N-1)}$ .

the first letter of the cipher text,  $C_c$  (using the components at the initial setting  $H_p=Q_c$ ), at 17 consecutive positions of the key (starting with selector position 1). The second row represents the 17 decipherments (starting with selector position 2) of the second letter of the cipher,  $N_c$ ; and so on for the decipherments of the first five letters of the cipher text. One of the diagonals in the diagram must represent the correct keying of the selector wheel, but at an arbitrary juxtaposition of the components; therefore the next step is to complete the plain component sequence for, at most, the 17 diagonals. This is shown in Fig. 96, below. In the generatrix diagram for position 10 we see the plaintext fragment **AMMUN**, so we know that the message was enciphered starting at that position of the selector wheel. The rest of the message can now easily be read.

<u>Pos. 1</u>	<u>Pos. 2</u>	<u>Pos. 3</u>		<u>Pos. 10</u>
G H Z K Z	U S P B Q	Z J J R G	***	L O O I P
J Y H M H	L T Q E S	H K K A J		I P P C Q
K D Y N Y	I V S F T	Y M M U K		C Q Q B S
M R D O D	C W T G V	D N N L M		B S S E T
N A R P R	B X V J W	R O O I N		E T T F V
O U A Q A	E Z W K X	A P P C O		F V V G W
P L U S U	F H X M Z	U Q Q B P		G W W J X
Q I L T L	G Y Z N H	L S S E Q		J X X K Z
S C I V I	J D H O Y	I T T F S		K Z Z M H
T B C W C	K R Y P D	C V V G T		M H H N Y
V E B X B	M A D Q R	B W W J V		N Y Y O D
W F E Z E	N U R S A	E X X K W		O D D P R
X G F H F	O L A T U	F Z Z M X		P R R Q A
Z J G Y G	P I U V L	G H H N Z		Q A A S U
H K J D J	Q C L W I	J Y Y O H		S U U T L
Y M K R K	S B I X C	K D D P Y		T L L V I
D N M A M	T E C Z B	M R R Q D		V I I W C
R O N U N	V F B H E	N A A S R		W C C X B
A P O L O	W G E Y F	O U U T A		X B B Z E
U Q P I P	X J F D G	P L L V U		Z E E H F
L S Q C Q	Z K G R J	Q I I W L		H F F Y G
I T S B S	H M J A K	S C C X I		Y G G D J
C V T E T	Y N K U M	T B B Z C		D J J R K
B W V F V	D O M L N	V E E H B		R K K A M
E X W G W	R P N I O	W F F Y E		A M M U N
F Z X J X	A Q O C P	X G G D F		U N N L O

FIGURE 96

k. One of the properties of the Kryha machine is that causal isomorphs may occur, but only at multiples of 17 for the original machine (or at multiples of the number of active screws for the improved model). As an example, let us study the following message known to have been enciphered with the original Kryha machine:

				5						10					15		17
	Y	R	H	O	Q	M	A	H	N	W	X	U	X	J	V	S	U
←	Q	X	R	W	X	T	I	L	A	G	S	D	A	Q	M	F	T
	D	K	Z	L	Q	J	D	K	H	Y	L	A	M	S	H	X	B
	Y	G	Z	F	J	X	G	H	E	K	M	F	R	X	X	X	K
←	G	K	B	O	X	V	F	B	Q	I	H	Y	S	X	L	D	Z
	W	Q	W	K	Y	I	H	S	Y	D	R	E	X	S	K	Z	J
	U	Y	O	V	H	B	X	O	W	D	F	J	F	N	C	M	J
←	H	F	Y	Z	D	X	K	T	P	T	V	C	L	B	M	D	G
	W	P	O	P	Z	I	Z	D	H	C	M	Q	M	V	N	Z	L
	V	O	U	J	Y	T	M	U	K	A	B	C	B	E	N	F	C
←	Y	B	O	X	K	P	Q	G	S	F	S	V	K	Z	N	B	D
	G	M	S	K	Z	E	R	P	O	V	W	K	Z	E	E	E	V
←	M	V	D	L	E	Q	K	D	T	B	P	C	B	C	A	E	V
	C	R	F	L													

(1) Several isomorphs have been found and these are listed below:

- a. R H O Q M A H N W X U X J V S U Q X R
- b. Y O V H B X O W D F J F N C M J H F Y
- c. O U J Y T M U K A B C B E N F C Y B O
- d. H E K M F R X X X K G K B O X V F B Q I H
- e. P O V W K Z E E E V M V D L E Q K D T B P

The derived chains are the following:

- a-b: RY QHOVC SMB AXF UJNWD
- a-c: ROJE HUC QY WAMT VNK XB SF
- b-c: HYOU VJCNE XMFBT WK DA
- d-e: HP XEOL FKVQT GMW RZ IBD

It is but a simple matter to amalgamate these partial chains into a complete equivalent primary component,

V J C N E W K D A S X M F B T Z P G L I Q R H Y O U,

which when decimated at an interval of +5 yields the original component:

Q U E S T I O N A B L Y C D F G H J K M P R V W X Z

(2) Since we are in possession of the cipher component, we can assume an arbitrary A-Z sequence for the plain component in order to reduce the cipher text to monoalphabetic terms. But since we do not know the starting position of the selector wheel, we must be prepared to take all 17 positions in turn, making trial reductions of the text to find the correct one as revealed by the expected  $\delta$  I.C. for the language. The conversion of the text starting at position 1 of the selector wheel is shown below:

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17
K:	7	6	7	5	6	7	6	8	6	10	5	6	5	7	6	5	9
C:	Y	R	H	O	Q	M	A	H	N	W	X	U	X	J	V	S	U
"P":	L	O	D	M	B	O	W	Y	H	R	I	G	X	L	J	K	D
C:	Q	X	R	W	X	T	I	L	A	G	S	D	A	Q	M	F	T
"P":	T	K	B	W	S	S	M	L	B	C	G	L	A	N	Z	O	Z

The I.C. of the entire converted text at this initial position of the selector wheel is 1.15. When, however,

```

      11 12 13 14 15 16 17 1 2 3 4 5 6 7 8 9 10
K:   5 6 5 7 6 5 9 7 6 7 5 6 7 6 8 6 10
C:   Y R H O Q M A H N W X U X J V S U
"P": L Q F Q D Q A Z J T N L C O N M E

      C:   Q X R W X T I L A G S D A Q M F T . . .
      "P": T M D A U U Q M D E L Q F Q D Q A

```

we reach initial selector position 11, we find that the I.C. is 1.68.⁵ The monoalphabetic substitution is now solved,

```

      11 12 13 14 15 16 17 1 2 3 4 5 6 7 8 9 10
K:   5 6 5 7 6 5 9 7 6 7 5 6 7 6 8 6 10
C:   Y R H O Q M A H N W X U X J V S U
"P": L Q F Q D Q A Z J T N L C O N M E
P:   D I V I S I O N H E A D Q U A R T

      C:   Q X R W X T I L A G S D A Q M F T . . .
      "P": T M D A U U Q M D E L Q F Q D Q A
P:   E R S O F F I R S T D I V I S I O

```

and the plain component is found to be the HYDRAULIC . . . XZ sequence.

⁵ For the statistically curious, the following are the I.C.'s of the trial reductions to monoalphabetic terms of the entire cipher text at the various selector positions:

1. 1.15	6. 1.14	10. 1.20	14. 1.18
2. 1.31	7. 1.15	11. 1.68	15. 1.10
3. 1.31	8. 1.14	12. 1.22	16. 1.20
4. 1.19	9. 1.31	13. 1.07	17. 1.35
5. 1.16			

The standard deviation of the  $\delta$  I.C. is given by the formula  $\sigma = \frac{\sqrt{2(c-1)}}{\sqrt{N(N-1)}}$ , which for this 225-letter message is 0.03, so the range of I.C.'s in the wrong cases, 1.07 to 1.35, might indicate astonishing deviations of  $2.3\sigma$  to  $11.7\sigma$ . But this apparent paradox is easily explained, since we know from subpar. *i* that the expected I.C. in a random case for the original Kryha machine is 1.14, and the formula given above for the standard deviation of the I.C. applies *only* to those situations wherein the expected I.C. for random is 1.00.

l. For the last example of solution of the original Kryha machine, let us assume that we have a cipher message and its compromised plain text. This is shown below, written on a width of 17.

```

 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17
B V T B L H T K P A Y U V M X H K
R E F E R R I N G T O Y O U R M E
N D T K X L B X X T T J M N E S L
S S A G E N U M B E R E I G H T T
P S J W O A N Q X I D X R M Z Z H
H R E E F I V E D A T E D O N E S
A I H T L K N O D Y B H J U A Q O
I X D E C E M B E R S T O P P A R
C Q X I U G M Z L K O C H P Y D D
A G R A P H S T H R E E B A K E R
M Y T M N U B M J Q O G R N R R R
A N D F O U R C H A R L I E O F A
X J H I T W A R E X J C I M R O G
D M I N I S T R A T I V E M E M O
O D O X B Z L T P M U Q M U E B V
R A N D U M N U M B E R O N E F O
G M W N N U L H V N U F S Q O R F
U R H A V E B E E N R E S C I N D
U Z X I B H J H L O M M N I D E T
E D S T O P B R O C K C O L I N F

```

(1) The first thing we do is to record the cipher equivalents of identical plaintext letters in the columns, at intervals of 1 row, 2 rows, . . . 9 rows which correspond to intervals of 1, 2, . . . 9 multiples of 7 on the cipher component. This is shown in the diagram below:

Interval N:	1	2	3	4	5	6	7	8	9
7N (mod 26):	<u>7</u>	<u>-12</u>	<u>-5</u>	<u>2</u>	<u>9</u>	<u>-10</u>	<u>-3</u>	<u>4</u>	<u>11</u>
	C M	H T	B T	I N	K U	S M	B O	--	V N
	W T	B W	R H	N B	D V	Q H	T U		
	L J	X C	I Q	T O		A X	J F		
	Y K	M N	O U	C F		X F	V M		
	J X	Z D	J C	M R		J N			
	R E	R B	V J	J M		H O			
	O D								
	G V								

In the first column we have the chain LJX, which should be spaced on the cipher component as

```

          5          10          15          20          25 26
L . . . . . J . . . . . X . . . . .

```

Adding to our sequence the XC from the second column, the JM from the fourth column, and AXF and JN from the sixth column, we obtain

```

L . C . F . . J . M . . . . X . . . . . N A .

```

Incorporating relationships from the other columns, we are able to complete the reconstruction of the cipher component:

L Y C D F G H J K M P R V W X Z Q U E S T I O N A B

(2) For the reconstruction of the plain component, we make a 26x26 matrix with the recovered cipher component at the bottom, and we distribute properly the plain-cipher relationships of column 1 of our matched plain and cipher, starting with R_p=B_c in the top row, S_p=N_c seven rows down in row 8, H_p=P_c in row 15, etc.; this is shown in Fig. 97, below, wherein the first four entries have been ringed.

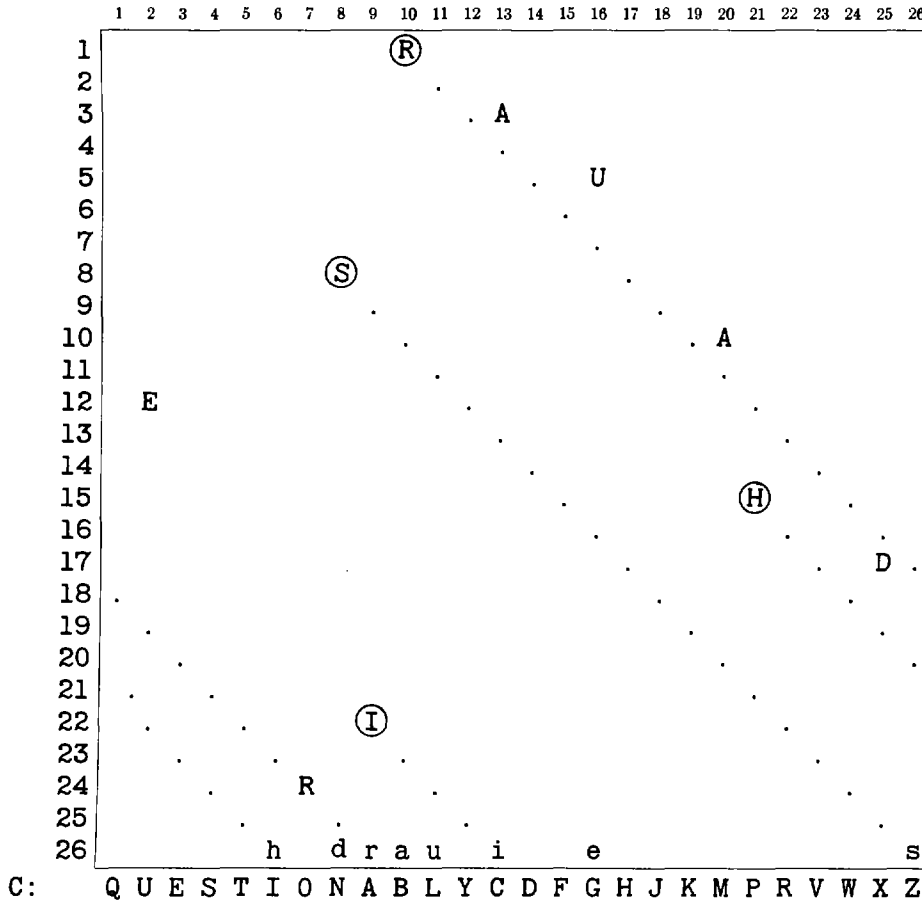


FIGURE 97

The partial plain component reconstructed from the values in the first column is

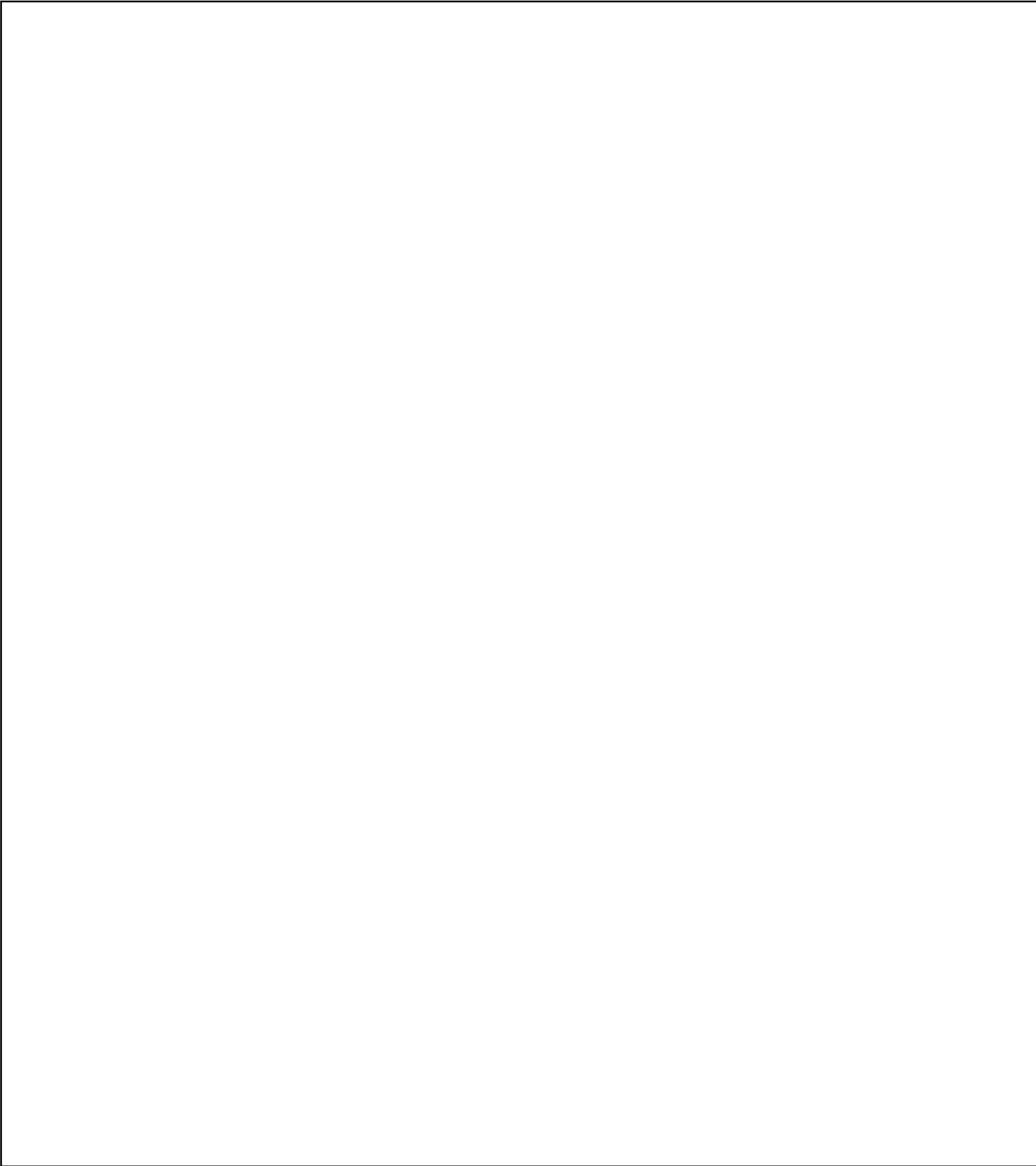
. . . . . H . D R A U . I . . . E . . . . . S

With the addition of the information in the other columns, the plain component is reconstructed as follows:

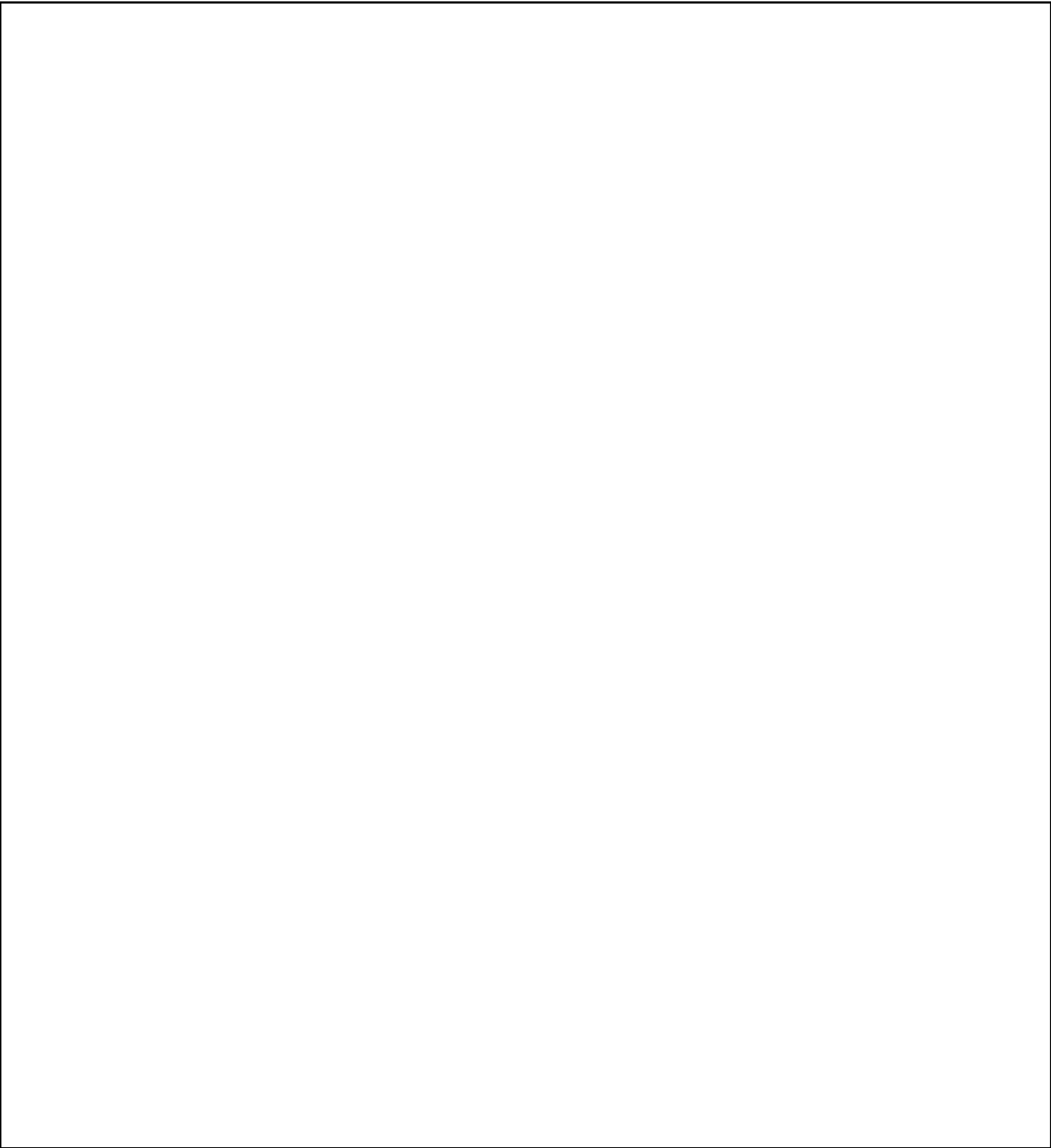
T V . Z X H Y D R A U L I C B E F G . K M N O P . S



(b) (1)  
(b) (3) -18 USC 798  
(b) (3) -50 USC 3024(i)  
(b) (3) -P.L. 86-36

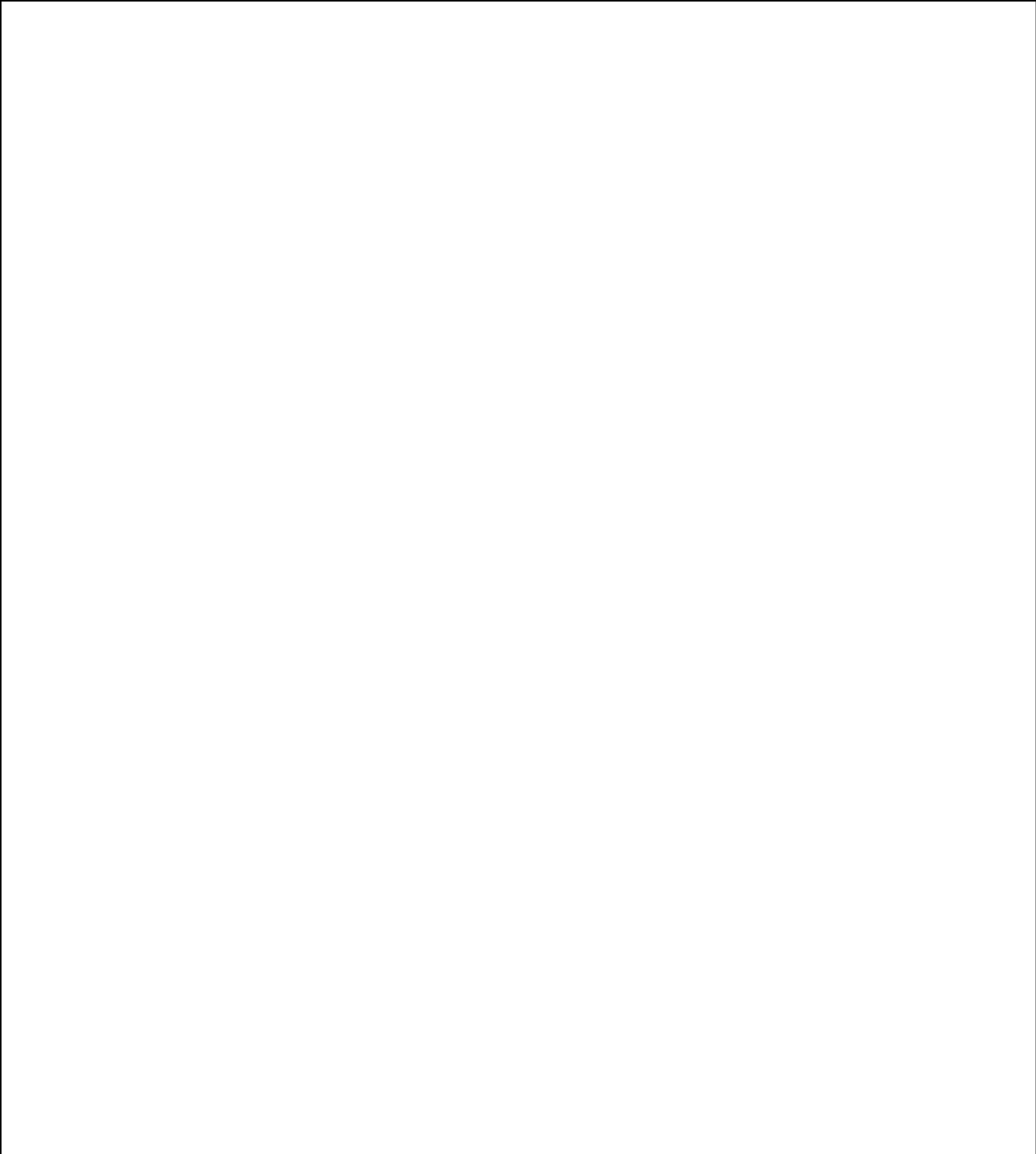


(b) (1)  
(b) (3)-18 USC 798  
(b) (3)-50 USC 3024(i)  
(b) (3)-P.L. 86-36

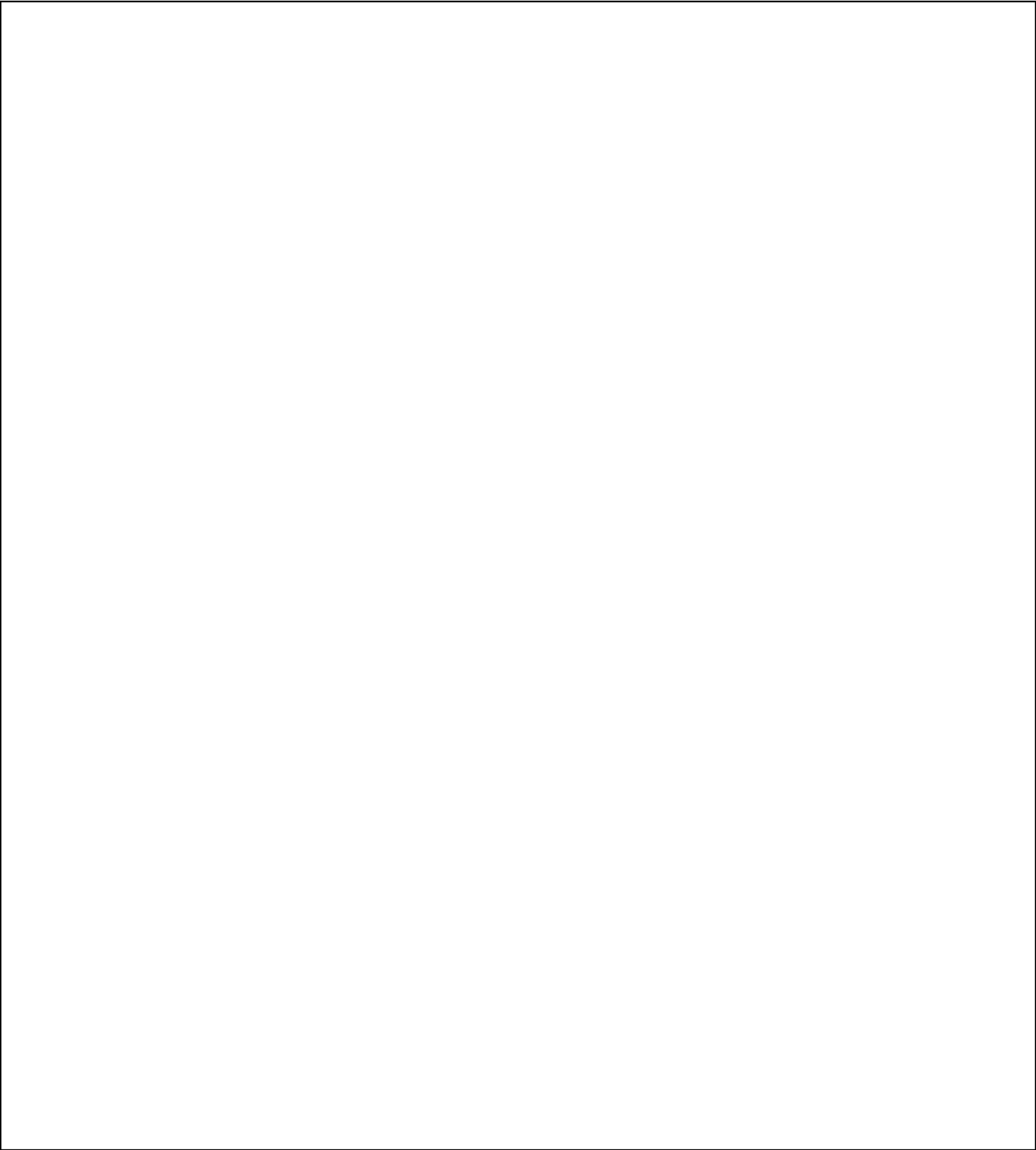


(b) (1)  
(b) (3)-18 USC 798  
(b) (3)-50 USC 3024(i)  
(b) (3)-P.L. 86-36

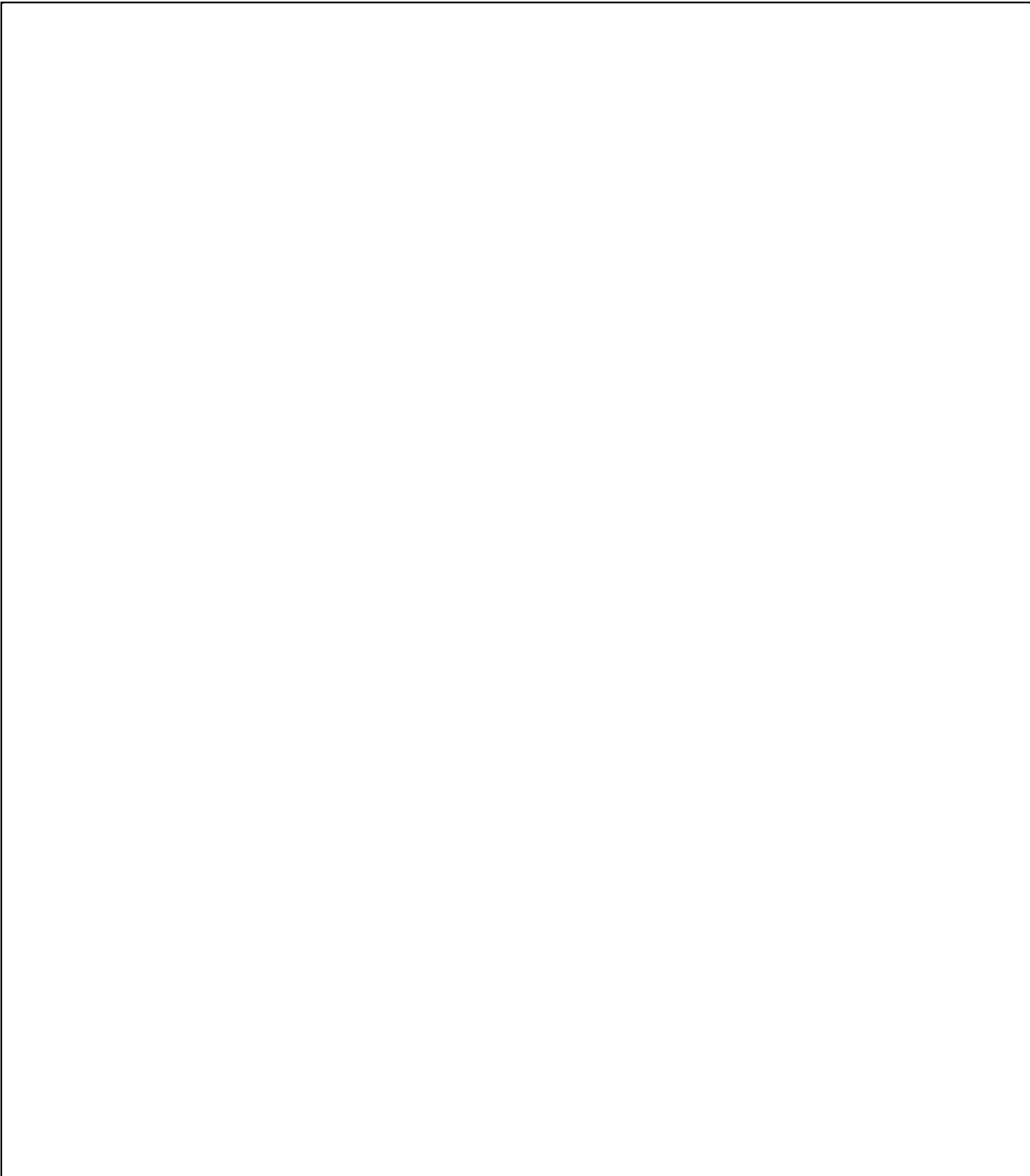




(b) (1)  
(b) (3)-18 USC 798  
(b) (3)-50 USC 3024(i)  
(b) (3)-P.L. 86-36



(b) (1)  
(b) (3)-18 USC 798  
(b) (3)-50 USC 3024 (i)  
(b) (3)-P.L. 86-36



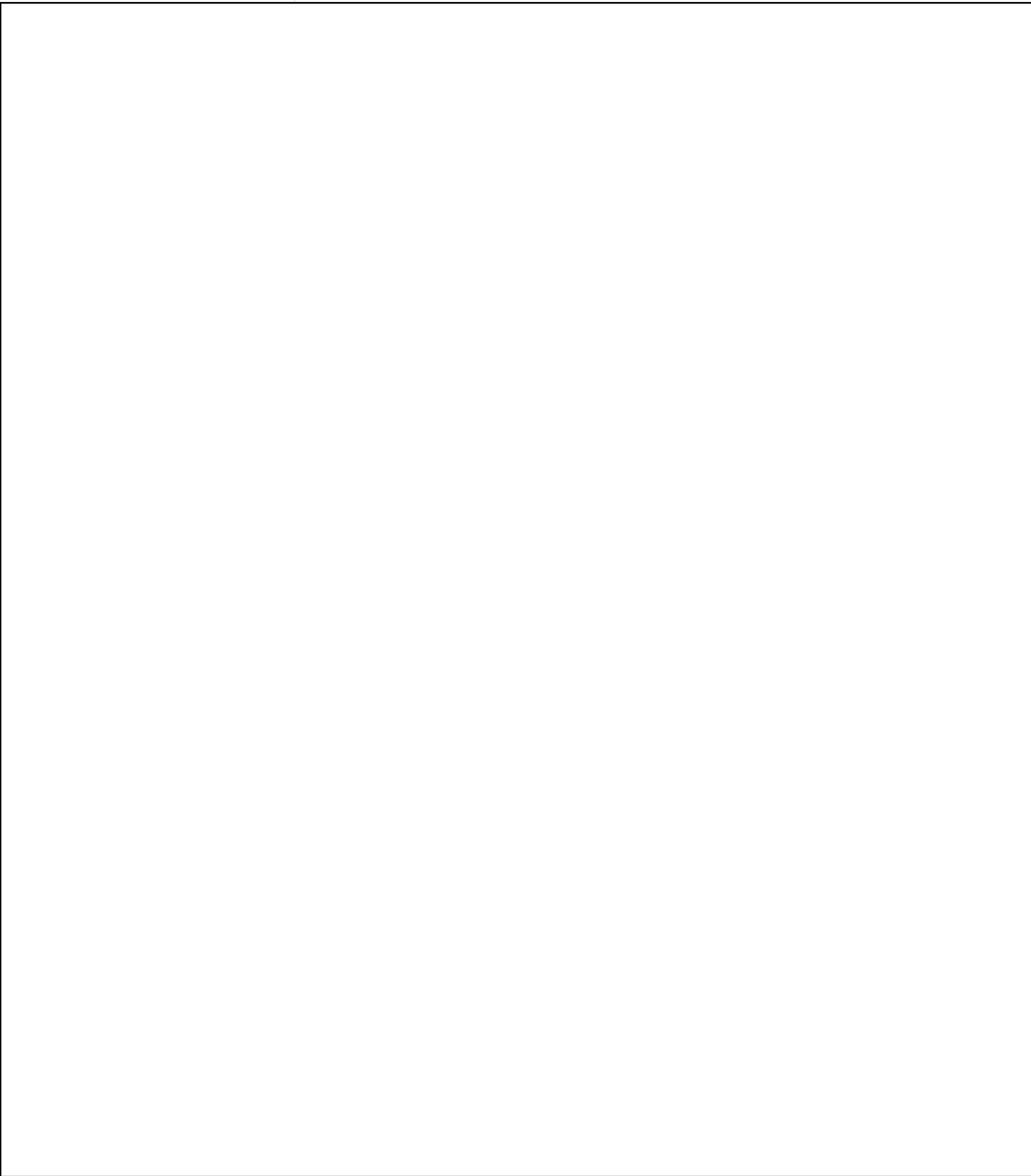
(b) (1)  
(b) (3)-18 USC 798  
(b) (3)-50 USC 3024 (i)  
(b) (3)-P.L. 86-36

207

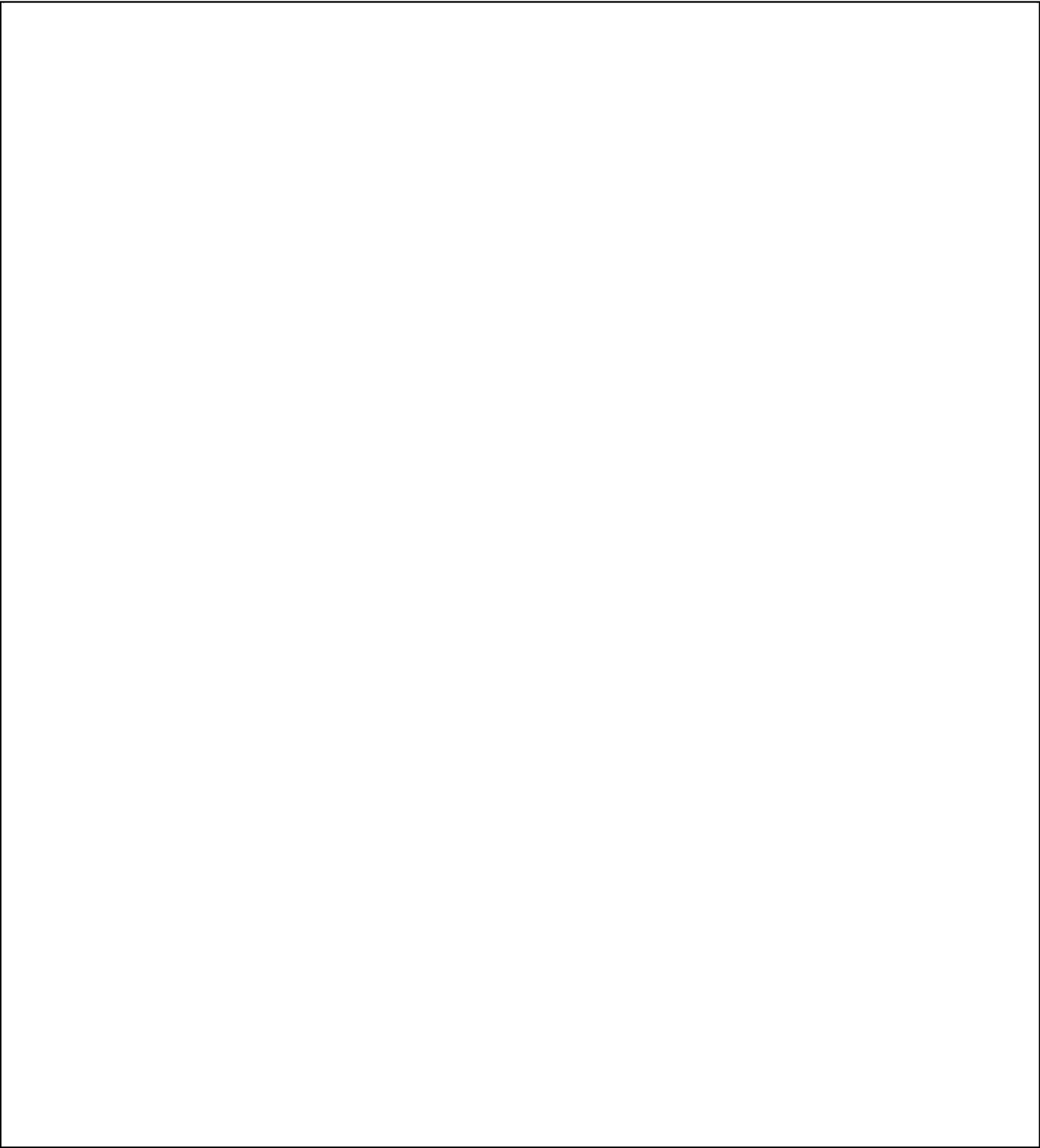
~~SECRET~~

~~SECRET~~

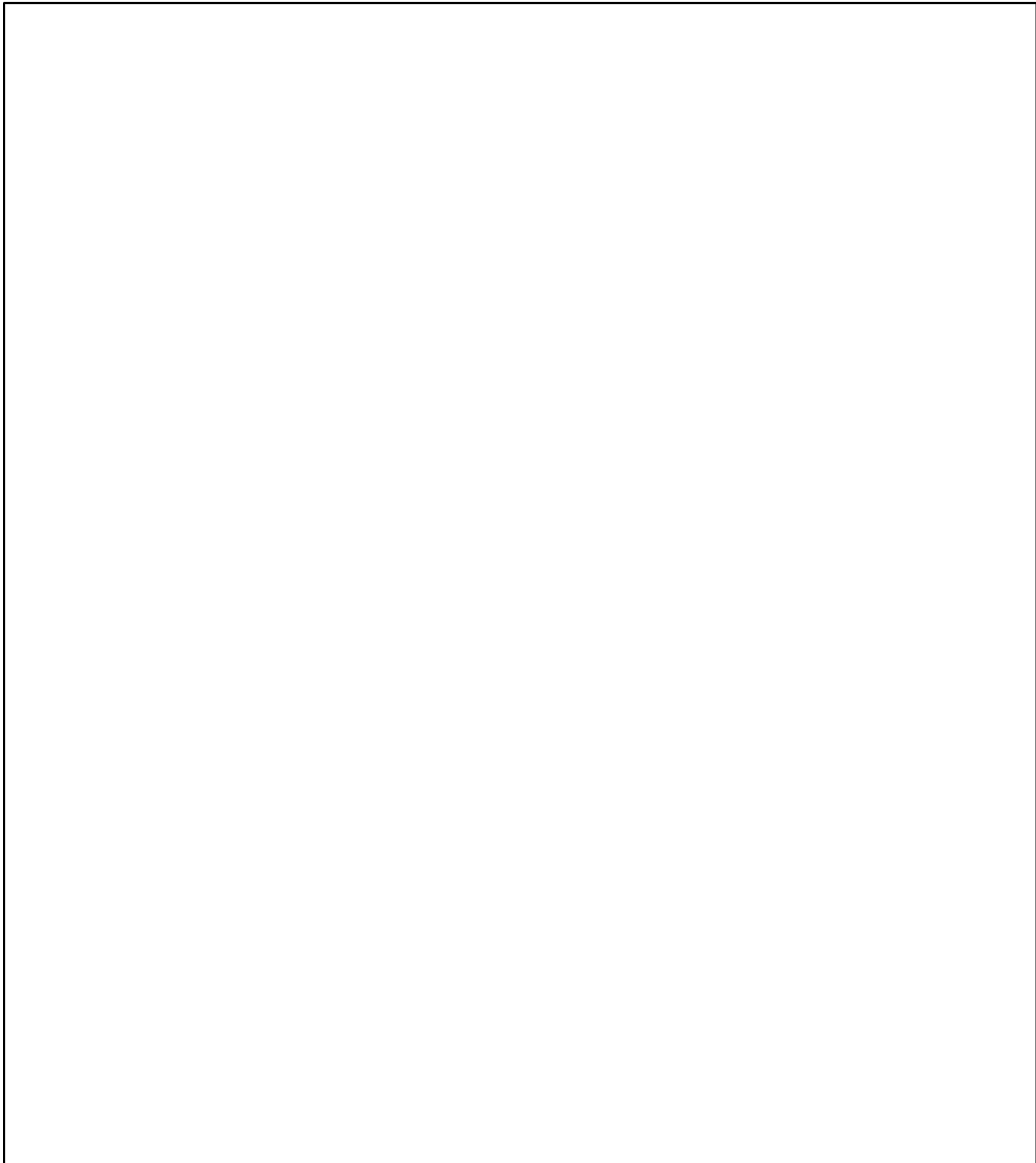
(b) (1)  
(b) (3)-18 USC 798  
(b) (3)-50 USC 3024(i)  
(b) (3)-P.L. 86-36



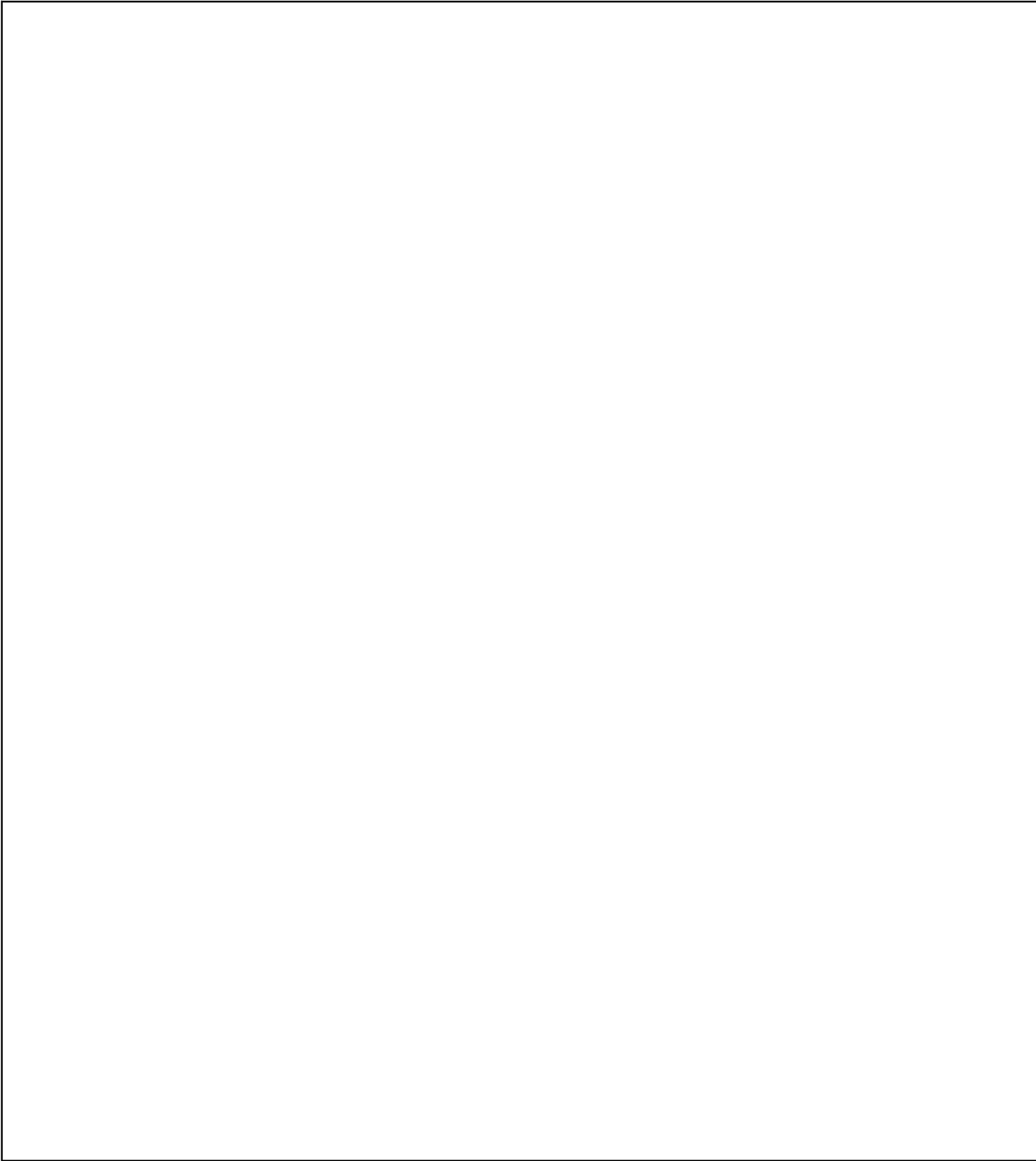
(b) (1)  
(b) (3)-18 USC 798  
(b) (3)-50 USC 3024 (i)  
(b) (3)-P.L. 86-36



(b) (1)  
(b) (3)-18 USC 798  
(b) (3)-50 USC 3024(i)  
(b) (3)-P.L. 86-36

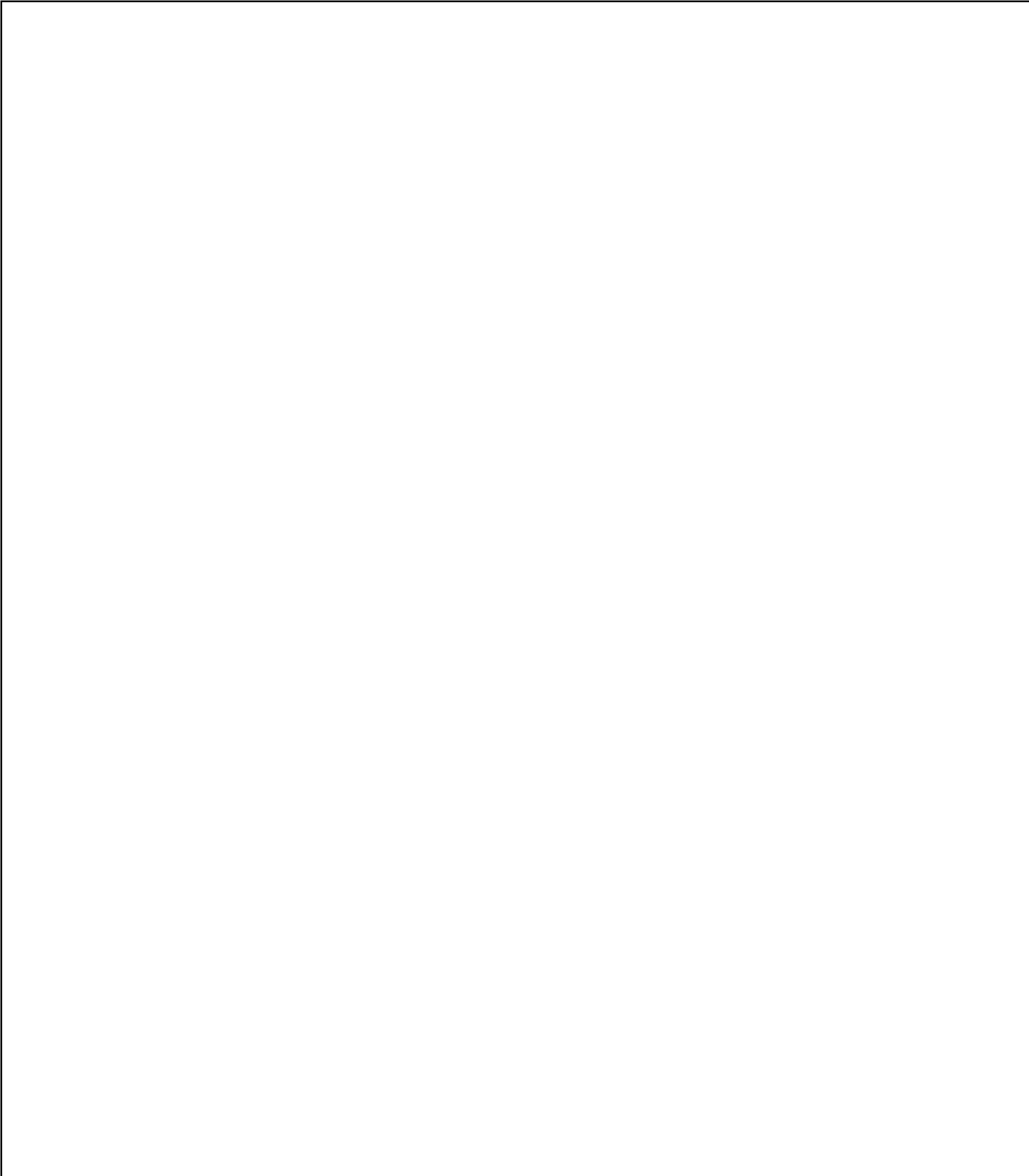


(b) (1)  
(b) (3) -18 USC 798  
(b) (3) -50 USC 3024 (i)  
(b) (3) -P.L. 86-36



(b) (1)  
(b) (3) -18 USC 798  
(b) (3) -50 USC 3024 (i)  
(b) (3) -P.L. 86-36

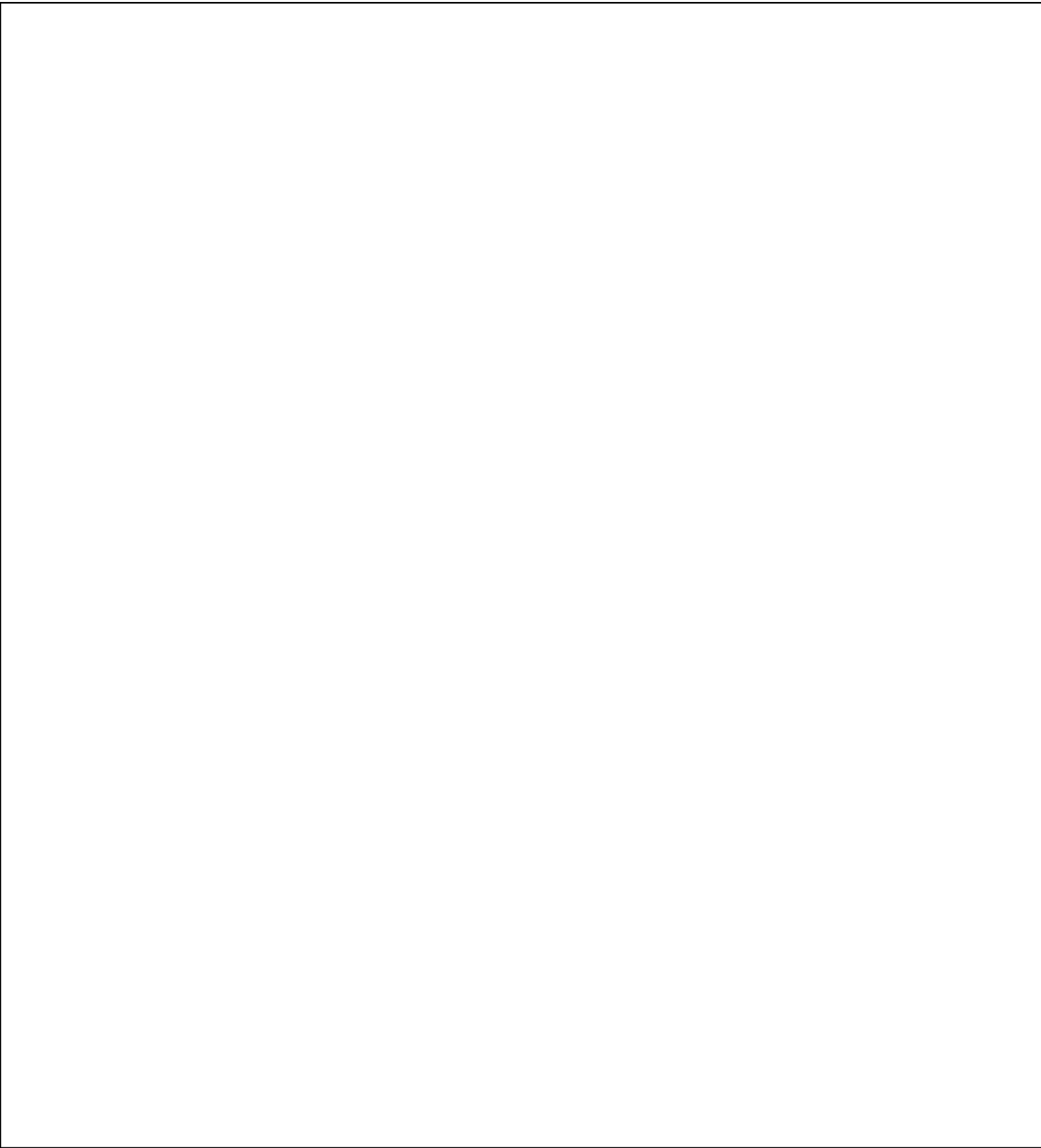




(b) (1)  
(b) (3)-18 USC 798  
(b) (3)-50 USC 3024(i)  
(b) (3)-P.L. 86-36

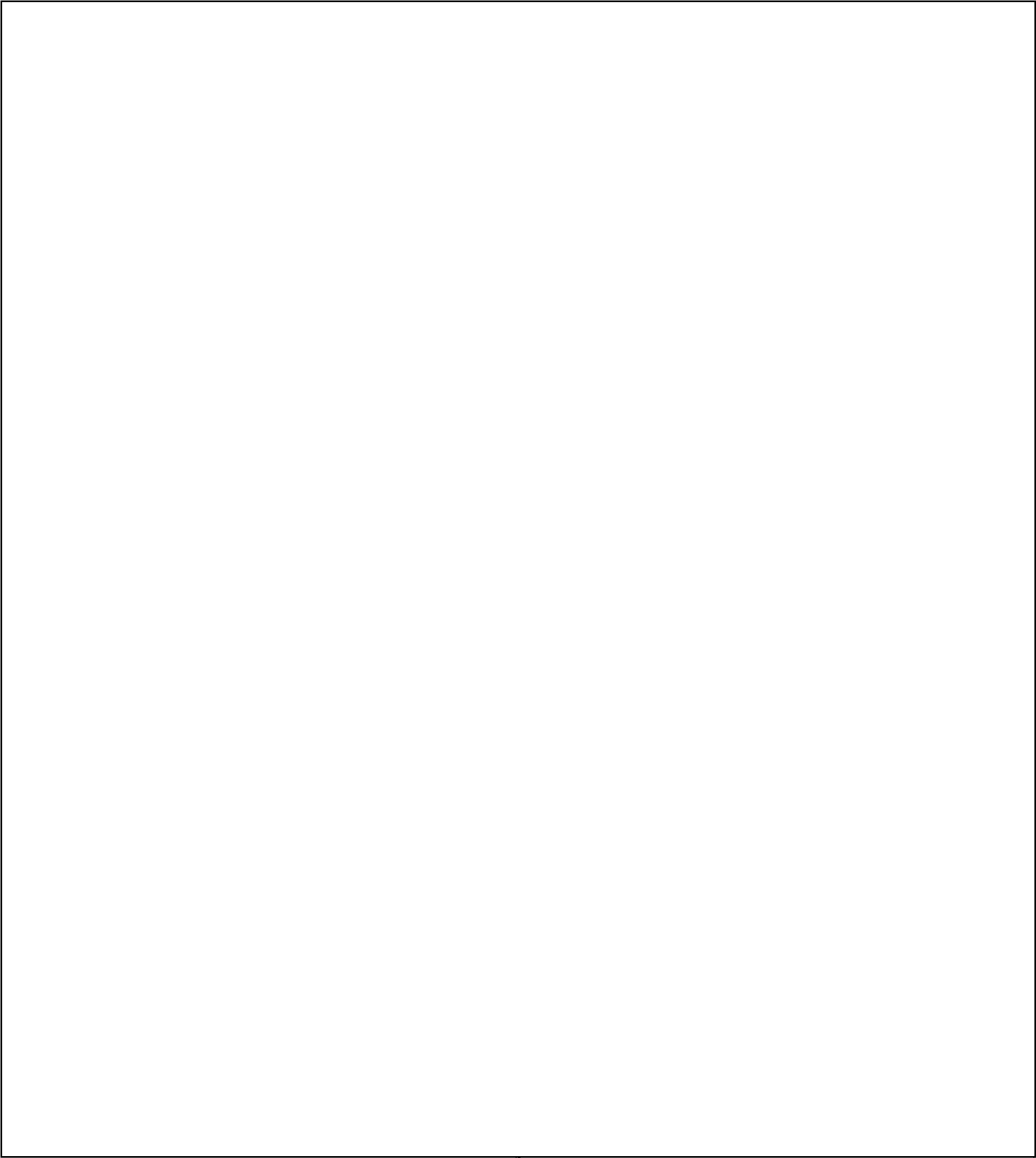


(b) (1)  
(b) (3)-18 USC 798  
(b) (3)-50 USC 3024(i)  
(b) (3)-P.L. 86-36

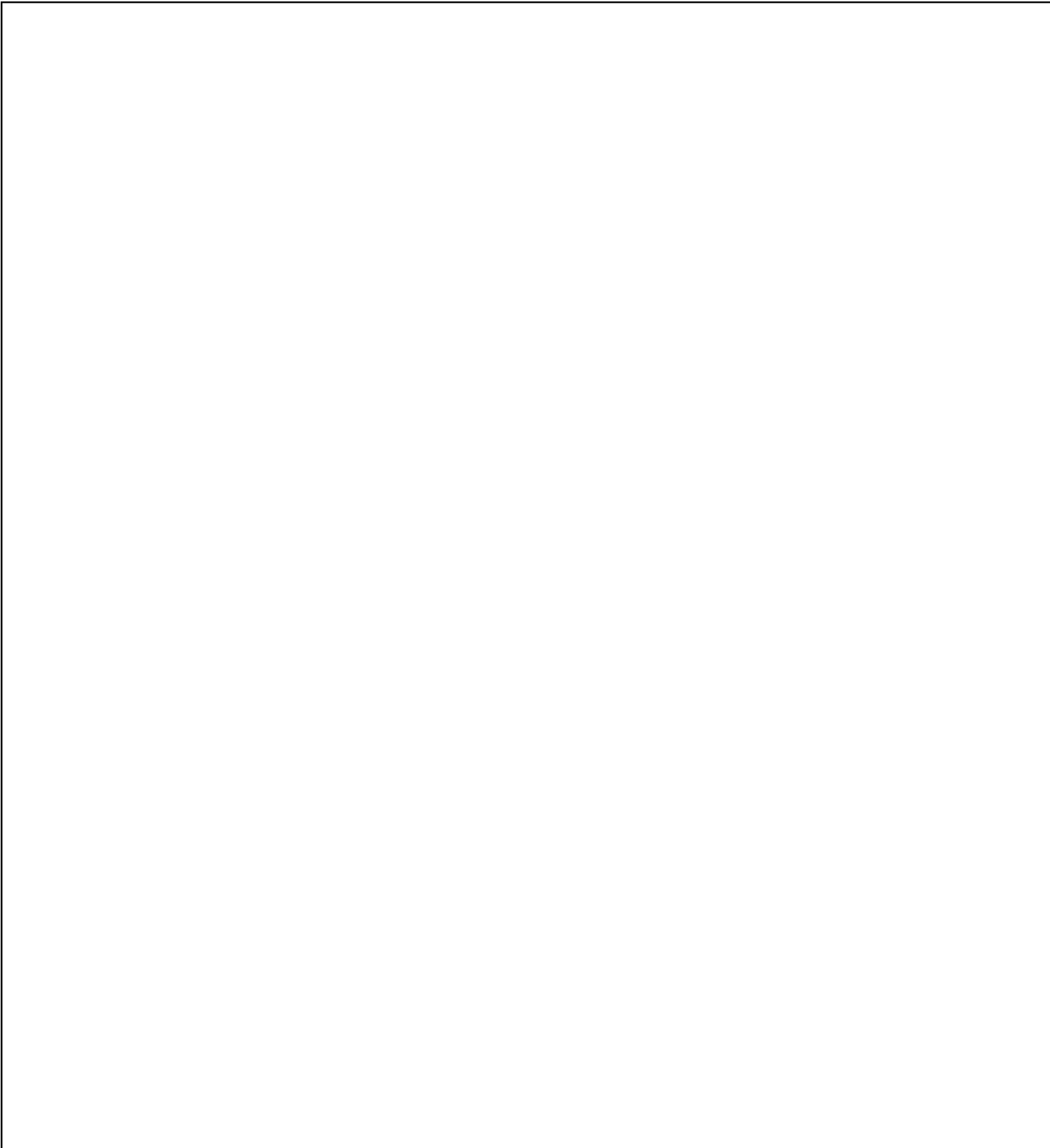


(b) (1)  
(b) (3)-18 USC 798  
(b) (3)-50 USC 3024(i)  
(b) (3)-P.L. 86-36

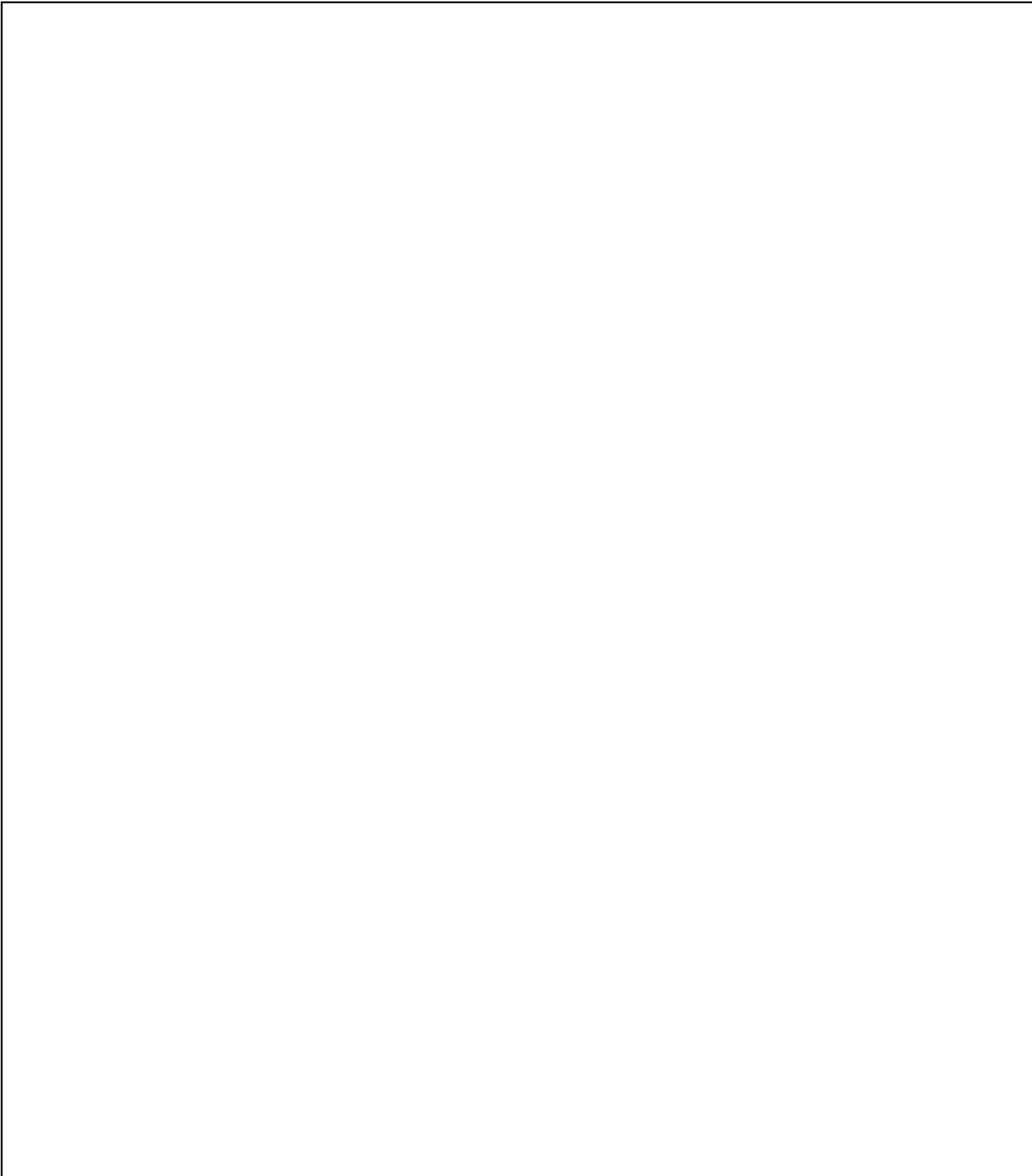
(b) (1)  
(b) (3) -18 USC 798  
(b) (3) -50 USC 3024(i)  
(b) (3) -P.L. 86-36



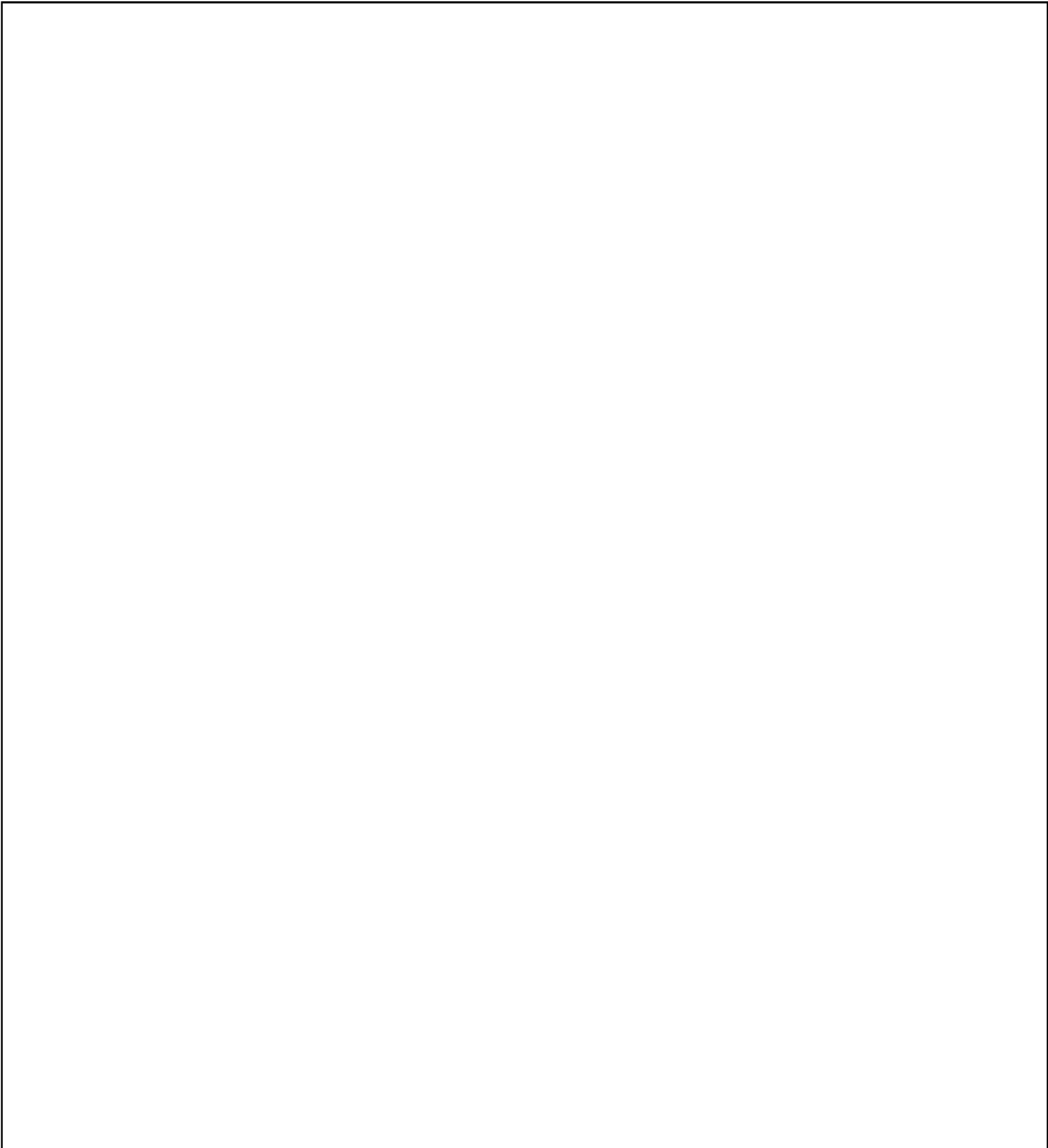
(b) (1)  
(b) (3)-18 USC 798  
(b) (3)-50 USC 3024 (i)  
(b) (3)-P.L. 86-36



(b) (1)  
(b) (3) -18 USC 798  
(b) (3) -50 USC 3024 (i)  
(b) (3) -P.L. 86-36

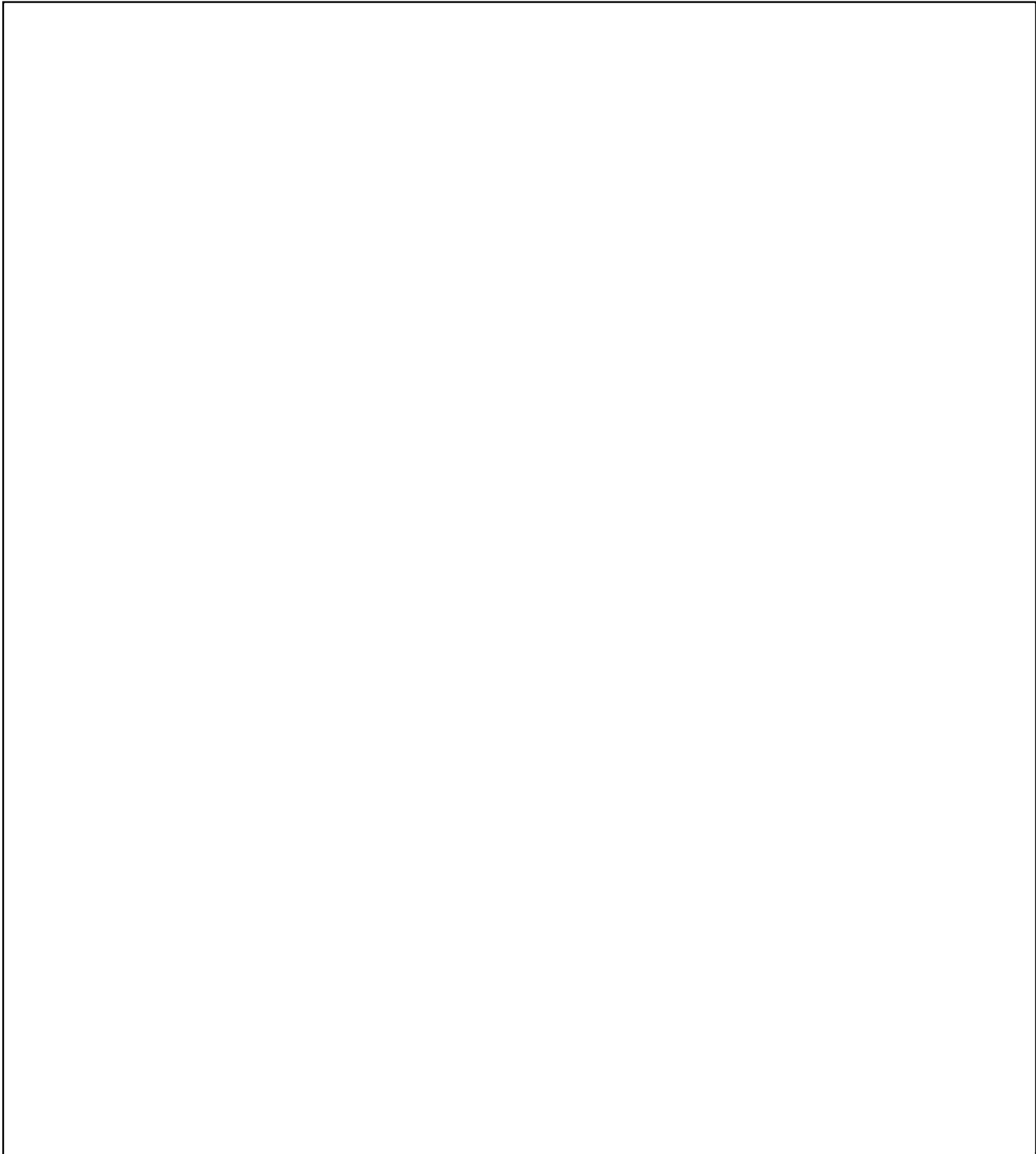


(b) (1)  
(b) (3)-18 USC 798  
(b) (3)-50 USC 3024(i)  
(b) (3)-P.L. 86-36

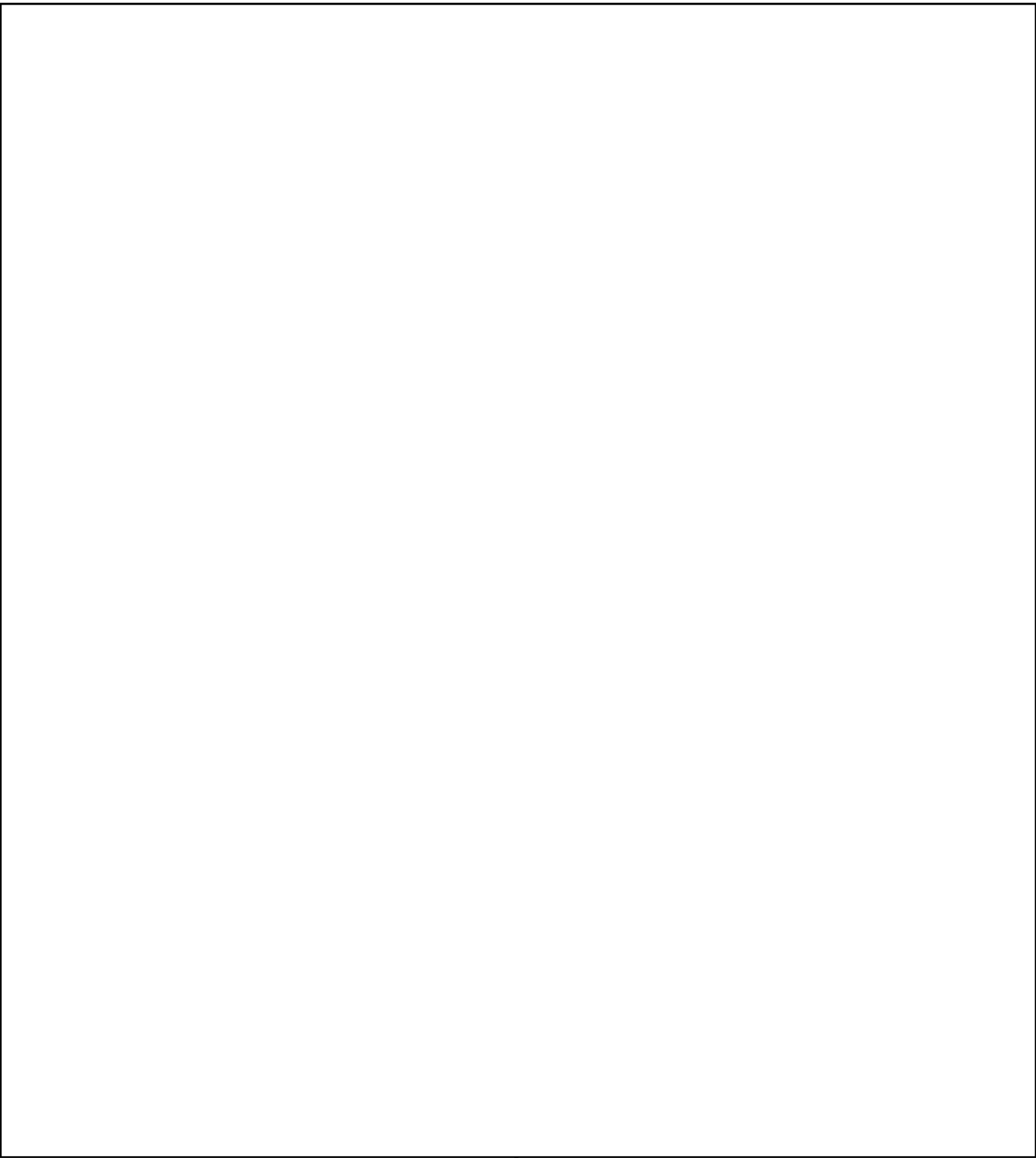


(b) (1)  
(b) (3)-18 USC 798  
(b) (3)-50 USC 3024(i)  
(b) (3)-P.L. 86-36





(b) (1)  
(b) (3)-18 USC 798  
(b) (3)-50 USC 3024(i)  
(b) (3)-P.L. 86-36



(b) (1)  
(b) (3) -18 USC 798  
(b) (3) -50 USC 3024 (i)  
(b) (3) -P.L. 86-36

55. Concluding remarks.—a. Some words on the diagnosis of systems employing the Wheatstone device or the Kryha machine might be apropos. In both cases, the expected monographic I.C. is 1.00 since every key letter has an equal chance of occurring. As for the expected digraphic I.C., in a Wheatstone system there are only 26 ways in which a plaintext digraph may be enciphered; therefore since the digraphic I.C. of English plain text is 4.66, the expected digraphic I.C. can be approximated by 1.00 plus 1/26 of the 3.66 bulge, or 1.14. The expected digraphic I.C. in a Kryha system (1.034 for the original machine, [redacted] is considerably less than that of the Wheatstone since there are in effect several variant possibilities for the encryption of a digraph after the first letter is determined—6 ways for the original Kryha, and 3 ways for the improved model.¹⁰ Cryptograms enciphered by the Wheatstone device would be replete with isomorphs at no consistent factorable interval; causal polygraphic repetitions within or between messages (at no consistent factorable intervals) would occur with the same frequency as those of a ciphertext autokey system with a single-letter introductory key (1/26 of the plaintext rate), since there is only 1 chance in 26 that a plaintext word, for example, would be enciphered both times at the same setting of the components; and since the Wheatstone produces aperiodic encipherment, no depth would be possible and therefore the kappa test would be inapplicable. Cryptograms enciphered by the Kryha machine could manifest isomorphs only at intervals of multiples of 17 [redacted]

[redacted] causal polygraphic repetitions within a message would be rare, at intervals of 442 [redacted]

b. The cryptographic principle of the Wheatstone was first employed in the device invented by Decius Wadsworth, 50 years before Wheatstone, as mentioned in an earlier footnote. (The Wadsworth device is in the possession of the Hamden Historical Society of Hamden, Connecticut.) A number of modifications of this principle have appeared, among which may be mentioned the devices invented by J. S. Beeman (1905) and William F. Friedman (1938). In the Beeman device (the first patented device embodying the Wheatstone principle) two disks, each composed of several members for varying the sequences of the two components, are mounted side-by-side within a frame and are relatively rotatable through gears containing 36 and 39 teeth, respectively. In the Friedman device, two gears are meshed side-by-side, the letters of the plain and cipher components being inscribed on the gears themselves.

c. The original Kryha machine was manufactured in three versions: the "standard" model, 10" x 8" x 4 1/2"; the "Liliput" (sic) model, a miniature version of the standard machine resembling a large pocket watch and intercommunicable with the standard model; and an electric model, in which a cipher unit is interposed between two electric typewriters. The "new" standard model, sold commercially since 1934, incorporated the selector wheel with the 52 adjustable screws. Subsequent Kryha patents covered three other versions: one in which the plain and cipher components were carried on two endless metal tapes; one in which the selector wheel was composed of various interchangeable sectors, each having a different number of gear teeth or irregularly spaced stop holes so that the user could assemble his selector wheel according to different specific keys; and one in which there were two selector wheels, one controlling the irregular displacement of the plain component and the other controlling the displacement of the cipher component.

d. The principle of the Kryha machine is found, with slight variations, in several other devices, among which may be mentioned the ones invented by the following: Peter G. G. Beyer (1931) of Copenhagen, whose device was sold commercially by The Danish Cipher Machine Co., Ltd.; Beue Tann (1934) of Chungking and Washington, D.C., whose device was called the "Comet" machine; Ernesto Cristofani (1935) of Rome, Italy; and Jean Francois Joseph Dupouy (1935) of France. Some of these were only slightly larger than a pocket watch, similar to the "Liliput" model sold by Kryha; others,

¹⁰ The way these digraphic I.C.'s are calculated may be of interest. For the original Kryha machine, the 17 key skips have a distribution of four 5's, six 6's, four 7's, and one each of 8, 9, and 10. The  $\gamma$  I.C. of this distribution is  $\frac{6(6^2 + 2(4^2) + 3(1^2))}{17^2} = 1.47$ ; dividing the bulge .14 for the general case (as in the Wheatstone) by 6/1.47 gives .034, so the digraphic I.C. is approximately 1.034. For the improved Kryha machine, the 52 key skips have a distribution of 31 3's, 19 4's, and two 5's. The  $\gamma$  I.C. is  $\frac{3(31^2 + 19^2 + 2^2)}{52^2} = 1.47$  again; dividing the bulge .14 by 3/1.47 gives .069, so the digraphic I.C. here is approximately 1.069.

(b) (1)  
 (b) (3) -18 USC 798  
 (b) (3) -50 USC 3024(i)  
 (b) (3) -P.L. 86-36

like the Kryha electric model, connected two solenoid-operated typewriters which printed the plaintext and ciphertext copies simultaneously. Some were nonprinting, while others printed on a tape or on a sheet of paper. In the Beyer device (one was a pocket model and another a larger, electromechanical machine) the plain and cipher components are irregularly displaced relative to one another according to a key sequence generated by two selector wheels, the one for the plain component having 58 teeth and 9 fixed stop pins, the one for the cipher component having 62 teeth and 10 fixed stop pins. Both components are displaced twice between encipherments, before and after the depression of an operating plunger, the amount of displacement being proportionate to the distance between two adjacent pins on a selector wheel. The "Comet" machine incorporated two mixed cipher sequences of 13 letters each which are slid relative to one another and against a mixed plain component in accordance with a key generated by a pair of 19- and 23-sector cam wheels. The period is either 13 times or 26 times the least common multiple of the product of the number of sectors in the two cams. The Cristofani Cryptograph incorporated a set of 10 small variable-pin wheels of different sizes (the patent drawing shows two each of sizes 8, 9, 10, 11, and 12) arranged in a circle around the cipher disk. All the pin wheels advance one step between encipherments, and the cipher disk is displaced from zero to five positions at each operation. The Dupouy tape-printing device incorporated a keying disk of 95 segments, any one of which could be removed to form an irregular pattern of stopping points for the rotating cipher component.

e. One further point might be brought out in connection with the analysis of the Kryha machine: the descriptive brochure accompanying it suggested the use of plaintext interruptors as an added security measure.¹¹ With the machine were furnished two sets of 26 black-on-white metal tab inserts for making up the plain and cipher components, and another set of 26 red-on-white tabs from which a letter (or letters) could be selected for the plaintext interruption. After enciphering the designated letter, an extra displacement would be imparted to the cipher component, thus interrupting the cycle. Causal isomorphs could still be produced, however, and through them the cipher component could be reconstructed.

(1) Let us now suppose that we have the following message at hand, known to have been enciphered on the original Kryha machine and suspected of beginning with the opening stereotype "REFERENCE YOUR MESSAGE NUMBER . . .":

S H V T T J T N H D Y I D T I P U J T Y X Q G G W V R F G R  
 C L I F P Z N N C W T S C P O S D H K A F S M B G P X T L V  
 J G U O D G B O H D O O C J W

Let it further be assumed that we have recovered the cipher component through isomorphs and found it to be the QUESTIONABLY keyword-mixed sequence:

Q U E S T I O N A B L Y C D F G H J K M P R V W X Z

Since two long isomorphs within a single message were at an interval not a multiple of 17, this indicates the possibility of the use of a plaintext interruptor procedure. Now if there is a single plaintext interruptor and that letter is T_p, for example (or for that matter any other letter not in the assumed crib), the matched plain and cipher would be written out as shown in Fig. 110a, below. If the interruptor letter is E_p, the write-out would be as shown in Fig. 110b.

REF E R E N C E Y O U R M E S S  
 S H V T T J T N H D Y I D T I P U  
 A G E N U M B E R  
 J T Y X Q G G W V

FIGURE 110a

R E - F E - R E - N C E - Y O U R  
 S H V T T J T N H D Y I D  
 M E - S S A G E - N U M B E - R  
 T I P U J T Y X Q G G W V

FIGURE 110b

¹¹ The mention of an added security measure is strange indeed, since the machine was already touted as having an incredibly high (i.e., infinite) security. Dr. Georg Hamel, Professor of Mathematics at the Technische Hochschule in Berlin-Charlottenburg, wrote a paper entitled "The Kryha Coding Machines: A Mathematical Opinion," in which he gave the number of ways in which a message could be enciphered as  $2.29 \times 10^{82}$ ; "Thus, if every person on earth (say 2,000,000,000 people) bought the machine then each of them could have  $1.14 \times 10^{73}$  independent keys without two persons ever having the same system." By comparison, the number of atoms in the universe,  $3 \times 10^{74}$  (personally vouched for by Sir Arthur Eddington), is only 26 times as large.

(2) In Fig. 110a we note the cipher equivalents of E_p in REFERENCE:

1	2	3	4	5	6	7	8	9
R	E	F	E	R	E	N	C	E
S	H	V	T	T	J	T	N	H

The interval on the known cipher component between H_c (at position 2) and T_c (at pos. 4) is 14, certainly possible when two skips are involved as may be seen by referring to the skip pattern of the original Kryha machine (at skip nos. 7, 8, or 16):

No:	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	1
Skip:	7	6	7	5	6	7	6	8	6	10	5	6	5	7	6	5	9	

(It may be seen that for two skips, the minimum interval is 11, the maximum 16; for three skips, the minimum is 16, the maximum 24.) The interval between T_c (pos. 4) and J_c (pos. 6) is 13, again quite possible for two skips; but the interval between J_c (pos. 6) and H_c (pos. 9) is 25, an impossible figure when only three skips are involved. Thus not only is T_p rejected as an interruptor, but it means that the interruptor letter must be one of those in the word REFERENCE. We now note in Fig. 110b the cipher equivalents of E_p in REFERENCE, on the trial that E_p is the interruptor letter.

1	2	3	4	5	6	7	8	9	10	11	12
R	E	-	F	E	-	R	E	-	N	C	E
S	H		V	T		T	J		T	N	H

The interval between H_c (pos. 2) and T_c (pos. 5) is 14, and there is no way to arrive at this number with three skips; in the next pair of letters, T_c (pos. 5) and J_c (pos. 8) are at an interval of 13, which likewise is impossible to make with three skips; thus E_p is also eliminated as a possible plaintext interruptor. By continuing this process, all letters are eliminated as interruptors except C_p and N_p.

(3) The write-outs of the matched plain and cipher for the assumptions of C_p and N_p are shown in Figs. 110c and d, below

				5						10				15			17
R	E	F	E	R	E	N	C	-	E	Y	O	U	R	M	E	S	
S	H	V	T	T	J	T	N		H	D	Y	I	D	T	I	P	
S	A	G	E	N	U	M	B	E	R								
U	J	T	Y	X	Q	G	G	W	V								

FIGURE 110c

										5				10			15	17
R	E	F	E	R	E	N	-	C	E	Y	O	U	R	M	E	S		
S	H	V	T	T	J	T		N	H	D	Y	I	D	T	I	P		
S	A	G	E	N	-	U	M	B	E	R								
U	J	T	Y	X	Q	G	G	W	V									

FIGURE 110d

In Fig. 110c the interval between Y_c (col. 4) and W_c (col. 9) is 12 on the cipher component with five skips involved; but since the 17 sets of five consecutive skips on the Kryha selector wheel total to 3, 5, 6, 7, 8, 9, and 11 (mod 26), C_p is ruled out as the interruptor. In Fig. 110d, the interval between H_c and W_c in col. 10 should be +7 on the cipher component which it is, thus proving that N_p is the interruptor letter. Now the cipher equivalents of SS_p at cols. 17 and 1, P_c and U_c, are at an interval of 7 on the component; since there are only four 7's in the keying sequence (at positions 1, 3, 6, and 14 of the selector wheel) the correct key must be one of the following, where position 1 of the keying sequence has been ringed:

- (1) 6 7 5 6 7 6 8 6 10 5 6 5 7 6 5 9 ⑦
  - (3) 5 6 7 6 8 6 10 5 6 5 7 6 5 9 ⑦ 6 7
  - (6) 6 8 6 10 5 6 5 7 6 5 9 ⑦ 6 7 5 6 7
  - (14) 6 5 9 ⑦ 6 7 5 6 7 6 8 6 10 5 6 5 7
- |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| R | E | F | E | R | E | N | - | C | E | Y | O | U | R | M | E | S |
| S | H | V | T | T | J | T |   | N | H | D | Y | I | D | T | I | P |
| S | A | G | E | N | - | U | M | B | E | R |   |   |   |   |   |   |
| U | J | T | Y | X | Q | G | G | W | V |   |   |   |   |   |   |   |



(b) (1)  
(b) (3) -18 USC 798  
(b) (3) -50 USC 3024(i)  
(b) (3) -P.L. 86-36

CHAPTER IX

FUNDAMENTALS OF KEY ANALYSIS

	Paragraph
Convenient sources of key.....	56
Manual key generation methods.....	57
Mechanical and electronic key generators.....	58
General analytic approaches.....	59
Analysis of key in a double transposition cipher.....	60
<div style="border: 1px solid black; width: 300px; height: 15px; display: inline-block;"></div> .....	61
Concluding remarks.....	62

**56. Convenient sources of key.**—*a.* In literal and digital cryptosystems of the additive family (i.e., true additive, subtractive, and minuend systems) using long keys the key is sometimes derived from a source easily available in the public domain, either in order to lessen the problems of key production and distribution or to avoid the possession of possibly incriminating materials when used by secret agents. Digital key from open sources has been taken from telephone directories (in this case an indicator might show the starting page, or the starting name), from statistical tables such as those found in ordinary almanacs, from tables of mathematical functions,¹ or from published tables of random numbers; these might be used with an indicator to show the starting point for the key. Literal key from open sources has often been taken from the pages of a novel or other book, again with an indicator procedure to show the starting point for the key to be used. The enciphering components in these cases have usually been direct or reversed standard alphabets.) Other convenient sources of digital or literal key that have been used are old plaintext messages, and old cipher or code messages.

*b.* The plain text used as key might be subject to variation: for instance, only every other word might be taken, or one- and two-letter words might be ignored, or only the first two or three letters of each word might be used; or, in the case of key from a book, only, say, the first five letters from each line might be used, or only the first five *columns* of letters on each page (as measured from the left-hand margin). In a specialized case of running plain text used as key only the 20 consonants were used, dropping the six vowels. When mathematical or other tables are used as key, the normal direction of reading the groups might be changed; or every 5th group, say, might be deleted. In the case of old cipher or code messages, every other group might be taken as key, or the columns of groups of a standard message format (e.g., ten groups per line) might be taken off vertically from right to left.

*c.* The scrambled sequence of code groups in the encode section of a two-part code book has been used as key, with an indicator to show the starting point in the sequence. The code groups have been read in the normal fashion down the column, or sometimes up the column; and sometimes the individual code groups have been reversed.

*d.* Other keys have either been generated by some deterministic method, manual or machine, or have been produced in a random fashion in bulk and put together in key books of convenient size for the users. Some of these methods will now be discussed.

**57. Manual key generation methods.**—*a.* There are many schemes for the generation by hand of long literal keys. For instance, in a basic 26-letter mixed sequence the letters in the sequence up to A might be taken, followed by the letters up to B, C . . . Z as in the following example:

H Y D R A / H Y D R A U L I C B / H Y D R A U L I C / H Y D / . . . .

This yields a key of length  $\frac{26(26+1)}{2} = 351$ .

¹ If these are 4-digit tables, a simple expedient that has been encountered for producing 5-digit key is by repeating the last digit.

b. Another scheme involves the 26 slides of a basic sequence,

A U L I C...Z H Y D R/B E F G J...A U L I C/C B E F G...R A U L I/D R A...

yielding a key of length 676. A simple variation of this idea is reversing the sequence of letters in the B, D, F . . . segments:

A U L I C...Z H Y D R/B C I L U...K J G F E/C B E F G...R A U L I/D Y H . . .

c. In another method for producing a 676-element key,

H Y D R A U L I C B E F G J K M N O P Q S T V W X Z  
I Z E S B V M J D C F G H K L N O P Q R T U W X Y A  
J A F T C W N K E D G H I L M O P Q R S U V X Y Z B  
K B G U D X O L F E H I J M N P Q R S T V W Y Z A C . . . ,

a basic 26-letter mixed sequence is succeeded by 25 isomorphic changes, either on the normal sequence as in the example above, or on the same mixed sequence (which amounts to nothing more than a simple slide),

H Y D R A U L I C B E F G J K M N O P Q S T V W X Z  
Y D R A U L I C B E F G J K M N O P Q S T V W X Z H  
D R A U L I C B E F G J K M N O P Q S T V W X Z H Y  
R A U L I C B E F G J K M N O P Q S T V W X Z H Y D . . . ,

or on an unrelated sequence,

H Y D R A U L I C B E F G J K M N O P Q S T V W X Z  
J C F V B E Y O D L S G H K M P A N R U T I W X Z Q  
K D G W L S C N F Y T H J M P R B A V E I O X Z Q U  
M F H X Y T D A G C I J M P R V L F W S O N Z Q U E . . . .

d. In the following method,

H Y D R U L I C B . . . X Z / H Y D R A U L I C E F . . . X Z / H Y D R A U L  
I B E F . . . X Z / H Y R A U L I C . . . X Z / H Y D R A U L I C B F . . . ,

a basic 26-letter sequence is transformed into 26 sequences of 25 letters each, by first dropping out A, then B, C . . . Z, yielding a key of  $26 \times 25 = 650$  letters. Here again a possible variation is the reversal of the sequence of letters in the 2d, 4th, 6th . . . segments.

e. Another method that has been proposed is writing the normal alphabetic sequence (or an agreed-upon mixed sequence) a fixed number of times under a transposition key, and taking off the columns of letters according to the numerical key. An even better idea is a double transposition, as in the following example:

B E R N E S W I T Z E R L A N D													M A N C H E S T E R E N G L A N D																			
2 4 11 9 5 13 15 7 14 16 6 12 8 1 10 3													11 1 12 3 9 5 16 17 6 15 7 13 8 10 2 14 4																			
A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	N	D	T	J	Z	P	F	V	A	Q	G	W	M	C	S	I	Y
Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	P	F	V	L	B	R	H	X	B	R	H	X	N	D	T	J	Z
G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	E	U	K	A	Q	G	W	M	K	A	Q	G	W	M	C	S	H
W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	X	N	D	T	J	Z	P	M	C	S	I	Y	O	E	U	D	T
M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	J	Z	P	F	V	L	O	E	U	K	A	Q	G	W	C	S	I
C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	Y	O	E	U	K	L	B	R	H	X	N	D	T	F	V	L	B
S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	R	H	X	N	I	Y	O	E	U	K	A	Q	G	W	M	C	S
I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	I	Y	O	J	Z	P	F	V	L	B	R						
Y	Z																															

T1

T2



The final key (D F U N Z . . .) is much more thoroughly disarranged than that of the first transposition alone (N D T J Z . . .) which consists of slides of two 13-letter sequences owing to the even length of the transposition key.

f. Digital keys can be generated in even more simple ways than literal keys. The simplest example of self-generated key that has been encountered is a stream composed of an ascending sequence of numbers as in the two following examples:

1011 1213 1415 1617 1819 2021 2223 2425 2627 2829 . . .  
2502 5125 2253 2542 5525 6257 2582 5926 0261 2622 . . .

Another procedure employed the file time, or the file time plus a sum check, to yield four-digit and five-digit numbers which were used in a fashion similar to the examples above.

g. When digital key is derived from plain text, a particularly popular method involves the use of the following diagram for the conversion:

1	2	3	4	5	6	7	8	9	0
A	B	C	D	E	F	G	H	I	J
K	L	M	N	O	P	Q	R	S	T
U	V	W	X	Y	Z				

Other schemes frequently encountered entail the use of a monome-dinome rectangle, or a bipartite matrix, such as in the following examples:

	9	4	8	1	2	7	6	5	0	3
-	R	E	P	U	B	L	I	C		
0	A	D	F	G	H	J	K	M	N	O
3	Q	S	T	V	W	X	Y	Z		

	6	7	8	9	0
1	R	E	P	U	B
2	L	I	C	A	D
3	F	G	H	K	M
4	N	O	Q	S	T
5	V	W	X	Y	Z

h. In another scheme for converting literal text from a book into digits, use is made of the following widely known memory training device:

1	2	3	4	5	6	7	8	9	0
T	N	M	R	L	Ŝ	K	F	P	S
D					Ĉ	Ĉ	V	B	Ĉ
TH					Ĝ	CK			Z
TH					Ĵ	G			
						Q			
						NG			

(W, H, and vowels have no value)

The conversion of plain language into digits is by *sounds*, and not by the alphabetical characters, as may be seen in the example below:²

THE CHARGE OF THE LIGHT BRIGADE WAS  
1 6 46 8 1 5 194 7 1 0  
WRITTEN BY ALFRED LORD TENNYSON  
4 1 29 584 15 411 2 0 2

² Note that the Ĉ and Ĝ sounds in the word CHARGE have a value of 6, while the G in LIGHT is not counted since it is not pronounced, and the G in BRIGADE has the value of 7.

i. The methods described in subpars. a-e, above, may also be adapted for the production of digital key. As for isomorphic key, using a basic 25-digit key as an example, nine subsequent rows of 25 digits each may be produced by adding a 1 or some other constant to each element of a row,

```

2 1 5 4 1 8 3 6 7 6 8 5 2 0 9 4 5 2 3 4 1 7 3 9 0
3 2 6 5 2 9 4 7 8 7 9 6 3 1 0 5 6 3 4 5 2 8 4 0 1
4 3 7 6 3 0 5 8 9 8 0 7 4 2 1 6 7 4 5 6 3 9 5 1 2
5 4 8 7 4 1 6 9 0 9 1 8 5 3 2 7 8 5 6 7 4 0 6 2 3 . . . .

```

or a 10-digit mixed sequence may be used to generate nine further rows,³

```

2 1 5 4 1 8 3 6 7 6 8 5 2 0 9 4 5 2 3 4 1 7 3 9 0
4 6 8 9 6 2 1 7 5 7 2 8 4 3 0 9 8 4 1 9 6 5 1 0 3
9 7 2 0 7 4 6 5 8 5 4 2 9 1 3 0 2 9 6 0 7 8 6 3 1
0 5 4 3 5 9 7 8 2 8 9 4 0 6 1 3 4 0 7 3 5 2 7 1 6 . . . .

```

or a long series of substitution alphabets such as

```

      1 2 3 4 5 6 7 8 9 0
(1)  5 8 2 0 1 6 9 7 3 4
(2)  6 1 9 5 7 2 0 3 8 4
(3)  6 4 7 1 5 0 2 8 3 9 . . .

```

might be used to generate a large number of rows from the basic sequence as in the following example:

```

2 1 5 4 1 8 3 6 7 6 8 5 2 0 9 4 5 2 3 4 1 7 3 9 0
8 5 1 0 5 7 2 6 9 6 7 1 8 4 3 0 1 8 2 0 5 9 2 3 4
1 6 7 5 6 3 9 2 0 2 3 7 1 4 8 5 7 1 9 5 6 0 9 8 4
4 6 5 1 6 8 7 0 2 0 8 5 4 9 3 1 5 4 7 1 6 2 7 3 9 . . . .

```

j. A frequently encountered key-generation method, especially for agent use, entails the use of Fibonacci treatment involving an introductory group of length *n*, and then (most usually) summing the *a+b* digits to yield the digit in the (*n*+1) position, summing the *b+c* digits to yield the digit in the (*n*+2) position and continuing this process to derive a key as long as necessary with which to encipher the message. The indicator in such cases is often the introductory priming group disguised by an additive (usually taken from one of the text groups of the cipher message); in some cases, however, the indicator is the introductory group left in the clear, as in the following examples employing 5-digit priming groups:

<u>Ind.</u>	10	15	20	<u>Message key</u>
31419	4 5 5 0 3 9 0 5 3 2 9 5 8 5 1			4 3 3 6 5 7 6 9 1 2 . . . .
27188	9 8 9 6 7 7 7 5 3 4 4 2 8 7 8			6 0 5 5 4 6 5 0 9 0 . . . .

In these two examples the developed key up to the 20th position was discarded as a safety measure, and the actual key used commenced with the 21st position.

k. Fibonacci variations are many. For example, if the introductory group consists of five digits, the formulas *a+e=f* or *a+b+c=f* might be used; or each succeeding five-digit group might be generated by a recursion procedure of *a+b=f*, *b+c=g*, *c+d=h*, *d+e=i*, but *e+a=j* (instead of the more usual *e+f=j*). Sometimes a row of *n* digits, say 25, might be generated by a Fibonacci treatment, and a second row established underneath the first one, either by shifting the basic sequence against itself at some offset

```

3 1 4 1 9 4 5 5 0 3 9 0 5 3 2 9 5 8 5 1 4 3 3 6 5
1 9 4 5 5 0 3 9 0 5 3 2 9 5 8 5 1 4 3 3 6 5 3 1 4

```

³ The 10-digit mixed sequence in this example, 2490316758, generates nine further rows, but it could be used to generate 99 further rows by successive changes of the mixed sequence to 3501427869, 4612538970 . . . , that is, by adding to the digits of the mixed sequence after each set of ten rows, yielding a key totalling 2500 digits.

or by adding a constant to the basic sequence,

3 1 4 1 9 4 5 5 0 3 9 0 5 3 2 9 5 8 5 1 4 3 3 6 5  
4 2 5 2 0 5 6 6 1 4 0 1 6 4 3 0 6 9 6 2 5 4 4 7 6

or by continuing the Fibonacci treatment for another 25 digits,

3 1 4 1 9 4 5 5 0 3 9 0 5 3 2 9 5 8 5 1 4 3 3 6 5  
7 6 9 1 2 3 5 0 3 5 8 5 3 8 3 3 8 1 1 6 1 9 2 7 7.

From here on a *vertical* Fibonacci treatment is applied to the columns, to yield a long key. Using the case just illustrated,

3 1 4 1 9 4 5 5 0 3 9 0 5 3 2 9 5 8 5 1 4 3 3 6 5  
7 6 9 1 2 3 5 0 3 5 8 5 3 8 3 3 8 1 1 6 1 9 2 7 7  
0 7 3 2 1 7 0 5 3 8 7 5 8 1 5 2 3 9 6 7 5 2 5 3 2

the length of the key would be  $60 \times 25 = 1500$  digits before it begins to repeat.

l. Key has sometimes been produced by means of an assembly of strips. The system entails a set of, say, 50 strips containing 50 digits each, from which a selection of 20 strips is made, aligned flush with each other or at a specified alignment, and the key groups are read in the order in which they occur. As an example, in Fig. 111a below is illustrated a set of ten strips, and in Fig. 111b is the selection of strips *b*, *f*, *c*, and *a* at the alignment 3204. (Note that, to avoid possible ambiguity, the top ten digits on each strip consist of a scramble of the digits 0 through 9.)

a	b	c	d	e	f	g	h	i	j
1	2	0	4	9	6	9	4	4	2
8	3	3	0	6	4	8	1	6	5
4	0	4	9	5	7	7	6	9	1
3	1	9	2	0	0	1	8	7	7
9	8	8	7	8	2	6	5	0	6
2	7	5	3	7	5	0	2	3	0
6	9	7	8	2	1	3	9	1	9
7	5	1	6	4	9	2	0	5	3
5	6	2	5	1	3	5	3	2	4
0	4	6	1	3	8	4	7	8	8
7	0	7	9	9	5	4	7	2	0
8	5	6	3	6	0	2	4	5	3
0	2	3	6	1	9	9	1	9	6
4	8	0	8	8	6	5	0	8	2
9	7	4	5	5	1	1	2	3	8
1	4	5	7	3	3	3	6	7	9
2	3	9	0	2	4	8	5	6	5
5	6	1	1	7	7	6	8	0	4
6	1	8	2	4	2	7	9	1	7
3	9	2	4	0	8	0	3	4	1

9	4	1	4	1	9	8	7	9	0
7	2	5	6	8	8	1	4	0	7
1	5	0	2	4	2	0	3	2	5
0	0	9	0	3	0	5	2	8	1
2	8	6	3	2	1	2	5	4	6
5	3	7	8	5	7	4	9	7	2
4	7	2	5	9	5	3	0	6	8
6	9	3	1	0	3	9	8	1	3
8	1	8	7	6	4	7	6	3	4
3	6	4	9	7	6	6	1	5	9

FIGURE 111a

f	a
6	1
4	8
7	4
0	3
2	0
3	8
0	5
1	1
8	9
7	3
9	8
5	5
6	0
4	9
0	6
5	1
2	3
8	4
7	7
4	2
3	8

b	c	a
2	0	1
3	2	8
0	5	4
1	1	9
8	9	2
7	3	6
9	8	5
5	5	7
6	0	1
4	9	2
0	6	6
5	1	7
2	3	6
8	4	3
7	7	0
4	2	4
3	8	5

2	1	1	1
5	7	5	0
0	5	0	2
8	3	9	5
3	4	6	4
7	6	7	6
9		2	8
1		3	3
6		8	4

FIGURE 111b

The key groups would be taken off starting with 3204 0533 and ending with 3464 7676. If more key is needed, a new selection and alignment would be made. (The process could have been facilitated in this case by selecting eight strips, taking off two groups at a time.)

m. A method that has achieved prominence is the use of a stencil with which to extract key from a key page, as illustrated in the example given in Fig. 112, below:

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	20	25	30	35																																																							
a.	0	4	4	9	3	5	2	4	9	4	7	5	2	4	6	3	3	8	2	4	4	5	8	6	2	5	1	0	2	5	6	1	9	6	2																																								
b.	0	0	5	4	9	9	7	6	5	4	6	4	0	5	1	8	8	1	5	9	9	6	1	1	9	6	3	8	9	6	5	4	6	9	2																																								
c.	3	5	9	6	(3 1 5 3)				(8 9 8 0)				(3 3 3 5)				1	3	5	4	6	2	7	7	9	7	4																																																
d.	5	9	8	0											9	4	9	7	0	0	1	3	0	2	1																																																		
e.	4	6	0	5											(6 0 1 3)				(9 2 2 8)				1	4	4	0	7	7	9	3	9	1	0																																										
f.	3	2	1	7																					7	0	7	0	0	7	8	6	7	4	3																																								
g.	6	9	2	3																					(6 1 4 0)				(0 1 1 7)				(4 1 5 9)				6	6	0	0	0	0	1	8	7	4	3																												
h.	1	9	5	6																															9	2	1	5	8	5	6	6	6	7	4																														
i.	4	5	1	5																															(4 9 3 8)				(7 6 0 7)				(4 3 6 6)				7	9	4	5	4	3	5	9	0	4	7																		
j.	9	4	8	6																																									8	8	1	5	5	3	0	1	5	4	0																				
	9	8	0	8																																									(2 6 4 5)				(4 0 4 4)				9	0	8	8	9	6	3	9	0	9	4												
	3	3	1	8																																																			5	4	8	5	8	1	8	8	6	9	5										
	8	0	9	5																																																			(1 0 0 4)				(8 2 7 0)				1	2	3	3	8	7	2	5	0	1	6		
	7	9	7	5	2	4	9	1	4	0	7	1	9	6																																									1	2	8	2	9	6	6	9	8	6	1	0	2	5	9	1	7	4	8	5	2
	1	8	6	3	3	3	2	5	3	7	9	8	1	4																																									5	0	6	5	7	1	3	1	0	1	0	2	4	6	7	4	0	5	4	5	5
	7	4	0	2	9	4	3	9	0	2	7	7	5	5	7	3	2	2	7	0	9	7	7	9																															0	1	7	1	1	9	5	2	5	2	7										
	5	4	1	7	8	4	5	6	1	1	8	0	9	9	3	3	7	1	4	3	0	5	3	3																															5	1	2	9	6	9	5	6	1	2	7										
	1	1	6	6	4	4	9	8	8	3	5	2	0	7	9	8	4	8	2	7	5	9	3	8	1	7	1	5	3	9	0	9	9	7																					3																				
	4	8	3	2	4	7	7	9	2	8	3	1	2	4	9	6	4	7	1	0	0	2	2	9	5	3	6	8	7	0	3	2	3	0																					7																				
	6	9	0	7	4	9	4	1	3	8	8	7	6	3	7	9	1	9	7	6	3	5	5	8	4	0	4	4	0	1	1	0	5	1	8																																								

FIGURE 112

The key page in this instance consists of 20 rows of 35 random digits each, and the index position (the upper left-hand corner) of the stencil may be positioned at any one of the first 16 digits in the first ten rows of the key page (in this example, it is placed at position c5). The apertures of the stencil expose 15 four-digit groups,⁴ and it may be used in any of the four positions, two obverse and two reverse. The advantage of such a system is the prolongation of life of key pages by means of frequent changes of the stencil (size, shape, and number of apertures per line) for different key periods; furthermore, it allows considerable flexibility in the choice of a message-to-message keying variable.

n. As a final comment, keys have been encountered which were produced by a person writing down random characters by hand, or with a typewriter. As may be imagined, these "random characters" are really not random, since it is inevitable that psychological factors enter into the "arbitrary" selection of characters.

58. Mechanical and electronic key generators.—a. Perhaps the most primitive "mechanical" generation of digital key is accomplished by means of printing slugs consisting either of single-digit type faces or of 4- or 5-digit groups. The slugs are assembled by hand into a chase or printing frame, and two or more copies are printed of several pages simultaneously. For example, in the case of 4-digit slugs there would be available a collection of one each of the 10,000 groups from 0000 to 9999, and a printing frame of four or eight pages of 100 groups each would be made up at the same time. After the requisite number of copies is printed, the used slugs would then be put back into the total collection, scrambled thoroughly, and another printing frame of four or eight pages would be made up.

⁴ Cases have been encountered wherein the apertures of the stencil expose single digits, these digits comprising a periodic repeating key.

b. Old teleprinter tapes, either of plain text or cipher text, have been used as keys; or two or more tapes have been added together and the resultant used as a composite key. For that matter, even a single tape could be read at two different positions and the characters added together to produce key in plaintext autokey fashion.

c. Punched-card equipment has been used to produce key. The simplest method, used for digital key, is to take a deck of cards on which is punched either plain language or random alphabetical text, and then list the cards *but omitting the zone punch* (i.e., the  $\emptyset$ , "x", and "y" punches). This results in the following conversion as a consequence of the card punching code:

1	2	3	4	5	6	7	8	9
A	B	C	D	E	F	G	H	I
J	K	L	M	N	O	P	Q	R
S	T	U	V	W	X	Y	Z	

Note that a  $\emptyset$  cannot be produced because all letters are coded by a combination of a digit punch from 1 to 9 plus an "x", "y", or " $\emptyset$ " zone punch.

d. The more usual punched-card method, however, is to start with a single "supermaster card" punched in all 80 columns, perhaps with exactly eight occurrences each of the digits 1 through 0. Then by means of a plugging, 79 more cards are produced from the "supermaster card." These cards are now thoroughly shuffled, and 40 or 50 columns are selected by means of a plugging and printed to constitute 80 lines of key. When the 80 cards have been listed, either the plugging is changed or the cards are shuffled anew, or both, to produce further sets of 80 lines of key. Sometimes the "supermaster card" is used to generate a total of 80 "master cards," and these "master cards" are then used to produce a second generation of 6400 cards which are thoroughly shuffled and from which a selection of, say, 2500 cards is made, after which columns are selected and listed as before.

e. Mechanical key generators have often employed a multiplicity of gears or variable-pin wheels with which to produce a long key. The best example of this type of key generator is the Hagelin C-38 cipher machine, which has six wheels of mutually prime lengths (26, 25, 23, 21, 19, and 17) which step once with each operation, so that the cycle is the product (101,405,850) of the wheel sizes. The same idea is applicable in the case of key generators employing several teleprinter tapes of mutually prime lengths. Other geared devices have used the principle of the Kryha cipher machine, involving a gear which moves irregularly, displacing a pair of enciphering components from 5 to 10 steps; after a cycle of the gear wheel (which can be varied, usually in the vicinity of 15 to 35) the sum of the displacements is prime to 26 so that the length of the key produced is 26 times the gear cycle. Still other generators have incorporated plaintext or ciphertext autokeying, or the principle of the Wheatstone cipher device which achieves a highly irregular motion of the pair of enciphering components because the stepping is predicated not only on the plain text being enciphered but also on the particular sequence of the letters in the plain component.

f. Often mechanical key generators are employed "off line," so to speak, to produce prefabricated key in advance of actual message encryption. For instance, a Hagelin C-38 machine may be used to encipher a constant plaintext letter, say A_p, which results in the production of pure Hagelin key; or, by prearrangement, plain text from a book or other source can be enciphered, yielding a highly complex resultant as key. Furthermore, in mechanical key generators the key produced is sometimes *cumulative* in nature, i.e., each key element is the sum of the key generated at that particular position plus all the preceding key elements.

g. One device that has appeared on the open market consisted of an array of print-wheels containing ten digits each which printed one page at a time, and after two (or more) copies have been printed the wheels advance to new positions and another page is printed. In Fig. 113, below, is illustrated a simplified sample of two successive pages (as printed) of ten rows of five 4-digit groups each. It will be noted that the numbers in the first and fifth groups advanced by 1 between the two pages, the numbers in

Page 63					Page 64				
0918	2009	3282	3952	0422	0919	2008	3285	3949	0423
9004	8549	5198	5065	9493	9005	8548	5201	5062	9494
7318	5020	4767	2626	6229	7319	5019	4770	2623	6230
7576	7649	2097	8774	9042	7577	7648	2100	8771	9043
5401	4405	6628	3100	0068	5402	4404	6631	3097	0069
0835	6991	7854	4278	1366	0836	6990	7857	4275	1367
2830	0326	8133	1059	4051	2831	0325	8136	1056	4052
5380	8623	8159	1362	5121	5381	8622	8162	1359	5122
9175	5374	6161	6226	5026	9176	5373	6164	6223	5027
8941	9269	0039	5839	1260	8942	9268	0042	5836	1261

FIGURE 113

the second group have retrogressed by 1, the numbers in the third group have advanced by 3, while the numbers in the fourth group have retrogressed by 3. (In the actual machine some of the wheels had repeated digits; the turnover points were not necessarily 9; and irregular motion was imparted to some of the wheels.) In order to disguise the relationship between successive pages, the pages were scrambled after a sufficient number was produced, and the pages were bound in individual key books.

h. Electronic key generators have now come to the fore, as might be expected. Some of them are weak in cryptoprinciple; some are merely electronic versions of pin-wheel or gear mechanisms. The more sophisticated of them, however, are electronic shift registers which produce binary key for the encryption of teleprinter characters, facsimile signals, or coded speech. These shift registers consist of a number of cells or stages, initially loaded with 0's and 1's for the start of the generation. As each binary key element is produced, the sequence of 0's and 1's is shifted to the right, dropping out the rightmost bit, and the leftmost stage is loaded with a new bit by some convention in the circuitry. The maximum cycle of such a register is  $2^n - 1$ , where  $n$  is the number of stages involved. In Fig. 114, below, is a sample register of 16 stages.

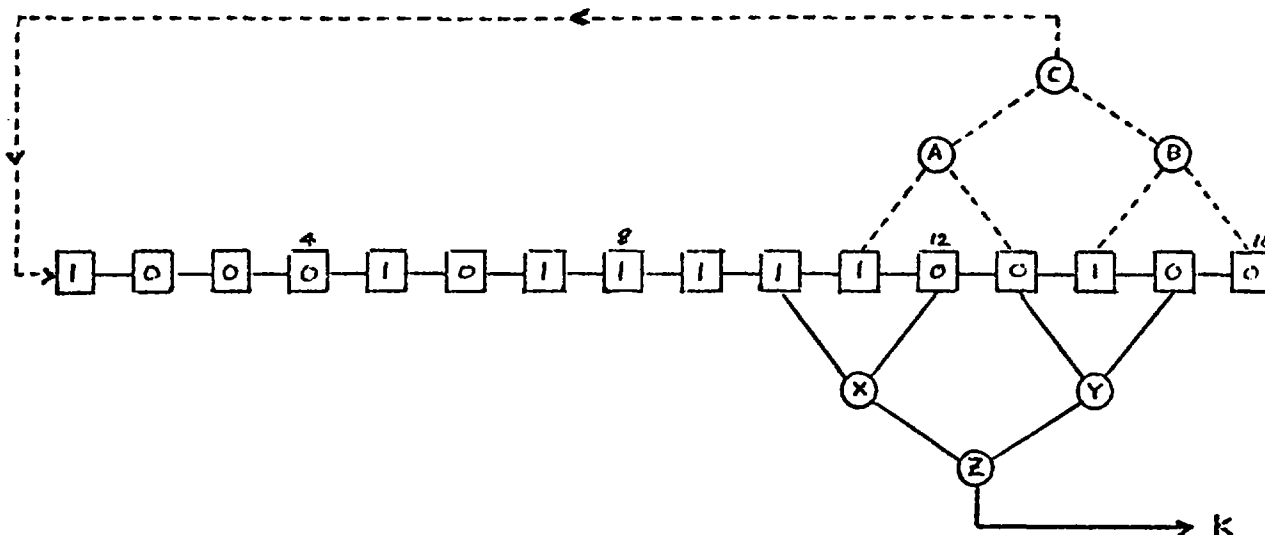


FIGURE 114



yields a distinct set of probabilities of the digits, shown below together with the theoretical distribution in tally-mark form (for English underlying text):

1	.1027	
2	.0614	
3	.0710	
4	.1265	≡
5	.2246	≡≡
6	.0560	≡≡≡
7	.0199	≡≡≡≡
8	.1097	≡≡≡≡≡
9	.1347	≡≡≡≡≡≡
0	<u>.0935</u>	≡≡≡≡≡≡≡
	1.0000	

The appearance of this distribution (and its equivalent in the language of the particular problem with which we might be concerning ourselves) should be memorized, together with its  $\gamma$  I.C. (in this case, for English,  $\gamma=1.28$ ), for its quick identification and interpretation when it is encountered. Once a numerical key is recognized as having arisen by means of this particular conversion process, the original plain text may easily be recovered by reading on simple generatrices, as in the following example:

	5	10	15	20	25	30																								
<u>6</u>	<u>5</u>	<u>1</u>	<u>8</u>	<u>9</u>	<u>3</u>	<u>5</u>	<u>8</u>	<u>5</u>	<u>1</u>	<u>4</u>	<u>4</u>	<u>9</u>	<u>5</u>	<u>2</u>	<u>5</u>	<u>4</u>	<u>5</u>	<u>5</u>	<u>1</u>	<u>8</u>	<u>9</u>	<u>1</u>	<u>7</u>	<u>5</u>	<u>5</u>	<u>1</u>	<u>8</u>	<u>6</u>	<u>1</u>	. . .
F	E	A	H	I	C	E	H	E	A	D	D	I	E	B	E	D	E	E	A	H	I	A	G	E	E	A	H	F	A	
P	O	K	R	S	M	O	R	O	K	N	N	S	O	L	O	N	O	O	K	R	S	K	Q	O	O	K	R	P	K	
Z	Y	U		W	Y		Y	U	X	X		Y	V	Y	X	Y	Y	U		U	Y	Y	U	Z	U					

d. Cases have been encountered in which key has been generated by enciphering plain text from a book through a Nihilist square which consists of a  $5 \times 5$  square inscribed with the normal A-Z sequence (I and J combined), and coordinates 1-5 in normal order for both rows and columns. This yields the following sets of probabilities and theoretical distribution:

<p>Rows:</p> <table style="border-collapse: collapse;"> <tr><td>1</td><td>.2865</td></tr> <tr><td>2</td><td>.1567</td></tr> <tr><td>3</td><td>.2426</td></tr> <tr><td>4</td><td>.2584</td></tr> <tr><td>5</td><td><u>.0558</u></td></tr> <tr><td></td><td>1.0000</td></tr> </table>	1	.2865	2	.1567	3	.2426	4	.2584	5	<u>.0558</u>		1.0000	<p>Columns:</p> <table style="border-collapse: collapse;"> <tr><td>1</td><td>.1572</td></tr> <tr><td>2</td><td>.1422</td></tr> <tr><td>3</td><td>.2099</td></tr> <tr><td>4</td><td>.3040</td></tr> <tr><td>5</td><td><u>.1867</u></td></tr> <tr><td></td><td>1.0000</td></tr> </table>	1	.1572	2	.1422	3	.2099	4	.3040	5	<u>.1867</u>		1.0000	<p>Composite distribution:</p> <table style="border-collapse: collapse; text-align: center;"> <tr><td>≡</td><td>≡</td><td>≡</td><td></td><td></td><td></td></tr> <tr><td>≡≡</td><td>≡≡</td><td>≡≡</td><td>≡</td><td></td><td></td></tr> <tr><td>≡≡≡</td><td>≡≡≡</td><td>≡≡≡</td><td>≡≡</td><td>≡</td><td></td></tr> <tr><td>1</td><td>2</td><td>3</td><td>4</td><td>5</td><td></td></tr> <tr><td colspan="5">Rows</td><td></td></tr> <tr><td></td><td></td><td></td><td></td><td></td><td>≡</td></tr> <tr><td></td><td></td><td></td><td></td><td></td><td>≡≡</td></tr> <tr><td></td><td></td><td></td><td></td><td></td><td>≡≡≡</td></tr> <tr><td></td><td></td><td></td><td></td><td></td><td>≡≡≡≡</td></tr> <tr><td></td><td></td><td></td><td></td><td></td><td>1</td></tr> <tr><td></td><td></td><td></td><td></td><td></td><td>2</td></tr> <tr><td></td><td></td><td></td><td></td><td></td><td>3</td></tr> <tr><td></td><td></td><td></td><td></td><td></td><td>4</td></tr> <tr><td></td><td></td><td></td><td></td><td></td><td>5</td></tr> <tr><td></td><td></td><td></td><td></td><td></td><td>Columns</td></tr> </table>	≡	≡	≡				≡≡	≡≡	≡≡	≡			≡≡≡	≡≡≡	≡≡≡	≡≡	≡		1	2	3	4	5		Rows											≡						≡≡						≡≡≡						≡≡≡≡						1						2						3						4						5						Columns
1	.2865																																																																																																																			
2	.1567																																																																																																																			
3	.2426																																																																																																																			
4	.2584																																																																																																																			
5	<u>.0558</u>																																																																																																																			
	1.0000																																																																																																																			
1	.1572																																																																																																																			
2	.1422																																																																																																																			
3	.2099																																																																																																																			
4	.3040																																																																																																																			
5	<u>.1867</u>																																																																																																																			
	1.0000																																																																																																																			
≡	≡	≡																																																																																																																		
≡≡	≡≡	≡≡	≡																																																																																																																	
≡≡≡	≡≡≡	≡≡≡	≡≡	≡																																																																																																																
1	2	3	4	5																																																																																																																
Rows																																																																																																																				
					≡																																																																																																															
					≡≡																																																																																																															
					≡≡≡																																																																																																															
					≡≡≡≡																																																																																																															
					1																																																																																																															
					2																																																																																																															
					3																																																																																																															
					4																																																																																																															
					5																																																																																																															
					Columns																																																																																																															

The nature of the dinomic key text, revealing plaintext properties underlying, makes it very easy to recover the original literal text from which the key was produced. Other schemes for obtaining digital key from plain text, such as encipherment with monome-dinome rectangles, are transparent and readily solvable if there is a sufficient sample of key available. Furthermore, there have been many cases in which key was derived from plain text enciphered by means of the same cryptosystem as was used to encipher the message.⁷ For example, if the enemy is using the following monome-dinome rectangle,

	9	4	8	1	2	7	6	5	0	3
-	R	E	P	U	B	L	I	C		
0	A	D	F	G	H	J	K	M	N	O
3	Q	S	T	V	W	X	Y	Z		

⁷ For an example of such a system used by secret agents in World War II, see pp. 206-210 of Alexander Foote, *Handbook for Spies*, New York, 1949.



this yields, for English plain text, the probabilities of the ciphertext digits (with  $\gamma$  I.C. of 1.63) and the theoretical distribution in tally-mark form shown below:

0	.2880	
1	.0363	
2	.0372	
3	.1808	≡
4	.1468	≡
5	.0354	≡
6	.0602	≡
7	.0268	≡
8	.0923	≡
9	<u>.0962</u>	≡
	1.0000	

			≡						
			≡	≡					
			≡	≡	≡				
			≡	≡	≡	≡			
			≡	≡	≡	≡	≡		
			≡	≡	≡	≡	≡	≡	
0	1	2	3	4	5	6	7	8	9

If, in solving an additive encipherment involving the foregoing rectangle, we recover the first 30 digits of key to be

0 8 0 3 1 9 3 4 5 0 3 9 4 0 9 0 0 0 4 3 4 4 3 1 4 0 0 3 6 4

we would recognize from the appearance of the key that it must be derived from the same population as the theoretical distribution given above; this is attested by the distribution of the key:

			≡						
			≡	≡					
			≡	≡	≡				
			≡	≡	≡	≡			
0	1	2	3	4	5	6	7	8	9

Even if we had recovered the following key,

6 8 6 7 0 9 7 3 2 6 7 9 3 6 9 6 6 6 3 7 3 3 7 0 3 6 6 7 4 3

			≡						
			≡	≡					
			≡	≡	≡				
			≡	≡	≡	≡			
0	1	2	3	4	5	6	7	8	9

we would still recognize from its appearance that it must be based upon plain text, and, because of its  $\gamma$  I.C. of 1.75 (close enough to the  $\gamma$  I.C. of 1.63), probably enciphered through the same monome-dinome matrix but with different coordinates. This is a hypothetical case, of course, but it might be apropos to include here the digit probabilities and theoretical distribution of cipher text produced by the true Nihilist system, involving an additive key produced by enciphering plain text through the same square as is used for the encryption of the message:

0	.0190	
1	.0000	
2	.0450	
3	.0753	
4	.1218	
5	.1897	
6	.1834	
7	.1617	
8	.1327	
9	<u>.0715</u>	
	1.0001	

0	1	2	3	4	5	6	7	8	9

e. The punched-card method of producing digital key by suppressing the zone punch of alphabetical material yields characteristic probabilities which are easy to recognize and interpret. In Fig. 115a, below, are the probabilities

0	.0000
1	.0753
2	.0739
3	.1590
4	.0931
5	.2248
6	.1192
7	.0477
8	.0567
9	<u>.1503</u>
	1.0000

FIGURE 115a

0	.0000
1	.0769
2	.1154
3	.1154
4	.1154
5	.1154
6	.1154
7	.1154
8	.1154
9	<u>.1154</u>
	1.0001

FIGURE 115b

of the digits when the data punched on the cards is English plain text, and in Fig. 115b are the probabilities when the data consists of random alphabetical characters. In tally-mark form the theoretical distributional appearance of these two cases is quite striking:

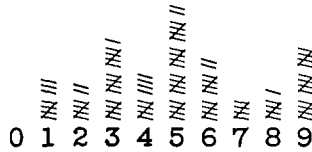


FIGURE 115c

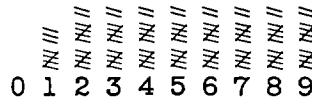


FIGURE 115d

The original plain text from which the key was derived may be easily recovered with a modification of the generatrix diagram shown in subpar. c, above.

f. Delta techniques play an important part in key analysis, as will now be shown. For example, if key recovered on true base from a cipher text were that given below,

3201 3404 3598 3784 3962 4133 4298 4456 4609 4757 . . . .

this appears to have been derived by some sort of mathematical progression or from a table of mathematical functions. A search in common mathematical tables reveals the source: in a table of 4-place logarithms, these are the logs of 209, 219, 229 . . . . But if the key were not on true base, so that the groups as recovered were

4435 4638 4832 5018 5196 5367 5532 5690 5843 5991 . . . .

this sequence could not be found in any of our available tables. We therefore take first differences (with borrowing subtraction) of the groups, and also further differences as shown in the diagram below:

	4435	4638	4832	5018	5196	5367	5532	5690	5843	5991	. . . .
$\Delta_1$ :	203	194	186	178	171	165	158	153	148		
$\Delta_2$ :		9	8	8	7	6	7	5	5		
$\Delta_3$ :			-1	0	-1	-1	1	-2	0		

The oscillation of the final differences is indicative of derivation from a mathematical table of some sort, with round-off error because of incomplete information. We therefore make a search in available mathematical tables for groups with successive differences of 203, 194, 186 . . . , which leads us to solution, discovering the addition (with carrying arithmetic) of a constant 1234. Note that if we had taken our first differences mod 10, we would have had the following:

	4435	4638	4832	5018	5196	5367	5532	5690	5843	5991	. . .
$\Delta_1$ :	203	204	1286	188	271	275	168	253	158		

These fluctuating differences would have caused us to try normal arithmetical differences instead of mod 10 ones, leading to solution as before.

g. In Figs. 116a and b, below, are given two further examples of key and differences:

K:	2323	2530	2755	2998	3259	3538	3835	4150	4483	4834	. . .
$\Delta_1$ :	207	225	243	261	279	297	315	333	351		
$\Delta_2$ :	18	18	18	18	18	18	18	18	18		
$\Delta_3$ :	0	0	0	0	0	0	0	0	0		

FIGURE 116a

K:	5818	6215	6684	7231	7862	8583	9400	0319	1346	2487	. . .
$\Delta_1$ :	397	469	547	631	721	817	919	1027	1141		
$\Delta_2$ :	72	78	84	90	96	102	108	114			
$\Delta_3$ :	6	6	6	6	6	6	6	6			
$\Delta_4$ :	0	0	0	0	0	0	0	0			

FIGURE 116b

The fact that the last differences are all 0's shows that the numerical data are self-contained and complete. Now it is a well-known mathematical fact that the second differences of a series of squares (or any decimation of the series) will be constant, as will be the third differences of a series of cubes, as may be seen from the following:

N	N ²	$\Delta_1$	$\Delta_2$
1	1		
2	4	3	2
3	9	5	2
4	16	7	2
5	25	9	2
6	36	11	

FIGURE 116c

N	N ³	$\Delta_1$	$\Delta_2$	$\Delta_3$
1	1			
2	8	7	12	
3	27	19	18	6
4	64	37	24	6
5	125	61	30	6
6	216	91		

FIGURE 116d

It therefore follows that the key in Fig. 116a is based on polynomials of the second degree, so we can solve a set of four simultaneous equations in four unknowns to arrive at an answer, as follows:

$$\begin{aligned}
(1) \quad & ax^2 + bx + c = 2323 \\
(2) \quad & a(x+1)^2 + b(x+1) + c = 2530 \\
(3) \quad & a(x+2)^2 + b(x+2) + c = 2755 \\
(4) \quad & a(x+3)^2 + b(x+3) + c = 2998 \\
(2) \quad & (ax^2 + 2ax + a) + (bx + b) + c = 2530 \\
(1) \quad & \underline{ax^2 + bx + c = 2323} \\
(5) \quad & \quad \quad 2ax + a + b = 207 \\
(3) \quad & (ax^2 + 4ax + 4a) + (bx + 2b) + c = 2755 \\
(2) \quad & \underline{(ax^2 + 2ax + a) + (bx + b) + c = 2530} \\
(6) \quad & \quad \quad 2ax + 3a + b = 225 \\
(6) \quad & 2ax + 3a + b = 225 \\
(5) \quad & \underline{2ax + a + b = 207} \\
(7) \quad & \quad \quad 2a = 18, \therefore a = 9
\end{aligned}$$

At this point we are in a quandary, since there is no clear-cut way to recover the values of  $x$  and  $b$ —indeed, there is an infinite set of values for  $x$  and  $b$  that will satisfy the equations. But let us try a bit of practical skulduggery. We see from (5) that  $18x + 9 + b = 207$ , so that  $18x + b = 198$ . Now since 18 is a divisor of 198, is it not possible that  $x = 11$ , making  $b = 0$ ? We then have the first several elements of key reduced as follows:

1.  $2323 = 9 \cdot 11^2 + 1234$
2.  $2530 = 9 \cdot 12^2 + 1234$
3.  $2755 = 9 \cdot 13^2 + 1234$

Even though there is an infinite set of values of  $x$  and  $b$  that would satisfy the equations, there is little doubt, based on psychological considerations, that the values are  $a = 9$ ,  $b = 0$ ,  $c = 1234$ , and  $x = 11$ . As for the key of Fig. 116b, we must solve the following set of five simultaneous equations in five unknowns:

$$\begin{aligned}
(1) \quad & ax^3 + bx^2 + cx + d = 5818 \\
(2) \quad & a(x+1)^3 + b(x+1)^2 + c(x+1) + d = 6215 \\
(3) \quad & a(x+2)^3 + b(x+2)^2 + c(x+2) + d = 6684 \\
(4) \quad & a(x+3)^3 + b(x+3)^2 + c(x+3) + d = 7231 \\
(5) \quad & a(x+4)^3 + b(x+4)^2 + c(x+4) + d = 7862
\end{aligned}$$

Here too there is an infinity of answers, but the psychologically most plausible one consists of the values  $a = 1$ ,  $b = 0$ ,  $c = 0$ ,  $d = 4487$ , and  $x = 11$ , simplifying the polynomial to  $x^3 + 4487$ .

*h.* For the next case to be considered, we have the following stretches of key recovered from reading three shallow depths (the message indicators are shown enclosed within parentheses):

Key "A"

(14342) 21900 30109 41280 71216 24400 93326 46025 41671 . . .

Key "B"

(09414) 28071 21624 40093 32646 02541 67110 51010 31452 . . .

Key "C"

(16715) 10510 10314 52188 22534 11141 87119 82119 71041 . . .

It is apparent from the relationships of the three keys that the sequence of 5-digit groups may be used at a slide. On closer examination, however, it is observed that if the keys are divided into tetranomes, the *a* digits are limited to 0, 1, or 2: this could mean that the enemy is using the encode section of one of his two-part code books as source of key. As for the indicators, they designate the group (with a sum-checking digit added) immediately preceding the first code group to be used as key. The beauty of this scheme to the cryptanalyst is that, if the code is still in use and has not been recovered to any extent, the sequence of key groups recovered above had the effect of transforming portions of the two-part code into a *one-part* code.⁸

i. In the next example let us assume that we have the following three keys available for study:

- (1) 3204 0533 1149 8992 7386 9857 5575 6010 4927 0668 . . .
- (2) 2601 3438 0744 1093 8289 7552 9176 5917 6325 4860 . . .
- (3) 3871 9508 2727 6159 7215 5696 0734 7680 8355 0002 . . .

We note, between keys (1) and (2), that the *a* digits of (2) are the same as the *a* digits of (1), but at a slide of 1; that the *b* digits of (2) are the same as the *b* digits of (1) at a slide of 4; that the *c* digits of (1) and (2) are identical; and that the *d* digits of (2) are the same as the *d* digits of (1) at a slide of 2. Likewise, it may be seen that the *a* digits of (1) are related to the *d* digits of (3); the *b* digits of (1) are related to the *c* digits of (3); the *c* digits of (1) are related to the *b* digits of (3); and the *d* digits of (1) are related to the *a* digits of (3). All this points to a system of generation with sliding strips, such as that illustrated in subpar. 57*l*, so that after the strips are synthesized the key for a new message could be extrapolated after a few groups have been recovered.

j. In another example let us study the following three keys recovered from the initial analysis of a cryptosystem:

- (1) 3153 8980 3335 6013 9228 6140 0117 4159 4938 7607 . . .
- (2) 6315 6898 4333 3601 0922 4614 2011 0415 1493 4760 . . .
- (3) 3072 0935 5135 3909 8677 0620 7452 9566 8194 7246 . . .

We immediately note that the *abc* digits of (1) are the same as the *bcd* digits of (2), and that the *d* digits of (1) are the same as the *a* digits of (3). At this point we might have conjectured a strip-generated system such as that of the preceding subparagraph, but the fact that no slides of the basic sequences between groups is noted suggests a stencil system, upon which we are able to synthesize the following partial sequences of the key page:

```

. . . 63153072 . . . . . 68980935 . . . . . 43335135 . . .
. . . 36013909 . . . . . 09228677 . . . . . 46140620 . . .
. . . 20117452 . . . . . 04159566 . . . . . 14938194 . . .
. . . 47607246 . . .

```

As more key is recovered it can be fitted into our partial reconstruction, and we would eventually arrive at the key page and stencil shown in Fig. 112. In this case the solution of the indicators used would materially aid in the correct interleaving of the odd and even rows of the key page, since the stencil itself has its apertures two rows apart.

⁸ In a related use of code books as sources of key, cases have been encountered in which the indicator in a transposition system consists of a code group (for example, LYUF, which might have the meaning "Mission accomplished," providing a 19-element key for the transposition). When the literal key is recovered from the numerical key used in the transposition, we also have an incidental code recovery for the group in question, if we did not have it before.

k. The key recovered from multiple anagramming of several identical-length transposition messages in the same key yields a partial cipher-to-plain (C→P) sequence which gives clues as to the nature of the transposition system. Let us take the following four 50-letter messages as an example:

Msg No. 1: N U R I L O R R H M H T D T E E O T G A R U U D E I D I N O  
 Msg No. 2: I P S L T O L L N O X T R E I U R N H L Y S T E N A O T T A  
 Msg No. 3: T Y T P O I E R R I E E N R U N S P N R O N H B A I R G O A  
 Msg No. 4: E O N S R S L U F E U T N T T E R O S L R N U P O A F A T R

Msg No. 1: H N V D M E Z I I N A C A E T A T S E R  
 Msg No. 2: E R U C S C I E Q E H E E O I L R Y I T  
 Msg No. 3: E T S W G N R S L E E K P O N T A A O T  
 Msg No. 4: T R O W Q P I E P E R S I O I O O Y S T

In the initial anagramming, 25 columns have been assembled, as shown below:

Msg No. 1: A M M U N I T I O N T R A I N S C H E D U L E D T . . .  
 Msg No. 2: H O S T I L E A R T I L L E R Y E X C E P T I O N . . .  
 Msg No. 3: E I G H T P R I S O N E R S T A K E N B Y O U R P . . .  
 Msg No. 4: R E Q U E S T A R T I L L E R Y S U P P O R T F O . . .

The partial C→P sequence recovered in the foregoing diagram is the following:

41 10 35 23 1 4 14 26 17 29 45 7 20 38 32 48 42 11 36 24 2 5 15 27 18

It is clear from the isomorphic repetition manifested in the key beginning at the 17th position, that, unless blank cells are encountered later on, the system is a single columnar transposition involving 16 columns with the numerical key as shown in the diagram below, constructed from the recovered portion of the C→P sequence:

14	4	12	8	1	2	5	9	6	10	15	3	7	13	11	16
41	10	35	23	1	4	14	26	17	29	45	7	20	38	32	48
42	11	36	24	2	5	15	27	18							

If, in another example, the portion of the recovered C→P sequence had been the following,

10 24 29 19 35 6 15 41 46 11 1 25 30 20 36 16 42 47 2 26 31 21 37 7 17,

the interrupted isomorphism observed is indicative of *blank cells* in the matrix, and the numerical key together with the blank pattern thus far recovered for the matrix of 10 columns is shown in the following diagram:

3	1	6	7	5	8	2	4	9	10
10	●	24	29	19	35	6	15	41	46
11	1	25	30	20	36	●	16	42	47
●	2	26	31	21	37	7	17		

If, as a third example, the C→P sequence recovered in the process of multiple anagramming had been the following,

17 56 40 06 30 82 98 80 20 86 60 12 46 70 44 93 50 24 75 01 34 90 65 05 97  
 39 55 16 54 29 59 69 85 19 79 09 11 23 33 49 92 43 63 74 96 15 04 64 89 27  
 38 68 78 58 28 53100 84 32 42 22 10 08 72 48 14 88 95 73 62 36 03 77 52 67  
 37 26 18 57 41 07 31 83 99 81 21 87 61 13 47 71 45 94 51 25 76 02 35 91 66

the isomorphic repetition beginning at the 78th position shows that double transposition with keys of lengths 7 and 11 must be involved, since 77 is an implausible key-length for single transpositions.

l. Slug key is usually produced by selection from a universe, say 10,000 for 4-digit slugs, comprising in this case all the groups from 0000 to 9999. When several pages are made up at the same time for printing, it is obvious that there will be no repetitions of groups between the pages since the population consists of unique slugs, all different. This absence of repetition between a set of pages permits us to conjecture the slug method of production, as may be seen by referring to the table below:

Probability of 0 tetranome repetitions			
N	1 chance in	N	1 chance in
50	*	300	93
100	**	350	483
150	3	400	3,257
200	7	450	28,492
250	23	500	323,857

(* = 88 chances in 100; ** = 61 chances in 100)

If, for example, we have four sets of 100 tetranomes each and we observe no group repetitions among them, and since this phenomenon is expected, by chance, only once in 3257 times, it is obvious that some kind of selection *without replacement* is involved, and slug key comes to mind, with four pages being assembled at a time.⁹ The slugs are then replaced by the clerk, and four more pages are assembled. Sometimes, however, the slugs are not replaced after the first four pages, and another set of four pages is made up from the remainder, which makes the phenomenon even more striking. Again, sometimes the slugs from four pages are not replaced into the population, but are scrambled among themselves to yield four new pages, consisting of the 400 groups comprising the previous set of four pages; although this key is nondeterministic, nevertheless it is of considerable help to the cryptanalyst, who needs to consider only a finite number of possible keys during exploitation instead of the total population of 10,000.

m. In the usual punched-card method for key production, a permutation is applied to the elements of a master card or cards to produce secondary cards. As an example, let us consider the following master card, which for simplicity's sake has only 30 columns punched,

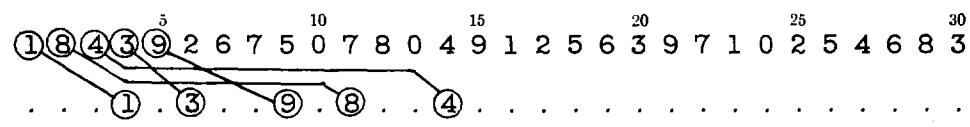
1 8 4 3 9 2 6 7 5 0 7 8 0 4 9 1 2 5 6 3 9 7 1 0 2 5 4 6 8 3

and let us assume that the plugging for the punching permutation is

01 02 03 04 05 06 07 08 09 10 11 12 13 14 15 16 17 18 19 20  
04 11 14 06 09 26 30 25 16 01 23 28 19 18 20 10 03 22 05 29

21 22 23 24 25 26 27 28 29 30  
27 07 21 13 02 12 15 08 17 24

The first five elements of the master card would be permuted as follows on the secondary card:



⁹ The possibility of generation by punched-card methods, with the cards containing one group each, should not be ignored.





If we assume that for a particular cryptosystem we need key in lines of only 10 digits each, we could establish a print plugging, say columns 3-12-25-8-17-2-19-13-21-5, yielding the listing shown in Fig. 118a, below. When the 30 cards have been listed, the print plugging could be changed to, let us say, 5-30-17-1-4-12-19-23-11-7, producing the listing shown in Fig. 118b. Since, however, there are undesirable properties of direct symmetry manifested in the columns of these diagrams, it would have been better if we had scrambled the rows of Fig. 117, say to a permutation of 10-4-27-30-1-8-7-3-5-29 . . . 28-6-2-9-26, so that the pluggings for the column selection would have yielded the keys in Figs. 118c and d.

	3	12	25	8	17	2	19	13	21	5
(1)	4	8	2	7	2	8	6	0	9	9
(2)	2	5	7	6	8	2	0	0	1	6
(3)	8	2	6	8	3	7	0	3	7	0
(4)	3	3	8	5	9	6	3	6	8	0
(5)	9	1	5	2	4	8	6	7	2	3
(6)	4	0	2	3	9	5	7	5	7	6
(7)	9	1	3	1	1	2	5	4	6	7
(8)	1	5	1	0	7	3	4	4	8	5
(9)	7	9	0	1	8	1	4	2	5	4
(10)	8	6	1	5	2	0	2	8	2	4
* * * * *										
(26)	3	7	4	9	6	9	1	0	2	3
(27)	6	8	9	1	7	4	0	1	8	1
(28)	7	2	1	7	5	9	1	5	3	0
(29)	5	7	7	8	4	1	5	9	9	1
(30)	4	6	8	2	4	7	9	6	4	5

FIGURE 118a

	5	30	17	1	4	12	19	28	11	7
(1)	9	3	2	1	3	8	6	6	7	6
(2)	6	6	8	0	1	5	0	8	8	7
(3)	0	7	3	1	0	2	0	5	2	5
(4)	0	5	9	5	1	3	3	2	7	4
(5)	3	4	4	9	5	1	6	3	6	4
(6)	6	4	9	6	9	0	7	1	8	2
(7)	7	2	1	0	6	1	5	0	5	8
(8)	5	8	7	0	0	5	4	1	2	3
(9)	4	3	8	3	0	9	4	5	3	9
(10)	4	9	2	6	3	6	2	9	1	4
* * * * *										
(26)	3	5	6	6	7	7	1	1	3	9
(27)	1	9	7	8	6	8	0	7	9	6
(28)	0	6	5	5	8	2	1	8	4	0
(29)	1	0	4	2	5	7	5	2	9	0
(30)	5	0	4	3	2	6	9	7	1	3

FIGURE 118b

	3	12	25	8	17	2	19	13	21	5
(10)	8	6	1	5	2	0	2	8	2	4
(4)	3	3	8	5	9	6	3	6	8	0
(27)	6	8	9	1	7	4	0	1	8	1
(30)	4	6	8	2	4	7	9	6	4	5
(1)	4	8	2	7	2	8	6	0	9	9
(8)	1	5	1	0	7	3	4	4	8	5
(7)	9	1	3	1	1	2	5	4	6	7
(3)	8	2	6	8	3	7	0	3	7	0
(5)	9	1	5	2	4	8	6	7	2	3
(29)	5	7	7	8	4	1	5	9	9	1
* * * * *										
(28)	7	2	1	7	5	9	1	5	3	0
(6)	4	0	2	3	9	5	7	5	7	6
(2)	2	5	7	6	8	2	0	0	1	6
(9)	7	9	0	1	8	1	4	2	5	4
(26)	3	7	4	9	6	9	1	0	2	3

FIGURE 118c

	5	30	17	1	4	12	19	28	11	7
(10)	4	9	2	6	3	6	2	9	1	4
(4)	0	5	9	5	1	3	3	2	7	4
(27)	1	9	7	8	6	8	0	7	9	6
(30)	5	0	4	3	2	6	9	7	1	3
(1)	9	3	2	1	3	8	6	6	7	6
(8)	5	8	7	0	0	5	4	1	2	3
(7)	7	2	1	0	6	1	5	0	5	8
(3)	0	7	3	1	0	2	0	5	2	5
(5)	3	4	4	9	5	1	6	3	6	4
(29)	1	0	4	2	5	7	5	2	9	0
* * * * *										
(28)	0	6	5	5	8	2	1	8	4	0
(6)	6	4	9	6	9	0	7	1	8	2
(2)	6	6	8	0	1	5	0	8	8	7
(9)	4	3	8	3	0	9	4	5	3	9
(26)	3	5	6	6	7	7	1	1	3	9

FIGURE 118d

Now suppose that we had recovered the 300 digits of key of Fig. 118a and had further obtained the first 50 digits of key of Fig. 118b. It is clear that *if we had written the key out in lines of 10 digits each* we would have noticed not only that the second column of Fig. 118a is identical to the sixth column of Fig. 118b, but also that there exist properties of direct symmetry, as previously mentioned, between the

columns, speeding up the recovery of the entire 30 basic columns of Fig. 117.¹¹ If on the other hand we had recovered the 300 digits of key of Fig. 118c plus the first 50 digits of key of Fig. 118d, and had again written out the recovered key in rows of 10 digits each, we could extend the first, third sixth, and seventh columns of Fig. 118d for a total of 30 positions. What this emphasizes is that writing out recovered key on trial widths may have a rewarding result for the alert cryptanalyst.¹²

n. For another case of analysis, let us assume that we have recovered the two following stretches of key:

Key "A"									
0918	2009	3282	3952	0422	9004	8549	5198	5065	9493
7318	5020	4767	2626	6229	7576	7649	2097	8774	9042
5401	4405	6628	3100	0068	0835	6991	7854	4278	1366
2830	0326	8133	1059	4051	5380	8623	8159	1362	5121
9175	5374	6161	6226	5026	8941	9269	0039	5839	1260

Key "B"									
0567	5311	1436	1095	1832	3813	3421	0599	9181	8372
5729	4534	9670	7495	4843	5298	2095	6406	7753	7472

It is noticed that if Key "B" is slid three groups to the left of Key "A", that the *a* digits in corresponding positions are predominantly hitting, or differing by only 1:

Key "A":	0918	2009	3282	3952	0422	9004	8549	5198	5065	9493
Key "B":	1095	1832	3813	3421	0599	9181	8372	5729	4534	9670
Key "A":	7318	5020	4767	2626	6229	7576	7649	2097	8774	9042 . . .
Key "B":	7495	4843	5298	2095	6406	7753	7472			

It is further noticed that the differences (with borrowing subtraction) of the 1st, 5th, 6th, 10th, 11th, 15th, and 16th groups is 177, and that the differences between the 2d, 7th, 12th, and 17th groups is -177. This suggests to us to write out the keys in rows of five groups each, as follows:

Key "A"					Key "B"				
0918	2009	3282	3952	0422	1095	1832	3813	3421	0599
9004	8549	5198	5065	9493	9181	8372	5729	4534	9670
7318	5020	4767	2626	6229	7495	4843	5298	2095	6406
7576	7649	2097	8774	9042	7753	7472			
5401	4405	6628	3100	0068					
0835	6991	7854	4278	1366					
2830	0326	8133	1059	4051					
5380	8623	8159	1362	5121					
9175	5374	6161	6226	5026					
8941	9269	0039	5839	1260					

¹¹ An interesting observation may be made about the average I.C. of the rows of Fig. 118a (including the missing rows 11-25), and of Fig. 118b. For Fig. 118a, since one row has a  $\phi$  count of 2, ten rows have  $\phi$ 's of 4, eleven rows have  $\phi$ 's of 6, six rows have  $\phi$ 's of 8, and two rows have  $\phi$ 's of 10, the  $\delta$  I.C. =  $\frac{(2/9) + 10(4/9) + 11(6/9) + 6(8/9) + 2(10/9)}{30} = 0.6519$ .

For Fig. 118b, the  $\delta$  comes out to be 0.7481. The property of an observed I.C. consistently below random is the result of the superflatness of the master card, which contains three each of the digits 0 to 9. A selection of any columns from the generated cards will always result in an expected average I.C. below 1.0000 for the rows; consequently, this phenomenon can be used to diagnose the method of generation of the key. In this case of 30 digits per card, the expected  $\delta$  I.C. is  $10(2/29)$  or 0.6897; if we approached this figure in testing a large number of row distributions, we would know that the master card generating the population must have contained 30 digits.

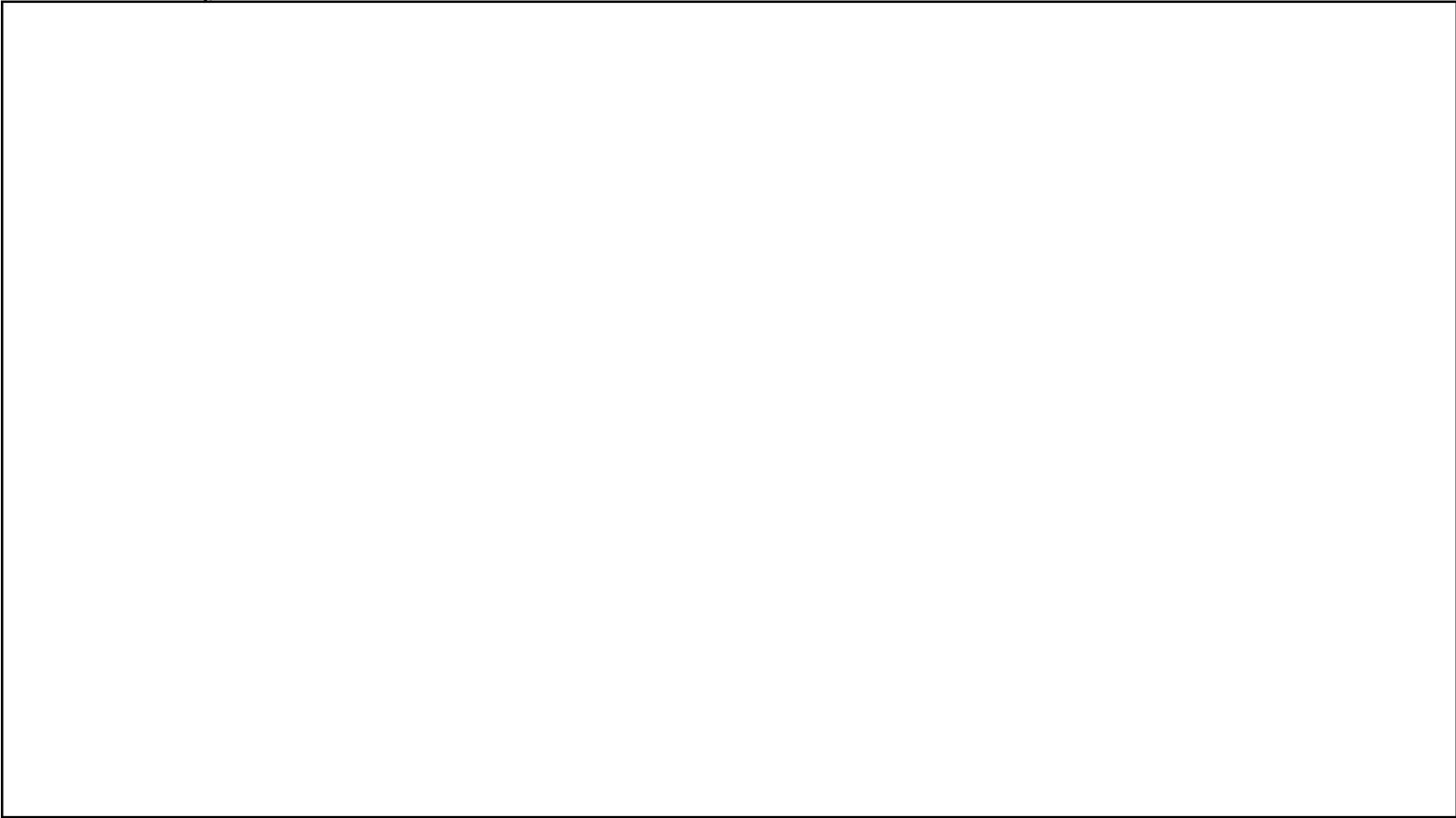
¹² It was emphasized previously that the general methods and procedures of cryptanalysis that apply to encrypted text also apply in the analysis of key. In this connection, if key text is written out on width *w* and the average I.C. for this array is considerably improved (let us say, doubled) over the over-all I.C. of the sample, it is indicative that the cycle of *w* has some significance in the generation of the key.

We now note that the groups in the third column of Key "B" are those of Key "A" but with an additive of 531 (=3·177) while the groups in the fourth column of Key "B" are those of Key "A" but with a subtractor of 531. This means that we have two pages of key 177 pages apart, produced by a key generator that operates on the following rule, after the 50 printing counters have been set to arbitrary initial positions: the counters in column 1 and column 5 advance one position (carrying arithmetic), the counters in column 2 retrogress by one position, the counters in column 3 advance three positions, and the counters in column 4 retrogress three positions. This conclusion is substantiated by the first three groups of Key "B", 0567 5311 1436, which are groups from the immediately preceding printed page, following the rule just given. If Key "A" were page 1 as printed, then pages 177 and 178 would be the following (page 177 is shown in fragmentary form):

Page 177				
1094				
9180				
7494				
7752				
5577				
1011				
3006				
5556				
9351				
9117	9093	0567	5311	1436

Page 178				
1095	1832	3813	3421	0599
9181	8372	5729	4534	9670
7495	4843	5298	2095	6406
7753	7472	2628	8243	9219
5578	4228	7159	2569	0245
1012	6814	8385	3747	1543
3007	0149	8664	0528	4228
5557	8446	8690	0831	5298
9352	5197	6692	5695	5203
9118	9092	0570	5308	1437

We can, of course, reproduce all the pages from 1 to 200 or more, if we desire, with which to read all the traffic in the system.



(b) (1)
(b) (3)-18 USC 798
(b) (3)-50 USC 3024(i)
(b) (3)-P.L. 86-36

60. Analysis of key in a double transposition cipher. a. Each problem in key analysis is a distinct and unique experience, as is indeed any problem in cryptanalysis. Nevertheless, as an example illustrating techniques of analysis as applied to key from a manual cryptosystem, we shall study the steps involved in the analysis of key derived from multiple anagramming of several identical-length messages in the same pair of double transposition keys. But in order to understand the reasons for our steps, we shall first examine the mechanics of double transposition encipherment.

b. Let a 51-letter plaintext message be represented by the consecutive numbers from 01 to 51, as inscribed in the T1 matrix shown below. The columns of the T1 matrix are taken off in numerical-

6	2	7	1	5	3	8	4
01	02	03	04	05	06	07	08
09	10	11	12	13	14	15	16
17	18	19	20	21	22	23	24
25	26	27	28	29	30	31	32
33	34	35	36	37	38	39	40
41	42	43	44	45	46	47	48
49	50	51					

T1

3	9	1	7	4	2	11	8	10	6	5
04	12	20	28	36	44	02	10	18	26	34
42	50	06	14	22	30	38	46	08	16	24
32	40	48	05	13	21	29	37	45	01	09
17	25	33	41	49	03	11	19	27	35	43
51	07	15	23	31	39	47				

T2

key order and inscribed in the rows of the T2 matrix, and the final cipher text, 20 06 48 33 15 . . . (the P→C sequence) is obtained by taking off the columns of the T2 matrix in numerical-

(b) (1)  
 (b) (3)-18 USC 798  
 (b) (3)-50 USC 3024(i)  
 (b) (3)-P.L. 86-36



We see that the numbers in the *columns* of the T2 matrix are consecutive, and that if we were to take off these columns according to the numerical key and inscribe them into a matrix of the same dimensions as the T1 matrix, these numbers would be consecutive in rows and would represent the sequence of the original plain text:

01	02	03	04	05	06	07	08
09	10	11	12	13	14	15	16
17	18	19	20	21	22	23	24
25	26	27	28	29	30	31	32
33	34	35	36	37	38	39	40
41	42	43	44	45	46	47	48
49	50	51					

d. Returning to our analysis thus far, we have already established the T1 matrix as having eight columns, so we inscribe the C→P sequence into a matrix of eight columns, as shown below:

27	47	09	11	31	02	42	44
23	34	50	38	18	30	05	26
14	43	37	01	08	17	33	22
41	25	46	29	49	07	20	13
04	21	28	16	36	48	10	40
32	12	24	06	45	35	51	03
19	39	15					

We now find the column containing the number 01 and set it down as follows:

11	38	01	29	16	06
----	----	----	----	----	----

We then look for the column containing the number 02 and set it down under the previous column so that the 02 is under the 01,

11	38	01	29	16	06		
		02	30	17	07	48	35

and we continue this procedure with the columns containing the numbers 03, 04, and 05, arriving at the following diagram:

11	38	01	29	16	06		
		02	30	17	07	48	35
44	26	22	13	40	03		
27	23	14	41	04	32	19	
		42	05	33	20	10	51

The next term in the sequence is 06, but it is already present in the diagram, as is also 07. In the column headed by 06 there is vacant space for 08 and 09, and in the column headed by 11 there is space for 12, so these segments are added to the diagram:

11	38	01	29	16	06								
47	34	43	25	21	12	39	02	30	17	07	48	35	
44	26	22	13	40	03	31	18	08	49	36	45		
27	23	14	41	04	32	19	09	50	37	46	28	24	15
		42	05	33	20	10	51						

It is clear that the diagram is only five rows deep, so we fill out our diagram as follows:

11	38	01	29	16	06	47	34	43	25	21	12	39						
47	34	43	25	21	12	39	02	30	17	07	48	35	44	26	22	13	40	03
44	26	22	13	40	03	31	18	08	49	36	45	27	23	14	41	04	32	19
27	23	14	41	04	32	19	09	50	37	46	28	24	15					
09	50	37	46	28	24	15	42	05	33	20	10	51						

We can now draw the outline of the T2 matrix in this diagram, since it is clear from the location of the numbers 20 and 25 that the column with the terms 11-15 belongs at the extreme left, and that the column with the terms 21-24 must be at the extreme right. The transposition key for the T2 matrix is established directly from this matrix, the 1 in the key being over the column headed by 01, the 2 of the key being over the column headed by 06, and so forth:

						3	9	1	7	4	2	11	8	10	6	5					
						11	38	01	29	16	06	47	34	43	25	21	12	39			
47	34	43	25	21		12	39	02	30	17	07	48	35	44	26	22	13	40	03		
		44	26	22		13	40	03	31	18	08	49	36	45	27	23	14	41	04	32	19
			27	23		14	41	04	32	19	09	50	37	46	28	24	15				
09	50	37	46	28	24	15	42	05	33	20	10	51									

At this point we inscribe the C→P sequence into the T1 matrix already known to have eight columns, and we recover the transposition key by following the sequence of rows in the T2 matrix; thus the terms 11 38 01 29 16 06 must be under key 1, the terms 47 34 . . . 12 39 under key 2, and so on. The recovered key is shown at the top of the T1 matrix below:

	6	2	7	1	5	3	8	4
27	47	09	11	31	02	42	44	
23	34	50	38	18	30	05	26	
14	43	37	01	08	17	33	22	
41	25	46	29	49	07	20	13	
04	21	28	16	36	48	10	40	
32	12	24	06	45	35	51	03	
19	39	15						

e. Now let us apply these techniques to the solution of an unknown example. It is assumed that we have recovered a C→P sequence from the anagramming of several messages of identical length enciphered by the same pair of double transposition keys. The C→P sequence is shown below, as is the P→C sequence together with its delta:

Term No.: 01 02 03 04 05 06 07 08 09 10 11 12 13 14 15 16 17 18 19 20  
 C→P: 14 35 40 23 02 07 37 63 01 70 47 57 52 19 30 06 13 22 46 51

Term No.: 21 22 23 24 25 26 27 28 29 30 31 32 33 34 35 36 37 38 39 40  
 C→P: 36 21 44 56 34 69 62 05 45 18 12 55 68 50 11 10 33 29 43 66

Term No.: 41 42 43 44 45 46 47 48 49 50 51 52 53 54 55 56 57 58 59 60  
 C→P: 25 54 61 17 32 42 67 16 49 28 04 09 39 15 31 65 60 27 08 41

Term No.: 61 62 63 64 65 66 67 68 69 70  
 C→P: 59 58 03 24 48 53 20 26 38 64

* * * * *

Term No.: 01 02 03 04 05 06 07 08 09 10 11 12 13 14 15 16 17 18 19 20  
 P→C: 09 05 63 51 28 16 06 59 52 36 35 31 17 01 54 48 44 30 14 67  
 Δ: -4 58 -12 -23 -12 -10 53 -7 -16 -1 -4 -14 -16 53 -6 -4 -14 -16 53 -45

Term No.: 21 22 23 24 25 26 27 28 29 30 31 32 33 34 35 36 37 38 39 40  
 P→C: 22 18 04 64 41 68 58 50 38 15 55 45 37 25 02 21 07 69 53 03  
 Δ: -4 -14 60 -23 27 -10 -8 -12 -23 40 -10 -8 -12 -23 19 -14 62 -16 -50 57

Term No.: 41 42 43 44 45 46 47 48 49 50 51 52 53 54 55 56 57 58 59 60  
 P→C: 60 46 39 23 29 19 11 65 49 34 20 13 66 42 32 24 12 62 61 57  
 Δ: -14 -7 -16 6 -10 -8 54 -16 -15 -14 -7 53 -24 -10 -8 -12 50 -1 -4 -14

Term No.: 61 62 63 64 65 66 67 68 69 70  
 P→C: 43 27 08 70 56 40 47 33 26 10  
 Δ: -16 -19 62 -14 -16 7 -14 -7 -16

f. From the differences of portions of the P→C sequence corresponding to the repetitions in the delta stream,

Term nos. 16-20:	48 44 30 14 67	Term nos. 26-30:	68 58 50 38 15
Term nos. 11-15:	<u>35 31 17 01 54</u>	Term nos. 31-35:	<u>55 45 37 25 02</u>
	13 13 13 13 13		13 13 13 13 13

the width of the T1 matrix is established as 13, so we inscribe the C→P sequence horizontally into a matrix of 13 columns:

14	35	40	23	02	07	37	63	01	70	47	57	52
19	30	06	13	22	46	51	36	21	44	56	34	69
62	05	45	18	12	55	68	50	11	10	33	29	43
66	25	54	61	17	32	42	67	16	49	28	04	09
39	15	31	65	60	27	08	41	59	58	03	24	48
53	20	26	38	64								

The column containing 01 is written horizontally, with the column containing 02 directly beneath it so that the 02 is under the 01:

01 21 11 16 59
02 22 12 17 60 64

We quickly add the columns containing 03, 04, and 05, properly juxtaposed:

01 21 11 16 59
02 22 12 17 60 64
47 56 33 28 03
57 34 29 04 24
35 30 05 25 15 20

At this point the column containing 06 seems to give conflicts, as does the column containing 07, so we add the columns containing 13 and 14 to go under our 12:

01 21 11 16 59
02 22 12 17 60 64
47 56 33 28 03   23 13 18 61 65 38
57 34 29 04 24   14 19 62 66 39 53
35 30 05 25 15 20

From here on it proceeds rapidly, and we arrive at the following diagram and the outline of the T2 matrix:

	9	2	10	12	7	6	1	5	3	4	13	14	8	11	15	
	40	06	45	54	31	26	01	21	11	16	59	63	36	50	67	41
63 36 50 67	41	07	46	55	32	27	02	22	12	17	60	64	37	51	68	42 08
37 51 68	42	08	47	56	33	28	03	23	13	18	61	65	38	52	69	43 09 48
52 69	43	09	48	57	34	29	04	24	14	19	62	66	39	53	70	44 10 49 58
70	44	10	49	58	35	30	05	25	15	20						

As before, the T2 key is derived by numbering the column headed by 01 as 1, the column headed by 06 as 2, and so forth to its complete recovery. The T1 key is obtained from our previous diagram of the C→P sequence inscribed into a matrix of 13 columns by following the breaks shown in the T2 matrix, above; thus the column 40 06 45 54 31 26 is given key number 1, the column 01 21 11 16 59 is given key number 2, and so on for the complete recovery of the T1 key.¹⁴

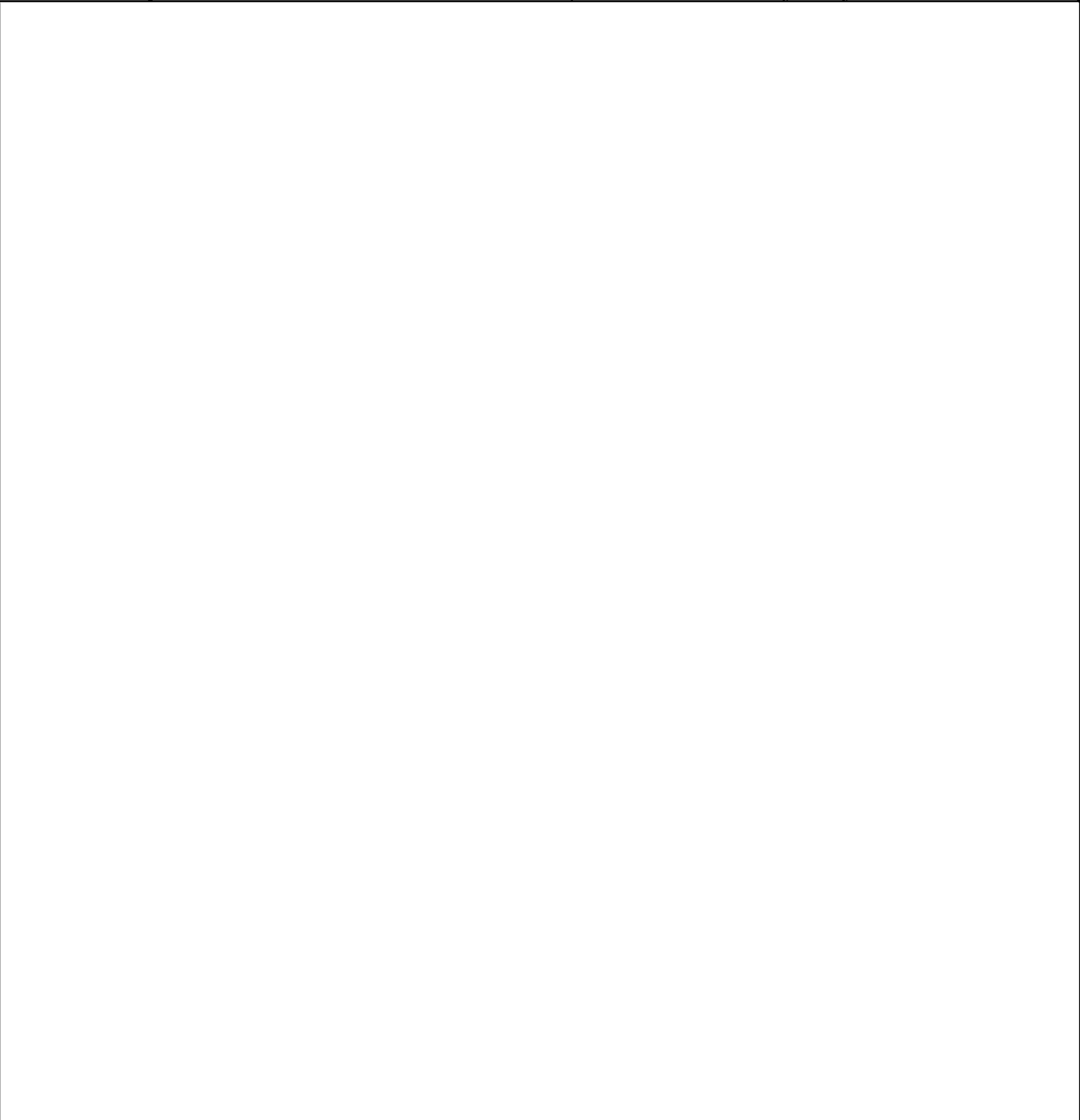
¹⁴ The T1 and T2 keys are derived from literal keys. See in this connection subpar. 62a.

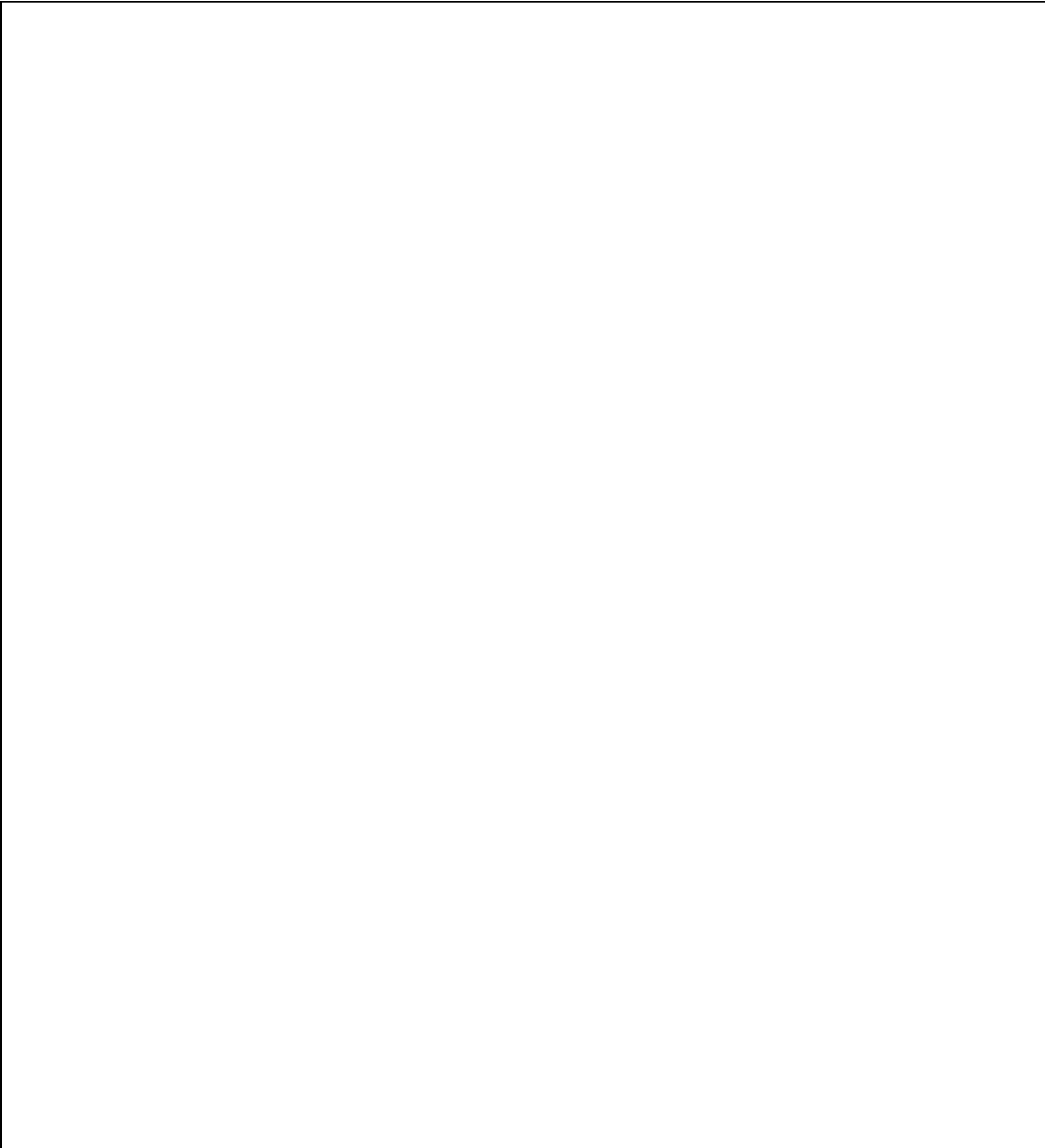


	11	13	1	8	5	4	6	3	2	12	7	10	9
14	35	40	23	02	07	37	63	01	70	47	57	52	
19	30	06	13	22	46	51	36	21	44	56	34	69	
62	05	45	18	12	55	68	50	11	10	33	29	43	
66	25	54	61	17	32	42	67	16	49	28	04	09	
39	15	31	65	60	27	08	41	59	58	03	24	48	
53	20	26	38	64									

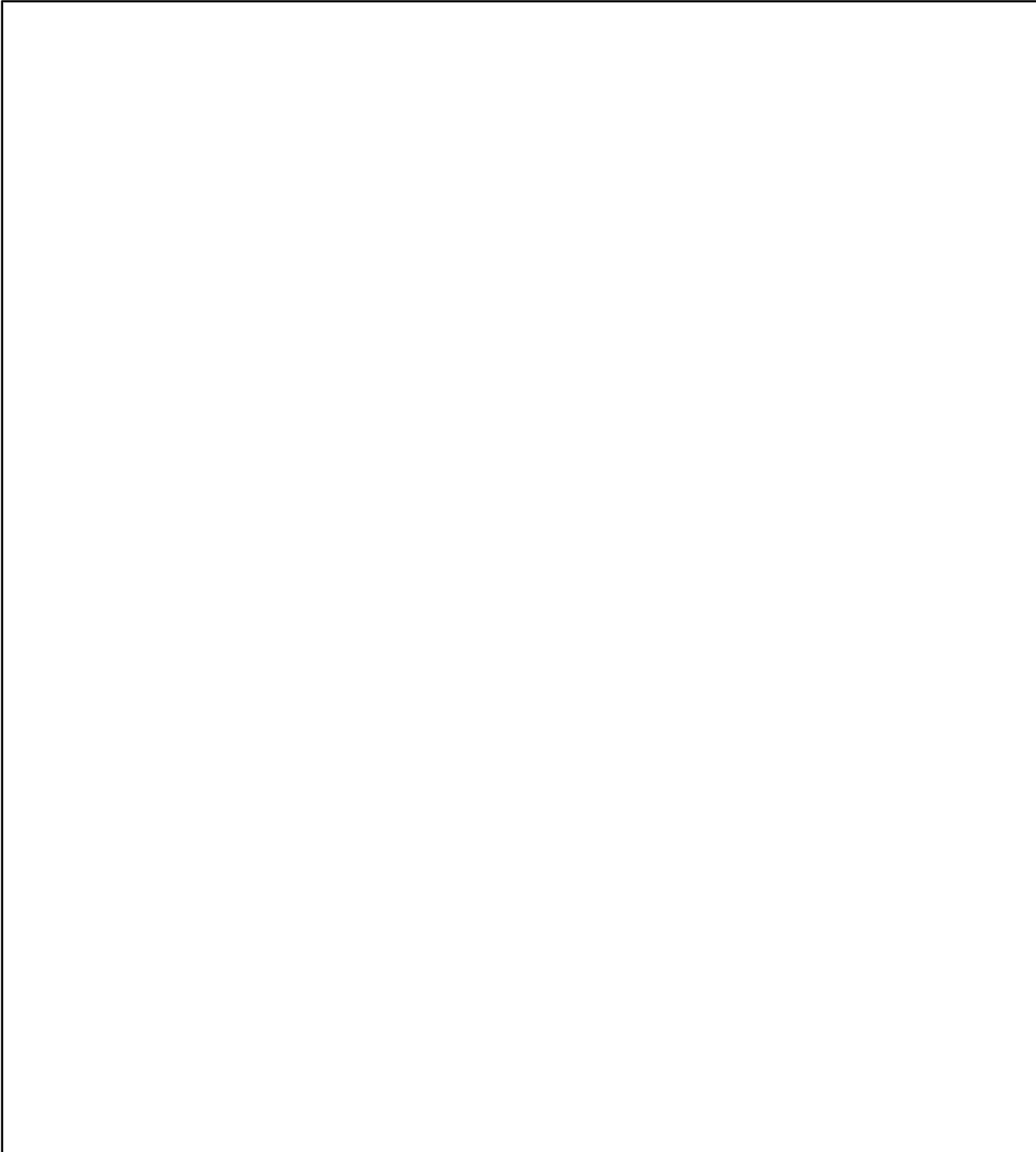
(b) (1)  
 (b) (3) -18 USC 798  
 (b) (3) -50 USC 3024(i)  
 (b) (3) -P.L. 86-36

g. There are several other methods for recovering double transposition keys from the C→P sequence, but the one just shown was deemed best from the standpoint of illustrative key analysis.

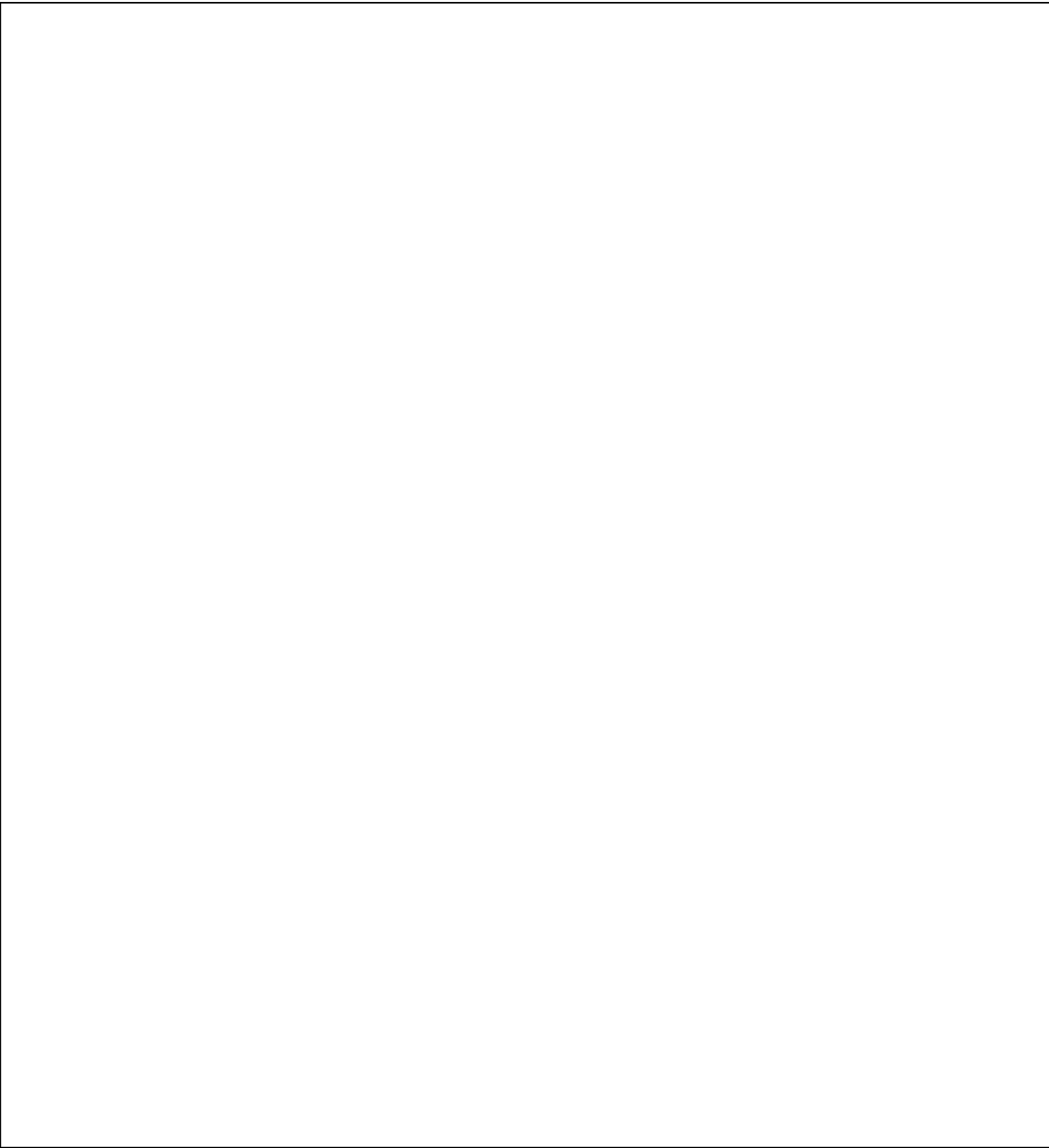




(b) (1)  
(b) (3)-18 USC 798  
(b) (3)-50 USC 3024(i)  
(b) (3)-P.L. 86-36



(b) (1)  
(b) (3)-18 USC 798  
(b) (3)-50 USC 3024 (i)  
(b) (3)-P.L. 86-36



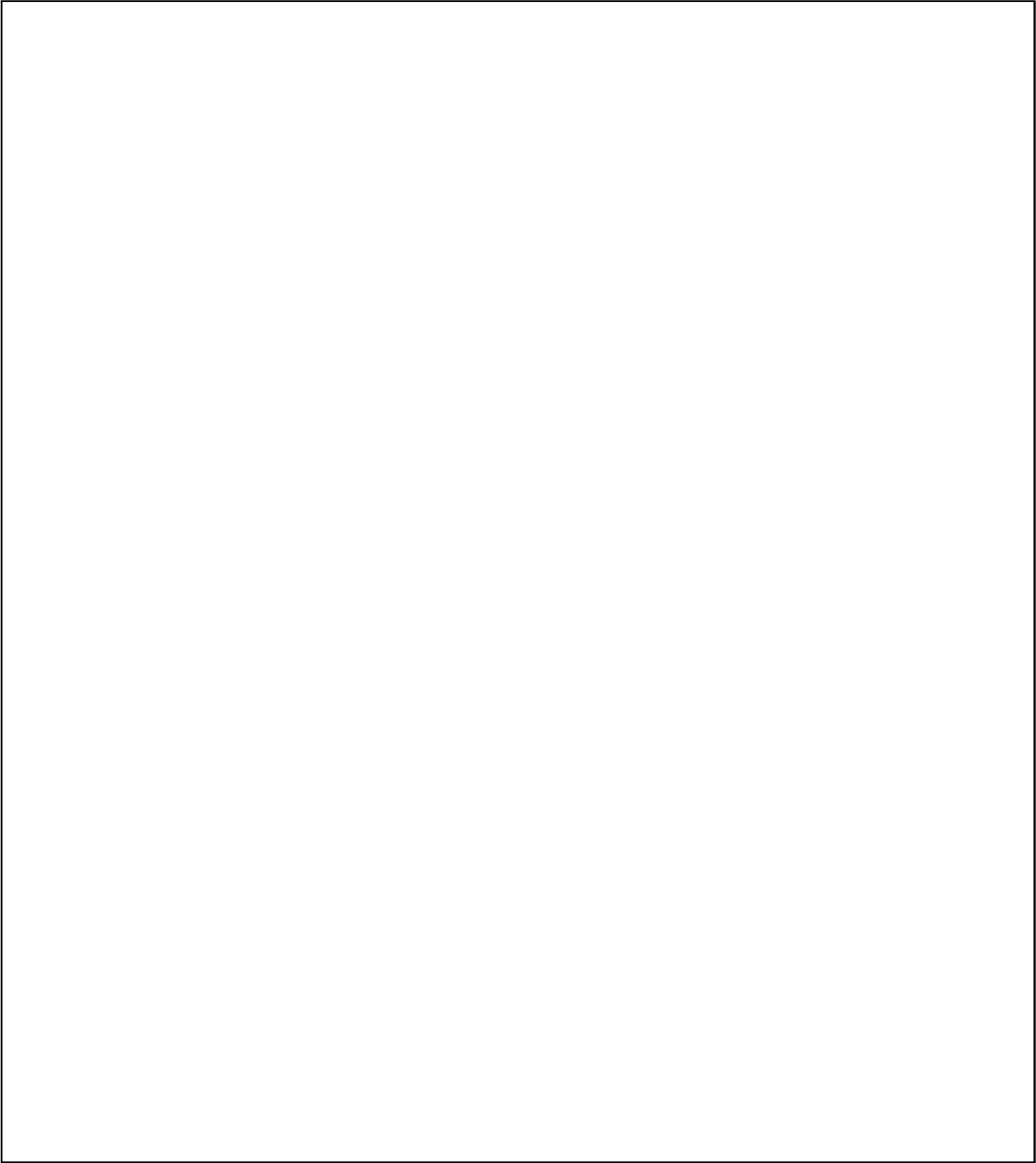
(b) (1)  
(b) (3)-18 USC 798  
(b) (3)-50 USC 3024 (i)  
(b) (3)-P.L. 86-36

(b) (1)  
(b) (3)-18 USC 798  
(b) (3)-50 USC 3024(i)  
(b) (3)-P.L. 86-36



(b) (1)  
(b) (3)-18 USC 798  
(b) (3)-50 USC 3024 (i)  
(b) (3)-P.L. 86-36

(b) (1)  
(b) (3)-18 USC 798  
(b) (3)-50 USC 3024 (i)  
(b) (3)-P.L. 86-36



(b) (1)  
(b) (3)-18 USC 798  
(b) (3)-50 USC 3024(i)  
(b) (3)-P.L. 86-36



(b) (1)  
(b) (3)-18 USC 798  
(b) (3)-50 USC 3024 (i)  
(b) (3)-P.L. 86-36

62. **Concluding remarks.**—*a.* In cryptographic practice 26-letter mixed sequences are often based upon key words. The recovery of these key words has been treated in par. 51 (on pp. 86–90) of *Military Cryptanalytics, Part I*. Likewise, numerical keys, especially those in transposition systems, are often based on underlying literal keys. The recovery of these underlying literal keys from the numerical keys has been treated on pp. 427–429 of *Military Cryptanalytics, Part II*.

*b.* A few final remarks on key analysis might be of assistance. When key is taken from the four-digit numbers in a telephone directory there is precious little to give it away, except for the observation that the number 0000 is never expected to appear; if it is encountered, the premise of a telephone directory as the source of the key is refuted. Furthermore, although there might be no discernible limitations in the directory of a large city, nevertheless cases have been encountered wherein, for instance, no telephone numbers began with the dinomes 07, 08, or 09, permitting easy identification of the particular directory. Psychological random, hand produced key, will have characteristics which can be identified as such; type-writer random key has similar attributes, including a very infrequent digit "1" when this digit is not on the number row but must be typed as a lower-case "L". Document analysis²¹ enters into the picture when key has been captured or surreptitiously photographed: in a simple case, the inadvertent occurrence of an upside-down digit in the key proves manufacture by single-digit slugs, whereas an entire group upside-down proves that group-slugs are involved in the production. The manufacture of key by punched-card methods may be indicated when the particular type-styles are identified with commercial electric accounting machines. The particular source or origin of the key might be indicated by the type of paper used, the chemical composition of the ink, or even the manner of stapling or binding. These are aspects of key analysis that should not be overlooked. The field, then, is pretty well all-embracing, and requires versatility of outlook and breadth of experience to achieve a significant margin of success.

---

²¹ In this connection, the following works may be of more than passing interest:  
Wilson R. Harrison, *Suspect Documents: Their Scientific Examination*, New York, 1958.  
Arthur J. Quirk, *Forged, Anonymous, and Suspect Documents*, London, 1930.  
Albert S. Osborn, *Questioned Documents*, New York, 1929.

(b) (1)  
 (b) (3) -18 USC 798  
 (b) (3) -50 USC 3024(i)  
 (b) (3) -P.L. 86-36

CHAPTER X

TELEPRINTER KEY ANALYSIS

General.....	Paragraph 63
Teleprinter key generation methods.....	64
	65
	66
	67
	68
	69
	70

63. General.—In *Military Cryptanalytics, Part I* and *Part II* we were introduced to Baudot systems and their encipherment.¹ The international Baudot code is given here below for ready reference:

UPPER CASE	WEATHER COMMUNICATIONS	SYMBOLS	+	⊕	○	/	3	↖	↘	↓	8	↙	↗	•	⊙	9	∅	1	4	Δ	5	7	⊖	2	/	6	+	-	<		SPACE	LTR. SHIFT	FIG. SHIFT
LOWER CASE	COMMUNICATIONS	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	BLANK	C.R.	L.F.	SPACE	LTR. SHIFT	FIG. SHIFT
	1	●	●		●	●	●				●	●					●	●			●	●	●	●	●	●	●					●	●
	2	●		●				●	●	●	●	●					●	●	●			●	●	●	●					●		●	●
	3			●			●	●	●	●	●			●	●	●	●			●	●	●	●	●	●						●	●	●
	4		●	●	●		●	●	●	●	●	●					●	●				●	●	●	●							●	●
	5	●						●	●			●	●	●	●	●	●				●		●	●	●	●	●					●	●

FIGURE 121

In Fig. 122a is given the Baudot combination table containing sums according to the rule that like impulses produce a “+”, unlike a “-”; in Fig. 122b is the complementary table of Baudot sums combined according to the rule that *unlike* impulses produce a “+”, like impulses a “-”. In most cases it is immaterial which rule of combination is assumed; but once a convention is established, it must be continued in the particular problem under study. In this discussion we shall assume the convention that, unless otherwise specified, like impulses produce a “+”, unlike a “-”. In the Baudot combination tables, the character representing the carriage return is symbolized by the digit “3”, the line feed by “4”, the figure shift by “5”, the blank by “7”, the letter shift by “8”, and the space by “9”.

64. Teleprinter key generation methods.²—a. One of the simplest ideas for the electromechanical generation of teleprinter key is the employment of 5 cam wheels or pin wheels, one for each “level” of Baudot key. As an elementary example, suppose a machine had five wheels in its key-generator component of lengths 11, 9, 8, 7, and 5, with pin (or notch) configurations as shown in Fig. 123 (“x” denotes an active pin, “o” an inactive pin).

¹ It might be well at this point to review the material covered in par. 56 (pp. 99-101 of *Military Cryptanalytics, Part I*, and in par. 97 (pp. 294-302) of *Military Cryptanalytics, Part II*.

² See also par. 14 on pp. 471-474 of Appendix 6 (“Cryptographic Supplement”), *Military Cryptanalytics, Part II*.

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	3	4	5	7	8	9
A	8	S	L	Y	X	Z	I	3	G	Q	W	C	7	T	9	R	J	P	B	N	5	4	K	E	D	F	H	V	U	M	A	0
B	S	8	3	K	U	J	M	L	7	F	D	H	G	R	V	T	Z	N	A	P	E	0	Y	5	W	Q	C	9	X	I	B	4
C	L	3	8	0	T	M	J	S	Q	G	V	A	F	X	D	U	I	5	H	E	P	K	4	N	9	7	B	W	R	Z	C	Y
D	Y	K	0	8	Q	5	N	4	T	X	B	9	R	G	C	7	E	M	W	I	Z	3	S	J	A	U	V	H	F	P	D	L
E	X	U	T	Q	8	W	9	R	0	Y	Z	N	4	L	I	3	D	H	5	C	B	7	F	A	J	K	P	M	S	V	E	G
F	Z	J	M	5	W	8	3	I	H	B	X	7	C	V	R	9	S	0	Q	4	Y	N	E	K	U	A	G	T	D	L	F	P
G	I	M	J	N	9	3	8	Z	A	C	R	Q	B	D	X	W	L	K	7	Y	4	5	P	0	T	H	F	U	V	S	G	E
H	3	L	S	4	R	I	Z	8	F	7	9	B	Q	U	W	X	M	E	C	5	N	Y	0	P	V	G	A	D	T	J	H	K
I	G	7	Q	T	0	H	A	F	8	L	P	J	S	Y	E	K	C	W	M	D	V	U	R	9	N	3	Z	5	4	B	I	X
J	Q	F	G	X	Y	B	C	7	L	8	5	I	3	0	N	4	A	V	Z	9	W	R	U	D	E	S	M	P	K	H	J	T
K	W	D	V	B	Z	X	R	9	P	5	8	4	N	M	3	I	U	G	Y	7	Q	C	A	F	S	E	0	L	J	T	K	H
L	C	H	A	9	N	7	Q	B	J	I	4	8	Z	E	Y	5	G	U	3	X	R	W	V	T	O	M	S	K	P	F	L	D
M	7	G	F	R	4	C	B	Q	S	3	N	Z	8	K	5	Y	H	D	I	W	9	X	T	V	P	L	J	E	0	A	M	U
N	T	R	X	G	L	V	D	U	Y	0	M	E	K	8	J	S	9	B	P	A	H	F	7	C	I	4	5	Z	3	W	N	Q
O	9	V	D	C	I	R	X	W	E	N	3	Y	5	J	8	Z	T	F	4	Q	7	B	H	G	L	P	K	S	M	U	0	A
P	R	T	U	7	3	9	W	X	K	4	I	5	Y	S	Z	8	V	A	N	B	C	Q	G	H	M	0	E	J	L	D	P	F
Q	J	Z	I	E	D	S	L	M	C	A	U	G	H	9	T	V	8	4	F	0	K	P	5	Y	X	B	7	R	W	3	Q	N
R	P	N	5	M	H	0	K	E	W	V	G	U	D	B	F	A	4	8	T	S	L	J	I	3	7	9	X	Q	C	Y	R	Z
S	B	A	H	W	5	Q	7	C	M	Z	Y	3	I	P	4	N	F	T	8	R	X	9	D	U	K	J	L	O	E	G	S	V
T	N	P	E	I	C	4	Y	5	D	9	7	X	W	A	Q	B	0	S	R	8	3	Z	M	L	G	V	U	F	H	K	T	J
U	5	E	P	Z	B	Y	4	N	V	W	Q	R	9	H	7	C	K	L	X	3	8	I	J	S	F	D	T	G	A	0	U	M
V	4	0	K	3	7	N	5	Y	U	R	C	W	X	F	B	Q	P	J	9	Z	I	8	L	M	H	T	D	A	G	E	V	S
W	K	Y	4	S	F	E	P	0	R	U	A	V	T	7	H	G	5	I	D	M	J	L	8	Z	B	X	9	C	Q	N	W	3
X	E	5	N	J	A	K	0	P	9	D	F	T	V	C	G	H	Y	3	U	L	S	M	Z	8	Q	W	R	7	B	4	X	I
Y	D	W	9	A	J	U	T	V	N	E	S	0	P	I	L	M	X	7	K	G	F	H	B	Q	8	5	4	3	Z	R	Y	C
Z	F	Q	7	U	K	A	H	G	3	S	E	M	L	4	P	0	B	9	J	V	D	T	X	W	5	8	I	N	Y	C	Z	R
3	H	C	B	V	P	G	F	A	Z	M	0	S	J	5	K	E	7	X	L	U	T	D	9	R	4	I	8	Y	N	Q	3	W
4	V	9	W	H	M	T	U	D	5	P	L	K	E	Z	S	J	R	Q	0	F	G	A	C	7	3	N	Y	8	I	X	4	B
5	U	X	R	F	S	D	V	T	4	K	J	P	0	3	M	L	W	C	E	H	A	G	Q	B	Z	Y	N	I	8	9	5	7
7	M	I	Z	P	V	L	S	J	B	H	T	F	A	W	U	D	3	Y	G	K	0	E	N	4	R	C	Q	X	9	8	7	5
8	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	3	4	5	7	8	9
9	0	4	Y	L	G	P	E	K	X	T	H	D	U	Q	A	F	N	Z	V	J	M	S	3	I	C	R	W	B	7	5	9	8

FIGURE 122a

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	3	4	5	7	8	9
A	7	G	F	R	4	C	B	Q	S	3	N	Z	8	K	5	Y	H	D	I	W	9	X	T	V	P	L	J	E	O	A	M	U
B	G	7	Q	T	0	H	A	F	8	L	P	J	S	Y	E	K	C	W	M	D	V	U	R	9	N	3	Z	5	4	B	I	X
C	F	Q	7	U	K	A	H	G	3	S	E	M	L	4	P	O	B	9	J	V	D	T	X	W	5	8	I	N	Y	C	Z	R
D	R	T	U	7	3	9	W	X	K	4	I	5	Y	S	Z	8	V	A	N	B	C	Q	G	H	M	0	E	J	L	D	P	F
E	4	0	K	3	7	N	5	Y	U	R	C	W	X	F	B	Q	P	J	9	Z	I	8	L	M	H	T	D	A	G	E	V	S
F	C	H	A	9	N	7	Q	B	J	I	4	8	Z	E	Y	5	G	U	3	X	R	W	V	T	O	M	S	K	P	F	L	D
G	B	A	H	W	5	Q	7	C	M	Z	Y	3	I	P	4	N	F	T	8	R	X	9	D	U	K	J	L	O	E	G	S	V
H	Q	F	G	X	Y	B	C	7	L	8	5	I	3	O	N	4	A	V	Z	9	W	R	U	D	E	S	M	P	K	H	J	T
I	S	8	3	K	U	J	M	L	7	F	D	H	G	R	V	T	Z	N	A	P	E	O	Y	5	W	Q	C	9	X	I	B	4
J	3	L	S	4	R	I	Z	8	F	7	9	B	Q	U	W	X	M	E	C	5	N	Y	O	P	V	G	A	D	T	J	H	K
K	N	P	E	I	C	4	Y	5	D	9	7	X	W	A	Q	B	O	S	R	8	3	Z	M	L	G	V	U	F	H	K	T	J
L	Z	J	M	5	W	8	3	I	H	B	X	7	C	V	R	9	S	O	Q	4	Y	N	E	K	U	A	G	T	D	L	F	P
M	8	S	L	Y	X	Z	I	3	G	Q	W	C	7	T	9	R	J	P	B	N	5	4	K	E	D	F	H	V	U	M	A	0
N	K	Y	4	S	F	E	I	3	O	U	A	V	T	7	H	G	5	I	D	M	J	L	8	Z	B	X	9	C	Q	N	W	3
O	5	E	P	Z	B	Y	4	N	V	W	Q	R	9	H	7	C	K	L	X	3	8	I	J	S	F	D	T	G	A	O	U	M
P	Y	K	0	8	Q	5	N	4	T	X	B	9	R	G	C	7	E	M	W	I	Z	3	S	J	A	U	V	H	F	P	D	L
Q	H	C	B	V	P	G	F	A	Z	M	0	S	J	5	K	E	7	X	L	U	T	D	9	R	4	I	8	Y	N	Q	3	W
R	D	W	9	A	J	U	T	V	N	E	S	O	P	I	L	M	X	7	K	G	F	H	B	Q	8	5	4	3	Z	R	Y	C
S	I	M	J	N	9	3	8	Z	A	C	R	Q	B	D	X	W	L	K	7	Y	4	5	P	O	T	H	F	U	V	S	G	E
T	W	D	V	B	Z	X	R	9	P	5	8	4	N	M	3	I	U	G	Y	7	Q	C	A	F	S	E	O	L	J	T	K	H
U	9	V	D	C	I	R	X	W	E	N	3	Y	5	J	8	Z	T	F	4	Q	7	B	H	G	L	P	K	S	M	U	O	A
V	X	U	T	Q	8	W	9	R	O	Y	Z	N	4	L	I	3	D	H	5	C	B	7	F	A	J	K	P	M	S	V	E	G
W	T	R	X	G	L	V	D	U	Y	0	M	E	K	8	J	S	9	B	P	A	H	F	7	C	I	4	5	Z	3	W	N	Q
X	V	9	W	H	M	T	U	D	5	P	L	K	E	Z	S	J	R	Q	O	F	G	A	C	7	3	N	Y	8	I	X	4	B
Y	P	N	5	M	H	O	K	E	W	V	G	U	D	B	F	A	4	8	T	S	L	J	I	3	7	9	X	Q	C	Y	R	Z
Z	L	3	8	0	T	M	J	S	Q	G	V	A	F	X	D	U	I	5	H	E	P	K	4	N	9	7	B	W	R	Z	C	Y
3	J	Z	I	E	D	S	L	M	C	A	U	G	H	9	T	V	8	4	F	O	K	P	5	Y	X	B	7	R	W	3	Q	N
4	E	5	N	J	A	K	O	P	9	D	F	T	V	C	G	H	Y	3	U	L	S	M	Z	8	Q	W	R	7	B	4	X	I
5	0	4	Y	L	G	P	E	K	X	T	H	D	U	Q	A	F	N	Z	V	J	M	S	3	I	C	R	W	B	7	5	9	8
7	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	3	4	5	7	8	9
8	M	I	Z	P	V	L	S	J	B	H	T	F	A	W	U	D	3	Y	G	K	O	E	N	4	R	C	Q	X	9	8	7	5
9	U	X	R	F	S	D	V	T	4	K	J	P	0	3	M	L	W	C	E	H	A	G	Q	B	Z	Y	N	I	8	9	5	7

FIGURE 122b

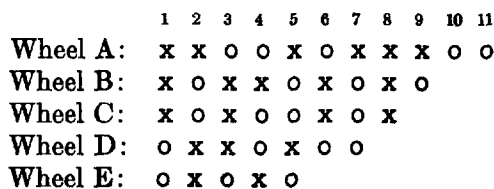


FIGURE 123

If these wheels are aligned at their initial positions as shown in Fig. 123, and if each wheel moves one step at each operation, the following would be the generation of the first 35 elements of key:³

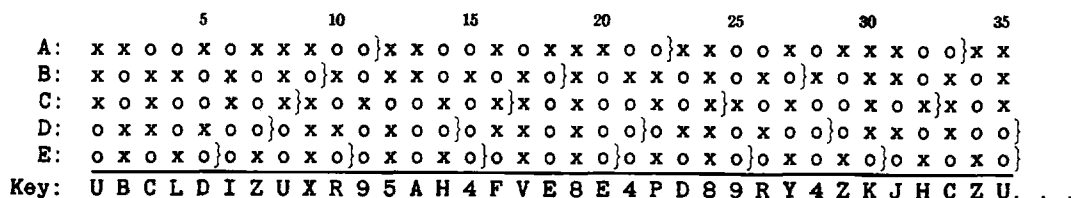


FIGURE 124.—Machine "A"

³ The braces in the diagram mark the cyclic repetitions of the five wheels.

Since the wheel sizes are relatively prime and each wheel moves one step at each operation, the length of the total key is  $11 \times 9 \times 8 \times 7 \times 5 = 27,720$ . Of the total of 40 pins on the five wheels, 20 are in the active position; nevertheless, the generated key is not flat, because in the A and B wheels there is a slight bias ( $6/11$  and  $5/9$ , respectively) in favor of a "+", while in the D and E wheels there is a slightly stronger bias ( $4/7$  and  $3/5$ ) in favor of a "-". Thus the highest probability, that of a key of A (=xxooo), is  $\frac{6 \times 5 \times 4 \times 4 \times 3}{27,720} = .0519$ , as compared with the random expectancy of  $1/32$  or 0.03125; this same probability will also hold for a key of U (=xxxoo), since the probability of either a mark or a space in the third level is 0.5. On the other hand, the lowest probability is that of a key of M (=ooxxx) or O(=oooxx), which is  $\frac{5 \times 4 \times 4 \times 3 \times 2}{27,720} = 0.0173$ . The gamma ( $\gamma$ ) I.C. of this key is  $\frac{32 \sum f^2}{27720^2} = 1.083$ , showing that the key is anything but flat, as has already been surmised.⁴ In its Baudot character form, UBCLDIZUXR . . ., nothing is discernible in the foregoing key; but if the component mark and space impulses are written out in the five levels as in Fig. 124, the cyclic repetitions may clearly be seen.

b. In order to increase the cryptosecurity of machine "A", the wheels might be used *in combination* to produce key for the five Baudot levels. In Fig. 125a, below, are the *wheel streams* of the "A" machine set at the same initial position and advancing one step after each operation. In Fig. 125b are the *key streams* for the five levels produced by adding wheels A and B together for the key of level 1, adding B and C for the key of level 2, C and D for level 3, D and E for level 4, and E and A for level 5. In this stretch of key, no cyclic repetitions are observable in the five levels: the first level has a period of  $11 \times 9 = 99$ ; the second, 72; the third, 56; the fourth, 35; and the fifth, 55. The total cycle is, of course, 27,720, since the motion of the wheels in this machine is the same as that of the "A" machine in Fig. 124.

	5	10	15	20	25	30	35
A:	x x o o x o x x x o o}	x x o o x o x x x o o}	x x o o x o x x x o o}	x x o o x o x x x o o}	x x o o x o x x x o o}	x x o o x o x x x o o}	x x
B:	x o x x o x o x o}	x o x x o x o x o}	x o x x o x o x o}	x o x x o x o x o}	x o x x o x o x o}	x o x x o x o x o}	x o x x o x o x
C:	x o x o o x o x}	x o x o o x o x}	x o x o o x o x}	x o x o o x o x}	x o x o o x o x}	x o x o o x o x}	x o x
D:	o x x o x o o}	o x x o x o o}	o x x o x o o}	o x x o x o o}	o x x o x o o}	o x x o x o o}	o x x o x o o}
E:	o x o x o}	o x o x o}	o x o x o}	o x o x o}	o x o x o}	o x o x o}	o x o x o}

FIGURE 125a

	5	10	15	20	25	30	35
A+B:	x o o o o o o x o o x x x x o o o o x o o o o x x o o o o x x x o o x						
B+C:	x x x o x x x x o o o o o o o o x x x x o x x x o o o o x x o o x x x						
C+D:	o o x x o o x o x o o o x o x x x x x x o o x o o o x x x o o x x o						
D+E:	x x o o o x o x x o x x x o x o x x x x x o o x x o o x o o o o o o x						
E+A:	<u>o x x o o x x o x x x x o o x o o o x o x o o x x x x x o o o x x o</u>						
Key:	J G P 9 4 G P J M T B B F E M 9 C C 8 C M 4 4 8 B T T M P U E E P P J . . .						

FIGURE 125b.—Machine "B"

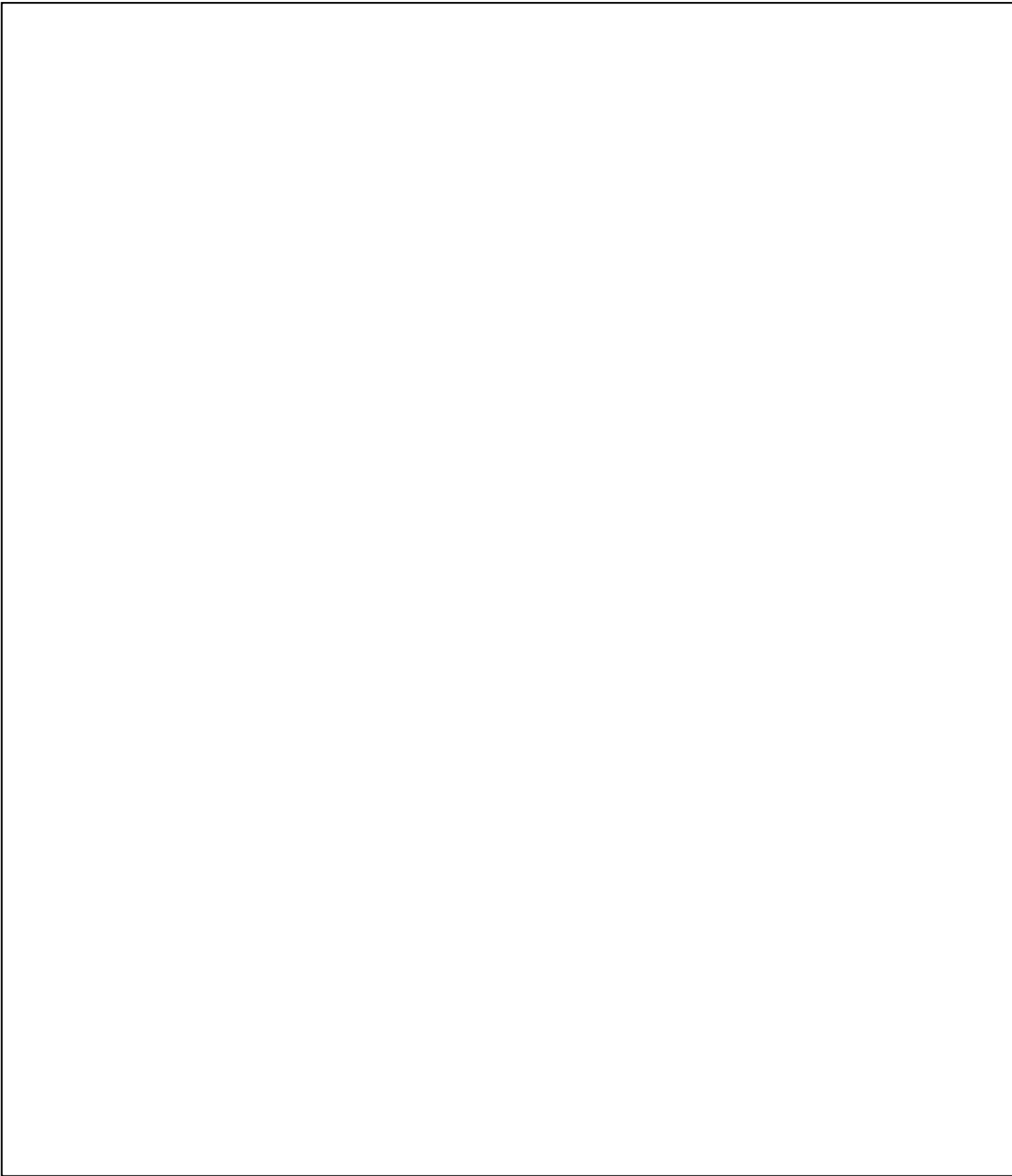
c. Since the wheels as combined in the "B" machine produce levels of periods 99, 72, 56, 35, and 55, it might be desirable to extend the periods where possible. This may be done by the simple expedient of combining the longest wheel, A, with the other four wheels for four of the levels, and combining wheel B with C for the fifth level. This produces the following key:

	5	10	15	20	25	30	35
A+B:	x o o o o o o x o o x x x x o o o o x o o o o x x o o o o x x x o o x						
A+C:	x o o x o o o x x x o o o o x x o o x o x o o x o x x x o x o o o o x						
A+D:	o x o x x x o x o x x o x x x o o x o x x x x x o o x o x x x o o o						
A+E:	o x x o o x x o x x x x o o o x o o o x o x o o x x x x x o o o x x o						
B+C:	<u>x x x o x x x x o o o o o o o o x x x x o o o o o o x x o o x x x</u>						
Key:	W M O I H M O W C R F F E S C I T T 8 T C H H 8 F R R C O Q S S O O W . . .						

FIGURE 126.—Machine "C"

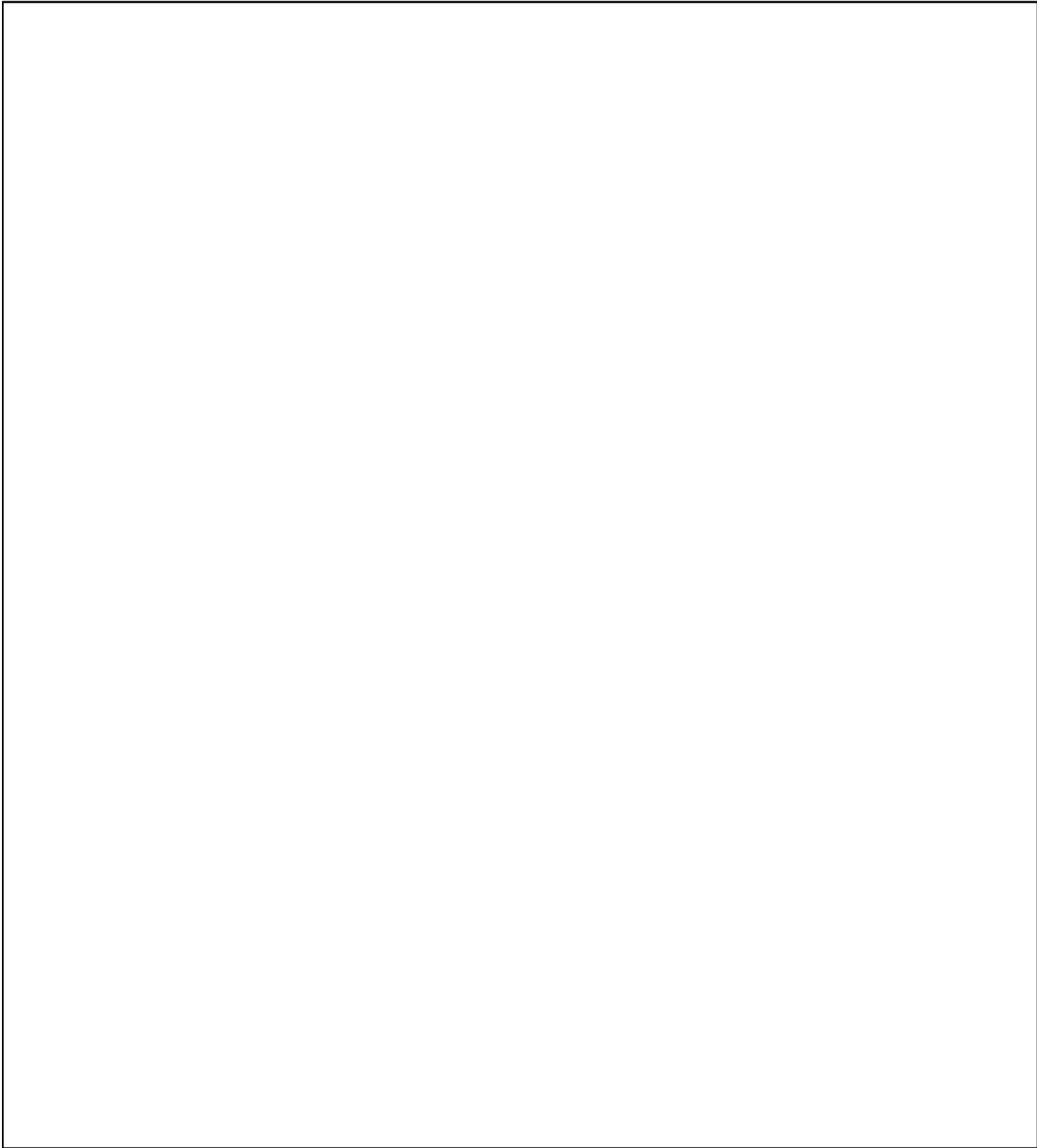
⁴ Since we are concerned with the universe or total population of this key, the correct statistic to be computed is the gamma I.C., not the delta I.C., which is that for a sampling of a universe.





(b) (1)  
(b) (3)-18 USC 798  
(b) (3)-50 USC 3024(i)  
(b) (3)-P.L. 86-36





(b) (1)  
(b) (3)-18 USC 798  
(b) (3)-50 USC 3024(i)  
(b) (3)-P.L. 86-36



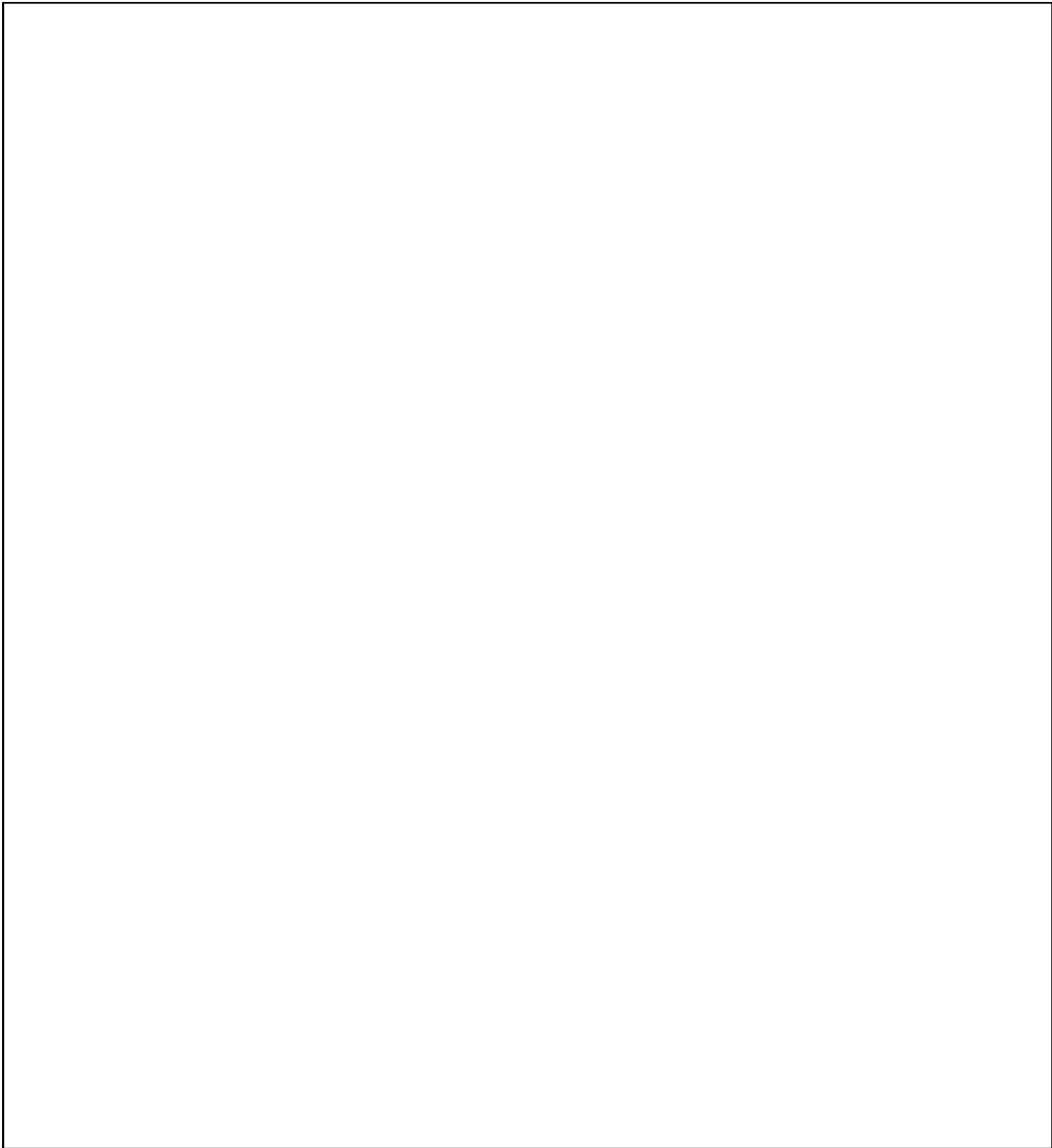
(b) (1)  
(b) (3)-18 USC 798  
(b) (3)-50 USC 3024 (i)  
(b) (3)-P.L. 86-36

(b) (1)  
(b) (3)-18 USC 798  
(b) (3)-50 USC 3024 (i)  
(b) (3)-P.L. 86-36

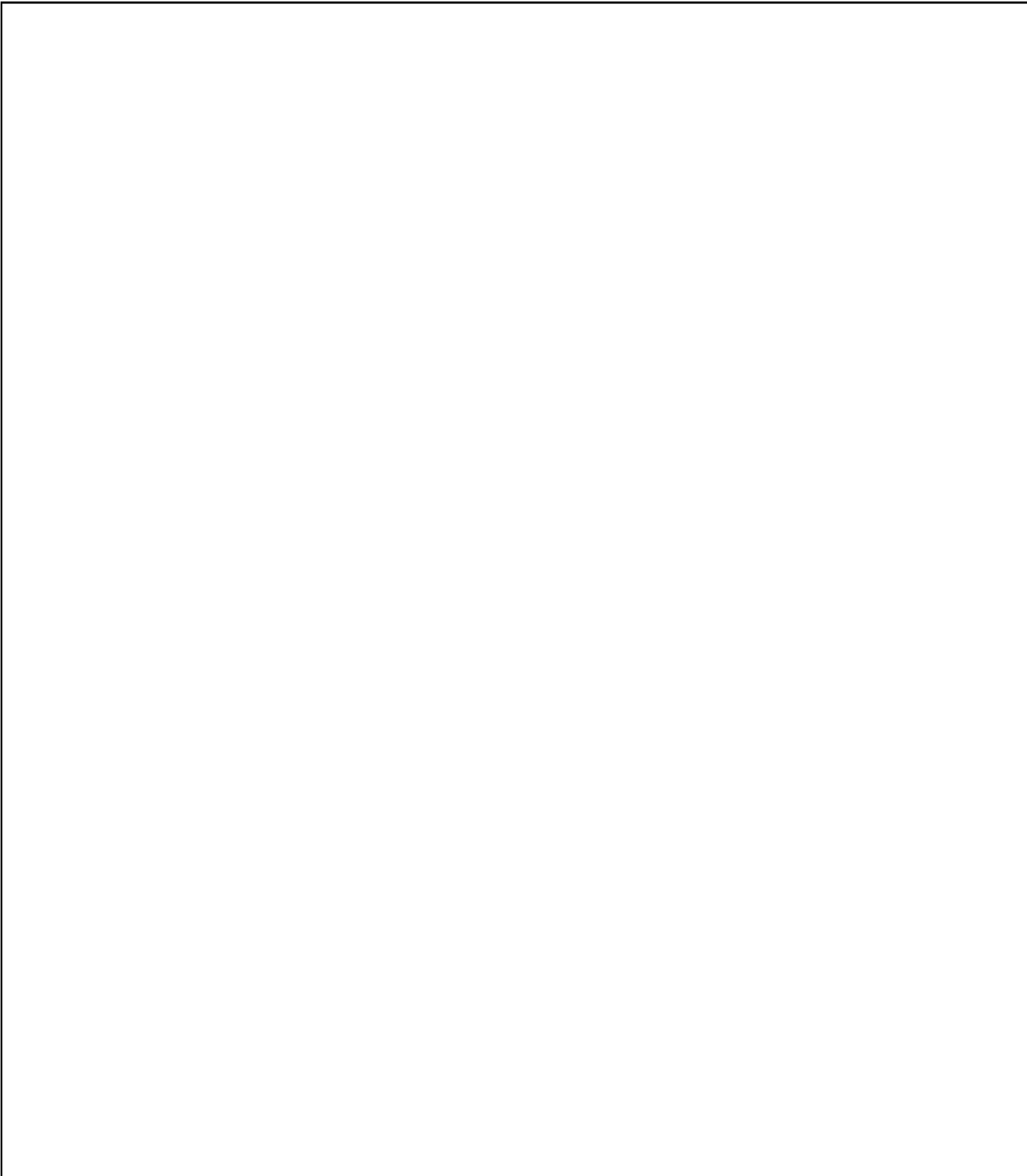


(b) (1)  
(b) (3)-18 USC 798  
(b) (3)-50 USC 3024 (i)  
(b) (3)-P.L. 86-36





(b) (1)  
(b) (3) -18 USC 798  
(b) (3) -50 USC 3024(i)  
(b) (3) -P.L. 86-36



(b) (1)  
(b) (3)-18 USC 798  
(b) (3)-50 USC 3024 (i)  
(b) (3)-P.L. 86-36

65. Analysis of combination streams.—a. Let us assume that we have

recovered the 35 elements of key of the "B" machine shown in Fig. 125b.

Key level 1 is as follows:

	5	10	15	20	25	30	35
x	o o o o o	x o o	x x x	x o o o o	x o o o o	x x o o o	x x x o o x

No cyclic phenomena are observable in this stream of binary impulses (also called binary digits or "bits"), and the conjecture is made that, unless a single wheel of size 34 or larger is involved, the stream might have been produced in a cipher teleprinter by the interaction of two regularly stepping wheels of different sizes.¹⁰ Consequently, the stream of bits is written on various trial widths, commencing with a width of 5 (see Fig. 136a, below). Now in each one of the width write-outs we will add the first row of bits to

1 2 3 4 5	1 2 3 4 5 6	1 2 3 4 5 6 7	1 2 3 4 5 6 7 8	1 2 3 4 5 6 7 8 9
x o o o o	x o o o o o	x o o o o o o	x o o o o o o x	x o o o o o o x o
o o x o	o x o o x x	x o o x x x x	o x x x x o o	o x x x x o o o
x x x x o	x x o o o o	o o o o x o o	o o x o o o o x	x o o o o x x o o
o o o x o	x o o o o x	o o x x o o o	x o o o o x x x	o o x x x o o x
o o o x x	x o o o o x	o x x x o o x	o o x	
o o o x	x x o o x			
x x o x				

FIGURE 136a

¹⁰ If we had recovered enough key, we could have noticed that the KL1 stream repeated after 99 positions.

(b) (1)
(b) (3)-18 USC 798
(b) (3)-50 USC 3024(i)
(b) (3)-P.L. 86-36

the second, the second row to the third, and so on. Since in binary arithmetic addition is identical with subtraction, this produces what amounts to a delta or difference stream at the particular interval, e.g., a "delta 9" (abbreviated  $\Delta_9$ ). At the correct assumption of the length of one of the wheels, the length of the other wheel will be disclosed by a repetition in the delta stream.¹¹ In Fig. 136b we show the

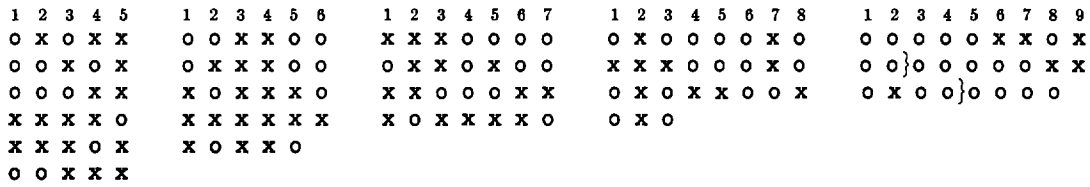


FIGURE 136b

delta streams as derived from the width write-outs of Fig. 136a; in the width write-out of 9, an 11-long delta repetition may be seen, thus proving that the sizes of the wheels involved are 9 and 11.

b. Knowing that the lengths of the wheels are 9 and 11, we can now recover the wheel patterns. We write the KL1 key stream on either one of the two widths, say 9. The first key element, "x", is assumed to have arisen from a combination of an "x" with an "x" on the two wheels; on this assumption, an "x" is recorded in the A-wheel portion of our diagram of the key write-out, and also at the beginning of every cyclic repetition of the other wheel. This is shown in Fig. 137a, below:

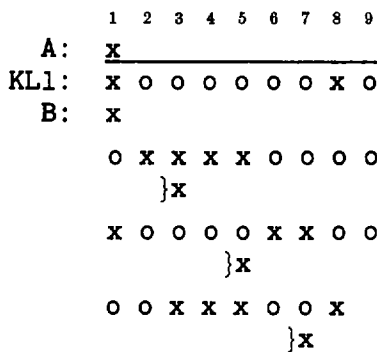


FIGURE 137a

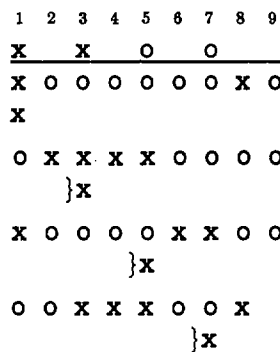


FIGURE 137b

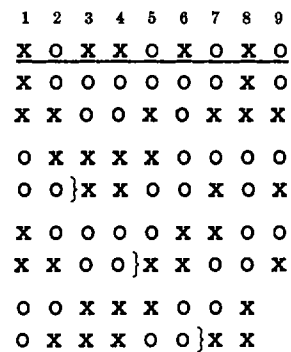


FIGURE 137c

The placement of the "x" impulses at the beginnings of the B-wheel streams enables us to derive three more values for the A wheel, as shown in Fig. 137b; the complete patterns of the two wheels are then quickly recovered, as shown in Fig. 137c. These are either the true patterns, or their inverse, since our assumption in Fig. 137a of an "x" on the two wheels to make the first "x" in the key stream was arbitrary—there is no way of proving this point.

c. The solution of the remaining wheels of the machine continues in similar fashion with the procedure just illustrated; or, if the cryptanalyst has a hunch that the 9- or 11-wheel has been used for another key level, perhaps level 2, he might try writing this level out under the two wheel patterns just recovered, as shown below:

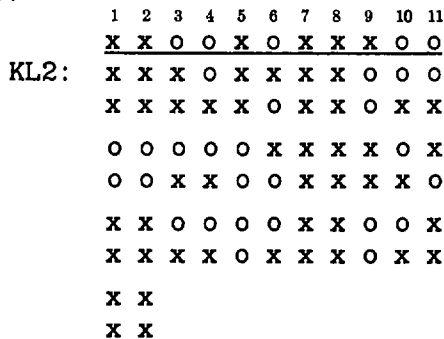


FIGURE 138a

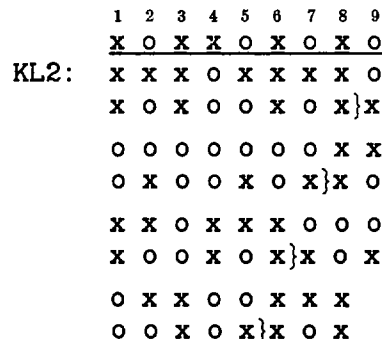


FIGURE 138b

¹¹ See also in this connection subpar. 97i on p. 301 of *Military Cryptanalytics, Part II*, with reference to the solution of a two-tape Baudot system.





e. In Figs. 140a and b, below, are shown two more incorrect assumptions (11-5 and 11-7), with conflicts indicated by the ringed values—one conflict is all it takes. (Note that we do not require all 35 elements of the recovered key level: it will suffice for our purposes to use just enough of the key stream to insure two or three values in each of the columns.) Finally, we have in Fig. 140c, below, the correct assumption of wheel sizes (11-9); there are no conflicts, and the two wheel patterns have been completely recovered:

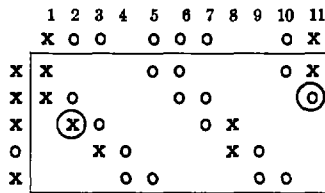


FIGURE 140a

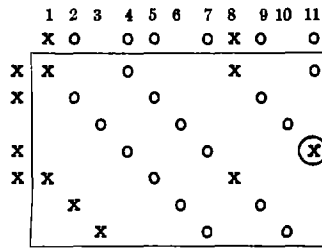


FIGURE 140b

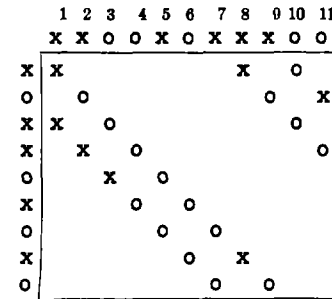


FIGURE 140c

f. As mentioned before, the wheels recovered will either be the true patterns, or their inverse: solution can be gotten either way. One thing that is proved, however, is the particular rule of combination, whether it is Vernam or mod 2. In subpars. b-e we assumed the Vernam rule, and it worked. But suppose we had used the mod 2 rule? As an example, let us take the situation of Fig. 137a, but with the incorrect rule. In Fig. 141a we assume that the first element of KL1, an "x", is the result of the combination of an "x" with an "o"; in Fig. 141b is the completed diagram with the patterns of the two wheels:

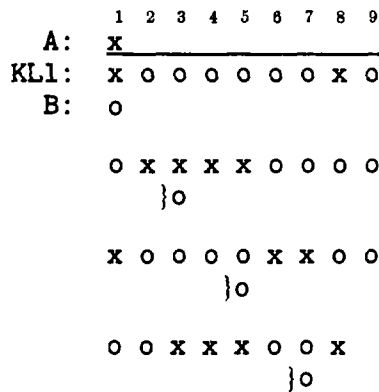


FIGURE 141a

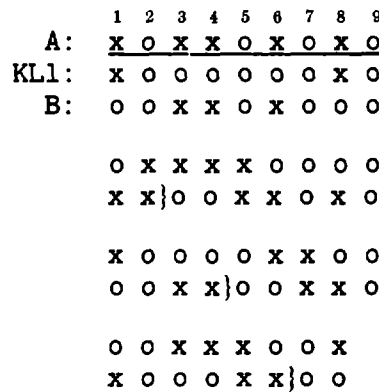


FIGURE 141b

It can be seen in Fig. 141b that, whereas one of the wheels (the 9-wheel) has the true pattern, the other has the inverse pattern, so it would be patently impossible to reconstruct the machine with an incorrect and incompatible "recovery". But the proof of Vernam addition has been evidenced from the start, had we been more observant—and had we known the earmarks—from the sample of 35 elements of the "B" machine key in Fig. 125b that we were analyzing: all the Baudot characters contain 1, 3, or 5 mark impulses, never 0, 2, or 4. Thus there is a maximum of only 16 different characters that can occur (there were actually only 13 in the sample). (Had mod-2 addition been involved, all the Baudot key characters would have been composed of 0, 2, or 4 marks.) The reason for this is not difficult to ascertain: because each wheel in our machine is present an even number of times during the formation of a Baudot character, it follows that the binary sum of the contribution of each wheel is an "x" (in the case of Vernam addition) or an "o" (in the case of mod-2 addition).¹⁴ As an example, the first key character in Fig. 125b

¹⁴ This observation holds true only if the wheels have single key-reading stations; if there are two or more reading stations it cannot be guaranteed (except in certain special cases) that the binary sum of the contribution of each wheel will be an "x".



<u>Levels</u>	5	10	15	20	25	30	35
123:	o o x x x x o o x o x o x o o o o x x x o o x x x o x o o o x o x o o						
124:	o x o x o } o x o x o } o x o x o } o x o x o } o x o x o } o x o x o } o x o x o }						
125:	x o o o x x x x o o o x x x x x x o x o x o x x o o x x x o o x o x o x x						
134:	x o x x o x o x o } x o x x o x o x o } x o x x o x o x o } x o x x o x o x o }						
135:	o x x o x o o } o x x o x o o } o x x o x o o } o x x o x o o } o x x o x o o }						
145:	o o o o o x x o x x x o x x o x o x x x o x o x x x o o x x x o x o x o						
234:	o o o x o x x o o o o x o o x o o x x x x x o x o o x x x x x o o x o						
235:	x x o o x o x x x o o } x x o o x o x x x o o } x x o o x o x x x o o } x x						
245:	x o x o o x o x } x o x o o x o x } x o x o o x o x } x o x o o x o x } x o x						
345:	o x o o o x o o x o x o x o x o x o x o x o x o x o x o x o x o x o x o						
12345:	x x x o o o o x o o x o o o x x o x x x x x o x x o x x o o x o x o x o						

FIGURE 142b

Now let us examine what brought this about, since we know the answer from Fig. 127. The sum of levels 124 yielded the 5-wheel, so we shall set down the arithmetic involved:

KL1 is composed of wheels A, B, C  
 KL2 is composed of wheels B, C, D  
 KL4 is composed of wheels A, D, E  
 The sum, by cancellation: E

It can be seen that by summing key levels 1, 2, and 4, four of the wheels are cancelled, leaving the E wheel alone in the residue. Similarly, the other four wheels are exposed uniquely in the residues of the following combinations of key levels:

KL1: A,B,C	KL1: A,B,C	KL2: B,C,D	KL2: B,C,D
KL3: C,D,E	KL3: C,D,E	KL3: C,D,E	KL4: A, D,E
KL4: <u>A, D,E</u>	KL5: <u>A,B, E</u>	KL5: <u>A,B, E</u>	KL5: <u>A,B, E</u>
Sum: B	Sum: D	Sum: A	Sum: C

If we study the following diagram of all the combinations of five wheels taken three at a time, plus the one combination of all five wheels taken together,

1. A B C - -
2. A B - D -
3. A B - - E
4. A - C D -
5. A - C - E
6. A - - D E
7. - B C D -
8. - B C - E
9. - B - D E
10. - - C D E
11. A B C D E

it may be seen that if we add any *two* of these lines together, we shall have an *even* number of wheels in the answer; and if we add any *three* lines together, we shall have an *odd* number of wheels in the answer.¹⁵ The reason for the inclusion of line 11 (summing all five wheels together) may be shown if we had to contend with the following combinations composing the level key streams, for example:

- |             |              |
|-------------|--------------|
|             | 1. A B C - - |
|             | 2. A B - D - |
| Key levels: | 3. A B - - E |
|             | 4. A - C D - |
|             | 5. - B C - E |

¹⁵ This answer is really a function of the number of reading stations involved, not the number of wheels, but in this case the two are synonymous.







In Fig. 145, below, we have written KL5 out on several trial widths, and at the bottom of each column we have recorded the *product* of the entries in the column, i.e., the combination according to the *multiplication rule* (oo, ox, xo = o); in other words, we record an "x" only if *every* impulse in the column is an "x", otherwise we record an "o".

1	2	3	4	5	1	2	3	4	5	6	1	2	3	4	5	6	7	1	2	3	4	5	6	7	8	1	2	3	4	5	6	7	8	9	10	11				
x	x	o	x	x	x	x	o	x	x	o	x	x	o	x	x	o	x	x	x	o	x	x	o	x	x	x	x	o	x	x	o	x	x	o	x	x	o			
o	x	x	x	o	x	x	o	x	x	o	x	x	o	x	x	o	x	o	o	x	x	o	x	x	x	x	o	x	x	o	x	x	o	x	x	o				
o	x	x	x	o	x	x	o	x	x	o	o	x	x	x	x	o	x	x	o	x	x	o	x	x	x	x	o	x	x	o	x	x	o	x	x	o				
x	x	x	x	x	x	x	o	x	x	x	o	o	x	o	x	x	x	x	x	o	x	x	x	x	x	x	x	o	x	x	x	x	x	o	x	x	o			
o	x	x	x	o	o	o	x	o	x	x	x	x	x	x	o	x	x	o	x	o	x	x	x	x	x	x	x	o	x	o	x	x	x	x	o	x	x	o		
o	x	o	x	x	x	x	o	x	x	o	o	x	x	x	x	x	x	x	o	x	x	x	x	o	x	x	o	x	o	x	x	x	o	x	x	o				
x	x	o	x	x	x	x	x	x	x	x	o	x	x	x	o	x	x	o	x	x	x	o	x	x	<u>x</u>	<u>x</u>	<u>x</u>	<u>o</u>												
x	x	o	x	x	o	x	x	x	x	o	o	x	x	x	o	x	o	x	x	x	o	x	x	x	<u>o</u>	<u>o</u>	<u>x</u>	<u>x</u>	<u>o</u>											
x	x	o	x	o	o	x	x	o	x	x	<u>x</u>	<u>o</u>	<u>o</u>	<u>x</u>	<u>x</u>	<u>o</u>	<u>o</u>	<u>o</u>	<u>o</u>	<u>o</u>	<u>o</u>	<u>o</u>	<u>o</u>	<u>o</u>																
x	x	x	x	o	o	x	x	x	o	o	o	o	o	o	o	o																								
x	x	o	x	x	<u>x</u>	<u>x</u>	<u>x</u>	<u>o</u>																																
o	x	x	x	o	o	o	o	o	o	o																														
<u>o</u>	<u>x</u>	<u>x</u>	<u>x</u>	<u>o</u>																																				
o	x	o	x	o																																				

FIGURE 145

It may be seen that in the write-outs of the correct widths (5 and 11), the patterns of the wheels are manifested; on any incorrect width, the sum of every column will be an "o", unless the amount of material available for analysis is too limited.

i. If only one wheel of a two-wheel Boolean summation stream had been recovered, the procedure is still simple. Suppose that in the preceding subparagraph we had neglected to try a width of 5, and that only the 11-wheel had been uncovered. We would write the cycles of the 11-wheel over the key stream, leaving a blank row in the middle for insertion of values from the other component wheel; these values are inserted in the unknown wheel stream ("?W") only when they are unambiguous on the Boolean assumption, i.e., when there is at least one "o" at a given position in the superimposed 11W and K streams, so that oo = o, and ox or xo = x. Thus:

		5		10		15		20		25		30		35																	
11W:	x	x	o	o	x	o	x	x	x	o	o	x	x	o	o	x	x	o	o	x	x	o	o	x	x	o	o	x	x		
?W:		<u>o</u>	<u>x</u>	<u>o</u>		<u>o</u>	<u>o</u>	<u>x</u>	<u>o</u>	<u>x</u>		<u>o</u>	<u>x</u>	<u>o</u>	<u>o</u>	<u>o</u>	<u>o</u>	<u>x</u>	<u>o</u>				<u>x</u>	<u>o</u>							
K:	x	x	o	x	x	o	x	x	x	o	o	x	x	x	o	o	x	x	o	o	x	x	o	o	x	x	o	o	x	x	
11W:		40		45		50		55		60		65		70																	
11W:	o	o	x	o	x	x	x	o	o	x	x	o	o	x	x	x	o	o	x	x	o	o	x	x	o	o	x	x	o	o	
?W:	<u>o</u>	<u>x</u>	<u>x</u>		<u>o</u>	<u>x</u>	<u>x</u>	<u>o</u>	<u>o</u>	<u>x</u>	<u>o</u>	<u>o</u>	<u>x</u>	<u>o</u>	<u>o</u>	<u>o</u>	<u>o</u>	<u>o</u>	<u>o</u>	<u>o</u>	<u>o</u>	<u>o</u>	<u>o</u>	<u>o</u>	<u>o</u>	<u>o</u>	<u>o</u>	<u>x</u>	<u>o</u>		
K:	o	x	x	x	x	x	o	x	x	x	x	o	x	o	x	x	o	x	x	o	x	x	o	x	x	o	x	x	o	x	x

From the location of the "x" and "o" entries in the middle row, we are able to eliminate wheel sizes for the unknown wheel on the basis of conflicts. For example, sizes 2, 6, and 7 are ruled out because of the clash of the "x" bit at position 4 with the "o" bits at positions 6, 10, and 11. The tabulation of wheel sizes eliminated up to 20 is shown below:

W	Positions	W	Positions	W	Positions	W	Positions
2	4-6	7	4-11	12	10-22	17	4-21
3	22-25	8	6-14	13	26-39	18	21-39
4	22-26	9	17-26	14	3-17	19	14-33
5		10		15		20	
6	4-10	11	3-14	16	3-22		



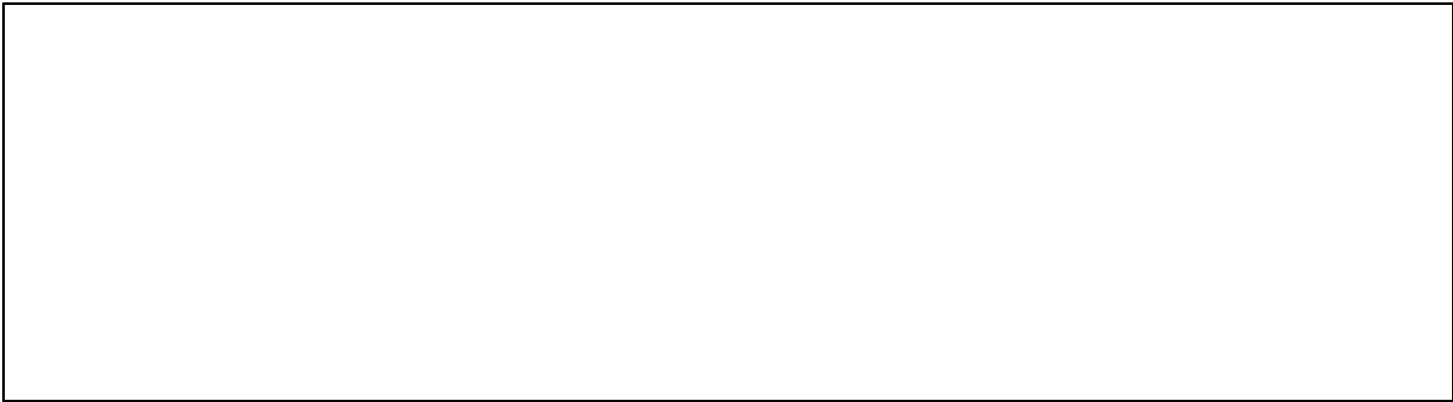
The absence of conflicts at an interval of 5 and any of its multiples points to the size of the unknown wheel; this is substantiated when we write out the partial bit stream on a width of 5, the bits in the columns being combined by the multiplication rule to disclose the pattern of the wheel:

1	2	3	4	5
		O	X	
O				O
O		X	O	
	X			
O	X			O
O	O			
	X	O		
O	X	X		
		O	X	
	X	O	O	
			X	O
		O	X	
O				O
<u>O</u>			<u>X</u>	<u>O</u>
O	X	O	X	O

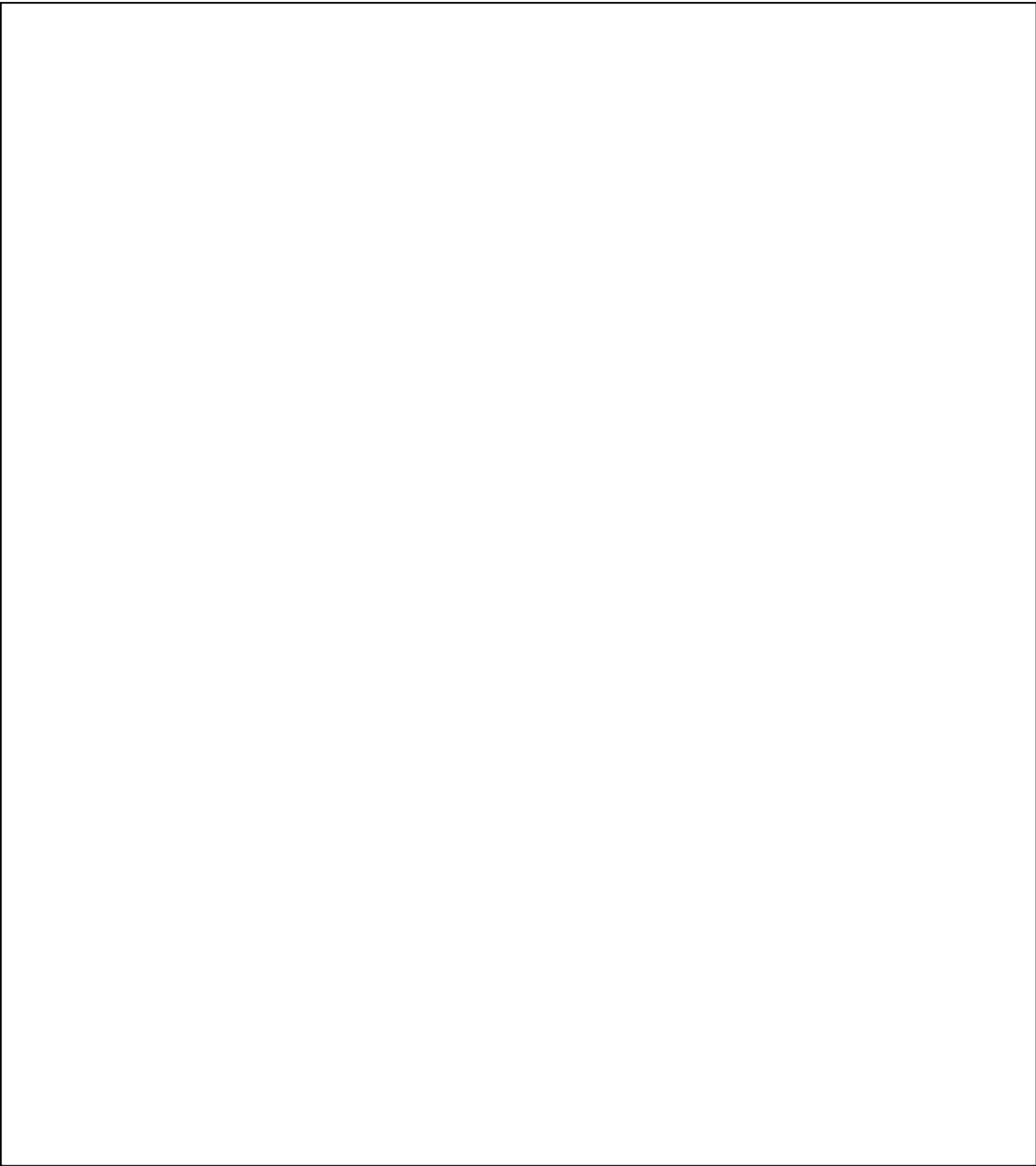
Notice that if we write the partial stream on widths of 10 or 15 the cyclic pattern of oxoxo is still clear in the product line, even though in the writeout on a width of 15 it is incomplete because of lack of sufficient material (this latter point must not be forgotten when dealing with limited amounts of data):

1	2	3	4	5	6	7	8	9	10
		O	X	O					O
O		X	O		X				
O	X		O	O		O			
	X	O		O	X	X			
		O	X		X	O	O		
		X	O		O	X			
<u>O</u>			O	O			X	O	
O	X	O	X	O	O	X	O	X	O

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
		O	X	O				O	O			X	O	
	X			O	X			O	O		O			
	X	O		O	X	X				O	X			
	X	O	O			X	O			O	X			
<u>O</u>			O	O		X	O							
O	X	O	X	O	O	X	X	O	O	O	O	X	O	

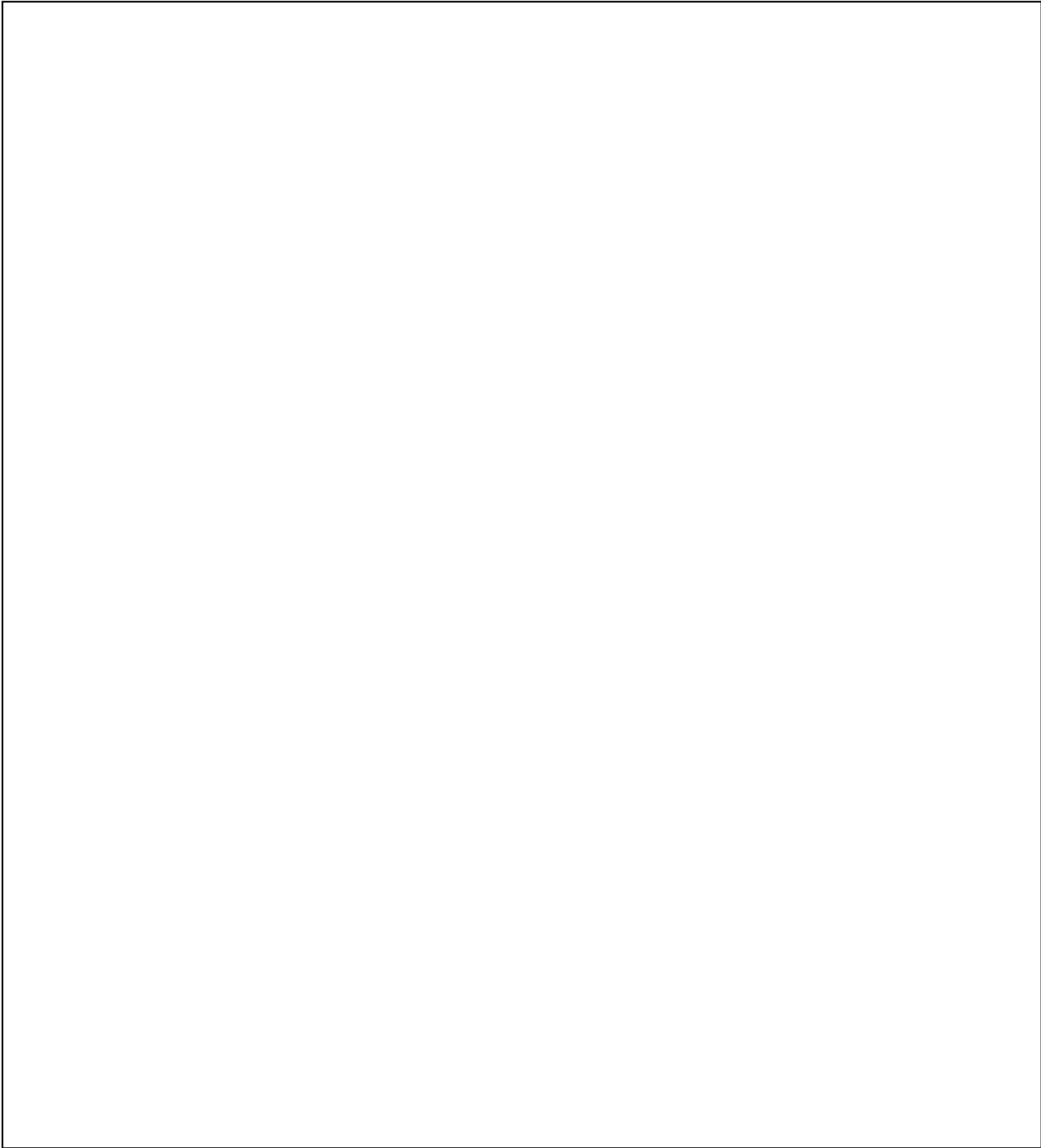


(b) (1)  
 (b) (3)-18 USC 798  
 (b) (3)-50 USC 3024(i)  
 (b) (3)-P.L. 86-36



(b) (1)  
(b) (3)-18 USC 798  
(b) (3)-50 USC 3024(i)  
(b) (3)-P.L. 86-36

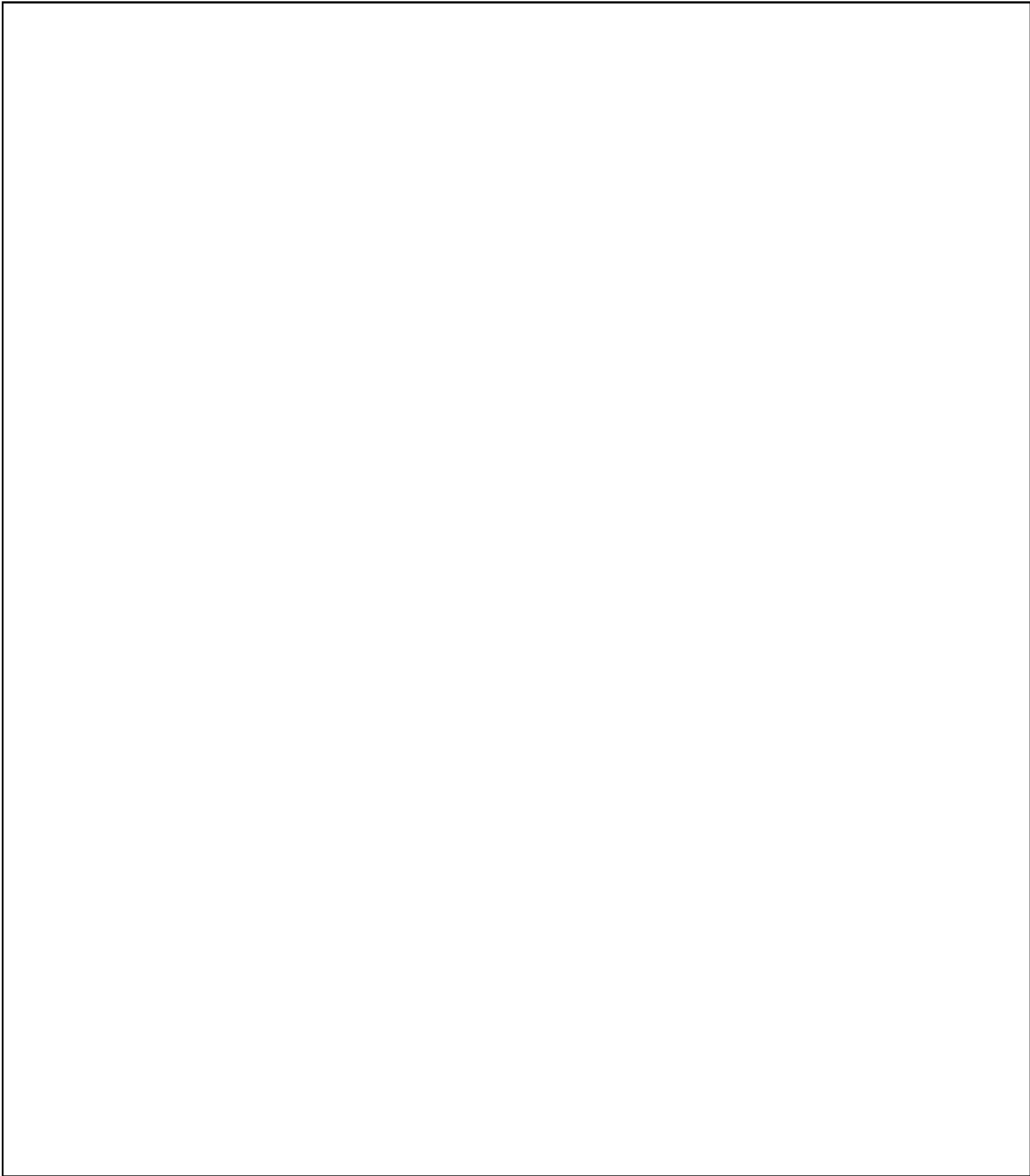
(b) (1)  
(b) (3) -18 USC 798  
(b) (3) -50 USC 3024 (i)  
(b) (3) -P.L. 86-36



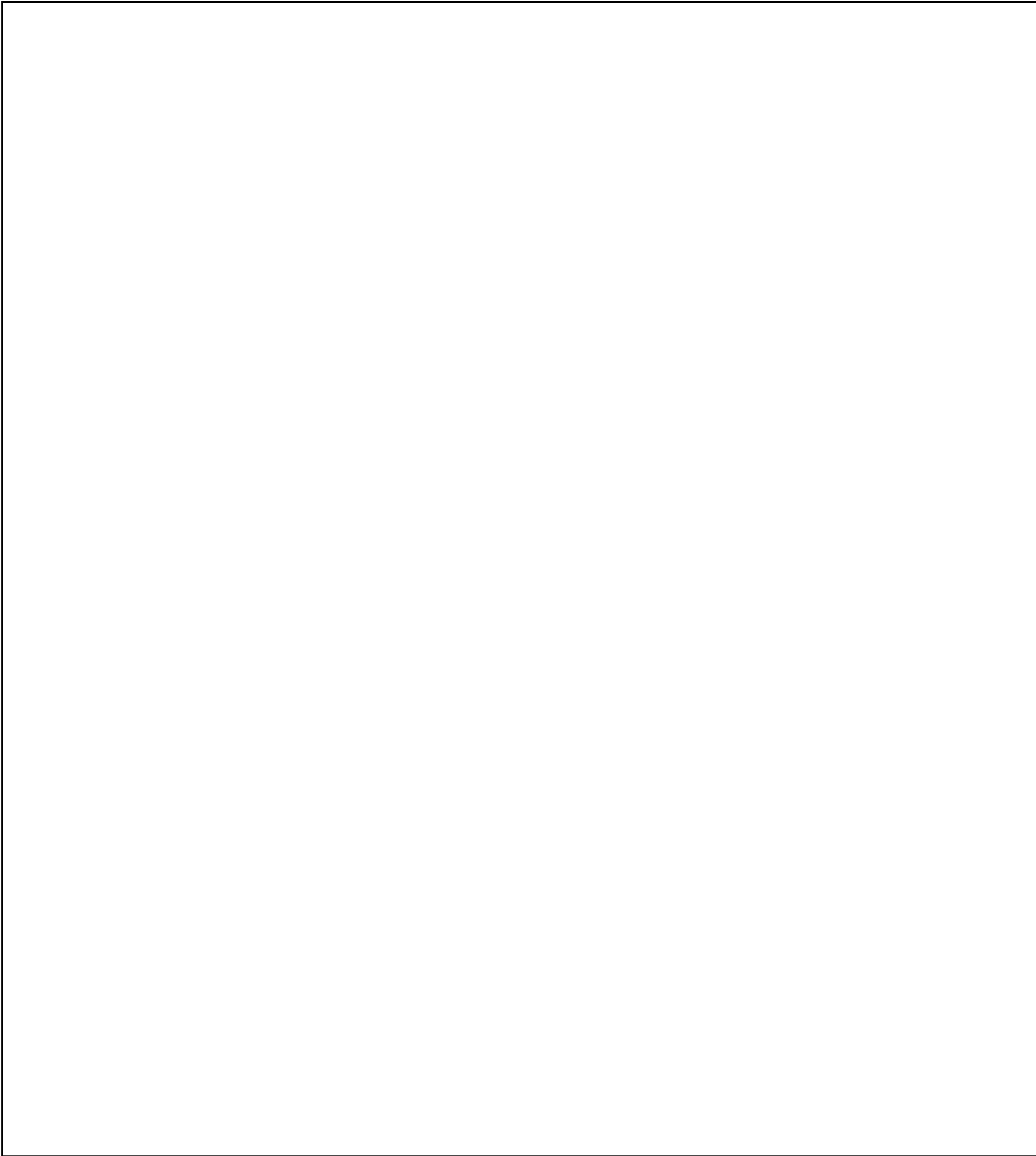
(b) (1)  
(b) (3) -18 USC 798  
(b) (3) -50 USC 3024 (i)  
(b) (3) -P.L. 86-36



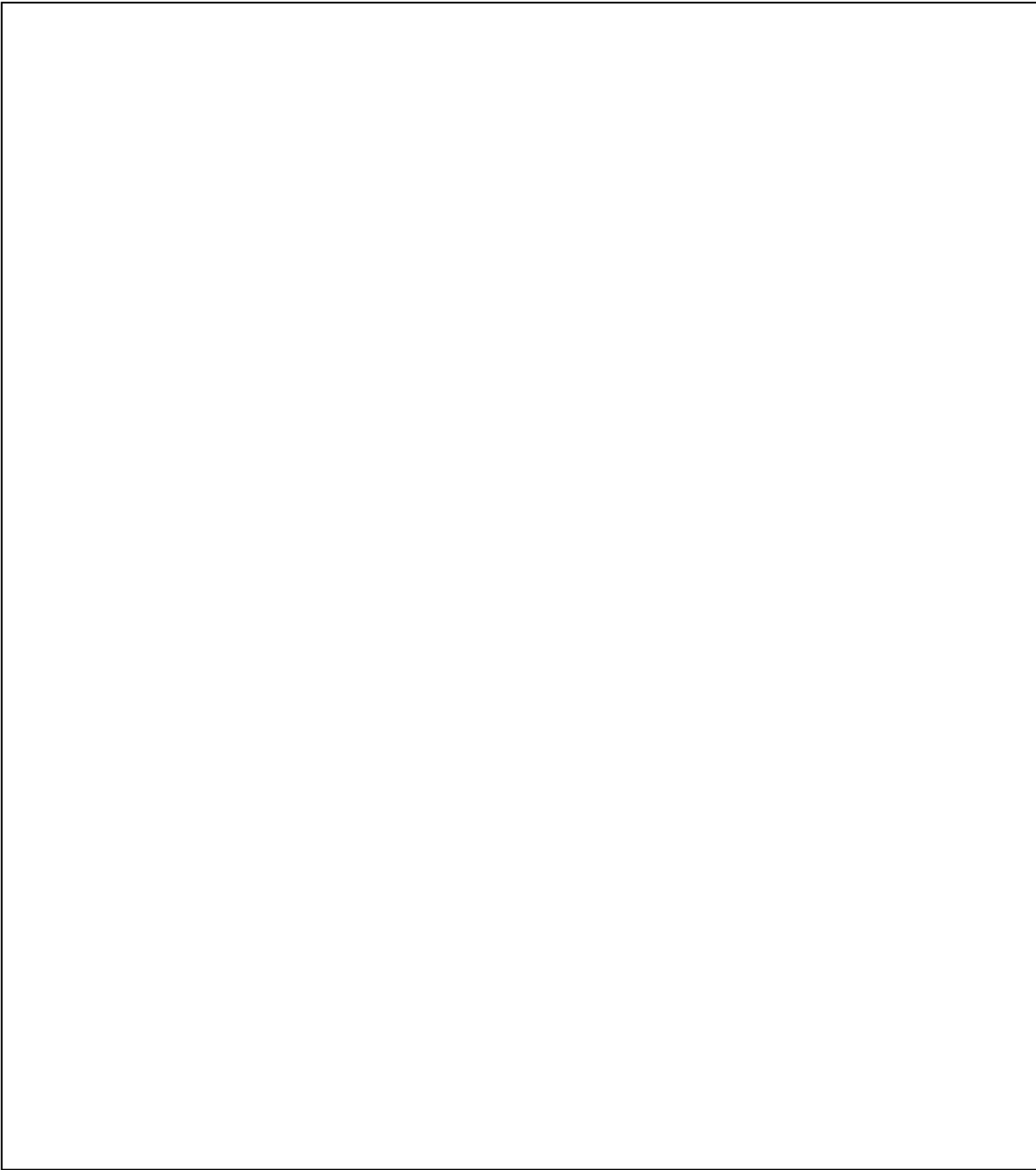
(b) (1)  
(b) (3)-18 USC 798  
(b) (3)-50 USC 3024(i)  
(b) (3)-P.L. 86-36



(b) (1)  
(b) (3) -18 USC 798  
(b) (3) -50 USC 3024(i)  
(b) (3) -P.L. 86-36



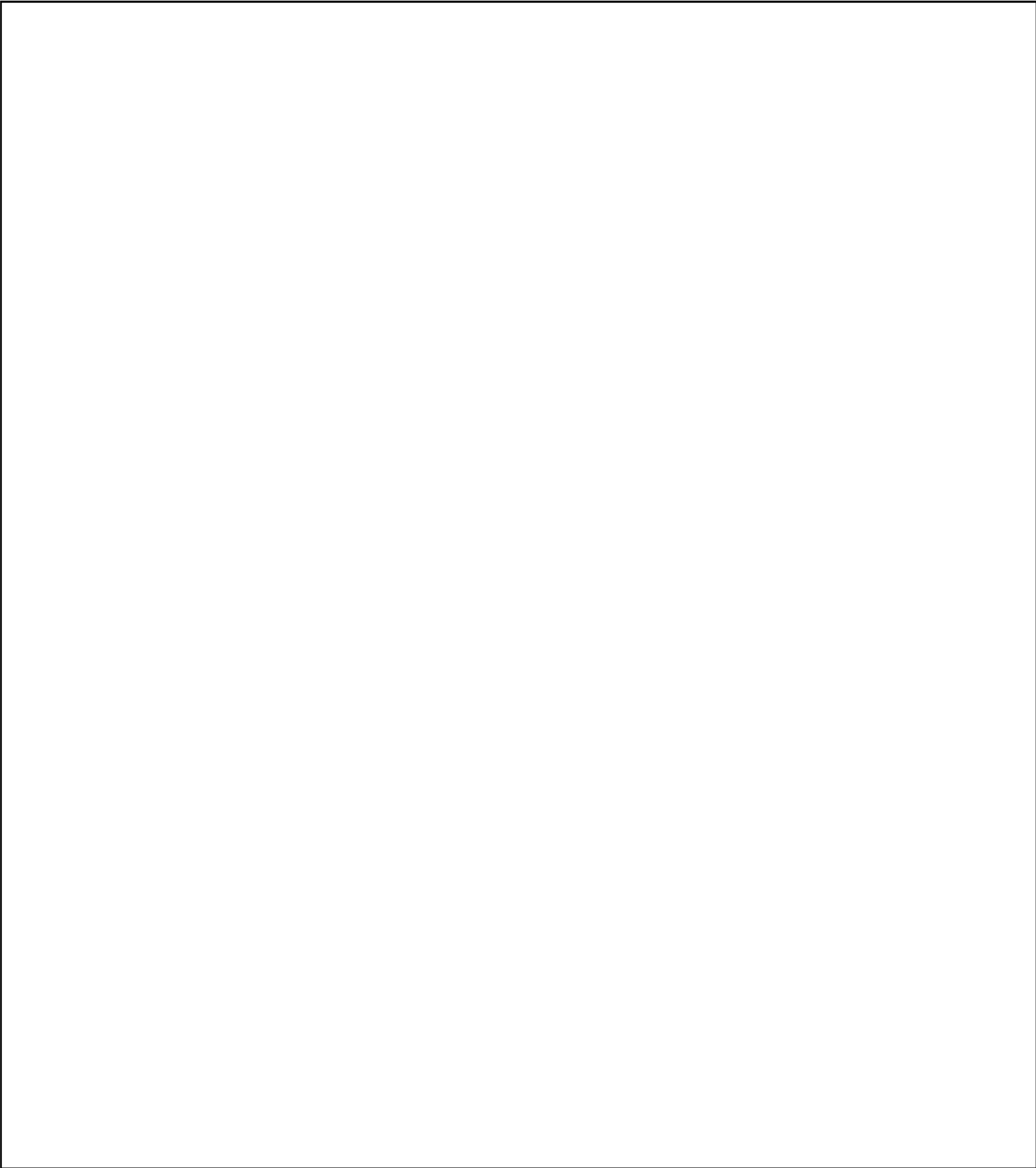
(b) (1)  
(b) (3)-18 USC 798  
(b) (3)-50 USC 3024(i)  
(b) (3)-P.L. 86-36



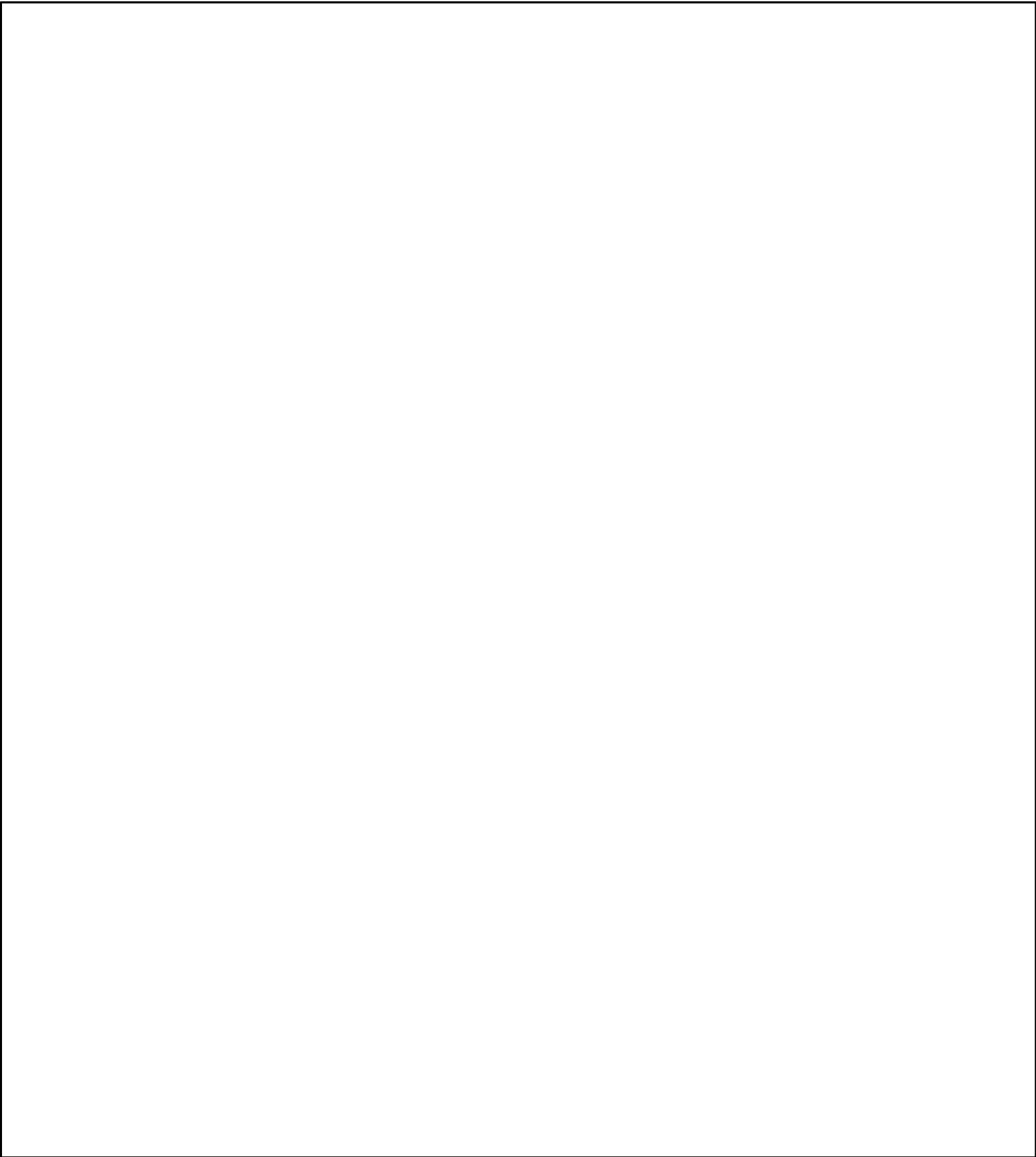
(b) (1)  
(b) (3)-18 USC 798  
(b) (3)-50 USC 3024(i)  
(b) (3)-P.L. 86-36



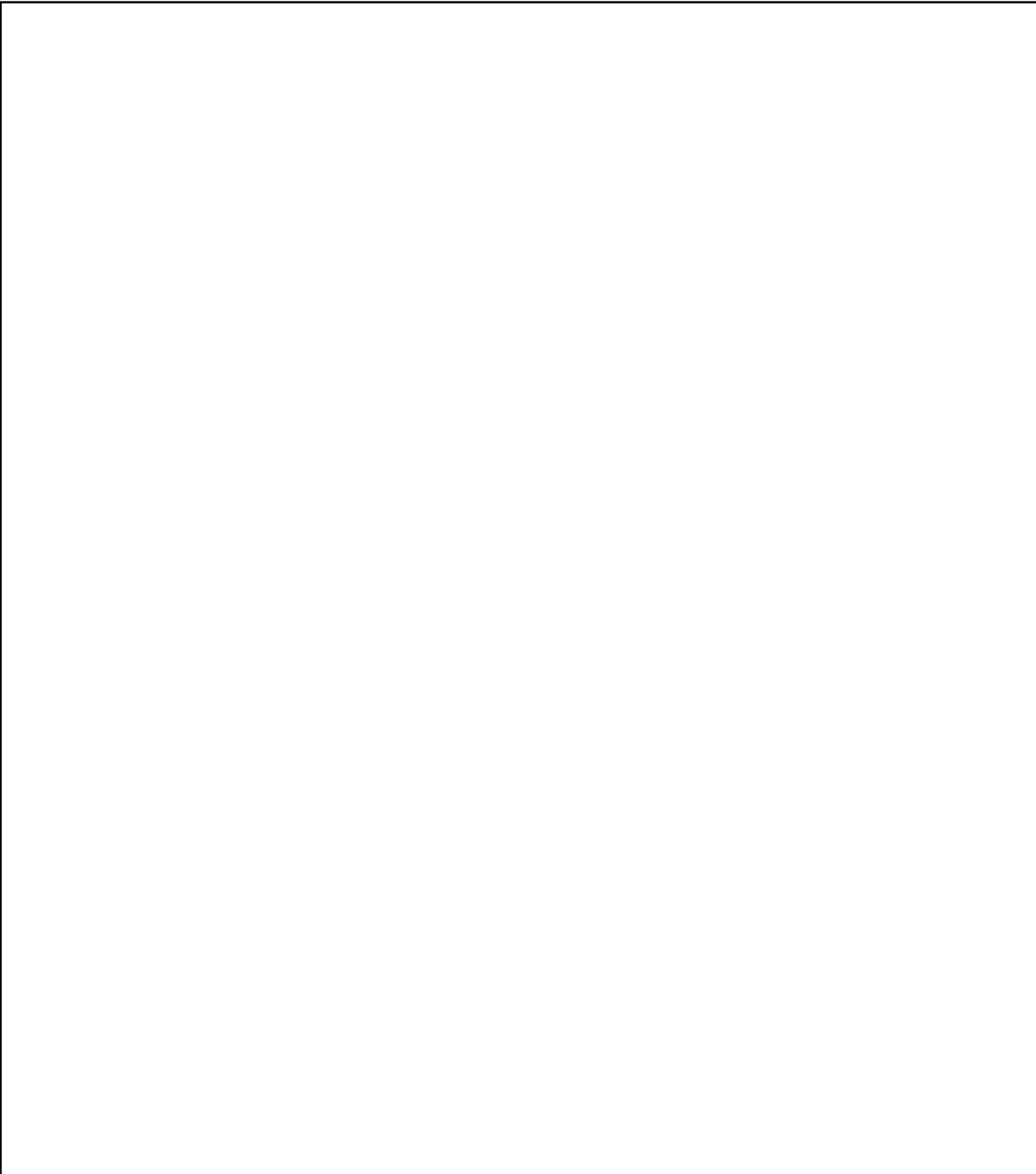
(b) (1)  
(b) (3) -18 USC 798  
(b) (3) -50 USC 3024(i)  
(b) (3) -P.L. 86-36



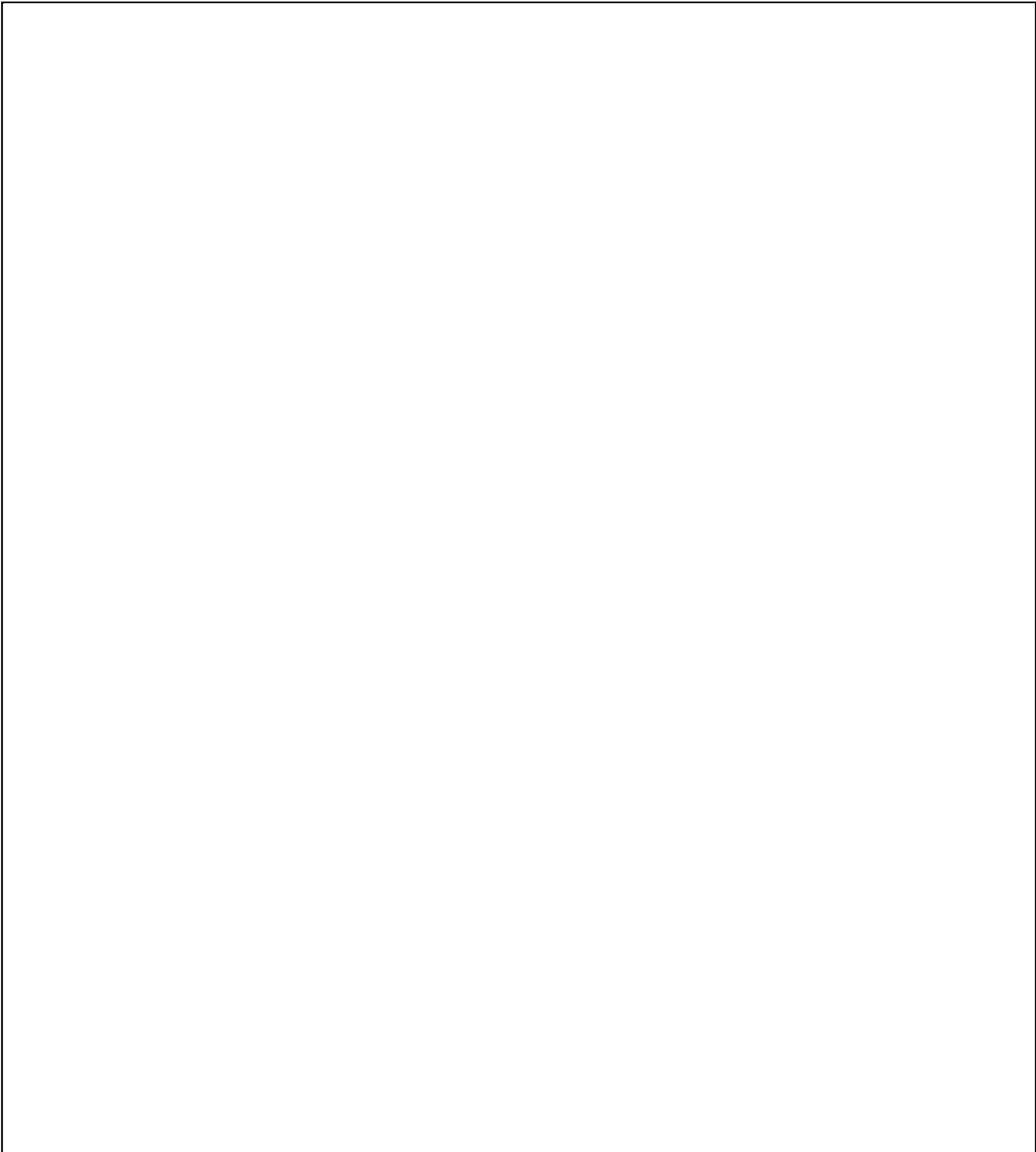
(b) (1)  
(b) (3) -18 USC 798  
(b) (3) -50 USC 3024 (i)  
(b) (3) -P.L. 86-36



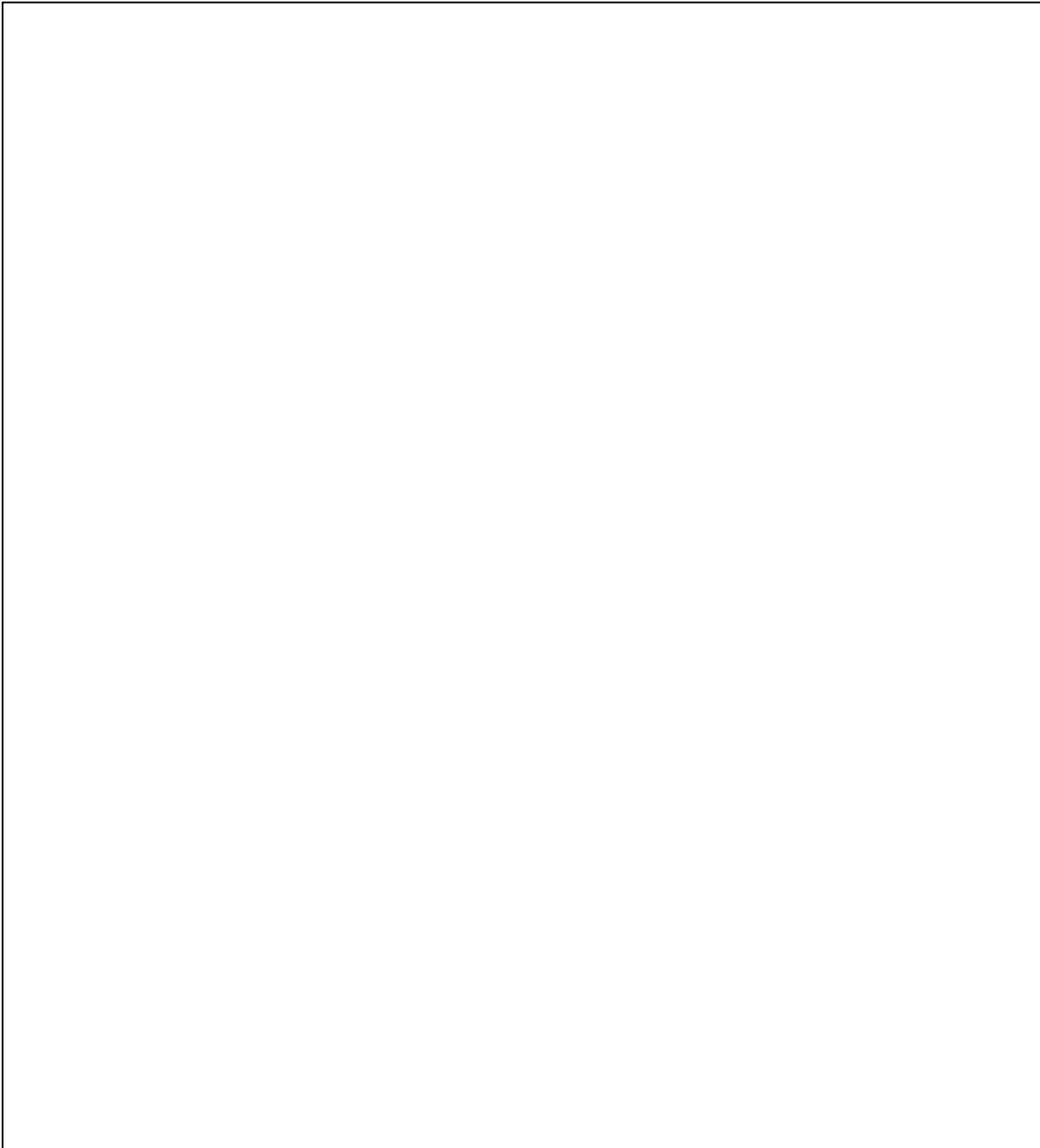
(b) (1)  
(b) (3)-18 USC 798  
(b) (3)-50 USC 3024(i)  
(b) (3)-P.L. 86-36



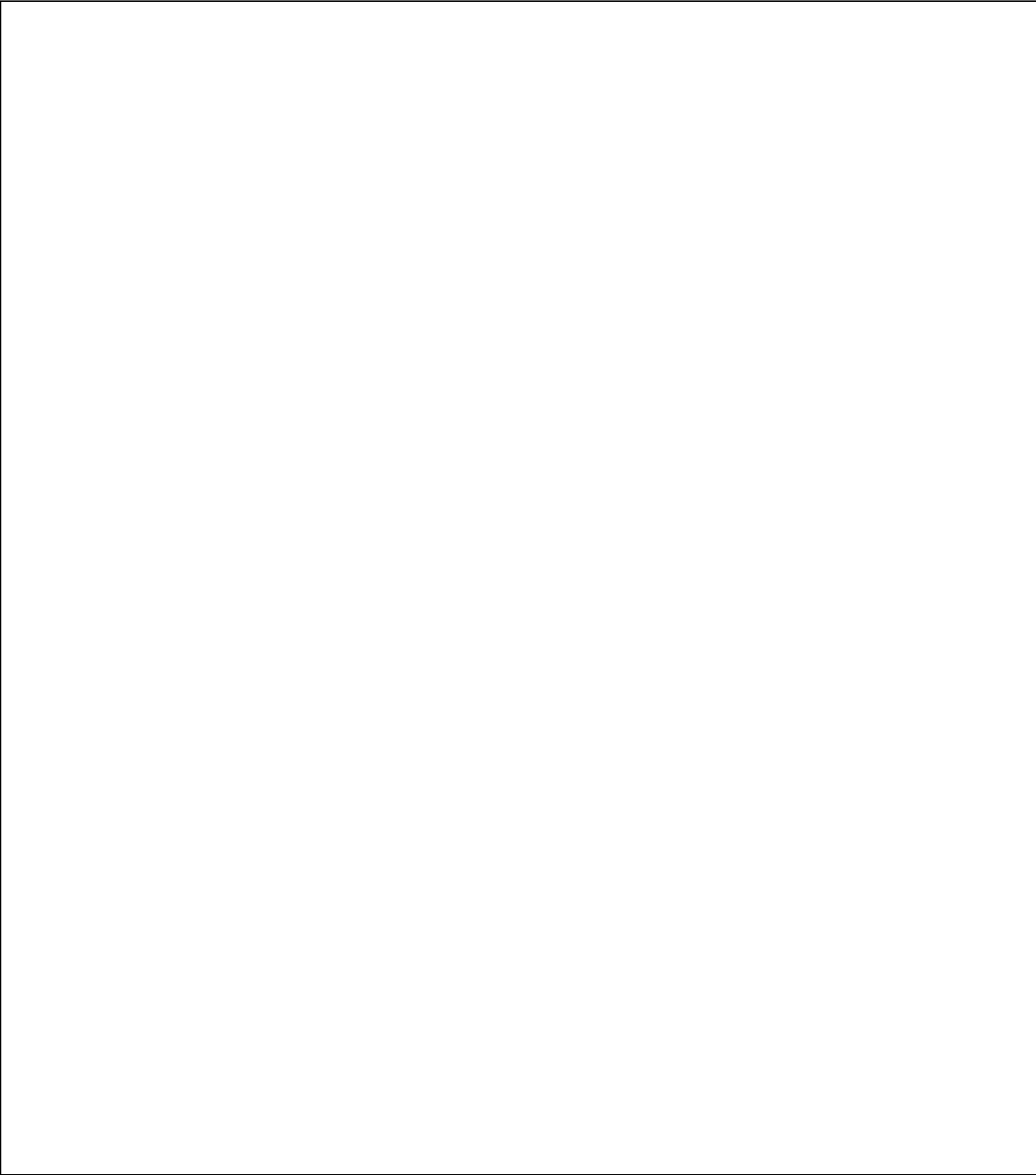
(b) (1)  
(b) (3)-18 USC 798  
(b) (3)-50 USC 3024(i)  
(b) (3)-P.L. 86-36



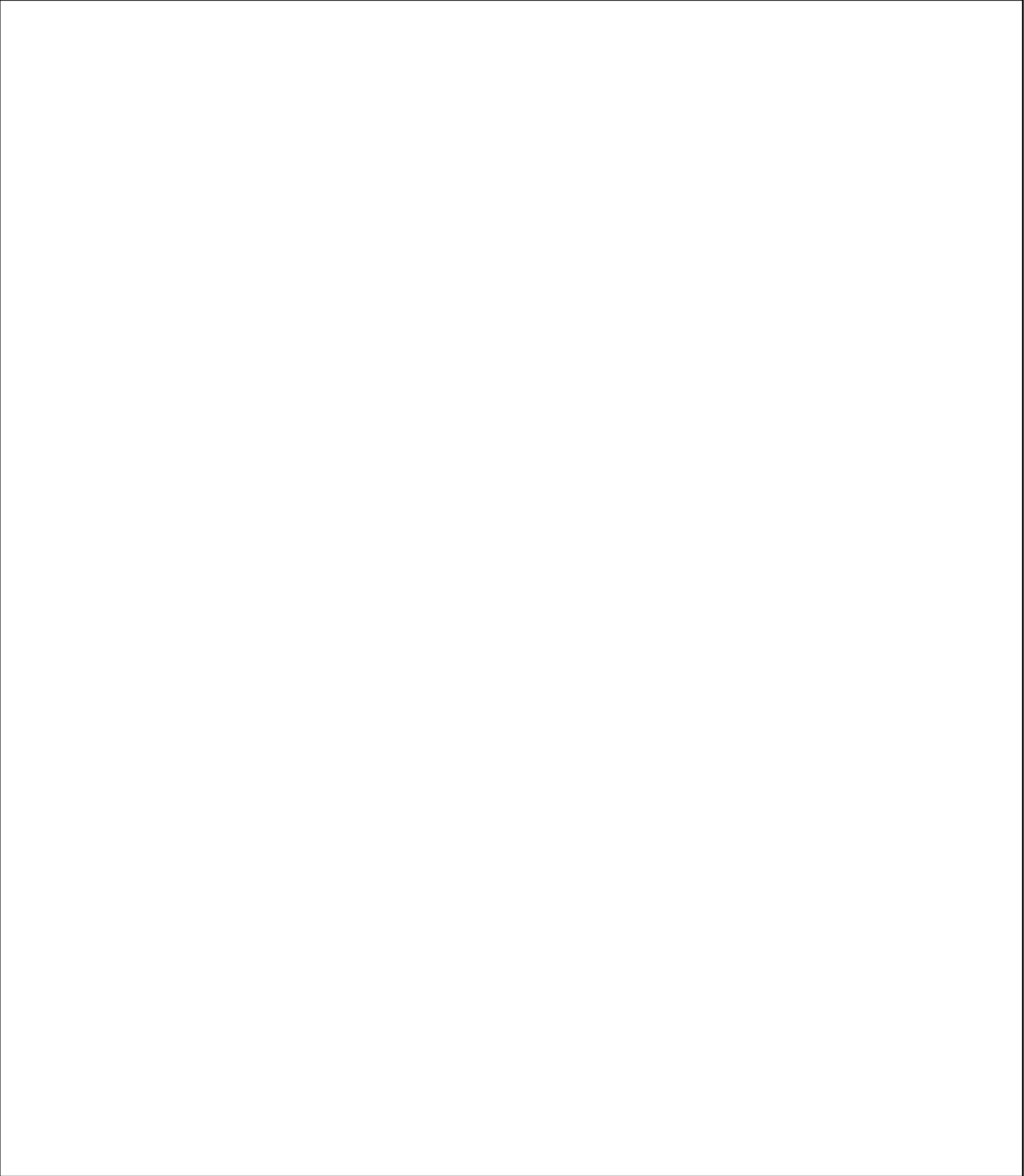
(b) (1)  
(b) (3)-18 USC 798  
(b) (3)-50 USC 3024 (i)  
(b) (3)-P.L. 86-36



(b) (1)  
(b) (3)-18 USC 798  
(b) (3)-50 USC 3024(i)  
(b) (3)-P.L. 86-36



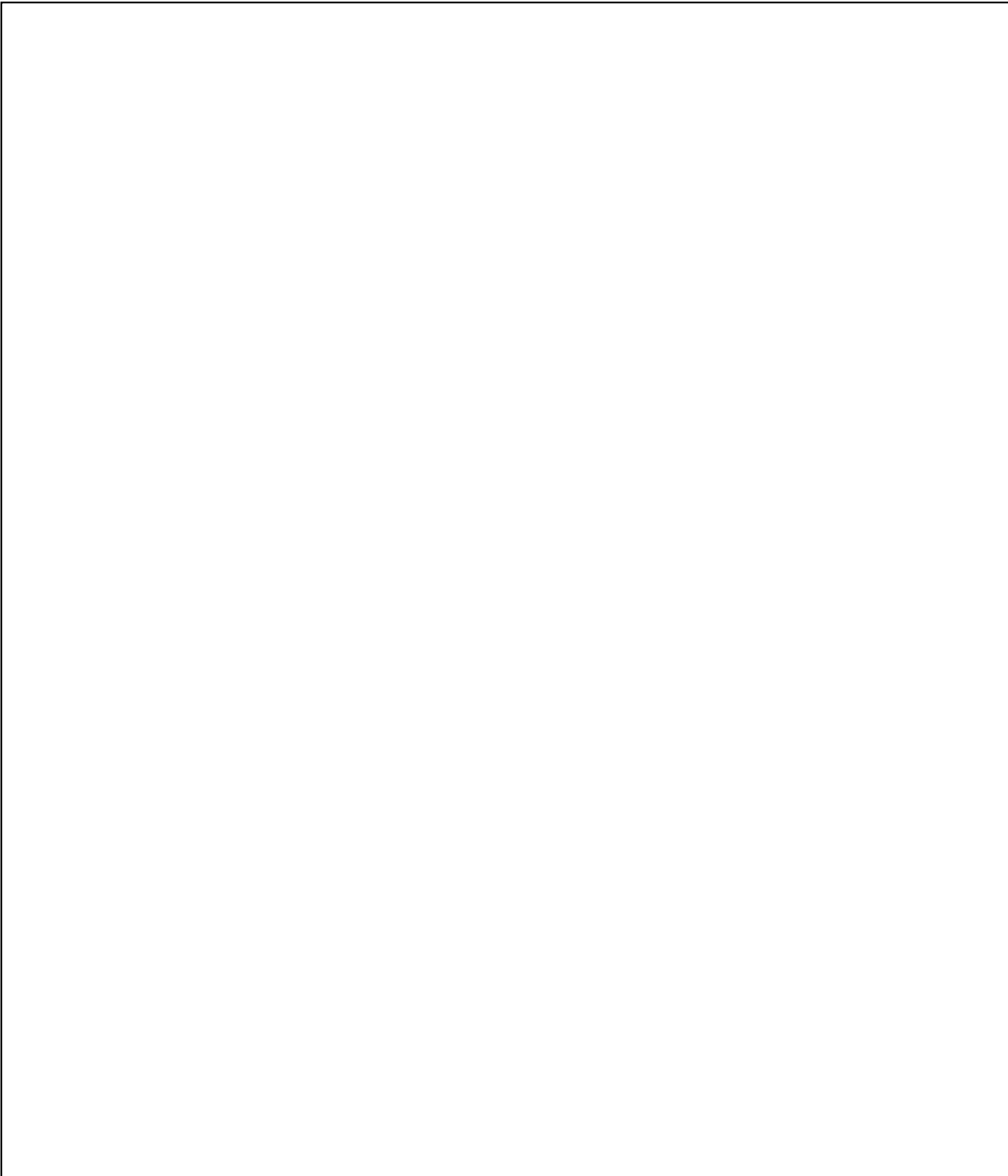
(b) (1)  
(b) (3)-18 USC 798  
(b) (3)-50 USC 3024 (i)  
(b) (3)-P.L. 86-36



(b) (1)  
(b) (3)-18 USC 798  
(b) (3)-50 USC 3024(i)  
(b) (3)-P.L. 86-36

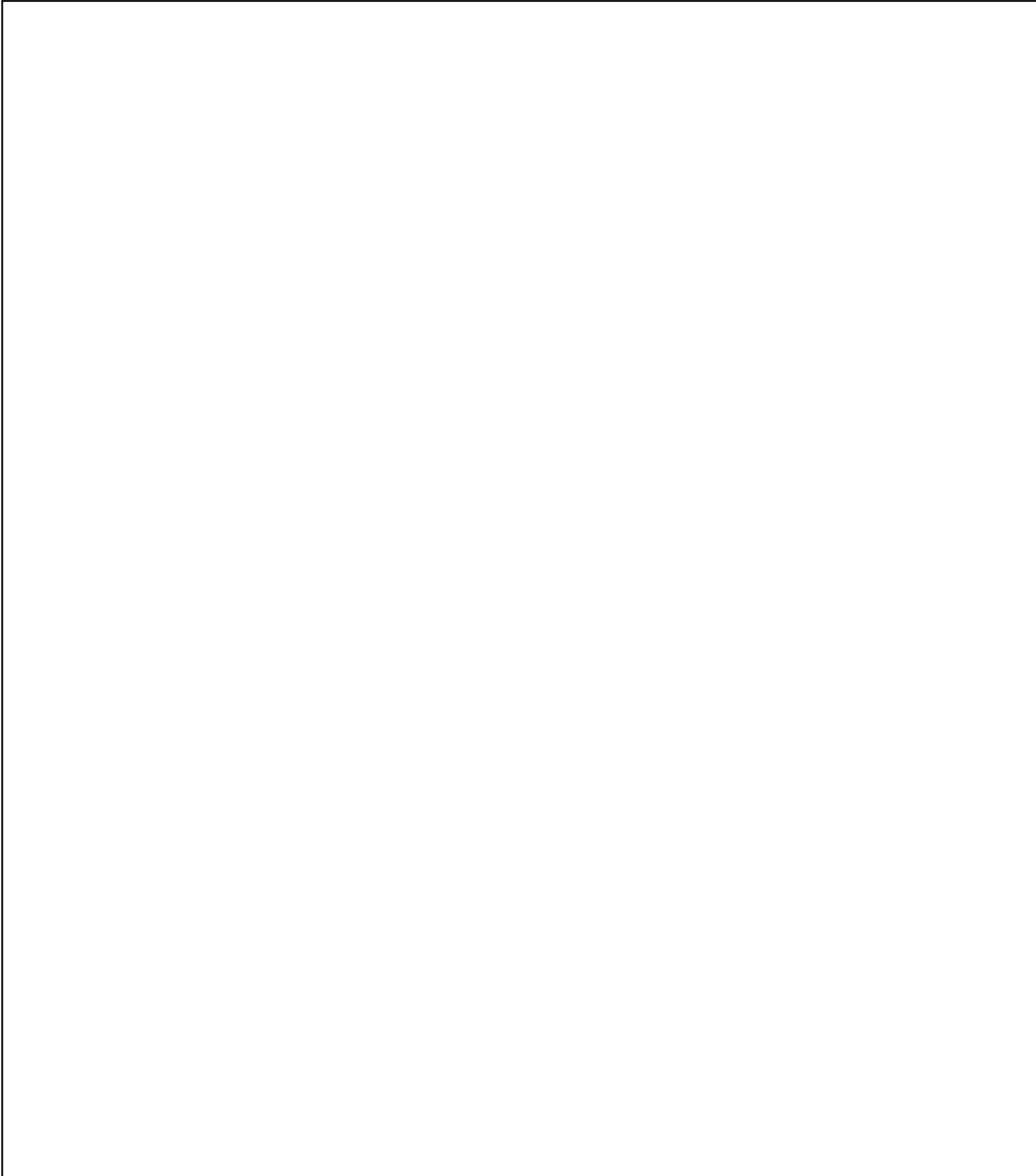


(b) (1)  
(b) (3) -18 USC 798  
(b) (3) -50 USC 3024(i)  
(b) (3) -P.L. 86-36



(b) (1)  
(b) (3) -18 USC 798  
(b) (3) -50 USC 3024 (i)  
(b) (3) -P.L. 86-36

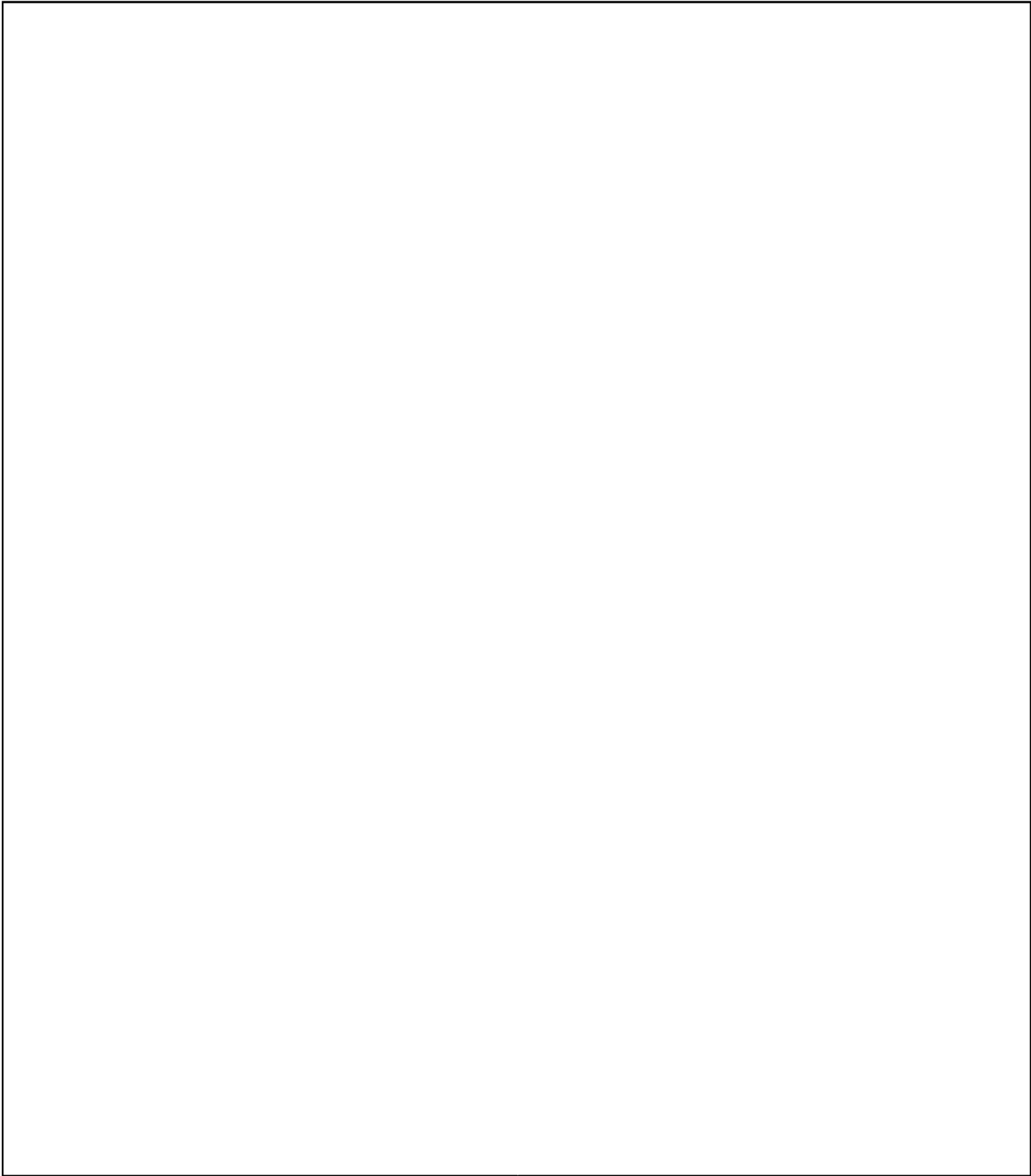
(b) (1)  
(b) (3)-18 USC 798  
(b) (3)-50 USC 3024(i)  
(b) (3)-P.L. 86-36



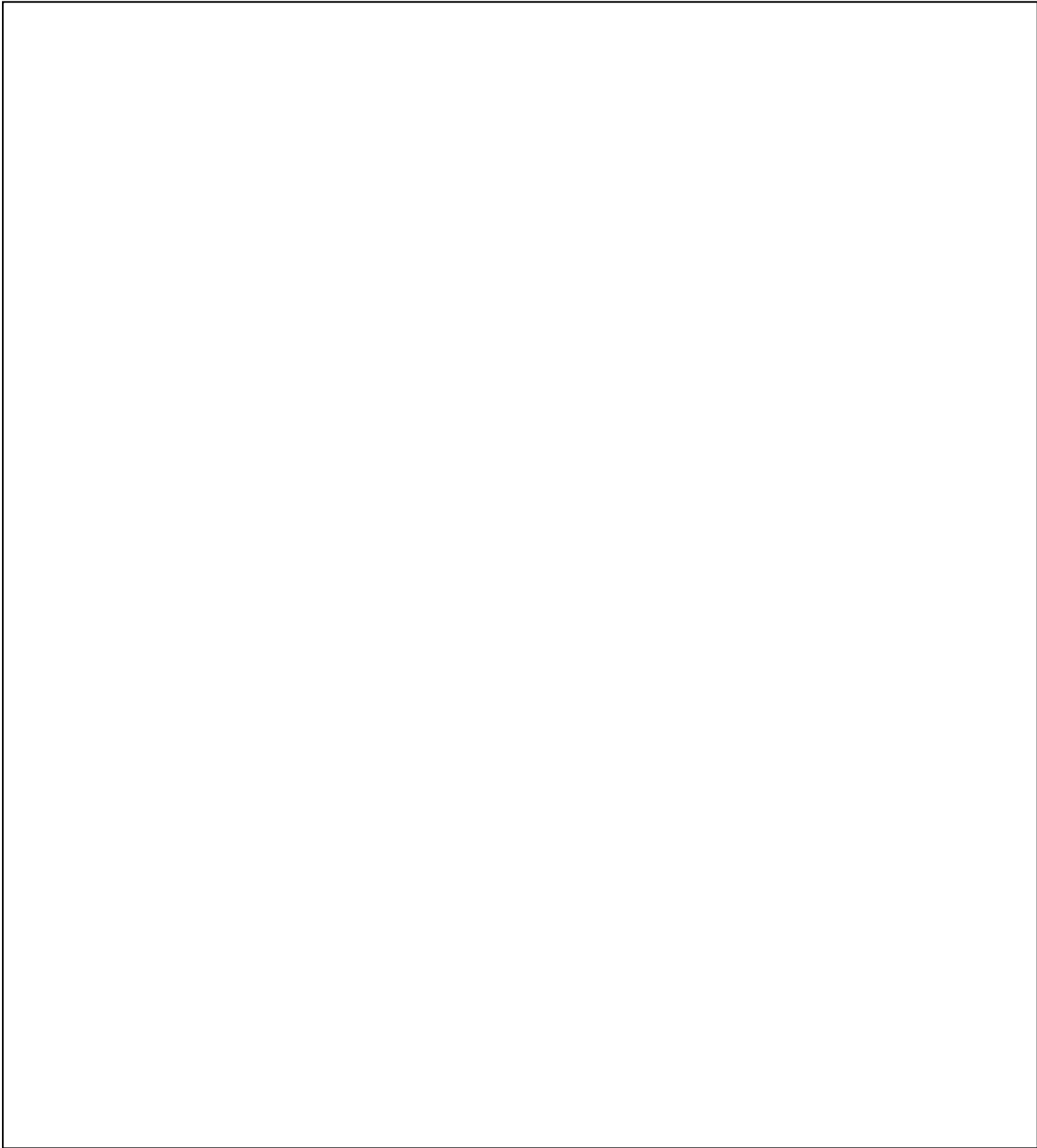
(b) (1)  
(b) (3)-18 USC 798  
(b) (3)-50 USC 3024(i)  
(b) (3)-P.L. 86-36



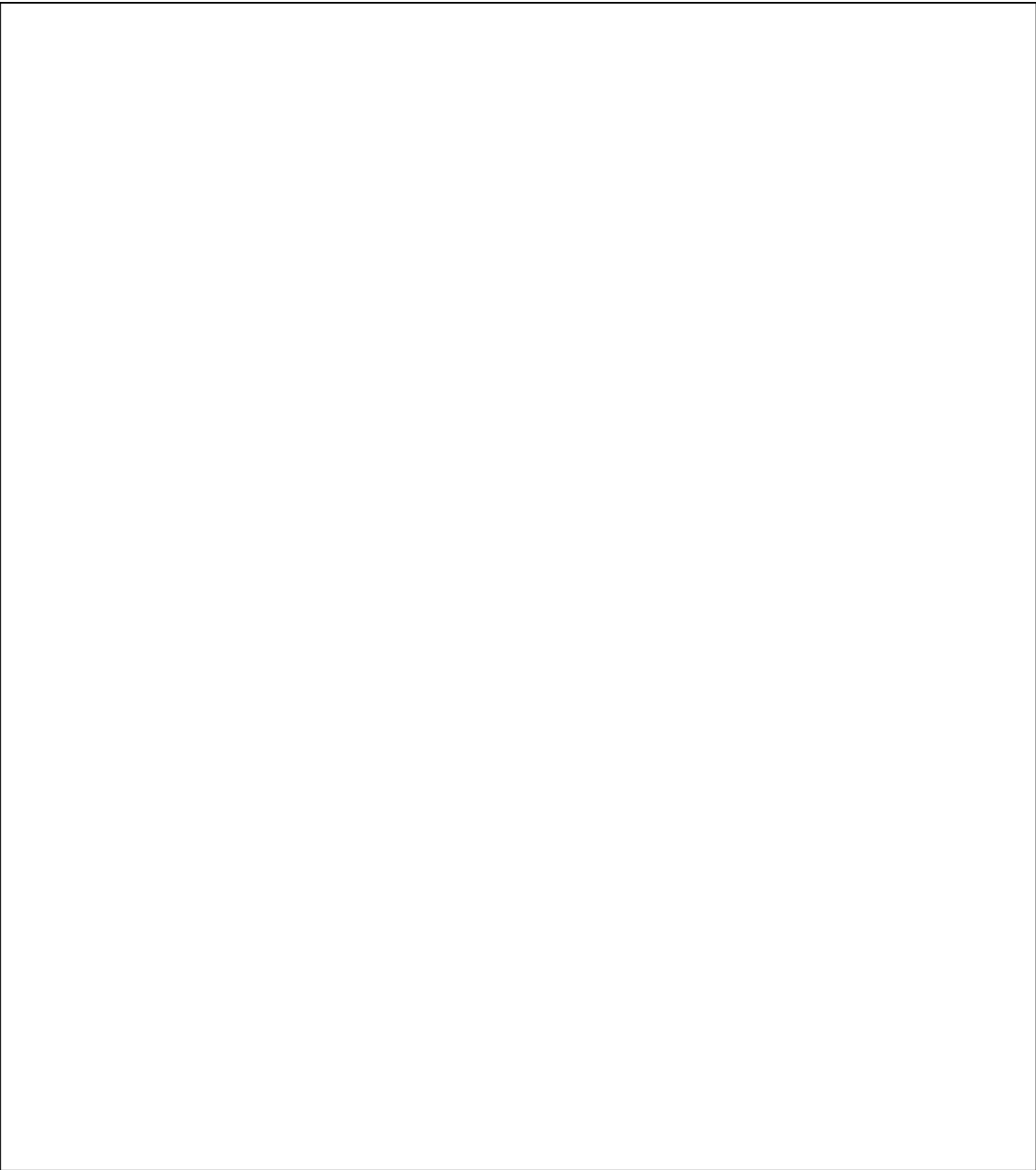
(b) (1)  
(b) (3)-18 USC 798  
(b) (3)-50 USC 3024(i)  
(b) (3)-P.L. 86-36



(b) (1)  
(b) (3)-18 USC 798  
(b) (3)-50 USC 3024(i)  
(b) (3)-P.L. 86-36

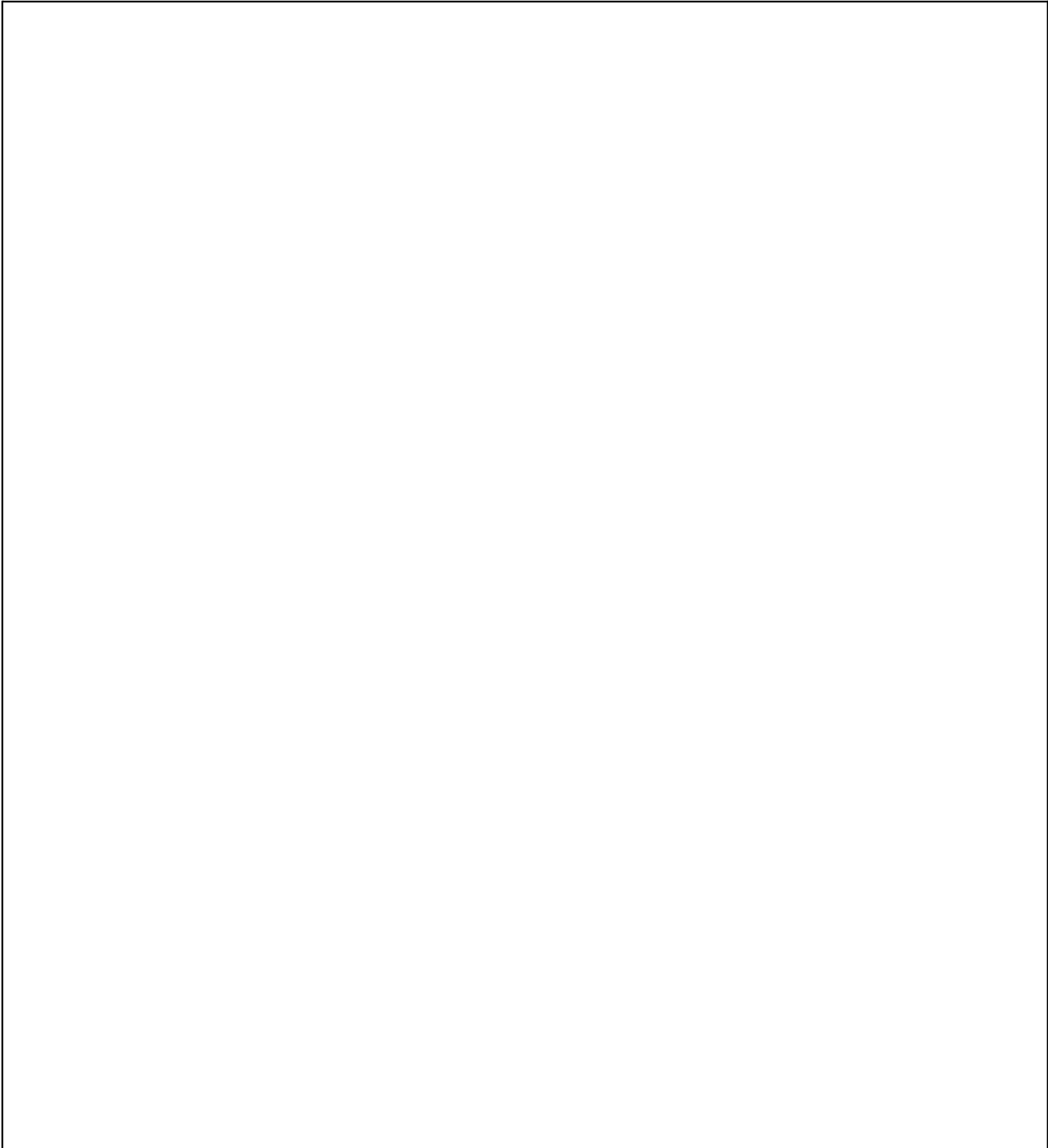


(b) (1)  
(b) (3)-18 USC 798  
(b) (3)-50 USC 3024 (i)  
(b) (3)-P.L. 86-36

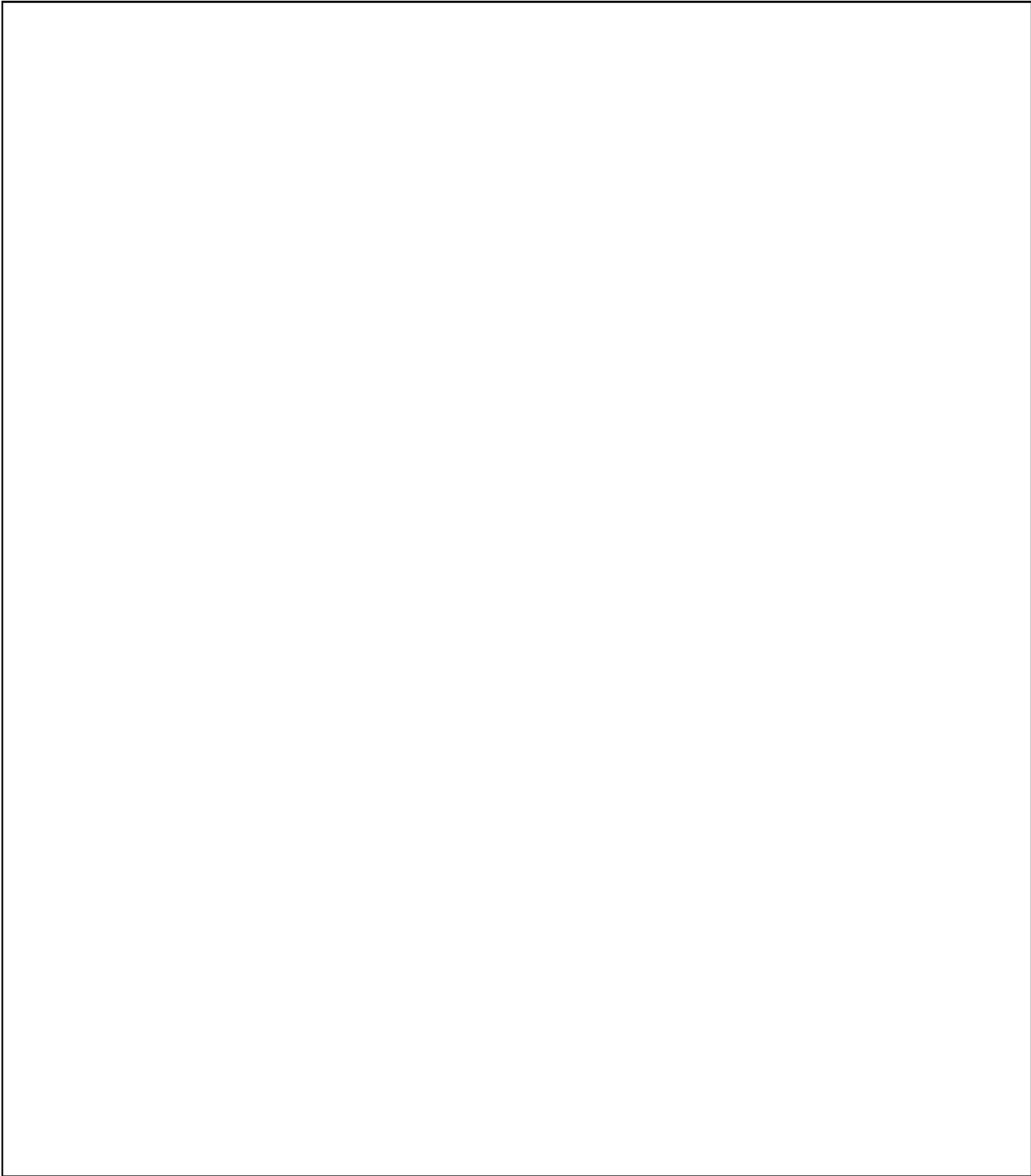


(b) (1)  
(b) (3)-18 USC 798  
(b) (3)-50 USC 3024 (i)  
(b) (3)-P.L. 86-36

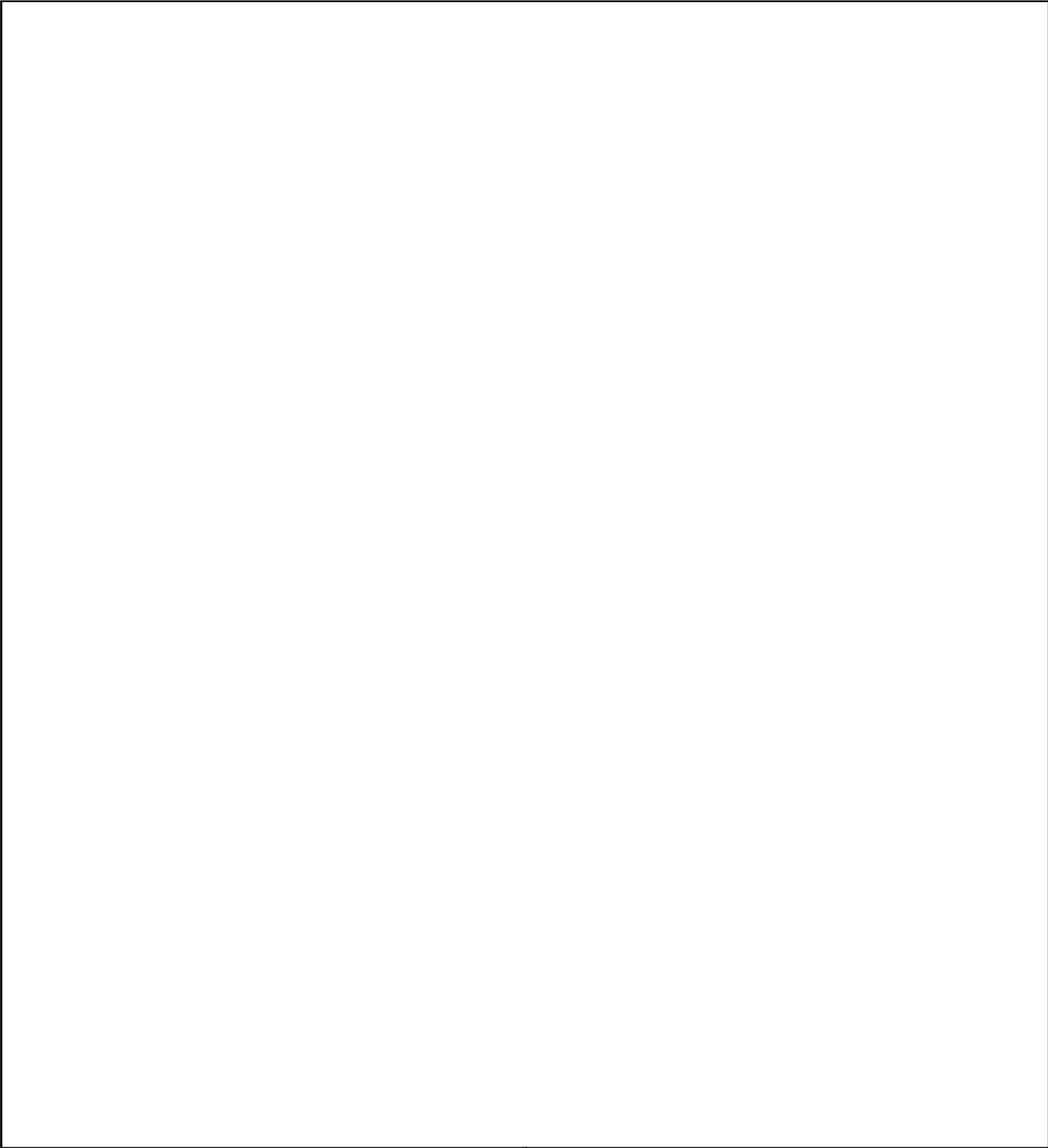




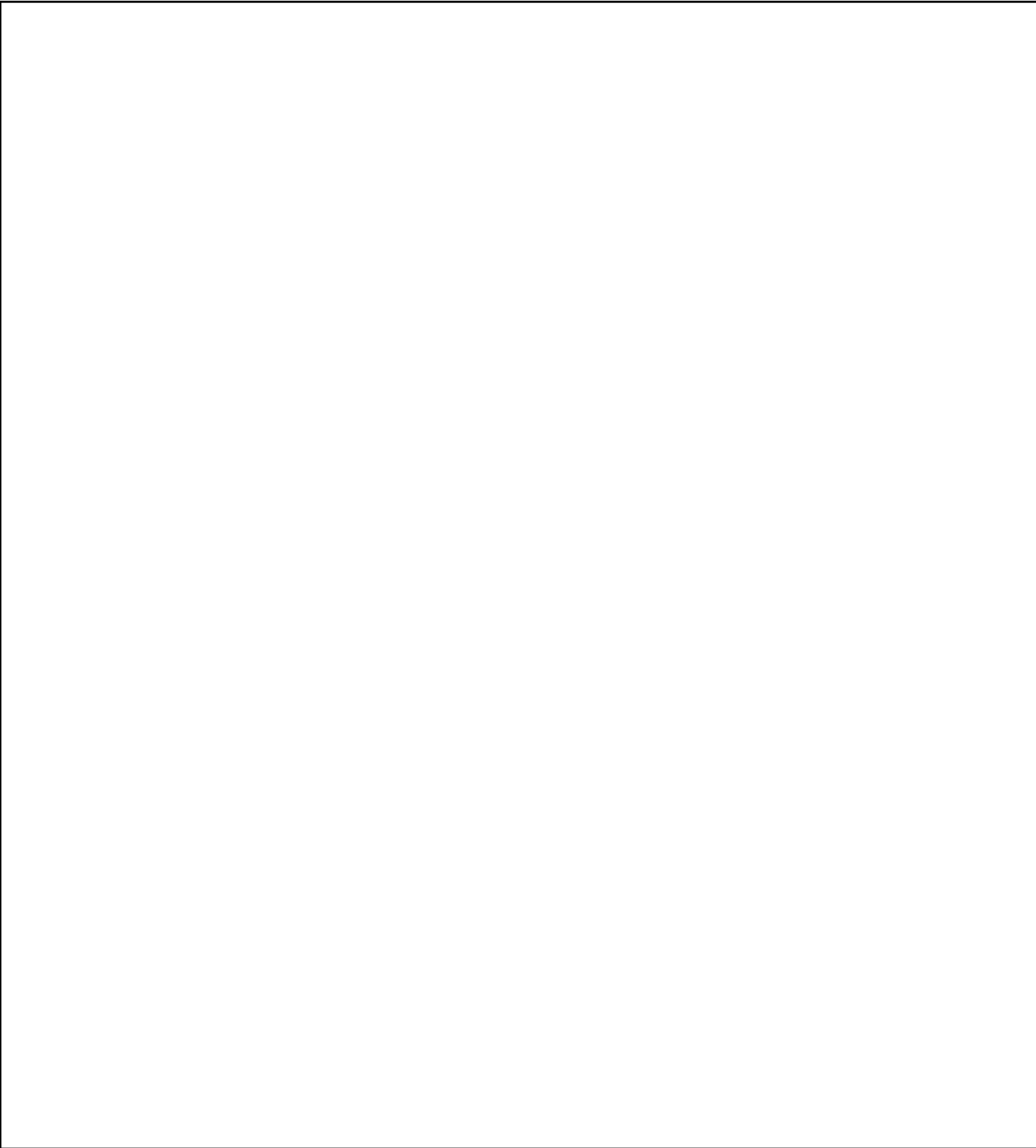
(b) (1)  
(b) (3)-18 USC 798  
(b) (3)-50 USC 3024(i)  
(b) (3)-P.L. 86-36



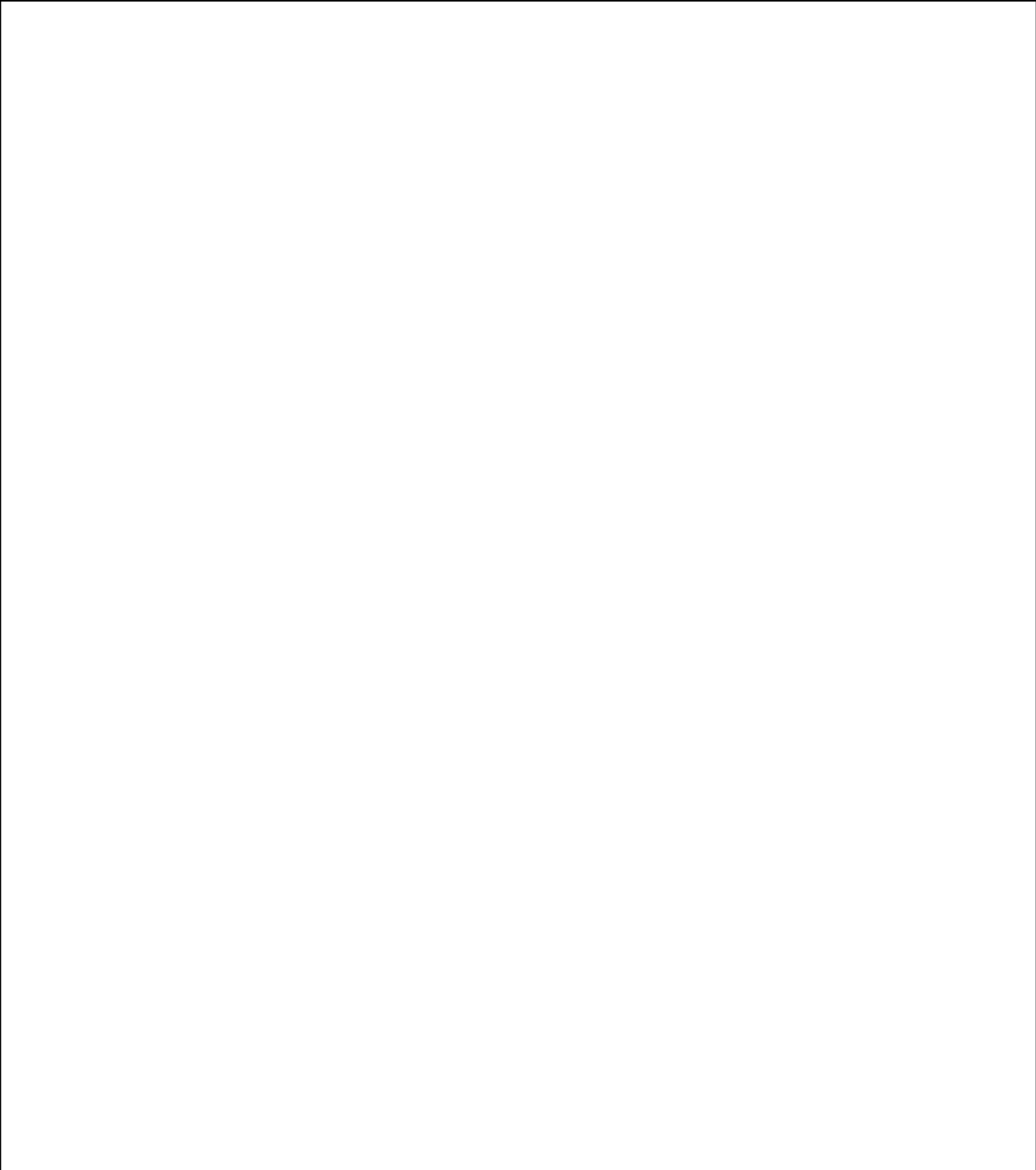
(b) (1)  
(b) (3)-18 USC 798  
(b) (3)-50 USC 3024(i)  
(b) (3)-P.L. 86-36



(b) (1)  
(b) (3)-18 USC 798  
(b) (3)-50 USC 3024(i)  
(b) (3)-P.L. 86-36



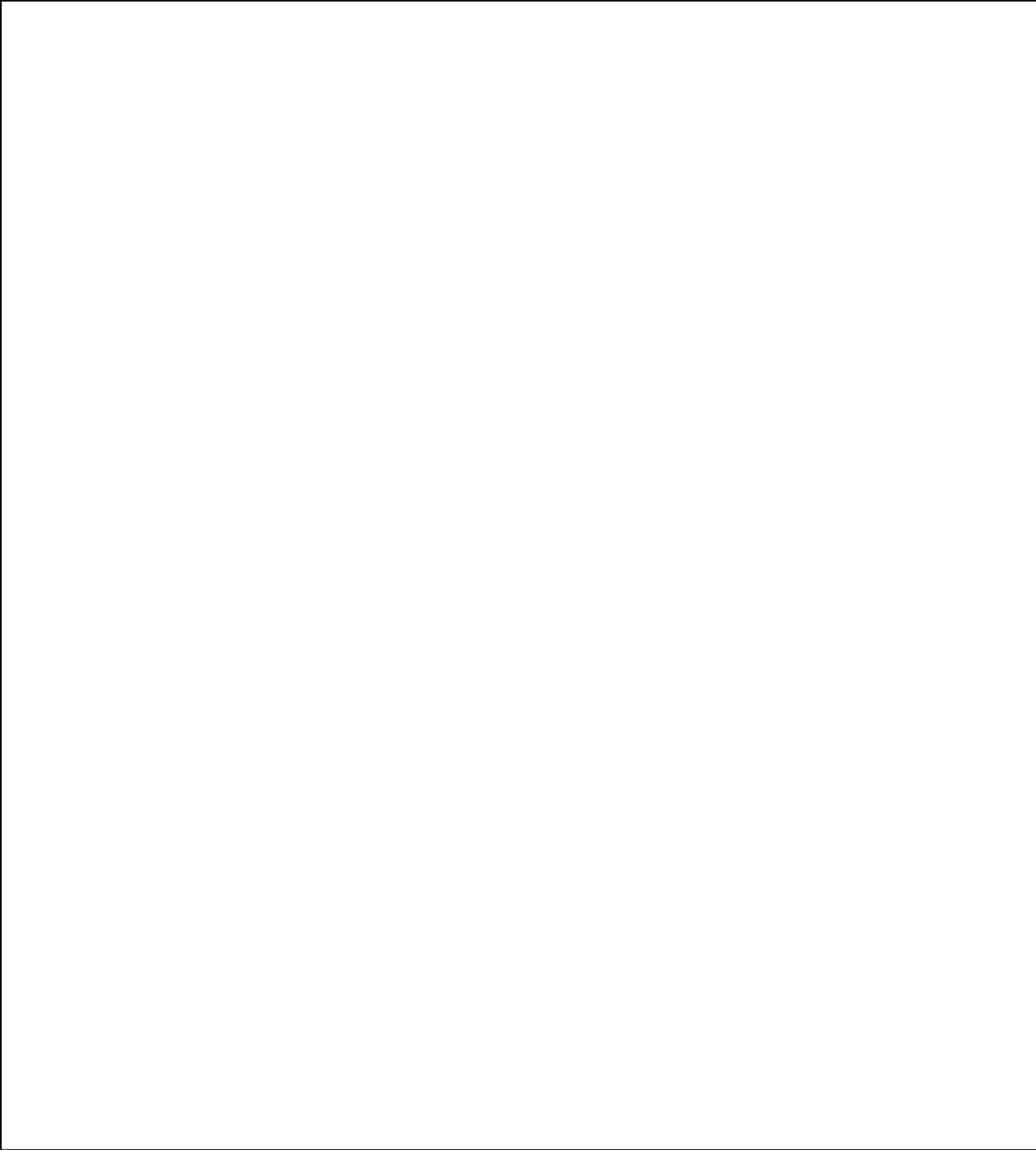
(b) (1)  
(b) (3) -18 USC 798  
(b) (3) -50 USC 3024 (i)  
(b) (3) -P.L. 86-36



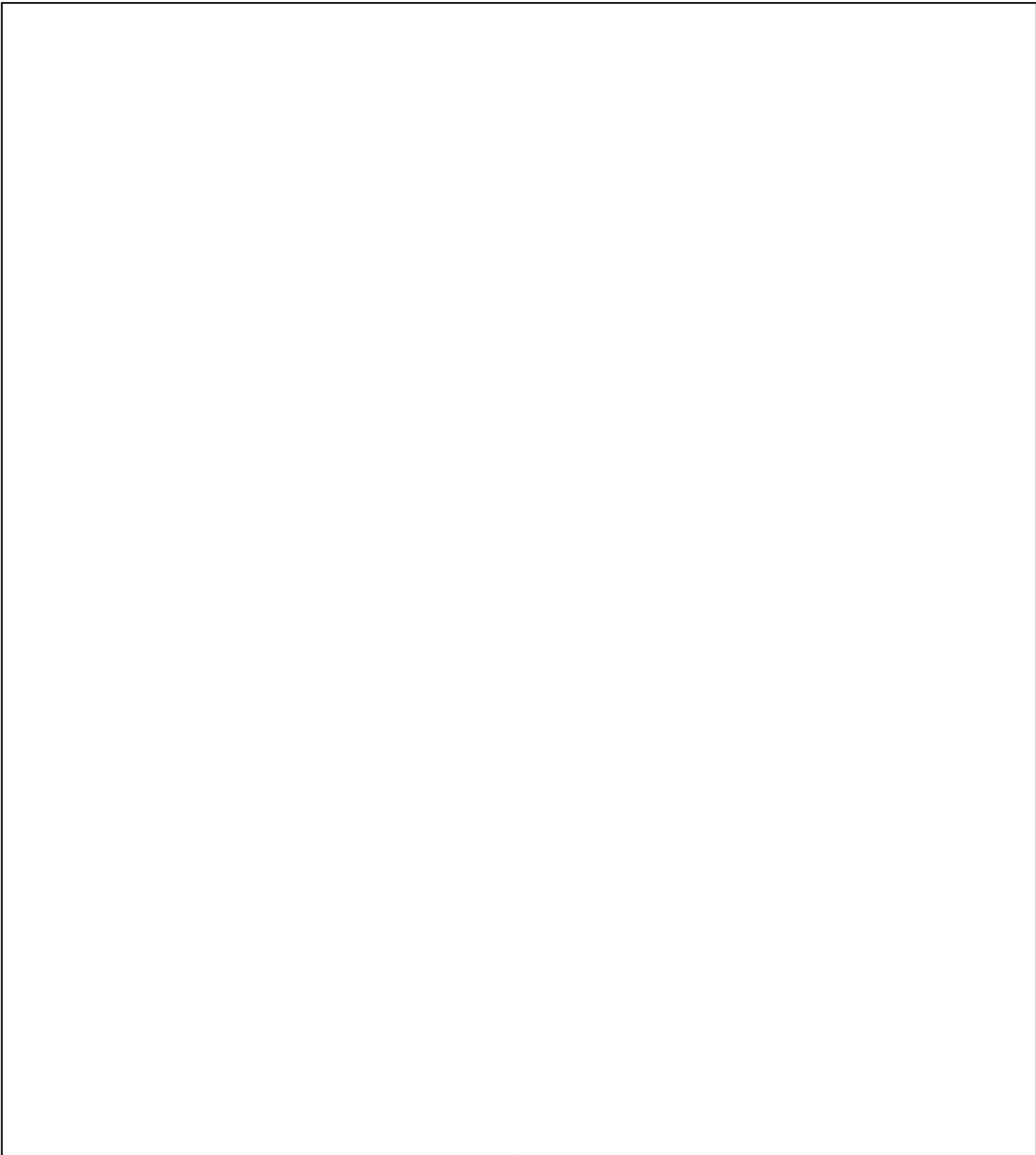
(b) (1)  
(b) (3)-18 USC 798  
(b) (3)-50 USC 3024(i)  
(b) (3)-P.L. 86-36



(b) (1)  
(b) (3) -18 USC 798  
(b) (3) -50 USC 3024 (i)  
(b) (3) -P.L. 86-36

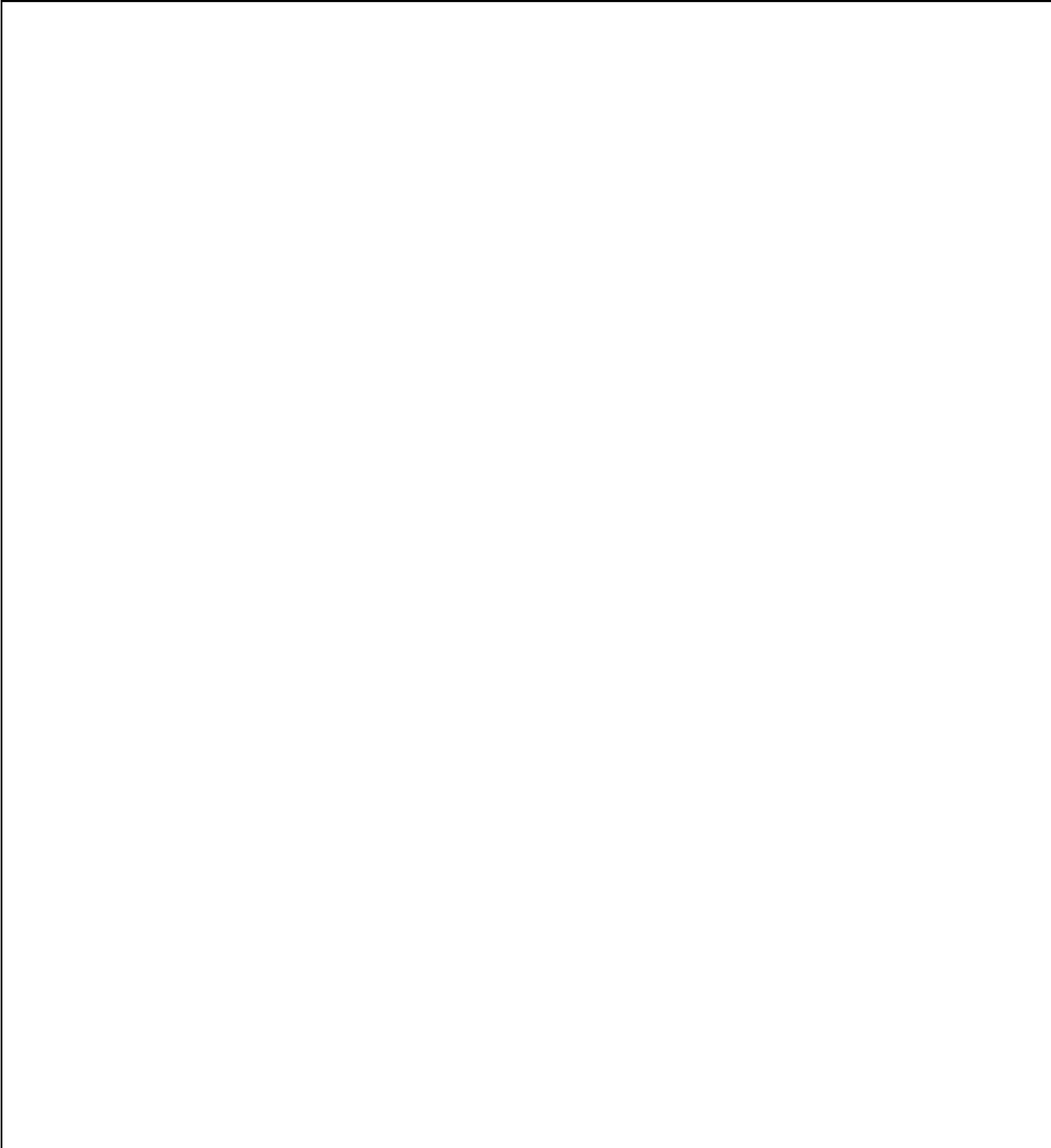


(b) (1)  
(b) (3)-18 USC 798  
(b) (3)-50 USC 3024 (i)  
(b) (3)-P.L. 86-36

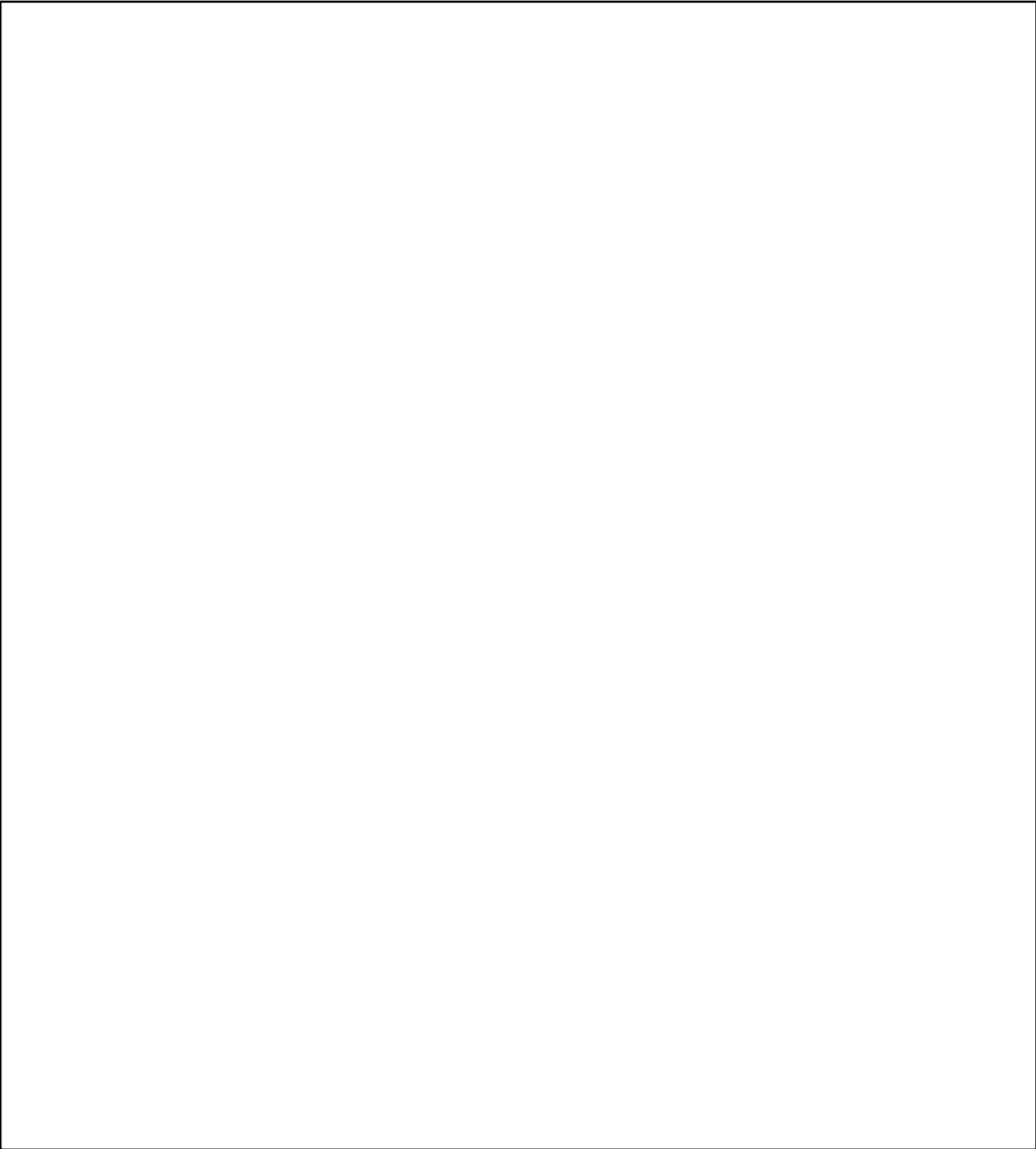


(b) (1)  
(b) (3)-18 USC 798  
(b) (3)-50 USC 3024(i)  
(b) (3)-P.L. 86-36

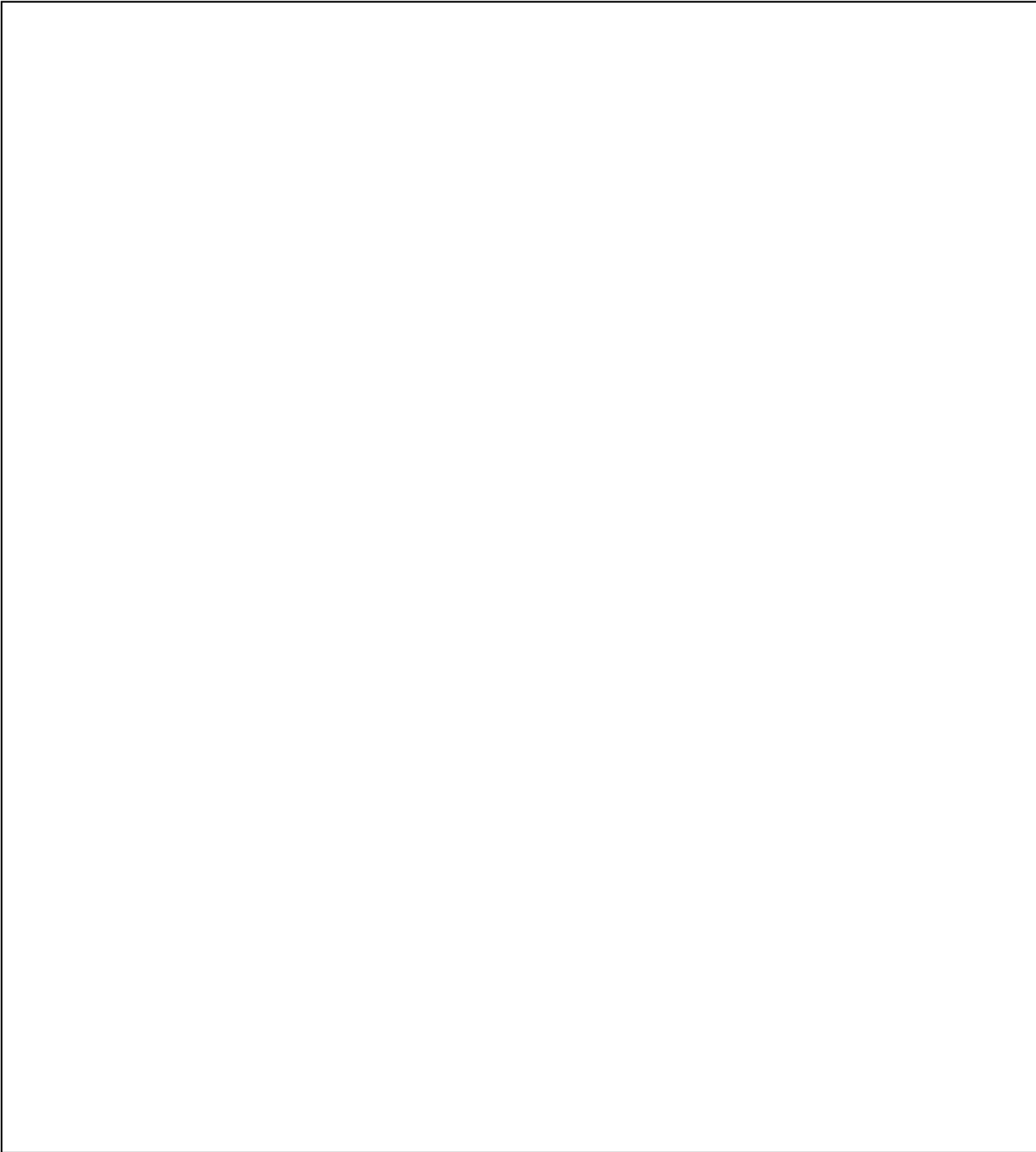




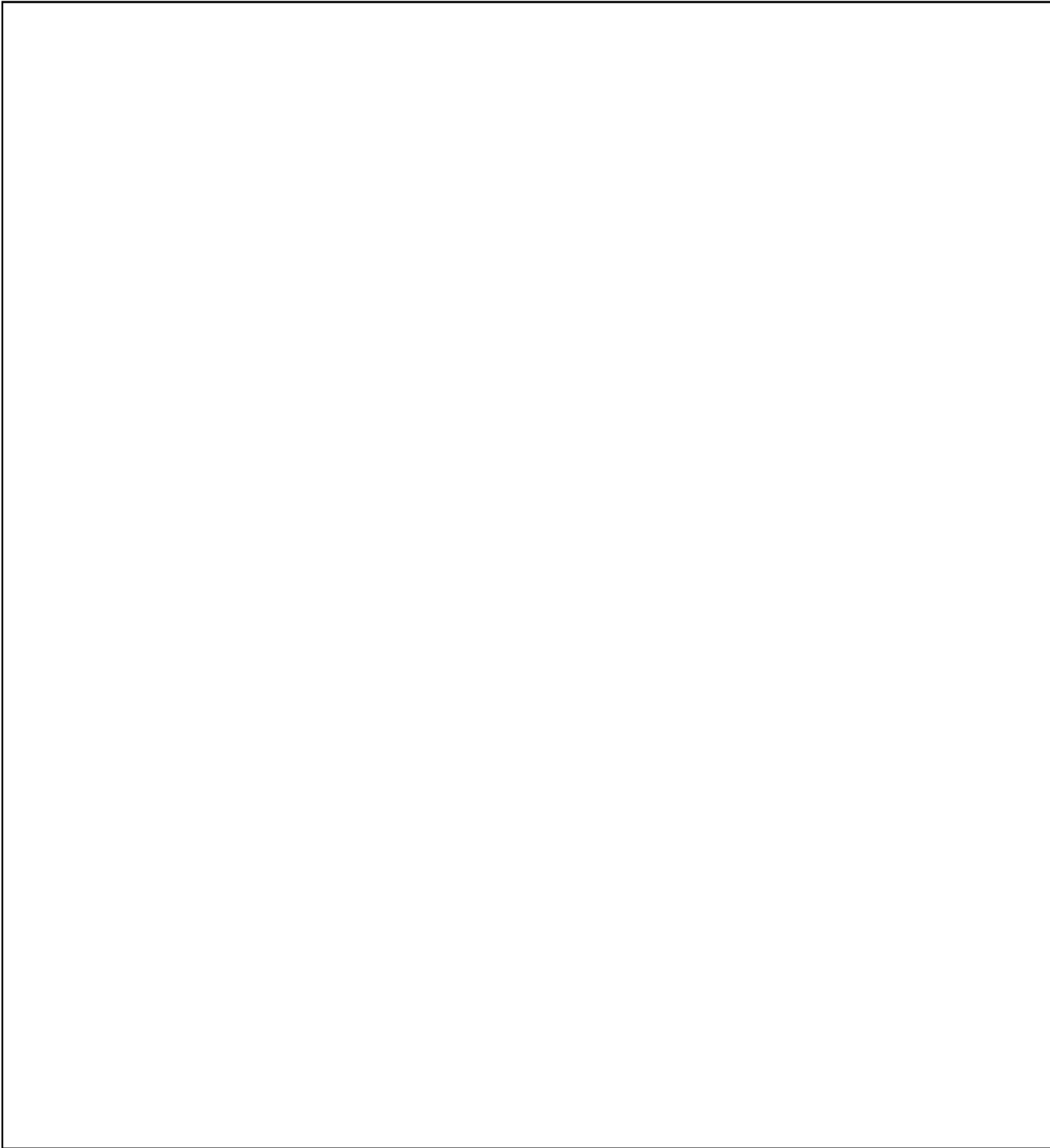
(b) (1)  
(b) (3)-18 USC 798  
(b) (3)-50 USC 3024(i)  
(b) (3)-P.L. 86-36



(b) (1)  
(b) (3) -18 USC 798  
(b) (3) -50 USC 3024 (i)  
(b) (3) -P.L. 86-36

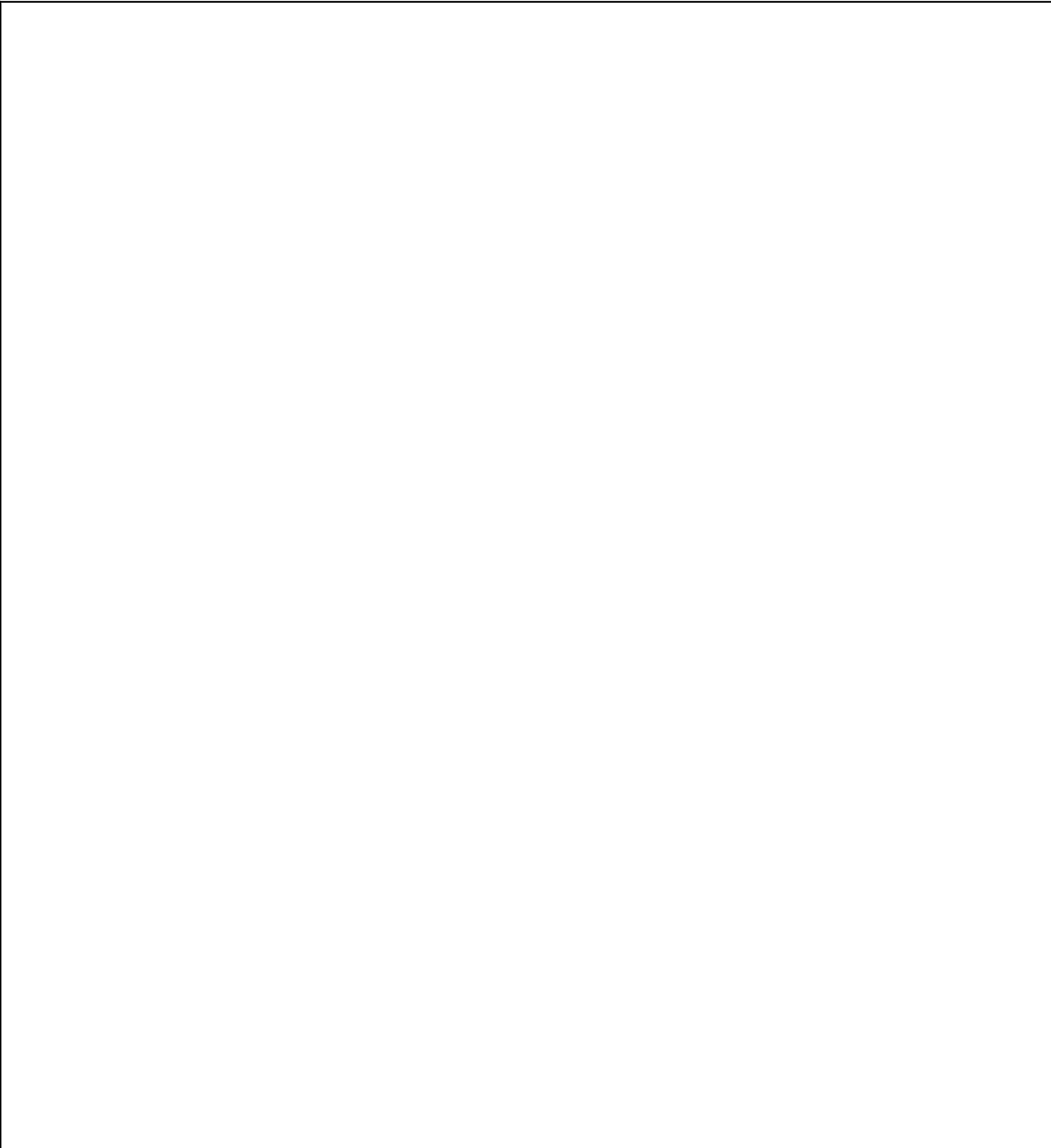


(b) (1)  
(b) (3)-18 USC 798  
(b) (3)-50 USC 3024 (i)  
(b) (3)-P.L. 86-36



(b) (1)  
(b) (3)-18 USC 798  
(b) (3)-50 USC 3024(i)  
(b) (3)-P.L. 86-36

(b) (1)  
(b) (3) -18 USC 798  
(b) (3) -50 USC 3024(i)  
(b) (3) -P.L. 86-36



(b) (1)  
(b) (3)-18 USC 798  
(b) (3)-50 USC 3024(i)  
(b) (3)-P.L. 86-36

(b) (1)  
(b) (3)-18 USC 798  
(b) (3)-50 USC 3024(i)  
(b) (3)-P.L. 86-36

CHAPTER XI

PRINCIPLES OF CRYPTODIAGNOSIS

	Paragraph
General.....	71
The basic steps in diagnosis.....	72
The diagnostician and his attributes.....	73
Embarking on the unknown cryptosystem.....	74
Preliminary actions in attacking the unknown cryptosystem.....	75
First step: manipulating the data.....	76
Second step: recognizing the phenomena.....	77
Third step: interpreting the phenomena.....	78
Post mortem.....	80

71. General.—a. It never hurts to know what it is we're talking about, so let us begin with the definition of "diagnosis" as given in *Webster's Third New International Dictionary*:

"*diagnosis*, n. 1. The art or act of identifying a disease from its signs and symptoms; also, the decisions reached. 2. A concise technical description of a taxonomic entity giving its distinguishing characters. 3. Investigation or analysis of the cause or nature of a condition, situation, or problem: a statement or conclusion about the nature or cause of a phenomenon."

From *Webster's New International Dictionary*, Second Edition, the following entries under "diagnosis" are of interest:

"*diagnosis*, n. 1. . . . 2. Determination of a type or condition through case or specimen study. 3. Conclusion arrived at through critical perception or scrutiny; hence, keen understanding of appearances."

Finally, let us set down the definition of "diagnosis" as it appears in the *NSA Basic Cryptologic Glossary* (June 1971):

"*diagnosis*, n. 1. In cryptanalysis, a systematic examination of encrypted text or key with a view to discovering the nature of the cryptosystem that produced it. 2. The result of such examination."

These definitions should clear the air and set the stage for the discussion which follows.

b. Let us first quote from a previous text¹ an extract which is particularly apropos, elaborating on the meaning of diagnosis:

(1) "Except in the case of the more simple types of cryptograms, the step often referred to as *diagnosis*, that is, ascertaining the general system according to which a given cryptogram has been produced is usually a difficult, if not the most difficult, step in its solution. The reason for this is not hard to find."

(2) "As will become apparent to the student as he proceeds with his study, *in the final analysis*, the solution of every cryptogram involving a form of substitution depends upon its reduction to monoalphabetic terms, if it is not originally in those terms. This is true not only of ordinary substitution ciphers, but also of combined substitution-transposition ciphers, and of enciphered code. If the cryptogram must be reduced to monoalphabetic terms, the manner of its accomplishment is usually indicated by the cryptogram itself, by external or internal phenomena which become apparent to the cryptanalyst as he studies the cryptogram. If this is impossible, or too difficult, the cryptanalyst must, by one means or another, discover how to accomplish this reduction, by bringing to bear all the special or collateral information he can get from all the sources at his command. If both these possibilities fail him, there is little left but the long, tedious, and often fruitless process of elimination. In the case of transposition ciphers of the

¹ *Military Cryptanalytics, Part I*, par. 17 (on pp. 20-21).

more complex type, the discovery of the basic method is often simply a matter of long and tedious elimination of possibilities. For cryptanalysis has unfortunately not yet attained, and may indeed never attain, the precision found today in qualitative analysis in chemistry, for example, where the analytic process is absolutely clear-cut and exact in its dichotomy. A few words in explanation of what is meant may not be amiss. When a chemist seeks to determine the identity of an unknown substance, he applies certain specific reagents to the substance and in a specific sequence. The first reagent tells him definitely into which of two primary classes the unknown substance falls. He then applies a second test with another specific reagent, which tells him again quite definitely into which of two secondary classes the unknown substance falls, and so on, until finally he has reduced the unknown substance to its simplest terms and has found out what it is. In striking contrast to this situation, cryptanalysis affords exceedingly few 'reagents' or tests that may be applied to determine positively that a given cipher belongs to one or the other of two systems yielding externally similar results. And this is what makes the analysis of an isolated, complex cryptogram so difficult. Note the limiting adjective 'isolated' in the foregoing sentence, for it is used advisedly. It is not often that the general system fails to disclose itself or cannot be discovered by painstaking investigation when there is a great volume of text accumulating from a regular traffic between numerous correspondents in a large organization. *Sooner or later* the system becomes known, either because of blunders and carelessness on the part of the personnel entrusted with the encrypting of the messages, or because the accumulation of text itself makes possible the determination of the general system by cryptanalytic, including statistical, studies. But in the case of a single or even a few isolated cryptograms concerning which little or no information can be gained by the cryptanalyst, he is often unable, without a knowledge of, or a shrewd guess as to the general system employed, to decompose the heterogeneous text of the cryptogram into homogeneous, monoalphabetic text, which is the ultimate and essential step in analysis. The only knowledge that the cryptanalyst can bring to his aid in this most difficult step is that gained by long experience and practice in the analysis of many different types of systems. In this respect the practice of cryptanalysis is analogous to the practice of medicine: correct diagnosis is the most important and often the most difficult first step toward success."

c. The parallels between cryptanalytic diagnosis—"cryptodiagnosis"—and medical diagnosis are very striking.² Medicine is far from an exact science—it really is an art—and the same is true of cryptanalysis. In medicine, complete diagnosis is often accomplished only after an autopsy; in cryptanalysis, complete diagnosis is sometimes possible only after a body of cryptomaterials is in the hands of the nevertheless-quite-competent analyst. Or another way of looking at it is that in medical as well as in cryptanalytic diagnosis, success may come only after the patient is dead or the system has expired; in either case, an autopsy could tell us what we *should* have done. Even with (or in spite of) the present state of medical knowledge, the causes of many diseases and their cures are still unknown; in cryptanalysis, there are many cipher systems for which no general solution exists or is known, even if we know the basic principles of the system in question.

d. Cryptanalysis may be thought of as consisting of two aspects, *diagnosis* and *exploitation*. Diagnosis of a cryptosystem is concerned with the discovery of (1) the *nature of the basic elements* (or tools) employed in the cryptosystem (e.g., the language, code book, additive key, transposition matrices, substitution alphabets), and (2) the *rules by which a cryptographer uses these elements* to convert plain text into encrypted text; diagnosis continues as long as any element or any enciphering principle remains unknown. Exploitation of a cryptosystem is concerned with (1) the *recovery of the basic elements* (e.g., the code book, additive key, transposition key, substitution alphabets) and (2) the subsequent *reading of the plain text*. Although the functions of diagnosis and exploitation are distinct, it is a mistake to assume that one finishes before the other commences. In general, some recovery of particular elements is incidental to the diagnostic process; similarly, a system can be partially exploited before diagnosis proper takes place (e.g., isolated spelling-group messages in a low- or medium-grade system are often read

² See in this connection Lambros D. Callimahos, "Cybernetics and Problems of Diagnostics; the Parallels Between Medicine and Cryptanalysis," appearing in the NSA *Technical Journal*, Vol. XIV, No. 1, Winter 1969.



before the mechanics of the system are fully understood—in fact, they can form the starting point of the diagnosis).

**72. The basic steps in diagnosis.**—*a.* The first attempt to formalize the discipline of diagnostics was made in 1563 by the Neapolitan physicist, physician, and cryptologist, Giovanni Battista della Porta; at the end of his treatise, *De Occultis Literarum Notis*, he appended a set of synoptic tables for cipher analysis, with bifurcated routes to be followed according to the particular phenomena displayed by the cipher under investigation. Three and a half centuries later there appeared, in 1918, a work by William F. Friedman entitled *Synoptic Tables for the Solution of Ciphers*, published by the Department of Ciphers of the Riverbank Laboratories at Geneva, Illinois, where Friedman was employed as a geneticist. This latter work consisted of nine tables, strictly dichotomous in nature, with which, it was hoped, an unknown system could be diagnosed. In the next attempt to devise synoptic tables for the analysis of cryptograms, Captain Roger Baudouin, in his *Éléments de Cryptographie* published in Paris in 1939, devised 17 tables which were to lay bare the cryptosystems of the moment. All of these attempts had something in common; they failed in their avowed purpose. The reason they failed is that, unfortunately, cryptodiagnosis does not lend itself to scientific rigor such as the taxonomy of qualitative analysis in inorganic chemistry. The construction of dichotomous charts, or variations thereof, is useless in the analysis across the board of systems that turn up in operational practice. So much for synoptic tables.

*b.* In *Military Cryptanalytics, Part I*, it was stated (on p. 18) that the art of cryptanalysis may be reduced to the following steps:

<i>Procedures in cryptanalysis</i>	<i>Requirements</i>
1. Arrangement and rearrangement of data to disclose nonrandom characteristics or manifestations (i.e., in frequency counts, repetitions, patterns, symmetrical phenomena, etc.).	Experience or ingenuity, and time (which latter may be appreciably lowered by the use of machine aids in cryptanalysis).
2. Recognition of the nonrandom characteristics of manifestations when disclosed.	Experience or statistics.
3. Explanation of the nonrandom characteristics when recognized.	Experience or imagination, and intelligence.

This was followed by the remark that "In all of the foregoing, the element of luck plays a very important part, as it is possible to side-step a large amount of labor and effort, in many cases if hunches or intuition lead the analyst forthwith to the right path. Therefore, the phrase 'or luck' should be added to each of the requirements above. In fact, it all boils down to the simple statement: 'Find something significant, and attach some significance thereto.'" All of this is of course an oversimplification; nevertheless it is an accurate description of the procedures of cryptanalysis—and, actually, *the steps of diagnosis*. But, in a more sophisticated or modern approach, cryptodiagnosis may be regarded as consisting of two aspects: (1) hypothesis formulation and (2) hypothesis testing; the formulation of a hypothesis will call for a particular diagnostic test or tests, which in turn will or will not produce the phenomena expected for that hypothesis, enabling the cryptanalyst to derive a measure of acceptance or rejection of the hypothesis. This will be elaborated upon in succeeding paragraphs.

**73. The diagnostician and his attributes.**³—*a.* What sort of person would we choose for the ideal diagnostician? What abilities, traits of character, and experience must he have? In order to answer these questions, we must look at the problem of diagnosis itself. In brief, the task of the diagnostician consists of collecting and organizing available material, searching for and recognizing phenomena, building up hypotheses and making every effort to knock them down again. Let us examine each stage and see what is required of our Compleat Diagnostician.

*b.* While the collecting and organizing of material and relevant information may frequently not be under the diagnostician's direct control, he must ensure that no useful evidence is beyond his reach. This means that he must be familiar with the collection process and must be able to specify the form in which the material is presented to him. With a fairly naïve encipherment system, or in any case if there is not too much material, he should normally start with the hard copies of the intercepted messages

³ This paragraph ("The diagnostician and his attributes") is taken, with but minor changes, from D. A. Wilson's delightful paper, "Education in Diagnosis," appearing in the *NSA Technical Journal*, Vol. XIV, No. 1, Winter 1969.

themselves, and preferably do his own logging of traffic, at least initially. With more sophisticated and more voluminous systems, he will be forced to make use of data processing machinery or a computer for logging or "diarization" (i.e., the process of indicating the positions at which interesting features or passages occur in the messages). Under these circumstances the computer may deign to show him only those stretches of material which it finds interesting. He must then firmly insist on seeing periodically a selection of "normal" traffic, in order that he may both remind himself of what normal traffic looks like and with luck find new phenomena which the computer blindly ignores. He must either himself be able to program or at least be able to communicate sensibly with the programmer.

c. The diagnostic expert must also familiarize himself with the cryptographic background of the system. He must study both predecessor and contemporary systems which may have been conceived under the same roof, and he must know something about the users of the system and be able to deduce the likely degree of cryptographic sophistication and the required portability of the encipherment material. He must appreciate the value of external and nontextual features of the transmissions (the traffic analyst will probably be able to explain some, but not all of these), and he has to be familiar with the likely causes of busts, due both to faulty operators and, in the case of machine ciphers, to faulty machinery.

d. Up to now, our Compleat Diagnostician appears as a technical administrator. The main quality required is the ability to digest large amounts of information and retain the main gist in the front of his mind while taking care not to push the smallest scrap out at the back. He must be thorough and careful. He also needs to have some organizational capability, a technical knowledge of cryptographic systems, transmission systems, and probably programming.

e. Having put his material into a convenient form, the analyst enters the most critical stage of the diagnostic process. He has to search for, and find, phenomena. Without any phenomena to work with, diagnosis is impossible. The first thing to do is to look at the material. As I. J. Good remarks in his "Standard Reagents and Diagnostician's Dictionary," it may be plain text! Even if it is not, interesting features may spring to the eye. Long repeats, limitations, suspicions of rough frequency counts, excesses of doublets, indications of a significant width, depths, isologs, indicators, and many more phenomena may be found in a quick, not necessarily systematic, look at a few messages.

f. Unless enough evidence has now been found to have a first shot at establishing and testing a hypothesis, the diagnostician moves on to obtaining and examining descriptive statistics—numerical summaries of the material. Examples are frequency counts, repeat rates or indices of coincidence, pattern counts, and level and density counts of teleprinter text. Often these will be done on computers.

g. Throughout this search, the analyst is on the lookout for anything out of the ordinary, any departure from normal procedure or normal-looking traffic, and also for any consistent feature throughout the traffic which would not be expected in a random sequence of letters. His main task is to decide which of the features he sees (or thinks he sees) are important in one of these ways. He must recognize phenomena; he must also recognize when a suspected feature is a nonphenomenon.

h. The qualities possessed by our Compleat Diagnostician which make him an expert in finding phenomena are elusive. Certainly experience of phenomena which have proved helpful in the past is important. Knowledge of enciphering systems and their features, combined with the background information of subpar. c may help him to decide what to look for, but he does not blindly follow the path along which they lead: new systems usually have new features. It is not enough to say that he is observant; the word is so general that in this context it is almost devoid of meaning. His powers of observation are peculiarly imaginative. While looking at his material he must have in mind a multiplicity of possible features he would like to find, but frequently the most important observations are phenomena he could not have forecast. He must have an appreciation of pattern, and his mind works in a way which would probably give him a good score in a diagrammatic intelligence test. Possibly sheer physical ocular athleticism or a wide field of vision may contribute. If we could define that something implicit in the statement that he has a cryptanalytic "green thumb" we would be much nearer to understanding the crux of the diagnostic process. It is this something that separates our Compleat Diagnostician from the run-of-the-mill analyst who views diagnosis as merely the application of a sequence of standard statistical tests.

i. The assessment of the phenomena which have come to light requires a judgment of their value—a statistical common sense based on the concept, and frequently on the practical application, of sig-

nificance tests. Furthermore, the diagnostician realizes that some of his significant features may really be only subphenomena, and is always ready to hunt for related features which will support a more general hypothesis. For instance, having observed a significant number of repeats at a certain distance he will want to know whether this is supported by a rough digraph count at that distance, or by repeats at multiples or factors of the original distance.

*j.* The next stage in the process is the setting up of hypotheses, to be followed by attempts to upset these same hypotheses. Each hypothesis should explain as many as possible of the observed phenomena. This explanation is then tested in two ways: first by deciding whether the remaining phenomena which have been seen conflict with the hypothesis, and second by predicting further phenomena which might be expected if the hypothesis is true and looking to see whether they exist.

*k.* In the more naïve systems the hypothesis will often be a complete tentative specification of the encipherment process, but this will rarely be the case with a sophisticated problem. Here the hypotheses will usually be either the restriction of the system to a general class (e.g., transposition of some kind, additive mod 26, binary linear recursive key), or a precise specification of some small detail (the existence of a Hagelin-type slide feature). The diagnosis of a sophisticated noncommercial machine may require the establishment of hundreds of viable partial hypotheses of this kind, gradually building up the complete picture from hosts of small details.

*l.* Here our Compleat Diagnostician needs the qualities of imagination, impartiality, deduction and ability to synthesize—in short, he is a good research scientist. He must be imaginative in his construction of hypotheses, deductive in predicting resultant expected phenomena, and impartial in his interpretation of the results of the tests of his hypothesis. The synthesis of many partial hypotheses brings in again his grasp of previous and contemporary systems—which must also have contributed to his selection of hypotheses in the first place. In machine systems a working knowledge of mechanics, electromechanics, or electronics is needed to diagnose faulty conditions and to predict other faults which are likely to occur.

*m.* Little has been said about the actual testing of hypotheses. Obviously our Compleat Diagnostician must be familiar with all the routine standard tests and conversant enough with testing theory to devise special tests where no appropriate ones are known. He must always ensure that his hypotheses can be tested—this will be a brake which keeps his imagination under control. Finally he remembers that the acid test of diagnosis is the reading of plain text, although the diagnostic process is seldom complete when the first sensible text emerges.

*n.* This concludes the list of qualities peculiarly appropriate to the diagnostician. Add to these the attributes we like to see in any senior cryptanalyst (perseverance, the ability to communicate and to keep a record of ideas and results, drive, supervisory capabilities, sheer common sense, etc.) and the list becomes formidable indeed. We begin to understand why so few really first-class diagnosticians emerge from the maelstrom of the cryptologic community.

**74. Embarking on the unknown cryptosystem.**—*a.* Let us suppose that we have been given traffic in an unknown cryptosystem and have been asked to solve the messages. In preparation for this likely event we will arm ourselves with information and facts, as outlined below.

*b.* The first step should be to find out all that is known, communications-wise and cryptologically speaking, about the origin of the messages. Is the target country known, say, Zendia, or is it undetermined? If it is Zendia, we (or someone in the research section) should tap all information sources about its past cryptologic history and national cryptographic habits, and we should obtain at least a general familiarity with its language, geography, political and military structure, industrial resources, and key personalities. If information on past cryptologic history is sparse, we take into account information on countries with which Zendia has an alliance, in case there is foreign influence in her communications.

*c.* We endeavor, through traffic analysis and other sources, to determine who the users of the cryptosystem might be—army, navy, air force, ambassadors, police, etc.—and in so doing, we make conjectures as to the probable content of the messages. We take note of the extent of use of the cryptosystem, and construct a cryptonet diagram.

*d.* If there is a predecessor system that has been read, we study decrypts and take note of the subject matter treated. Is there a high incidence of stereotyped beginnings or endings, or are there fairly rigid formats to some of the messages, and if so, between what stations or organizations? What procedures

are there, if any, for the use of nulls, message bisection, and padding, and what conventions are there for the spelling out of digits? On what links or lanes have exploitable violations or weaknesses occurred in the past?

e. If the cryptosystem does not have a readable predecessor, does plain-language traffic intercepted on the links carrying the encrypted traffic yield any information that might be used as a break-in into the system? Is there any information of potential cryptanalytic value in the associated chatter? Do other intelligence sources yield any information of use? Do the formats of the messages (e.g., 5-digit, 4-letter), or the traffic volume, or the message lengths (e.g., a preponderance of messages exactly 32 groups long) give any suggestions as to the probable system? What are the probable cryptosecurity requirements of the system? If it is military traffic at corps or army level, the security of the system is expected to be high, possibly machine cipher, used under favorable operating conditions, with sufficiently rugged equipment, operated by personnel with adequate training. On the other hand, military traffic at, say, regimental level may be expected to be less secure, possibly a manual system, one which might be used under unfavorable operating conditions by personnel inadequately trained and under pressure of time or the exigencies of combat conditions. What is the probable reason for the introduction of the system; or, if it has a predecessor, the reason for the change of system?

f. Where the language of the encrypted messages is known or can be assumed, it goes without saying that we should equip ourselves with the necessary cryptolinguistic letter frequency and other data that will aid us in our analysis. All too frequently, especially in the rarer languages, such information has not been compiled in sufficient detail, or its existence is unknown, or worse yet, cannot be found.

**75. Preliminary actions in attacking the unknown cryptosystem.**—a. Let us assume that a pile of 5-letter traffic in an unknown cryptosystem has been placed on our desk. The messages bear an apparent discriminant, DICID, in the A1 position; therefore they may be presumed to be homogeneous.⁴ The nationality of the target is uncertain, but the nets on which the traffic has been intercepted are presumed to be Zendian. We have taken into consideration the points discussed in par. 74, and we have rolled up our sleeves in preparation for the battle of wits: our cryptanalytic prowess against the enemy's cryptographic strength.

b. We begin by leafing casually, even unsystematically, through the messages, to see what we can see—and at this stage we really don't know what we expect to see—it suffices to keep an open, observant mind.⁵ After a brief period of sampling the visible "flavor" of the messages, looking for anything that seems peculiar or out of the ordinary, we sort the traffic with the idea of assurance of maximum cryptographic homogeneity. If we have enough traffic, we can afford to restrict ourselves to sorting the traffic by net or even link, and within that by date; otherwise, we would be content with logging one or two months' messages, say, in date-time⁶ order. The logs optimally should contain all of the elements of the preamble and, say, the first five and last five groups of text. (If the volume of the traffic is too great,

⁴ Homogeneity is a relative term, with different meanings in different contexts: in speaking of an enciphered code system, homogeneous traffic might be considered as embracing messages encrypted with the same code book and additive book; in a machine system, homogeneous traffic might be interpreted as consisting of messages enciphered with the same internal pin- and lug-settings, or the same rotor order; in a transposition system, homogeneous messages might be thought of as those enciphered with the same matrix and transposition key; in a Playfair system, since there is only one variable, viz., the Playfair square, homogeneous messages would be those enciphered with the same square. These are anything but precise definitions; for example, if the enemy were using several types of code and enciphered code systems, and also Playfair systems, the several different Playfair systems taken together might be considered as a homogeneous grouping vis-à-vis the other nonrelated systems. In the case at hand, since the A1 groups of all the messages are the same 5-letter group, DICID, the traffic is homogeneous to that degree. But there are varying degrees of homogeneity: there might be another nontextual indicator among the groups of the message (or even in the preamble) which could further delimit the homogeneity; or only the traffic within a certain time period (e.g., month, week, day, 6 hours) might be homogeneous in the second degree; or only the traffic within a particular geographical area; or only traffic within a specified net or link, or even lane; or, for that matter, only traffic from a particular originator, regardless of addressee.

⁵ A mistake, unfortunately all too common in operational practice, is disassociating plain-language messages and chatter from the encrypted traffic before it gets to the cryptanalyst. We should endeavor to examine the rolls of intercept copy as they come from the intercept operator, before they are cut up and the encrypted messages removed. Also, in sorting out duplicate messages, we should make sure that apparent "duplicates" are not really *bust messages*: fingers have been burnt in this situation more than once.

⁶ File date-time, when this is in the preamble or postamble, and not intercept date-time.

this would call for the logs to be prepared by machine methods; otherwise, hand logging should suffice ⁷—besides, we would become more intimately familiar with the traffic if the messages were logged by hand. Even if the logs are made by machine, it might not be a bad idea to take a limited amount of material, say an active link on a particular day or week, and log that much by hand for its instructional value.) The logs are then examined to see if anything of interest turns up; e.g., repeated groups between the messages near their beginnings or endings, limitation or association of characters near the beginnings and endings, or any correlation between preamble components and text groups. Columnar frequency counts of the *a*, *b*, *c*, *d*, and *e* positions of the A2 (and perhaps the A3) groups of the messages are taken; if the A2 (or A3) is an indicator group, such counts might reveal limitations or other phenomena often associated with indicators. Similar counts might be made with the Z0 and Z1 groups.

c. We now examine the messages themselves, assisted by our log. We take a good look at the messages having (1) the same serial number (i.e., station serial number, or message center number if there be one), (2) identical A2 groups (or if an indicator were not apparent as in this DICID system, identical A1 groups), (3) identical file date/times, (4) identical group counts, (5) sequential station serial numbers, (6) limitations in the beginning or ending groups, (7) polygraphic repetitions in the beginning or ending groups, either within or between messages, and (8) isomorphic beginnings or endings, which might arise from identical underlying plain text enciphered by different keys. Traffic emanating from each originator is compared, taking special note of messages going to the same addressee; and it might not be amiss, for that matter, to compare traffic going to each addressee, taking note of messages from the same originator. Traffic from both ends of a link is compared for possible polygraphic repetitions or other phenomena between messages which might earmark the use of identical keys (even including a mistake in the use of the wrong pad in a one-time-pad system which could then enable the reading of the resultant two messages in depth if the components are known or can be assumed). We also keep our eyes open for sets of messages that are likely to have similar—perhaps even proforma—content, which might be profitable to study separately. Practice traffic, if identified at this stage, should be removed from the message file. Suspected bust messages, resends, isologs, staggers, and any unusual situations should be worked on without delay; but we should be reasonable about the time spent on unsystematic fiddling at this stage. We study the group counts of the messages for evidence of key-length limitations and number of nontextual groups, and we do the “remainder test” for evidence of the length of the underlying cryptographic units.

**76. First step: manipulating the data.**—*a.* At the outset, it should be clear why diagnosis in cryptanalysis is at all possible: the plain text underlying cryptograms has pronounced properties of frequency variation and repetition, and these properties can be made to show through the cryptographic disguise by proper manipulation of the encrypted text. It is obvious that if the underlying text were flat, having no properties distinguishable from random, nothing would be manifested in its encryption, no matter what striking properties or characteristics were inherent in the application of the cryptosystem. In other words, flat “plain text” plus key, no matter how rough, will yield flat (i.e., random) cipher. But the converse is also true: rough plain text plus flat key will also yield flat cipher. Therefore, *as long as the cryptosystem has sufficiently nonrandom properties in its make-up, if the underlying plain text has a characteristic roughness, diagnosis and solution are possible.* But given the case of the encryption of plain text in a one-time-pad system in which the key is produced by a random process and has no limitations, characteristics, or patterns that are distinguishable from random, and where neither the key nor any portion of it is ever used again for the encryption of another message, solution is demonstrably impossible.

*b.* Even in the absence of cryptanalysis of messages, the patent characteristics of the encrypted texts and the manner in which traffic is passed from originator to addressee can yield information when there is either adherence to or departure from *established norms*: this is the essence of traffic analysis.⁸ For example, three-letter traffic suggests a three-letter code system; the composition of a radio net and the manner of its working yield information on the relative subordination of the units or organizations involved; the relaying of a message from A to B to C discloses the existence of certain information channels, and if the message is reencrypted on the second leg of its journey an isolog will be produced;

⁷ As we log each message, we look over the *entire* text, to catch anything that might be unusual.

⁸ See in this connection par. 74 of Appendix 7 (“Communication Intelligence Operations”), *Military Cryptanalytics Part I*, and also Appendix 7 (“Introduction to Traffic Analysis”), *Military Cryptanalytics, Part II*.

a sudden increase in traffic volume on a particular link or net, which had been stable for some time, can be the prelude to an impending operation or activity.

c. When we manipulate data from the texts of messages, we are looking for characteristics of the underlying plain text to show through in some degree. When we examine our traffic logs, we look for signs that are characteristic, for example, of isologs, retransmissions, apparent mistakes of communications or cryptography; we find these because we know how these features are reflected in the logs. For example, in searching for isologs we look for messages of the same or nearly the same group count, sent within a relatively short time span (say, from less than an hour up to a day or two) from one originator to (preferably) the same addressee, or sent from an originator to two or more (possibly subordinate) addressees; and we also look for isologs on other legs of possible relays. Mistakes (so-called "busts") can be uncovered by astute observation, or we can also be helped immeasurably by operator chatter such as "You set the 47-wheel incorrectly, you blithering idiot!" which tells us that the cryptosystem is in all probability a machine system, and that the machine has a "47-wheel" (this might be either a 47-point wheel, or one with 47 marked positions on it, or simply a wheel marked "No. 47").

d. In this numbered paragraph, emphasis will be placed on the manipulation of data to uncover nonrandom characteristics or manifestations. Par. 77 deals with recognizing phenomena, and par. 78 with interpreting phenomena; but because cryptodiagnosis really does not keep entirely separate the steps of manipulating data and recognizing and interpreting phenomena, the discussion in pars. 76-78 perforce will overlap in these aspects.

e. The study of the group counts of messages can yield information of considerable importance to the cryptanalyst, as can be shown by the two examples which follow. In studying these group counts, we could make a simple tabulation in group-count order; we could group the data into classes such as all messages of group counts 21-25, 26-30, etc.; we could group them into two classes, those messages with an odd number of groups, and those with an even number; or we could study the group counts of messages (1) having a particular discriminant or indicator, (2) sent by a particular station, or (3) sent at a particular time of the day. The data manipulation in the two examples below consists merely of recording the group counts in a form suitable for study: in this case, in group count order.

(1) For the first example, the group counts of 100 messages have been tabulated; the traffic (apparently high-grade because of the importance of the users, and also because of the lack of visible properties) consists of messages sent in 5-digit groups, with a group count range of 21-99. In the diagram below, the columns labelled "GR" are the group counts, the columns labelled "Msgs" give the number of messages having the particular group count. The striking peaks at group counts of 32, 63, and 94 are noted. As a possible explanation of this phenomenon, we could arrive at the hypothesis (1) that there is involved a key book containing blocks of 30 key groups each, or a stencil system with 30 5-digit key-groups exposed by the apertures, (2) that the location of the first block is given by two indicator groups, and (3) that subsequent blocks require but one indicator group to designate their location. Under this hypothesis, then, it would be possible to have a 32-group message, but not 33, because the next greater length would have to be 34: 32 groups for the first block including the indicators, and one more indicator plus one more text group. Likewise, the next message length after 63 groups must be 65, and the next after 94 must be 96. This hypothesis is strengthened by the absence of messages having group counts of 33, 64, and 95. A further hypothesis is made that the underlying text is cipher text rather than code text. The reasoning behind this assumption is that the cryptographic clerk, mindful of the key-length limitation of 30 groups, tries out of either laziness or economy not to go only one or two groups beyond the block limitation; thus, he might abbreviate a signature, or spell the last STOP or two as "STP," or make other slight changes—easier in a *cipher* system than in a *code* system—to avoid exceeding the imposed limitation. And as for the reason why the preponderance of plain texts happens to be groups of 30 and its multiples, perhaps it is because of the particular contents of the messages, or because of certain habits being followed as regards padding to fill out a convenient 30 groups—quién sabe? With further examination and analysis of the traffic, we should be able to prove or disprove our hypotheses—at least we have made a beginning, and we can pursue the trail we have hewn for ourselves.

GR Msgs	GR Msgs	GR Msgs	GR Msgs	GR Msgs	GR Msgs	GR Msgs	GR Msgs
21	1	31	1	41		51	1
22	1	32	6	42	2	52	1
23	1	33		43		53	2
24		34	1	44	1	54	
25	1	35	3	45	2	55	4
26		36	3	46		56	
27	1	37	2	47	1	57	1
28		38	1	48		58	1
29	1	39		49	2	59	2
30	1	40		50	3	60	4
						61	4
						62	1
						63	8
						64	
						65	1
						66	1
						67	1
						68	2
						69	
						70	1
						71	1
						72	2
						73	
						74	2
						75	
						76	2
						77	1
						78	2
						79	
						80	1
						81	
						82	2
						83	
						84	1
						85	1
						86	
						87	1
						88	
						89	1
						90	2
						91	
						92	2
						93	
						94	5
						95	
						96	
						97	1
						98	1
						99	1
						100	

FIGURE 166

(2) For the second example, we shall study the group counts of 200 messages from an actual operational situation. The traffic, presumably high-grade, consists of messages sent in 5-digit groups, and the group-count range is from 23 to 100 groups.

GR Msgs	GR Msgs	GR Mscs	GR Msgs	GR Msgs	GR Msgs	GR Msgs	GR Msgs
21		31	1	41	1	51	1
22		32	1	42	4	52	
23	1	33		43	1	53	4
24		34	1	44	1	54	5
25		35	3	45	1	55	4
26	1	36	2	46	3	56	4
27		37	1	47	1	57	1
28	1	38	2	48	2	58	6
29		39	2	49	1	59	4
30		40	1	50	5	60	4
						61	4
						62	4
						63	3
						64	2
						65	4
						66	7
						67	1
						68	4
						69	4
						70	9
						71	4
						72	1
						73	3
						74	8
						75	6
						76	2
						77	1
						78	6
						79	4
						80	3
						81	4
						82	5
						83	1
						84	2
						85	3
						86	6
						87	3
						88	4
						89	1
						90	4
						91	1
						92	1
						93	2
						94	2
						95	1
						96	2
						97	1
						98	4
						99	1
						100	2

FIGURE 167

If nothing about the traffic were known, it would be wise to determine the size of the underlying cryptographic units, if possible, and also uncover any evidence as to the existence of nontextual groups that might be indicators. The procedure called for here is the *remainder test*, applicable when the last group has been padded with an indeterminate number of disguised nulls necessary to complete the group. If the text is sent in 5-character groups, the modular (remainder) counts after dividing by 2 (testing for underlying dinomic text), by 3 (for trinomic text), and by 4 (for tetranomic text) have the following expected percentages: ⁹

<i>Dinomic</i>	<i>Trinomic</i>	<i>Tetranomic</i>
2N + 0 = 60%	3N + 0 = 40%	4N + 0 = 40%
2N + 1 = 40%	3N + 1 = 20%	4N + 1 = 20%
	3N + 2 = 40%	4N + 2 = 20%
		4N + 3 = 20%

If the underlying text is pentanomic, or if it consists of irregular-length units, the remainder test will be inconclusive. (Parenthetically, *tetranomic* text when examined on a *dinomic* basis also gives a distribution of 60% and 40% for remainders of 0 and 1, respectively, but there is no confusion since the tetranomic examination will give its proof. If, however, *dinomic* text is examined on a *tetranomic* basis, the distribution will be 30%, 20%, 30%, 20% for remainders of 0, 1, 2, and 3, respectively.) As an illustration, if the underlying text is, say, trinomic, the messages with group counts exactly divisible by 3 with no remainder will account for 40%, those with a remainder of 1 will account for 20%, and those with a remainder of 2 will account for 40%. If, however, there is one nontextual group present, the counts will be shifted cyclically one position downward, resulting in a distribution of 40%, 40%, 20% for remainders 0, 1, and 2; and if there are two nontextual groups present, the counts will be displaced cyclically two positions downward, resulting in a distribution of 20%, 40%, 40% for remainders 0, 1, and 2. In the

⁹ The reason for these percentages is not difficult to see. Taking the example of underlying dinomic text, we might have to add 1, 2, 3, or 4 nulls to complete the final group, unless it is already a complete group of five; thus we have the following five cases:

- a. 12121 21212 (2N+0)
- b. 12121 21212 12XXX (2N+1)
- c. 12121 21212 1212X (2N+1)
- d. 12121 21212 12121 2XXXX (2N+0)
- e. 12121 21212 12121 212XX (2N+0)

It can be seen that in three of the five cases (60%) the group counts of messages are exactly divisible by 2 with no remainder, and in two of the five cases (40%) there is a remainder of 1. In underlying trinomic text, we have the following five cases:

- a. 12312 31231 23123 (3N+0)
- b. 12312 31231 23123 123XX (3N+1)
- c. 12312 31231 23123 12312 3XXXX (3N+2)
- d. 12312 31231 23123 12312 3123X (3N+2)
- e. 12312 31231 23123 12312 31231 23XXX (3N+0)

In two of the cases (40%) the group counts are exactly divisible by 3, in one case (20%) there is a remainder of 1, and in two cases (40%) there is a remainder of 2. In underlying tetranomic text, we have the following five cases:

- a. 12341 23412 34123 41234 (4N+0)
- b. 12341 23412 34123 41234 1234X (4N+1)
- c. 12341 23412 34123 41234 12341 234XX (4N+2)
- d. 12341 23412 34123 41234 12341 23412 34XXX (4N+3)
- e. 12341 23412 34123 41234 12341 23412 34123 4XXXX (4N+0)

In two of the cases (40%) the group counts are exactly divisible by 4, and in the remaining three cases there is one case each (20%, 20%, 20%) of remainders of 1, 2, 3.



example given in Fig. 167, the group counts have the following remainders when examined on hypotheses of underlying dinomic, trinomic, and tetranomic text:¹⁰

<i>Dinomic</i>	<i>Trinomic</i>	<i>Tetranomic</i>
2N + 0 = 121 (60.5%)	3N + 0 = 67 (33.5%)	4N + 0 = 39 (19.5%)
2N + 1 = 79 (39.5%)	3N + 1 = 63 (31.5%)	4N + 1 = 36 (18.0%)
	3N + 2 = 70 (35.5%)	4N + 2 = 82 (41.0%)
		4N + 3 = 43 (21.5%)

It is clear that the underlying text must be tetranomic, and that there are two nontextual groups (probably indicators) present.¹¹

f. An important phase of cryptanalysis, one which can be crucial especially in the early stages of analysis, is the study of indicators. In general, there are two kinds of indicators: (1) system indicators (also called "discriminants"), which define the sets of cryptomaterials used, and (2) message indicators, which define the specific application of the cryptomaterials or keys. Indicators may be recognized as such (1) if they are repeated in the message text; (2) if they possess distinctive patterns; (3) if they have limitations or characteristics in their elements; (4) if there are associations in the messages between the indicators and another group (which may be a text group, a second indicator, or an indicator check group); (5) if there are associations between the indicator and some element or elements in the preamble; or (6) if they have a roughness different from that of the message texts. These several aspects will now be illustrated.

(1) Below are exemplified sets of groups with patently obvious patterns and characteristics, different from the rest of the message texts, which categorize them as indicators:

(a)	(b)	(c)	(d)	(e)	(f)	(g)	(h)
COBRA	BABAX	AIRBC	ZEBEC	DARIC	59329	81473	LAMIV
GRAVY	NONOX	EGQBC	ZEVUB	GOSUK	07726	04739	DCGBI
ALBUM	PIPIX	EFNBC	ZEMIN	JENIM	83573	35320	CVYML
NYLON	GAGAX	BKRBC	ZESOW	CUVOD	30317	52691	RBTTN
BONUS	ZUZUX	DGOBC	ZEDIG	MIWEH	92102	29903	VCYLK
EAGLE	MEMEX	AJLBC	ZELEM	BORAB	14230	75858	MIVFB
ROYAL	TUTUX	CFLBC	ZEWIZ	BOQAC	48754	18761	ZDDTX
YODEL	DODOX	BIPBC	ZEDAD	LAZUF	25186	93227	HSACD
GLORY	HAHAX	DJLBC	ZEZUF	HIXEB	31947	43042	QGXR P
LIVER	QE QEX	CHMBC	ZECOG	KUTIL	73820	56435	TPJLV

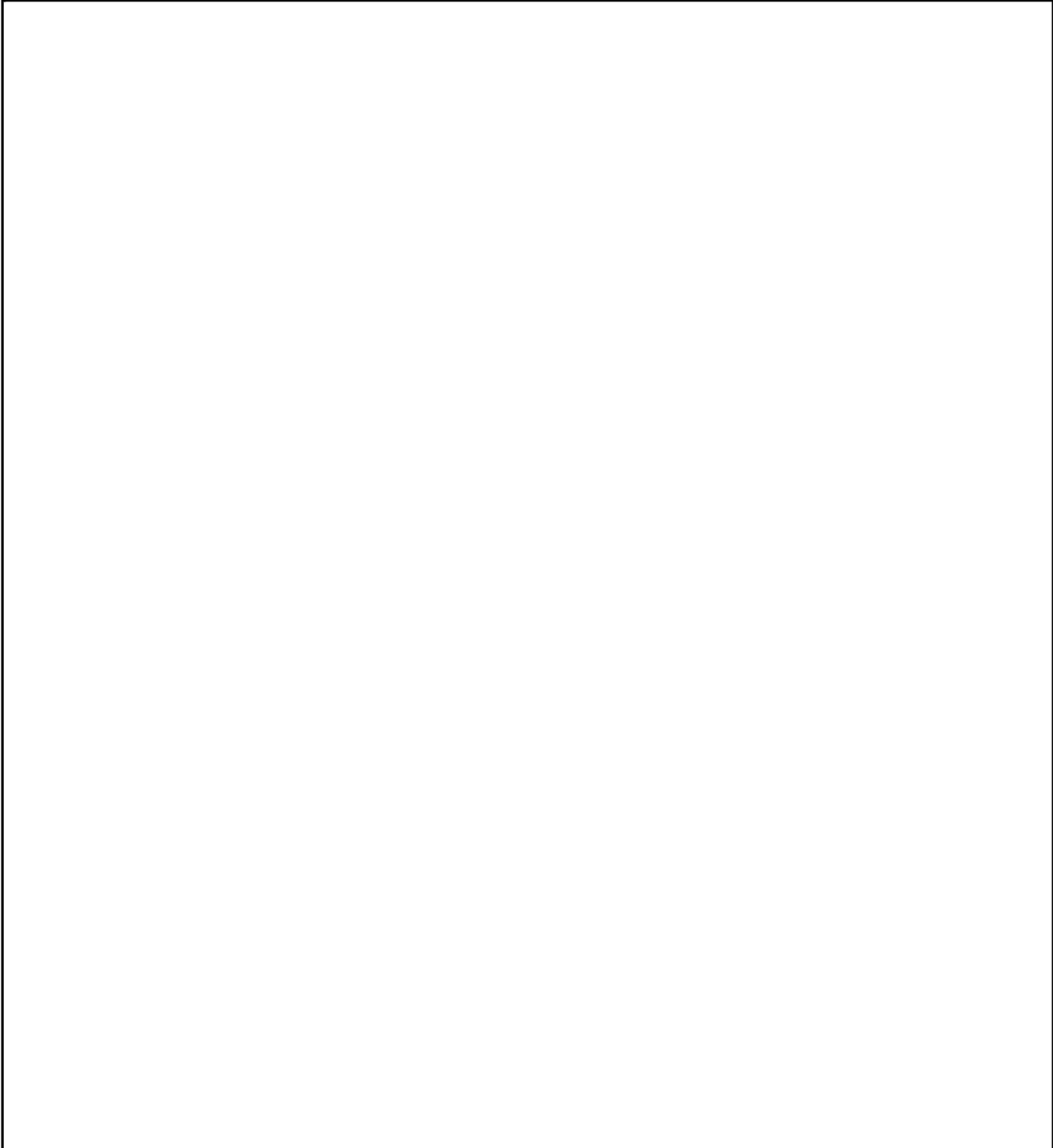
¹⁰ The easiest way to take remainder counts is with a desk calculator, "zoning" the keyboard into four (and then three) areas with the column markers, and recording the group counts four (and then three) at a time from the group-count record sheet: the accumulated totals will appear in the four (and then three) areas of the indicating dials. The remainder counts for the dinomic hypothesis are obtained easily from those of the tetranomic hypothesis, by adding together the counts of remainders 0 and 2, and those of 1 and 3: these are now the dinomic remainder totals for 0 and 1, respectively.

¹¹ Note, as an additional example, the remainder counts of the 100 messages given in Fig. 166:

<i>Dinomic</i>	<i>Trinomic</i>	<i>Tetranomic</i>
2N + 0 = 52	3N + 0 = 34	4N + 0 = 25
2N + 1 = 48	3N + 1 = 32	4N + 1 = 21
	3N + 2 = 34	4N + 2 = 27
		4N + 3 = 27

The remainder test here is inconclusive, showing that the underlying text either is pentanomic or consists of units of irregular length. Since in that example we had come to a conclusion that the underlying text was cipher rather than code, we can arrive at the tentative hypothesis that what we are faced with is probably an enciphered monome-dinome system. As a parenthetical aside, it is important when employing the remainder test (1) that the material under study be homogeneous, and (2) that the group counts are not biased in favor of a particular group count, which might give misleading results.

In set (a) the indicators are self-evident, with 5-letter dictionary words used to convey the specific keying information; set (b) apparently embraces a potential 100 (or perhaps 120) keys or starting positions; set (c), 210 keys or starting positions; set (d), 100 keys or starting positions; and set (e), 2500 keys or starting positions. From sets (d) and (e) we may reconstruct the permutation tables¹² involved, supporting our contention as to the total number of possible indicators. Set (f) consists of sum-checking groups, and set (g) consists of groups self-summing to a constant 3, mod 10. Set (h) is harder to analyze, but on close examination it is seen that the middle letter is the mod 26 sum of the first two, and the last letter is the mod 26 sum of the third and fourth letters.



(b) (1)  
(b) (3) -18 USC 798  
(b) (3) -50 USC 3024(i)  
(b) (3) -P.L. 86-36

(4) When indicators are enciphered, particularly in numerical cryptosystems, an additive key for encrypting the plaintext indicator has often been taken from a text group or groups near the beginning of the message or near the end. (Sometimes elements of the preamble, such as the group count, the message center number ¹³—if there is one—or the file date/time have also been used as key.) These latent indicators

¹³ The message center number (abbreviated "MCN") is a serial number assigned by a message center; this should not be confused with the station serial number (abbreviated "NR") which is that assigned by the radio operator to all messages in order of their transmission.

(b) (1)  
(b) (3)-18 USC 798  
(b) (3)-50 USC 3024(i)  
(b) (3)-P.L. 86-36

are made patent by manipulation; subtracting all pairs of groups digit-by-digit, say A1 to A5 and Z4 to Z0, might uncover relevant phenomena. Let us study the following example of a log:

To	From	NR	FDT	GR	A1	A2	A3	A4	A5	Z1	Z0
DRW	WTZ	451	160752	62	30303	67470	82148	08651	32823	06647	09384
DRW	WTZ	452	160805	81	30303	21387	46095	50582	23172	53594	08128
DRW	WTZ	453	160817	65	30303	74582	98111	74502	84102	70193	85211
DRW	WTZ	454	160824	46	30303	82083	05559	64462	29489	54930	38196
DRW	WTZ	455	160830	84	30303	51756	74288	10975	66593	34461	28475

Since the A1 is patently a discriminant, there might be an indicator in the A2 position; and if a text group is used for encipherment of the indicator, testing various groups near the beginning or end as trial additives might uncover some phenomenon. In the case at hand, subtracting the A3 from the A2 groups yields the following:

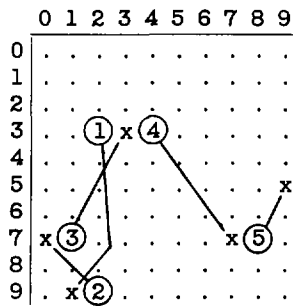
85332  
85392  
86471  
87534  
87578

The fact that the *a* and *b* digits sum to *c*, and that the numbers are in ascending sequence, is very interesting. Further study discloses an even more interesting phenomenon: since there are two nontextual groups (the discriminant and indicator), if we deduct 2 from each of the group counts, we can show that the messages are "tailing," with the system incorporating 10×10 additive pages of 100 groups each and the coordinates in normal order.¹⁴ Note that we could have seen the relationship between the A2 and A3 groups by differencing: the vertical differences between the *a* positions of the groups in the A2 column match the differences of the *a* positions of the groups in the A3 column; furthermore, the vertical differences in the A2 and A3 groups of the top two messages have the first trinome in common, as is also the case with the vertical differences of the last two messages.

(5) In the next example,

To	From	NR	FDT	GR	A1	A2	A3	A4	A5	Z1	Z0
CLD	SJO	827	171155	95	11033	14571	58536	64823	37867	83165	27120
CLD	SJO	828	171224	56	11033	38649	16650	19091	45648	56692	34603
CLD	SJO	829	171243	58	11033	81101	38012	48610	45432	66482	13393
RGF	SJO	361	171258	70	11033	79374	00559	60726	02491	41273	72458
RGF	SJO	362	171319	83	11033	23070	13078	70066	06315	58817	48815

¹⁴ In the diagram below we have plotted the message starting points and their lengths. Message no. 451 began at coordinates 3-2 for a total of 60 text groups ending at position 9-1; no. 452 began with the very next key group (9-2) for 79 text groups, ending at position 7-0; no. 453 began at position 7-1 and ended at position 3-3; no. 454 began at 3-4 and ended at 7-7; and no. 455 began at 7-8 and must have ended at 5-9.



the plaintext indicators underlying the A2 groups are uncovered by using the Z1 groups as key, recognizing the indicators as such on the basis of the sum-checking digits in the *c* position; had there not been this property of the indicators, an additional trial of the Z0 groups as key for the A3 groups would reveal the following deciphered indicator groups:

31416	31416
82057	82057
25729	25729
38101	38101
75263	75263

Differencing techniques here too can reveal the existing relationships in the example above. The difference between a pair of A2 and A3 groups will be found to be the same as the difference between the Z1 and Z0 groups of the same message.

(6) The preceding example had the plaintext indicators repeated in the A2 and A3 groups. In the next example,

To	From	NR	FDT	GR	A1	A2	A3	A4	A5	Z1	Z0
CTX	LFY	392	180806	81	55555	34464	40158	20920	96282	92540	91715
TIF	LFY	807	180821	24	55555	93215	83125	36436	78925	90360	01133
OLZ	LFY	496	180828	35	55555	66641	13894	05305	48820	46652	13841
FHJ	LFY	112	180845	60	55555	43193	79067	46951	94151	16094	33057
JRU	LFY	504	180905	54	55555	75541	32884	27036	57595	91953	09218

applying the Z0 groups as key for the A2 groups yields sum-checking *c* digits as the only noticeable property. But if we subtract the Z0 groups also from the A3 groups, we have the following:

43759	59443
92182	82092
53800	00053
10146	46010
76333	33676

The two separate indicator elements *ab* and *de* in the A2 groups have been transposed in the A3 groups to avoid a simple repetition of the indicator. In this example had we differenced the A2 and A3 groups, we would have uncovered the sum check in the *c* position, since the effect of the Z0 group would have been cancelled.

(7) For the next example we shall consider the following log:

To	From	NR	FDT	GR	A1	A2	A3	A4	A5	Z1	Z0
LXM	ZZA	739	191447	67	67890	27312	97444	61173	81932	61179	31051
LXM	OXL	624	191520	49	67890	56749	00750	18548	07446	23799	62749
LXM	NZM	124	191555	93	67890	03990	36773	56735	18857	52724	89122
LXM	DXY	368	191614	85	67890	05209	24516	79381	83011	94912	98336
LXM	KIR	902	191637	72	67890	50825	63650	73362	44065	66430	86021

This case is related to that in subpar. (6); the A2 and A3 groups contain the underlying indicators, and the keying groups are the A4 and Z0 groups. The second indicator is the same as the first, except that instead of summing the *ab* digits to *c*, the *cd* digits are summed to *e*, thus:

66249	66493
48201	48011
57265	57651
36928	36280
87563	87639

Here the relationships are harder to spot, but the difference between the *ab* digits of the A2 group and those of the A3 group will be the same as the difference between the *ab* digits of the A4 group and those of the Z0 group.

(8) Thus far in our examples the indicators have been in a fixed position in the body of the messages. The next case incorporates "floating indicators," with predetermined rules as to their location in the messages:

To	From	NR	FDT	GR	A1	A2	A3	A4	A5	Z1	Z0
MDX	HOU	751	210912	68	98765	69334	39494	63952	24737	19070	21798
MDX	HOU	751	220840	85	98765	60943	67038	70277	05392	17176	29317
MDX	HOU	751	230811	43	98765	67523	84674	43996	81846	76694	05132
MDX	HOU	752	230837	59	98765	00056	81271	15763	45263	56082	77857
MDX	HOU	753	230950	17	98765	71342	75778	56826	96091	73637	17872
MDX	HOU	754	231102	46	98765	14684	40901	85617	22495	34301	46549
MDX	HOU	751	240815	74	98765	58537	10507	92279	28474	68925	89235
MDX	HOU	752	241047	68	98765	42019	95611	21290	25709	21960	86403
MDX	HOU	753	241203	37	98765	44181	59813	62977	48329	47713	09960
MDX	HOU	754	241321	37	98765	51870	72113	49999	68212	99837	29780

This is more difficult of analysis, but the trial application of the Z0 group against the beginning groups of the messages yields the following at the indicated positions:

To	From	NR	FDT	GR	A1	A2	A3	A4	A5
MDX	HOU	751	210912	68	98765	48646	.....	.....	.....
MDX	HOU	751	220840	85	98765	.....	48721	.....	.....
MDX	HOU	751	230811	43	98765	.....	.....	48864	.....
MDX	HOU	752	230837	59	98765	.....	.....	48916	.....
MDX	HOU	753	230950	17	98765	.....	.....	49054	.....
MDX	HOU	754	231102	46	98765	.....	.....	49178	.....
MDX	HOU	751	240815	74	98765	.....	.....	.....	49249
MDX	HOU	752	241047	68	98765	.....	.....	.....	49306
MDX	HOU	753	241203	37	98765	.....	.....	.....	49469
MDX	HOU	754	241321	37	98765	.....	.....	.....	49532

The rule for placing the floating indicator is not difficult to see: the units digit of the date governs the location of the indicator in the first 10 groups of the message, after the discriminant. Note also the last two 37-group messages, sent by an originator to the same addressee, a little over an hour apart; they may be isologs.

(9) The following example involves another case of floating indicators:

To	From	NR	FDT	GR	A1	A2	A3	A4	A5	Z1	Z0
ITV	SKG	201	250600	64	24680	49951	05973	17328	19856	16096	31859
ITV	SKG	202	250637	81	24680	20531	50244	59455	34690	83026	42522
ABS	SKG	751	250654	53	24680	30825	33446	99810	85035	26193	11881
DLL	SKG	401	250745	72	24680	71010	36895	00313	78387	52886	58753
ITV	SKG	203	250801	46	24680	25459	32083	81420	61717	76691	47303
KZN	SKG	601	250836	79	24680	59825	34904	28755	99683	46873	11595
USR	SKG	551	250855	78	24680	62863	88235	73903	37875	93751	95778
ITV	SKG	204	250916	81	24680	91342	18577	80532	17122	68066	13001
USR	SKG	552	250941	87	24680	12787	89220	86111	15909	21642	01989
ABS	SKG	752	251137	63	24680	38095	25720	05164	10654	85863	27886

This, too, is difficult of analysis, but the trial application of the Z0 group against the beginning groups of the messages yields the following at the indicated positions:

To	From	NR	FDT	GR	A1	A2	A3	A4	A5
ITV	SKG	201	250600	64	24680	.....	.....	.....	88007
ITV	SKG	202	250637	81	24680	88019	.....	.....	.....
ABS	SKG	751	250654	53	24680	.....	.....	88039	.....
DLL	SKG	401	250745	72	24680	.....	88142	.....	.....
ITV	SKG	203	250801	46	24680	88156	.....	.....	.....
KZN	SKG	601	250836	79	24680	.....	.....	.....	88198
USR	SKG	551	250855	78	24680	.....	.....	88235	.....
ITV	SKG	204	250916	81	24680	88341	.....	.....	.....
USR	SKG	552	250941	87	24680	.....	88341	.....	.....
ABS	SKG	752	251137	63	24680	.....	.....	88388	.....

After a few moments' study we arrive at the rule for placing the floating indicator: the units digit of the group count, *mod 5*, governs the placement in the first five groups after the discriminant. Note also the two messages with the same indicator, 88341, which could be a possible depth:

To	From	NR	FDT	GR	A1	A2	A3	A4	A5
ITV	SKG	204	250916	81	24680	(88341)	18577	80532	17122 . . .
USR	SKG	552	250941	87	24680	12787	(88341)	86111	15909 . . .

The *a* digits of the first three text groups (1, 8, 1) hit in the two messages, and the *b* digits of the three text groups yield even differences between the two messages; if there is a high hit rate among the *a* digits in the two messages as superimposed,¹⁵ or if the even differences of the *b* digits prevail,¹⁶ we shall have proof that the messages are in depth.

(10) As the final example of enciphered indicators, let us study the following log:

To	From	NR	FDT	GR	A1	A2	A3	A4	A5	Z1	Z0
CBI	BOW	002	010832	68	13579	59361	53381	82796	87762	82303	01952
CBI	BOW	001	030816	46	13579	03530	18529	68995	43932	77362	25994
CBI	BOW	002	040820	50	13579	13891	24972	17752	54294	83479	13151
CBI	BOW	005	070848	82	13579	55748	57242	45415	99143	06959	50829
CBI	BOW	001	110800	95	13579	53311	68617	27855	91717	88907	50983
CBI	BOW	001	160812	45	13579	81754	63746	49393	34151	19255	06040
CBI	BOW	003	190825	63	13579	09277	01671	13900	55676	98488	24012
CBA	BOW	001	220815	78	13579	85836	16035	63707	34246	66010	47101
CBI	BOW	004	230837	72	13579	81942	95559	61989	41353	46767	83744
CBI	BOW	001	270802	59	13579	94482	55379	77472	58894	68471	04047

After some experimentation with differencing various groups, we arrive at subtracting A5 from A2, yielding the results shown in Fig. 168a, below. Interesting properties are uncovered, but the backward progression of the groups as deciphered does not please us, so we subtract A2 from A5, as shown in Fig. 168b. We now have serial indicators in the last three deciphered digits (except for apparently two missed messages), but there is something wrong with the initial dinomes. If we now take vertical differences of the consecutive initial dinomes, we observe that the differences (2, 1, 3, 4, 5, 3, 3, 1, 4) correspond exactly with the vertical differences on the consecutive file dates, if the differencing is done with borrowing subtraction instead of the more usual mod-10 arithmetic; we therefore subtract the dates from the (A5-A2) groups, yielding the plaintext indicators as shown in Fig. 168c. This means that the cryptographer's

¹⁵ Perhaps the underlying text is 5-digit code with a severe limitation in the *a* position.

¹⁶ This could be the result of an underlying 5-digit code wherein the *b* digits of all the groups have the same parity, all odd or all even.

method of encryption was first to add the two digits of the date (with carrying addition) to the *ab* positions of the plaintext indicator, and then use the A2 group as an additive (mod 10) for the modified indicator, burying the enciphered indicator in the A5 position.

A2	A5	A2-A5	A2	A5	A5-A2	Date	A5-A2	Ind.
59361	87762	72609	59361	87762	38401	01	38401	37401
03530	43932	60608	03530	43932	40402	03	40402	37402
13891	54294	69607	13891	54294	41403	04	41403	37403
55748	99143	66605	55748	99143	44405	07	44405	37405
53311	91717	62604	53311	91717	48406	11	48406	37406
81754	34151	57603	81754	34151	53407	16	53407	37407
09277	55676	54601	09277	55676	56409	19	56409	37409
85836	34246	51690	85836	34246	59410	22	59410	37410
81942	41353	40699	81942	41353	60411	23	60411	37411
94482	58894	46698	94482	58894	64412	27	64412	37412

FIGURE 168a

FIGURE 168b

FIGURE 168c

g. Before leaving the subject of indicators there are still a few points that should be brought out; these are listed below.

(1) As already shown, indicators may be in the clear, or they may be enciphered. An indicator may be inserted in the message preamble, or it may be derived by selecting certain elements of the preamble. In some systems the indicator may be either the page, row, and column of the additive book, or it may be one of the actual key groups on a page of key. If it is the latter case the quoted key may be the one used to encipher the first group of the message, or it may be the one immediately preceding the key group used to begin the text encryption.

(2) In the preceding examples the discriminants were shown in the clear as the A1 group, but there is no reason why they cannot be enciphered and for that matter also hidden among the text groups (as indeed has occurred operationally). The remarks on indicator encryption and on floating indicators apply equally well to discriminants. The discriminant may not necessarily be an entire group: it could be part of a group, even a single character.

(3) Whether indicators are in the clear or are enciphered, sometimes a single indicator suffices. But more often, indicators (either in the clear or enciphered) are repeated as a check. For example, when the A2 is consistently repeated as the Z0, this is most probably an indicator (unless it is a control group as discussed below). Sometimes the indicator is confirmed by a check indicator; for example, the check indicator being such that the mod-10 sum of the indicator and its check is 0 0 0 0 0, or the five digits of the check indicator comprise the sums *ab*, *bc*, *cd*, *de* and *ea* of the indicator digits. Cryptographers usually prefer to vary the appearance of the plaintext check indicator when it is enciphered, as has been shown in some of our examples.

(4) Discriminant (and also indicator) encipherment is sometimes governed by *control* elements in the message text or preamble, or both; these elements are not the actual key elements, but rather designate where the actual keys (from a separate list) may be found. The control elements might be found in an individual group, or they can be scattered. For example, the units digit of the group count in conjunction with the *a* element of the A3 group might designate the page of a 100-page key book to be consulted, and the *de* elements of the A3 might designate the row-column position of the key group which is to be used to encrypt the discriminant or indicator. In analysis, messages with hitting groups in the suspected discriminant position are examined, to determine which textual or preamble elements also hit consistently and thus point to the control elements involved. In the sets of message beginnings below, in which there are hits in the A1 group (the suspected position of a discriminant), it is apparent that the only consistent control for the discriminant encipherment must be the units digit of the group count, the *c* position of the A4 group, the *b* position of Z1, and the *e* position of Z0. (The last set, which is in apparent conflict with our findings, must involve a *noncausal* repetition of the A1 group.)



To	From	NR	FDT	GR	A1	A2	A3	A4	A5	Z1	Z0
DES	UAC	637	251435	83	53464	62080	46684	25906	94912	93313	67702
KCO	LRK	509	031102	53	53464	52104	75216	20969	66024	03580	81512
TVJ	UHW	225	171526	93	53464	25338	24300	35987	64073	73964	73262
IGR	BIU	618	131014	57	64291	92726	04269	82279	67823	54781	63600
IFZ	LPT	924	240819	47	64291	21641	21992	45263	15030	24618	29740
MOJ	SWT	036	291650	87	64291	74983	85054	94288	58692	64956	90970
KUD	RYU	492	161055	46	67629	21079	75093	02955	32116	53449	87202
NBW	CMV	578	180918	43	67629	25596	02364	80665	49911	98818	34797

(5) There are cases in which no discriminant is used, the appearance of the text being sufficient to denote the system; e.g., where a single unenciphered code system is being used, or a transposition system, or a bipartite system with self-evident row- and column coordinates. In these cases the only indicator will be a message indicator, if one is necessary.

(6) There have been instances when the key in certain low-grade systems was determined by the units digit of the group count (thus amounting to a single indicator digit), continuing in either an ascending or descending numerical sequence to produce a 10-digit cyclic key. In other instances the units digit (n) of the group count was the first key digit, the second key digit was (n+1), and thereafter the key was derived from the initial dinome by Fibonacci treatment, i.e.,  $a+b=c$ ,  $b+c=d$ , etc. Thus if the units digit of the group count were 2, the starting dinome would be 23, and the resulting Fibonacci sequence would be 2358314594 . . . which has a cycle of 60. (Other Fibonacci cycles, wherein  $a+b=c$ , have lengths of 20, 12, 4, 3, and the trivial length 1.) Additive keys for low-grade systems have sometimes also been taken from several elements appearing in the preamble of the messages. For example, the file date and time could constitute a 6-digit cyclic key; or the file date/time reversed plus the group count and the mod-10 sum of the latter could constitute a 9-digit additive key.

(7) In the study of indicator usage the analyst should be on the lookout for evidence both of tailing and trailing,¹⁷ not only on the basis of a chart as exemplified earlier, but also on the basis of the sequence of settings of various machine cryptosystems with which he is familiar. (As a parenthetical aside, although one-time-pad systems are wont to have tailing indicators, the assumption of a one-time-pad system is the last assumption an analyst should make about an unknown cryptosystem; after all, the keys may be used serially, and then re-used from the beginning again. There have been too many cases of traffic put aside under the label of "one-time-pad system" that was subsequently solved as some other type of system.)

(8) It is important to examine indicators of sequential messages, whether these indicators are in the clear, or enciphered, or decrypted, because sometimes the indicators may be related in some fashion from message to message. As an elementary example, let us suppose that we have intercepted a string of five messages from one originator, as shown in the log extract below:

To	From	NR	FDT	GR	A1	A2	A3	A4	A5	Z1	Z0
GJB	YPO	314	281142	63	56156	86175	75356	63698	07426	54252	93651
GJB	YPO	315	281159	42	56156	47823	78625	51818	41757	46728	29160
GJB	YPO	316	281220	49	56156	15057	90977	77279	38000	81647	10762
GJB	YPO	317	281312	55	56156	65528	06001	61452	49192	17321	17383
GJB	YPO	318	281336	50	56156	10704	72147	72350	14144	19735	80114

¹⁷ It might be well to define these two terms as given in the *Basic Cryptologic Glossary*:

"tailing, n. The practice of beginning the encipherment of one message with the elements of key immediately following those used to encipher the last textual element of the preceding message; equivalent in a machine cipher to starting the second message at the position reached by the machine on completion of the first."

"trailing, n. The practice of beginning the encipherment of one message with elements of key at a comparatively short interval after those used to encipher the last textual element of the preceding message; equivalent in a machine cipher to starting the second message at a machine position a few steps after that reached by the machine on completion of the first message."

The phenomena present in the A2 indicator groups make it possible to predict the indicators for succeeding messages, after it is noted that the Fibonacci addition of  $a + b$ ,  $b + c$ ,  $c + d$ ,  $d + e$ , and  $e + a$  of the digits of one indicator form the digits of the indicator for the next message. In another example, we have a log extract of five sequential messages that have been intercepted:

To	From	NR	FDT	GR	A1	A2	A3	A4	A5	Z1	Z0
WHM	PJY	428	051600	55	77788	86173	68548	16136	11573	52552	44611
WHM	PJY	429	051623	58	77788	57492	13347	57418	49468	43852	60739
WHM	PJY	430	051635	47	77788	33565	33239	07394	14333	45477	66794
WHM	PJY	431	051655	73	77788	80957	62416	86251	89835	69485	43263
WHM	PJY	432	051702	52	77788	13412	56209	92192	22184	27255	69611

In this example, the Fibonacci treatment has been applied *vertically* between messages in the column of A2 indicator groups, so that it becomes possible to predict the indicators for succeeding messages.¹⁸

(9) As a final note of caution on indicators, the number of possible different indicators in a particular indicator system does not necessarily reflect the number of possible distinctly different effective indicators. In an example given earlier, the first letters of the 5-letter groups were limited to the A-E range, the second letters to those in the F-K range, and the third letters to those in the L-R range (the last two letters appeared as a constant digraph, therefore possess no information value). The number of possible indicators is then  $5 \times 6 \times 7$  or 210; this number is either the total number of keys, or the total number of starting points in the key, or a lesser number of either, if *variants* happen to be involved; for all we know, if A and E are variants, as are also F/J, G/K, L/P, M/Q, and N/R, the number of distinct indicators is reduced to  $4 \times 4 \times 4$  or 64.

*h.* Having treated the diagnostics of message length characteristics and indicators, we shall now take up the manipulation of message texts. Both individual messages and sets of messages are subjected to study, in a manner calculated to make latent phenomena patent through manipulative processes (or, for that matter, to make patent phenomena more obvious). Depending on the volume of traffic at hand, we segregate messages by visible characteristics such as indicators, or we segregate messages sent within a relatively narrow time span; we compare messages sent by the same originator; or we compare those sent on the same day of the week (to uncover possible weekly re-use of keys), or on the same day of the month (to uncover possible monthly key rotas). As mentioned before, any phenomena uncovered may suggest subsequent steps to be taken. At this stage, the pertinency and utility of logging methods may be decisive. The manner of preparing worksheets and of summarizing statistical data play an important part in the timely solution of a cryptosystem. Sometimes the particular order of procedures and tests makes little difference, and at other times the order is of considerable importance.

*i.* In all of one's endeavors, the successful cryptanalyst's precept should be kept foremost in mind: "Try the simplest thing first." It is surprising how often this admonishment is disregarded, to the later chagrin of the cryptosinner. The comments by I. J. Good under the topic "rational behavior" are particularly germane to this discussion:¹⁹

"The principle of rational behavior is to maximize 'expected utility' per unit time. An example is that some experiments are worth performing mainly because they are quick and easy. The reasons are: (a) being quick, the 'expectation' of (value of the test)  $\div$  (time expended) is liable to be large because the denominator is small; (b) being easy, the hypothesis behind the experiment is usually simple and therefore has a nonnegligible initial probability of being true; (c) if easy things were not the most important, human beings would *already* be extinct.

"If of two hypotheses that are equally easy to test, one is much more useful if true, it may be more worth testing than the other, even if much less probable. This principle is perhaps more important in cryptanalysis than in other branches of science. Its relevance is sometimes obscured by the use of expressions such as 'I don't like this hypothesis,' which ought to mean 'I don't think its expected utility per unit testing time is large,' but is liable to mean 'I think its probability is low.' "

¹⁸ The observant reader might note that the Z0 group in the two examples above is an indicator check; let him uncover the procedures involved.

¹⁹ *Standard Reagents and Diagnostician's Dictionary* (p. 2), National Security Agency, 1966.

Taking a case in point, the process of completing the plain-component sequence using standard alphabets is not very likely to bear fruit in an operational problem; *but when it does, it's marvelous*. There isn't much effort involved in the procedure (especially if we possess already prepared alphabet strips), and the time it takes is very small compared with many other aspects of cryptanalysis. To illustrate the value of trying the process anyway, let us suppose that we have some traffic in an unknown cryptosystem, the messages being sent in 5-letter groups except for the A1 which is always a 5-digit number. No unusual statistical properties, repetitions, or other phenomena have been observed, and we might even suspect a high-grade system to be involved (if we know nothing about the cryptographic history of the target country). Nevertheless, if we try completing the plain-component sequence on the basis of direct standard alphabets, we would obtain a solution, as shown below for one of the message beginnings (the A1 here was 26996):

C: U S V I Q J O Z Y F Q E G N O D A K I F E H A Y Y K N Z K D . . .  
 V T W J R K P A Z G R F H O P E B L J G F I B Z Z L O A L E  
 W U X K S L Q B A H S G I P Q F C M K H G J C A A M P B M F  
 X V Y L T M R C B I T H J Q R G D N L I H K D B B N Q C N G  
 Y W Z M U N S D C J U I K R S H E O M J I L E C C O R D O H  
 Z X A N V O T E D K V J L S T I F P N K J M F D D P S E P I  
 A Y B O W P U F E L W K M T U J G Q O L K N G E E Q T F Q J  
 B Z C P X Q V G F M X L N U V K H R P M L O H F F R U G R K  
 C A D Q Y R W H G N Y M O V W L I S Q N M P I G G S V H S L  
 D B E R Z S X I H O Z N P W X M J T R O N Q J H H T W I T M  
 E C F S A T Y J I P A O Q X Y N K U S P O R K I I U X J U N  
 F D G T B U Z K J Q B P R Y Z O L V T Q P S L J J V Y K V O  
 G E H U C V A L K R C Q S Z A P M W U R Q T M K K W Z L W P  
 H F I V D W B M L S D R T A B Q N X V S R U N L L X A M X Q  
 I G J W E X C N M T E S U B C R O Y W T S V O M M Y B N Y R  
 J H K X F Y D O N U F T V C D S P Z X U T W P N N Z C O Z S  
 K I L Y G Z E P O V G U W D E T Q A Y V U X Q O O A D P A T  
 L J M Z H A F Q P W H V X E F U R B Z W V Y R P P B E Q B U  
 M K N A I B G R Q X I W Y F G V S C A X W Z S Q Q C F R C V  
 N L O B J C H S R Y J X Z G H W T D B Y X A T R R D G S D W  
 O M P C K D I T S Z K Y A H I X U E C Z Y B U S S E H T E X  
 P N Q D L E J U T A L Z B I J Y V F D A Z C V T T F I U F Y  
 Q O R E M F K V U B M A C J K Z W G E B A D W U U G J V G Z  
 R P S F N G L W V C N B D K L A X H F C B E X V V H K W H A  
 S Q T G O H M X W D O C E L M B Y I G D C F Y W W I L X I B  
T R U H P I N Y X E P D F M N C Z J H E D G Z X X J M Y J C

It can be seen that the encipherment is effected three letters at a time with a particular key letter, and the shifting of the components is apparently never greater than 9 positions. Knowing the mechanics of the system, we can now read all messages with comparative ease, even though the meaning of the A1 might not be understood for some time.²⁰ The chances of solving such a system by any other means are rather slim, yet the simplest technique of all gives a quick—and effortless—answer.

²⁰ The method of key generation is as follows: Each correspondent has a secret fixed key which is used as a subtractor to encipher a randomly chosen plaintext indicator, and the enciphered form is sent as the A1 group of the message. The plaintext indicator consists of a 5-digit group wherein the e digit, as a safety factor, is the noncarrying sum of the first four digits; this indicator is then used as a priming key to generate a Fibonacci sequence by the formula  $a + b = f$ . Thus, in the example above, the secret key 12345 is added to the A1 group (26996) to yield the plaintext indicator 38231, from which is generated the sequence 105421596364599 . . . This sequence (omitting any zeroes that might occur in order to avoid enciphering more than three letters at one setting) is then used, starting with the initial alignment of the components at  $A_p = A_e$ , to give the successive displacements 1542159636 which will read the first 30 letters of the message.

j. In the manipulation of message texts we perform essentially only a few basic processes, those necessary to reveal hoped-for phenomena, just as the physician begins his first examination by looking at the patient's tongue, taking his temperature, and tapping his knee with his little hammer—all this in the hope of disclosing something untoward. The cryptanalyst's manipulation entails the manner of recording original and derived data, writing and rewriting data in various forms and formats most suitable for the particular purpose or study, and the transformation or reduction of data. Initially, the manipulation and examination is done by hand, at least for a few messages—there still is no computer equal to the human brain—while waiting for the results of machine examination to come back. We proceed with machine processing (a) if nothing of interest turns up, (b) if what turns up cannot be interpreted, and (c) if examining a volume of traffic. Emphasis on the initial importance of looking at the material does not belittle machine techniques, which are valuable and often essential; it is rather a plea not to use machine techniques too early, for the vital clue may not respond to any of the mechanized tests, even with a very large library of routines.

k. The cryptanalyst takes various kinds of frequency counts in the hope of disclosing a significant roughness which is then mashed for his still; he indexes groups in the search for polygraphic repetitions; he examines patterns in the search for isomorphs; he writes out the texts and other data in various formats; he superimposes and compares messages, looking for an excess hit rate or other phenomena of significance; he derives secondary data such as differences, delta streams, or parity streams; and he compares sets of original and derived data. In the manipulative stage, much depends upon the cryptanalyst's experience and ingenuity if he is to avoid unnecessary work and achieve his results economically. We shall now give examples to illustrate these various points in as general a context as possible in order to show that their application is universal, whether manual or machine cryptosystems are involved, or whether the examination is performed by manual or machine methods.

l. We shall use as our first example the 200-letter message below, with which a number of points can be illustrated:

P Y L P P N A F T H T K S S F Z P M Y X X X J N U M H K Z K  
 R U H B S Q I E B S F M V W C F Y D T F D F I J B Y A Q D X  
 X O J O C N X W N N P R U J S J I H H W B N P V B V C G K Y  
 H S T Z V Y C F Y D V N E U M O O O Z G B U Z P I Y M H H J  
 W D Z D U C C E F N Q I K G F N G C S J U Q U K T V X R D Q  
 Y Y M T M Z R U C W F I H Y L E G G G A X K L F Z Z Q T O Q  
 G T R Y T Z Y B R X D Z I G M S O M L Y

A cursory examination shows a rather high doublet rate of 15 when we expect 7.7, but when this is evaluated it turns out to be a deviation of  $2.6\sigma$ , enough to be interesting, but not enough to be exciting.²¹ We have not forgotten so soon the admonishment contained in subpar. i, above—standard alphabets just might be involved in some fashion or other; but the generatrices of this test show nothing. A unilateral frequency distribution is taken,



²¹ The calculation is performed as follows: the expected number of doublets in this sample is  $\frac{199}{26}$  or 7.7; the standard deviation may be taken as the square root of the expected number, which is  $\sqrt{7.7}=2.8$ ; the excess doublets over the expected is  $15.0-7.7=7.3$ ; and the sigma is obtained by dividing the standard deviation into the excess number, so  $\frac{7.3}{2.8}=2.6\sigma$ .

which to the unpracticed eye might look "a little rough," but the I.C. is actually lower (0.97) than the average expected for a random sample of this size.²² In searching for polygraphic repetitions, we find just one repeated tetragraph, CYFD. In a sample of this size, the chance of a random tetragraphic repetition is small; in fact, it may be shown that if we had 1000 samples of 200 letters each of random text, we would expect to find a repetition in only 43 of them.²³ The repetition CYFD is at an interval of 52, an interesting number to a cryptanalyst since it has a factor of 26. When the cryptogram is written out on a trial width of 26, the columnar  $\phi$  values sum to 80 as shown in the diagram below:

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26			
P	Y	L	P	P	N	A	F	T	H	T	K	S	S	F	Z	P	M	Y	X	X	X	J	N	U	M			
H	K	Z	K	R	U	H	B	S	Q	I	E	B	S	F	M	V	W	C	F	Y	D	T	F	D	F			
I	J	B	Y	A	Q	D	X	X	O	J	O	C	N	X	W	N	N	P	R	U	J	S	J	I	H			
H	W	B	N	P	V	B	V	C	G	K	Y	H	S	T	Z	V	Y	C	F	Y	D	V	N	E	U			
M	O	O	O	Z	G	B	U	Z	P	I	Y	M	H	H	J	W	D	Z	D	U	C	C	E	F	N			
Q	I	K	G	F	N	G	C	S	J	U	Q	U	K	T	V	X	R	D	Q	Y	Y	M	T	M	Z			
R	U	C	W	F	I	H	Y	L	E	G	G	G	A	X	K	L	F	Z	Z	Q	T	O	Q	G	T			
R	Y	T	Z	Y	B	R	X	D	Z	I	G	M	S	O	M	L	Y											
$\Sigma$	4	2	2	-	4	2	4	2	2	-	6	4	2	12	6	4	4	2	4	2	8	2	-	2	-	-	-	=80

²² The delta I.C. is calculated by the formula  $\delta = \frac{c\Sigma f(f-1)}{N(N-1)}$ , where c is the number of categories,  $\Sigma f(f-1)$  is the observed value of  $\phi$ , and N is the sample size. The expected value of the  $\delta$  I.C. for random is 1.0. In this example,  $\delta = \frac{26(1478)}{200 \times 199} = 0.97$ . The  $\delta$  I.C. is the correct statistic to be used for samples from a population, since it compensates for sample size. Another statistic, the gamma ( $\gamma$ ) I.C., with the formula  $\gamma = \frac{c\Sigma f^2}{N^2}$ , is the measure of roughness to be used when we have the universe or total population of a particular case.

²³ The expected numbers of two-, three-, and fourfold occurrences of trigraphs, tetragraphs, and pentagraphs in 26-category random text for samples up to 1000 letters are given in the following table:

No. of letters	Exp. no. of trigraphs			Tetragraphs		Penta.
	E(2)	E(3)	E(4)	E(2)	E(3)	E(2)
100	0.269	0.001		0.010		
200	1.10	0.004		0.043		0.002
300	2.48	0.014		0.096		0.004
400	4.40	0.033		0.171		0.007
500	6.85	0.064		0.270		0.011
600	9.81	0.111	0.001	0.389		0.015
700	13.3	0.175	0.002	0.530		0.021
800	17.3	0.261	0.003	0.693		0.027
900	21.8	0.371	0.005	0.877		0.034
1000	26.8	0.505	0.008	1.08	0.001	0.042

Similarly, the expected numbers of two-, three-, and fourfold repetitions of trinomes, tetranomes, and pentanomes in 10-category random text for samples up to 1000 digits are given in the following table:

No. of digits	Exp. no. of trinomes			Exp. tetranomes			Pentanomes	
	E(2)	E(3)	E(4)	E(2)	E(3)	E(4)	E(2)	E(3)
100	4.49	0.147	0.004	0.49	0.002		0.046	
200	16.3	1.08	0.053	1.95	0.013		0.199	
300	33.3	3.31	0.246	4.35	0.043	0.001	0.447	
400	53.6	7.12	0.707	7.67	0.102	0.002	0.795	
500	75.8	12.6	1.57	11.9	0.197	0.002	1.24	0.002
600	98.8	19.7	2.95	16.9	0.337	0.005	1.79	0.004
700	122	28.3	4.94	22.8	0.531	0.009	2.43	0.006
800	144	38.3	7.64	29.5	0.785	0.016	3.17	0.008
900	165	49.4	11.1	37.0	1.11	0.025	4.01	0.012
1000	184	61.3	15.3	45.2	1.50	0.038	4.95	0.017



By using the principles of indirect symmetry of position,²⁵ we can amalgamate these chains and construct a sequence which, when decimated at the proper interval, will yield the QUESTIONABLY . . . XZ keyword-mixed sequence, the original cipher component of the system. Having the cipher component at hand, we are now able to effect a *reduction to monoalphabetic terms* of the complex cipher text, if we know or can assume the motion of the cipher component; in the case of a progressive alphabet system, the motion is at a constant interval, either to the right or to the left. If we arbitrarily assume the normal sequence for the plain component, with the two components juxtaposed at the setting  $A_p=Q_c$ , and decipher the beginning of the cryptogram by moving the cipher component to the right after each decipherment,

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26
C:	P	Y	L	P	P	N	A	F	T	H	T	K	S	S	F	Z	P	M	Y	X	X	X	J	N	U	M
"P":	U	M	M	X	Y	M	O	V	M	Z	O	D	P	Q	C	O	K	K	D	R	S	T	N	E	Z	S
C:	H	K	Z	K	R	U	H	B	S	Q	I	E	B	S	F	M	V	W	C	F	Y	D	T	F	D	F
"P":	Q	T	B	V	Z	G	W	Q	L	J	P	N	V	Q	C	I	M	O	E	H	F	I	A	L	L	N
C:	I	J	B	Y	A	Q	D	X	X	O	J	O	C	N	X	W	N	N	P	R	U	J	S	J	I	H
"P":	F	S	L	O	M	F	T	F	G	P	B	R	Y	U	M	M	X	Y	M	O	V	M	Z	O	D	P

the distribution of the resultant "plain text"

A B C D E F G H I J K L M N O P Q R S T U V W X Y Z

with its I.C. =  $\frac{26(252)}{78 \times 77} = 1.09$  is not satisfactory. But when we decipher the beginning of the cryptogram by moving the cipher component to the *left* after each decipherment,

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26
C:	P	Y	L	P	P	N	A	F	T	H	T	K	S	S	F	Z	P	M	Y	X	X	X	J	N	U	M
"P":	U	K	I	R	Q	C	C	H	W	H	U	H	R	Q	A	K	E	C	T	F	E	D	V	K	D	U
C:	H	K	Z	K	R	U	H	B	S	Q	I	E	B	S	F	M	V	W	C	F	Y	D	T	F	D	F
"P":	Q	R	X	P	R	W	K	C	V	R	V	R	X	Q	A	E	G	G	U	V	R	S	I	R	P	P
C:	I	J	B	Y	A	Q	D	X	X	O	J	O	C	N	X	W	N	N	P	R	U	J	S	J	I	H
"P":	F	Q	H	I	E	V	H	R	Q	X	H	V	A	U	K	I	R	Q	C	C	H	W	H	U	H	R

the distribution of this "plain text"

A B C D E F G H I J K L M N O P Q R S T U V W X Y Z

with its I.C. =  $\frac{26(388)}{78 \times 77} = 1.68$  shows that this converted text has been reduced to a simple substitution which we can now readily solve, discovering in the process that the plain component is the HYDRAULIC . . . XZ keyword-mixed sequence.

n. There are certain situations, rarely predictable in advance, wherein it is profitable (nay, even mandatory) to derive a delta stream of the cipher text, typically by differencing the first element of text from the second, the second from the third, and so on, on a known or assumed modulus or scale. The value of this technique will be apparent in the examples which follow.

(1) For the first example, we shall assume that we are in possession of a small volume of traffic sent in 5-letter groups in an unknown cryptosystem. The over-all I.C. of the traffic is close to 1.0, as are the I.C.'s of the individual messages. A few polygraphic repetitions, both within and between messages, are in evidence, more than expected at random; the intervals between the repetitions have no common factor, but the closest ones are at an average of approximately 22 letters apart, and then at an average of approxi-

²⁵ Cf. Chapter VI, *Military Cryptanalytics, Part II.*





Not only is there corroboration for the assumption of HEADQUARTERS, but the spacing of the cipher equivalents for the repeated plaintext letters along a distance measured on the normal sequence proves that there is a constant motion of one step of the cipher component during the encryption of a word. This leads easily to the recognition of the numbers SEVEN, EIGHT, and THREE in the text; the threefold occurrence of the word STOP; and, in the second pair of lines, the cipher text XGFIOJLF is identified as the word DECEMBER from the pattern of the possible equivalents for a repeated letter (E_p):

D E C E M B E R  
X G F I O J L F  
G(h)I(j k)L

The message is now on the way to solution: when solved, the beginning is found to read "REURAD NUMBER SEVEN FIVE SEVEN DATED ONE EIGHT DECEMBER STOP . . ."; the plain component is found to be the HYDRAULIC . . . XZ keyword-mixed sequence; and the cryptosystem is determined to be a modified progressive alphabet system in which the normal-sequence cipher component moves one step after the encipherment of each letter, with a double step at the end of each word.

(3) For the second example of the delta technique, let us assume that we are faced with traffic in an unknown cryptosystem, but that historical precedent indicates the possibility of cyclic repeating keys. The messages are transmitted in groupings of five dinomes. A typical message, with its associated frequency distribution, is the following:

41	70	19	05	97	76	72	58	07	21	11	07	54	46	74	07	40	57	35	56
20	13	07	81	18	44	07	02	56	91	38	22	17	43	57	41	98	34	79	29
76	44	97	96	03	81	06	86	71	68	88	13	16	47	46	13	51	78	29	13
34	05	42	65	56	55	14	72	46	25	81	21	44	11	61	85	16	16	42	65
52	44	41	08	59	26	14	00	90	07	30	16	28	09	43	51	30	89	12	23
82	06	32	39	09	49	25	98	15	22	88	33	26	65	64	42	46	76	53	53
28	28	33	17	32	41	36	96	20	01	41	87	72	60	16	31	65	28	39	74
49	68	51	99	72	24	55	63	16	86	33	37	42	82	27	58	28	70	98	10
14	48	31	90	72	78	61	19	67	22	92	26	44	37	29					

00 1	10 1	20 2	30 2	40 1	50	60 1	70 2	80	09 2
01 1	11 2	21 2	31 2	41 5	51 3	61 2	71 1	81 3	91 1
02 1	12 1	22 3	32 2	42 4	52 1	62	72 5	82 2	92 1
03 1	13 4	23 1	33 3	43 2	53 2	62 1	73	83	93
04	14 3	24 1	34 2	44 5	54 1	64 1	74 2	84	94
05 2	15 1	25 2	35 1	45	55 2	65 4	75	85 1	95
06 2	16 6	26 3	36 1	46 4	56 3	66	76 3	86 2	96 2
07 6	17 2	27 1	37 2	47 1	57 2	67 1	77	87 1	97 2
08 1	18 1	28 5	38 1	48 1	58 2	68 2	78 2	88 2	98 3
09 2	19 2	29 3	39 2	49 2	59 1	69	79 1	89 1	99 1

The I.C. of  $\frac{100(312)}{175 \times 174} = 1.025$  is not informative; there are no polygraphic repetitions of significance; and writing the text on widths has produced nothing of consequence. We shall now try deriving delta streams; first, a delta at an interval of one dinome (with mod 10 arithmetic):

C: 41 70 19 05 97 76 72 58 07 21 11 07 54 46 74 07 40 57 35 56 . . .  
Δ: 39 49 96 92 89 06 86 59 24 90 96 57 92 38 33 43 17 88 21

The entire delta stream at this interval reveals nothing of interest, so we next take a delta stream at an interval of two dinomes, deriving the following Δ₂ stream:

C: 41 70 19 05 97 76 72 58 07 21 11 07 54 46 74 07 40 57 35 56 . . .  
Δ₂: 78 35 88 71 85 82 35 73 14 86 43 49 20 61 76 50 95 09

This stream too shows nothing; but when we finally take a  $\Delta_{12}$ , we obtain the following:

C:	41 70 19 05 97	76 72 58 07 21	11 07 54 46 74	07 40 57 35 56
$\Delta_{12}$ :			13 76 65	02 53 81 63 08

C:	20 13 07 81 18	44 07 02 56 91	38 22 17 43 57	41 98 34 79 29
$\Delta_{12}$ :	23 92 96 84 64	08 33 05 16 44	03 76 97 30 50	60 80 90 72 27

C:	76 44 97 96 03	81 06 86 71 68	88 13 16 47 46	13 51 78 29 13
$\Delta_{12}$ :	20 53 69 74 96	48 59 45 83 34	19 94 40 03 59	27 58 97 23 37

C:	34 05 42 65 56	55 14 72 46 25	81 21 44 11 61	85 16 16 42 65
$\Delta_{12}$ :	63 47 64 52 40	18 78 69 95 57	62 18 10 16 29	20 60 61 38 93

C:	52 44 41 08 59	26 14 00 90 07	30 16 28 09 43	51 30 89 12 23
$\Delta_{12}$ :	16 29 60 87 15	15 53 25 84 91	98 51 76 65 02	53 81 63 08 23

C:	82 06 32 39 09	49 25 98 15 22	88 33 26 65 64	42 46 76 53 53
$\Delta_{12}$ :	92 09 02 23 81	40 82 47 85 43	76 10 44 69 32	13 47 37 38 65

C:	28 28 33 17 32	41 36 96 20 01	41 87 72 60 16	31 65 28 39 74
$\Delta_{12}$ :	13 06 55 84 16	86 72 54 84 35	98 34 54 42 83	24 33 87 03 88

C:	49 68 51 99 72	24 55 63 16 86	33 37 42 82 27	58 28 70 98 10
$\Delta_{12}$ :	29 67 10 12 00	64 49 32 51 68	04 63 03 24 76	69 56 56 43 57

C:	14 48 31 90 72	78 61 19 67 22	92 26 44 37 29
$\Delta_{12}$ :	08 62 08 63 30	96 44 61 49 52	04 16 30 99 98

The 9-dinome repetition revealed in the  $\Delta_{12}$  stream is proof (1) that there is a 21-dinome identical underlying plaintext passage at the positions indicated by the two occurrences of the repetition, and (2) that, if this be a system involving a cyclic repeating numerical key, the length of this key is 12 dinomes.²⁶

²⁶ Note that the period here could not have been revealed by any other means, say writing the cipher text on this width—the underlying text is not rough enough to yield a significant I.C. on the correct width.

The solution from here on is straightforward,²⁷ based on the reduction of the periodic cryptogram to monoalphabetic terms. For example, if in the fragment of the worksheet below, the cipher dinome 46 at position B2 is assumed to be (arbitrarily) 00_p, then the cipher dinome 28 at position H9 must also represent 00_p, since the delta repetition has already proved the location of the identical underlying plain text. The derivation of the additives from these decipherments enables the recovery of other plaintext dinomes, finally culminating in the recovery of the entire 12-dinome keying sequence (to a relative base) and the reduction of the cipher text to monoalphabetic terms. (The completion of the solution of this problem, including the recovery of the plain text, is left to the interested reader.)

		1	2	3	4	5	6	7	8	9	10	11	12
K:			46							28			
A.	(C)	41	70	19	05	97	76	72	58	07	21	11	07
	(P)												
B.	(C)	54	46	74	07	40	57	35	56	20	13	07	81
	(Δ)	13	76	65	02	53	81	63	08	23	92	96	84
	(P)		00										
					*	*	*	*	*				
G.	(C)	44	11	61	85	16	16	42	65	52	44	41	08
	(Δ)	10	16	29	20	60	61	38	93	16	29	60	87
	(P)												
H.	(C)	59	26	14	00	90	07	30	16	28	09	43	51
	(Δ)	15	15	53	25	84	91	98	51	76	65	02	53
	(P)									00			
I.	(C)	30	89	12	23	82	06	32	39	09	49	25	98
	(Δ)	81	63	08	23	92	09	02	23	81	40	82	47
	(P)												
					*	*	*	*	*				
O.	(C)	67	22	92	26	44	37	29					
	(Δ)	49	52	04	16	30	99	98					
	(P)												

(4) Related to the process of the derivation of delta streams is the process of *autokeying*, which may uncover phenomena when this principle has been incorporated in the cryptosystem. Taking as an illustration the message beginning below,

3667 8406 8424 5012 4749 1868 9463 3122 2118 9456 . . . .

if we perform a *ciphertext autokeying* decipherment, the key is actually at hand, since it is the cipher text itself, but it must be displaced against itself at an interval corresponding to the length of the introductory key. Under the assumption of an introductory key of one digit, the matched cipher, key, and resultant plain text are shown below:

K:	366	7840	6842	4501	2474	9186	8946	3312	2211	8945
C:	3667	8406	8424	5012	4749	1868	9463	3122	2118	9456 . . . .
P:	-301	1666	2682	<u>1511</u>	2375	2782	1527	0810	0907	<u>1511</u>

It is obvious that the unknown intermediate text is 4-digit code, with a limitation of 0, 1, and 2 in the first position of code groups. Although the foregoing example with an introductory key of one digit is a trival case of ciphertext autokey, an initial key of unknown length would not pose any problems. Taking the case of the message beginning

3442 7900 4372 1948 4469 0128 0539 8863 9783 4489 . . . .

²⁷ Cf. subpars. 83g-j on pp. 230-235 of *Military Cryptanalytics, Part II*.

all that would be required is to try various offsets of the cipher text against itself, and one of the decipherments would be the actual plain text (to true base, of course); this is shown in the diagram below:

K(5):	344	2790	0437	2194	8446	9012	8053	9886	3978	
K(4):	3442	7900	4372	1948	4469	0128	0539	8863	9783	
K(3):	3	4427	9004	3721	9484	4690	1280	5398	8639	7834
K(2):	34	4279	0043	7219	4844	6901	2805	3988	6397	8344
K(1):	344	2790	0437	2194	8446	9012	8053	9886	3978	3448
C:	3442	7900	4372	1948	4469	0128	0539	8863	9783	4489 . . .
P(1):	-108	5210	4945	9854	6023	1116	2586	9087	6815	1041
P(2):	-18	3731	4339	4739	0625	4227	8734	5985	3496	6145
P(3):	-9	3583	5378	8227	5085	6538	9359	3575	1154	7655
P(4):	-	4568	7472	7676	3521	6769	0411	8334	1920	5706
P(5):	-	-666	2682	<u>1511</u>	2375	2782	1527	0810	0907	<u>1511</u>

On the trial of an offset of 5, the underlying 4-digit plain code is revealed. (The missing first 5 digits would have to be determined by context after a volume of code text has been solved, or by analysis of the beginnings of messages.)

(5) In deriving a stream by the *plaintext autokeying* method, the "plain text" resulting from a decipherment at the correct offset will either be the true plain, or one of 9 equivalent versions. For example, in the message beginning below,

0331 2722 8840 3662 3502 7950 3679 7891 0997 8662 . . . ,

the decipherment at a one-digit offset is predicated on the supposed identity of the first plaintext digit. If we arbitrarily assume that the first plaintext digit is 3, we obtain the following decipherment:

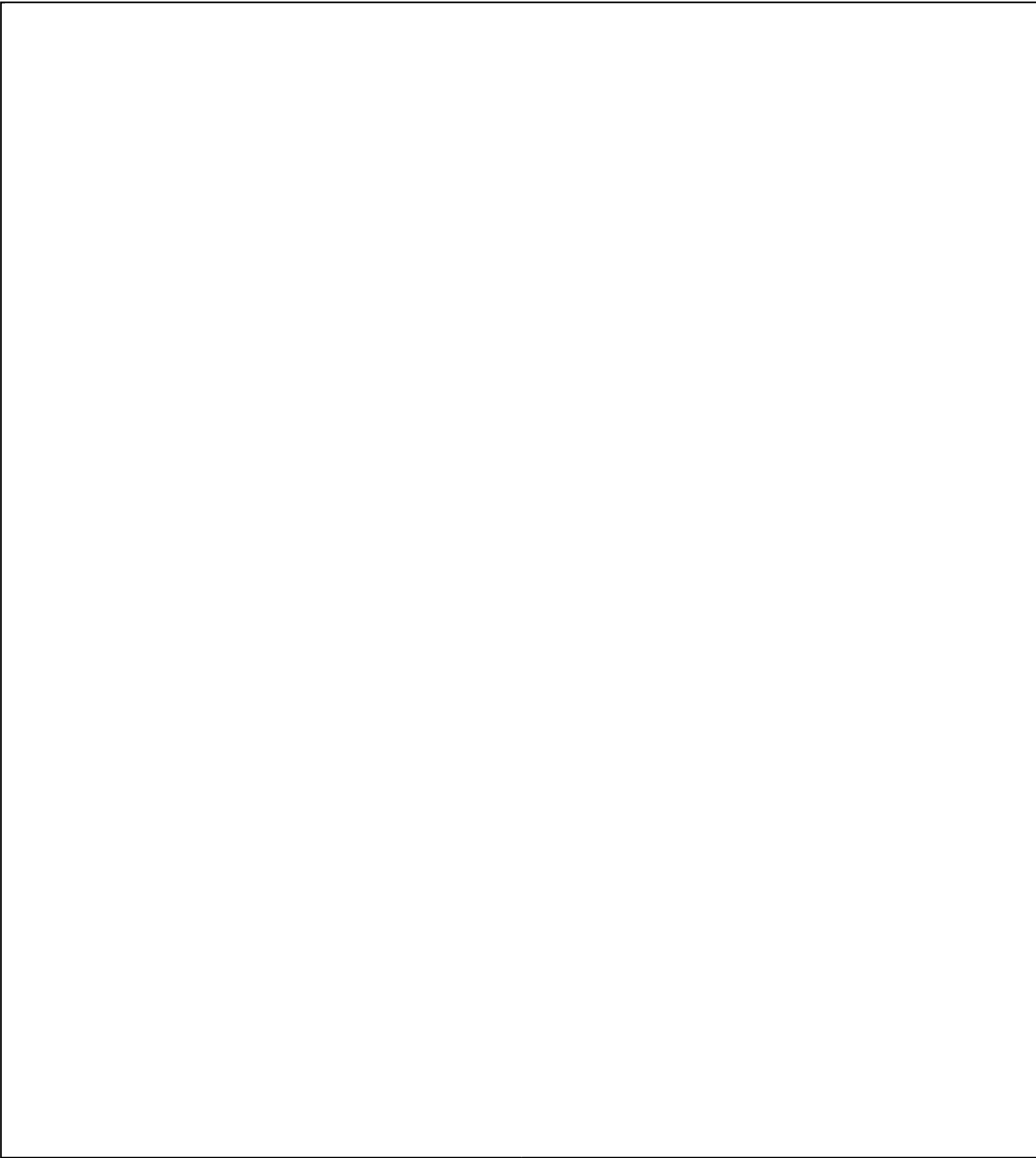
K:	303	8439	3531	9424	8500	2541	9425	4354	7363	4424
C:	0331	2722	8840	<u>3662</u>	3502	7950	3679	7891	0997	<u>8662</u> . . .
P:	3038	4393	5319	<u>4248</u>	5002	5419	4254	3547	3634	<u>4248</u>

(Note the trinomic repetition in the original cipher text, which becomes a tetranomic repetition when treated by the plaintext autokey method.) If we "complete the plain-component sequence" from this decipherment by going down the columns in alternate directions (down the normal numerical sequence in the odd columns, and down the reversed normal sequence in even columns), as shown in Fig. 169, below, we would recognize in the asterisked row the properties of code text having the limitation of 0, 1, and 2 in the *a* position of the code groups. The foregoing case of plaintext autokey with a one-digit introductory key was quite simple; if the initial key were much longer, and the nature of the intermediate text unknown, the problem becomes exceedingly difficult—in fact, it is only fairly recently that a method of solution has been discovered.²⁸

"P":	3038	4393	5319	4248	5002	5419	4254	3547	3634	4248
	3038	4393	5319	4248	5002	5419	4254	3547	3634	4248
	4947	5202	6228	5157	6911	6328	5163	4456	4543	5157
	5856	6111	7137	6066	7820	7237	6072	5365	5452	6066
	6765	7020	8046	7975	8739	8146	7981	6274	6361	7975
	7674	8939	9955	8884	9648	9055	8890	7183	7270	8884
	8583	9848	0864	9793	0557	0964	9709	8092	8189	9793
	9492	0757	1773	0602	1466	1873	0618	9901	9098	0602
	*0301	1666	2682	1511	2375	2782	1527	0810	0907	1511
	1210	2575	3591	2420	3284	3691	2436	1729	1816	2420
	2129	3484	4400	3339	4193	4500	3345	2638	2725	3339

FIGURE 169

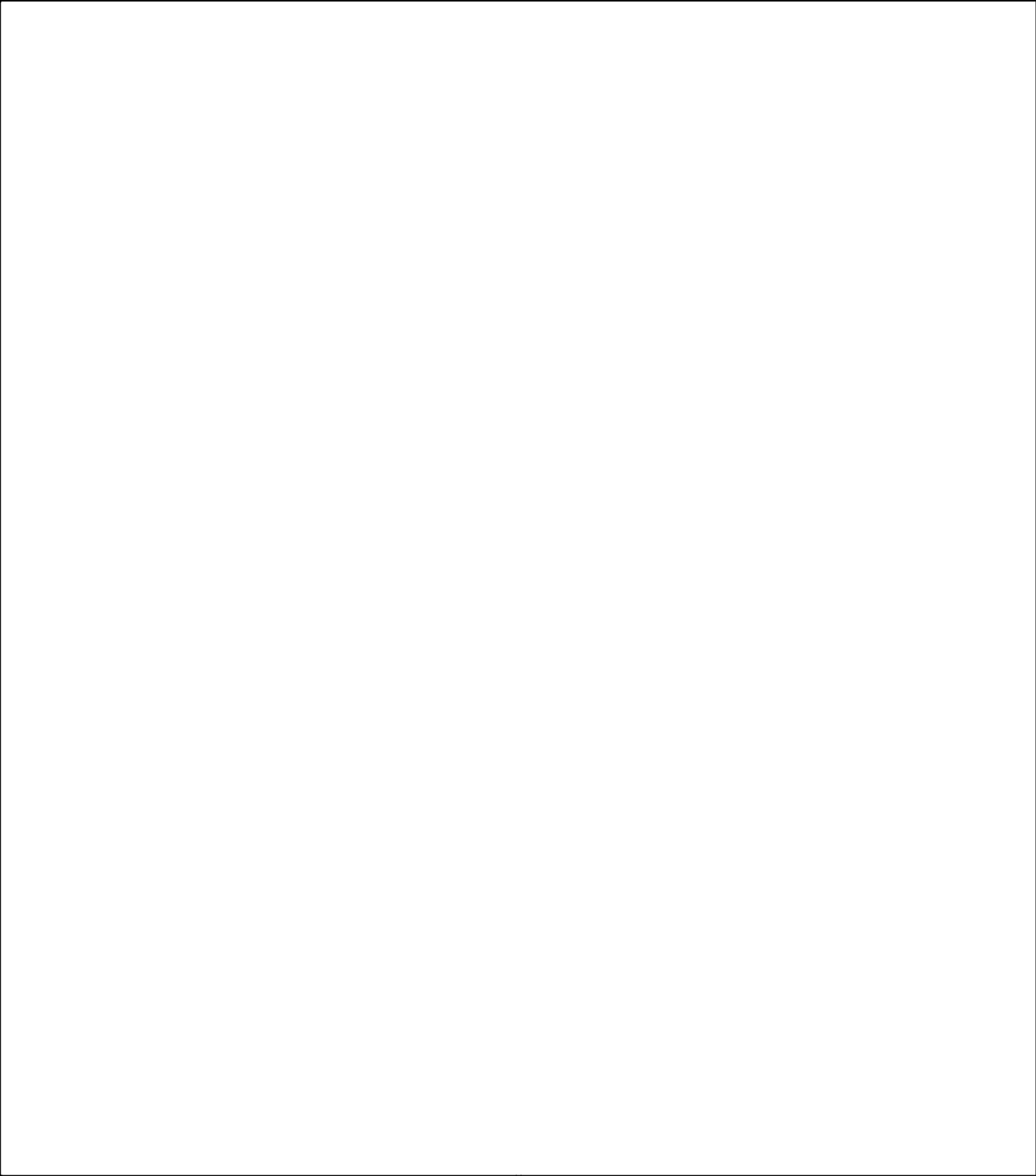
²⁸ See Lambros D. Callimahos, "The Analysis of Digital Plaintext Autokey Systems," appearing in the *NSA Technical Journal*, Vol. XIV, No. 2, Spring 1969.



(b) (1)  
(b) (3)-18 USC 798  
(b) (3)-50 USC 3024(i)  
(b) (3)-P.L. 86-36



(b) (1)  
(b) (3)-18 USC 798  
(b) (3)-50 USC 3024(i)  
(b) (3)-P.L. 86-36

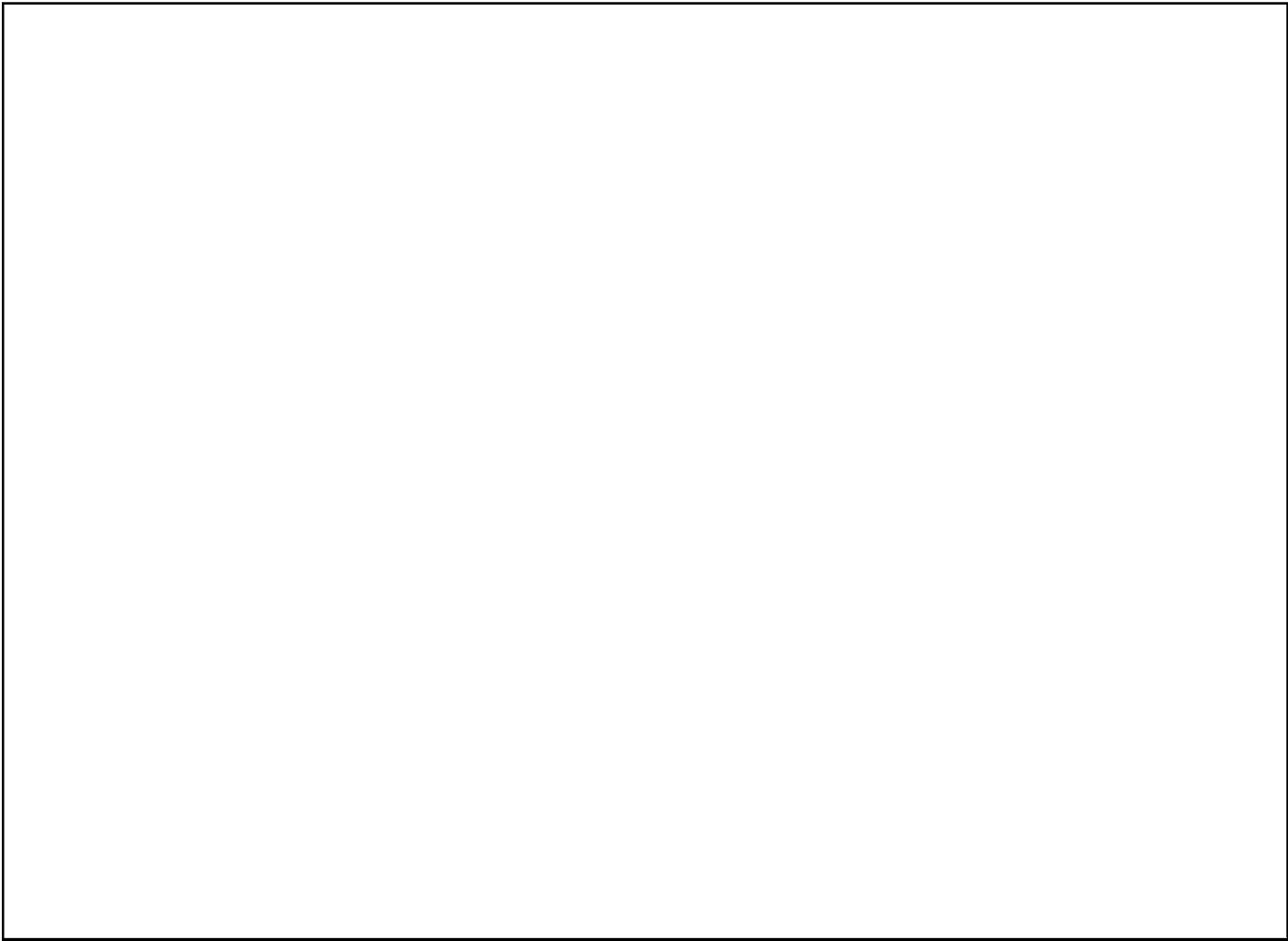


(b) (1)  
(b) (3)-18 USC 798  
(b) (3)-50 USC 3024 (i)  
(b) (3)-P.L. 86-36



(b) (1)  
(b) (3)-18 USC 798  
(b) (3)-50 USC 3024 (i)  
(b) (3)-P.L. 86-36





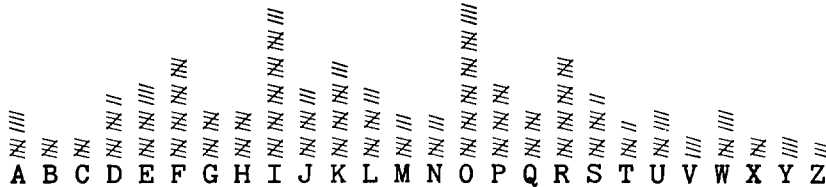
77. **Second step: recognizing the phenomena.**—*a.* The manipulative processes described in the preceding paragraph are undertaken in order to disclose nonrandom characteristics or manifestations. The second step in diagnosis is the *recognition* of the nonrandom characteristics or manifestations when disclosed. When, for example, we make a uniliteral frequency distribution of cipher text we are really hoping that some roughness or other property will be manifested—otherwise we wouldn't even have bothered to make the distribution. And after making the distribution, what's the use of it if we don't recognize the fact that it is rough? The recognition of phenomena, then, implies some sort of measurement, either by eye (relying on past experience and visual memory), or by statistical means, which takes it out of the realm of the subjective. After finding a phenomenon—or what is thought to be a phenomenon—an evaluation should follow. It's not enough to say "I think the doublets are high." How many are there? *Count them.* And, even more important, *how many doublets are expected at random in a sample of this size?*

³² Note the repeating key, **HEAVY WATER**, manifested in one of the columns of Fig. 171.

(b) (1)  
(b) (3)-18 USC 798  
(b) (3)-50 USC 3024 (i)  
(b) (3)-P.L. 86-36

b. Some phenomena cannot really be measured (or measured accurately) but permit of their recognition because of either past experience or intuitive feeling of something that's "not quite right." For example, let us examine the following intercepted message and its frequency distribution:

FOROF JIEOF KGMVQ IFORR IFRWM ASEFL QPOIE XCZIF ASDOF GHIRF  
QWERP PIFRI FORFO ASDIK JDGHJ ASPQE POIRP MNCCO ASDFK QPOIR  
OIKOP ASDEW UIOKP KOIJL POIEQ MNBVX IKFRI ROEWJ KIOLK LPOIU  
RETYU UINMH GHTYU IOKLP REDFS QAWSE DRFTG GYHUJ JIKOL ZSERD  
XDRTF QAWSZ RDXCF VGYUH NJIOK MLOKN LPOOP LKJHB FGJHK CVBNM  
QPWOL EORIK TIORI TUGJI TUHDG NJKHF LKOIL SEWDX QLASW NBJMB



The  $\delta$  I.C. here is  $\frac{26(4332)}{300 \times 299} = 1.256$ , which represents a sigmage of  $10.85\sigma$ ,³³ highly significant indeed. In subjecting the cryptogram to close scrutiny, we find many points of considerable interest. For example, (1) we observe only 7 doublets and 6 A-A doublets when we expect 14.4 of each; (2) there are 7 tetragraphic repetitions (IFOR, LPOI, OASD, POIR, QAWS, QPOI, UIOK) when we expect not quite a tenth (0.096) of one; (3) there are 23 trigraphic repetitions when we expect only 2.48; (4) on a width of 5, the average I.C. is 1.44, a deviation of  $3.0\sigma$ , and on a width of 15 the average I.C. is 1.52, a deviation of  $2.5\sigma$ . We could find other statistical phenomena with which to build up an impressive case for some esoteric cryptosystem, the likes of which had not been seen by man before; but an experienced cryptanalyst

³³ The standard deviation of the  $\delta$  I.C. is given by the formula  $\sigma = \frac{\sqrt{2(c-1)}}{\sqrt{N(N-1)}}$  where c is the number of categories, and

N is the sample size. Thus, in this example,  $\sigma = \frac{\sqrt{2(26-1)}}{\sqrt{300 \times 299}} = .0236$ . The sigmage (S) is obtained by dividing the standard

deviation into the "bulge" of the I.C., with the formula  $S = \frac{\delta - 1.00}{\sigma}$ , so in this case  $S = \frac{0.256}{.0236} = 10.85\sigma$ . The sigmage of the

$\delta$  I.C. is interpreted with the chi-square distribution; in this case,  $10.85\sigma$  may be found to represent about 1 chance in 20,000,000,000 of having occurred at random. The table below gives the interpretation of sigmages from 1 to 5, according to the chi-square and Normal distributions, whichever is applicable in the particular case; the sigmage in the first column will be equaled or exceeded by pure chance, on the average, once every  $\chi$  times as shown in the table.

Values of  $\chi$

S	Chi-square distribution		Normal distribution
	c=10	c=26	
1	6. 6	6. 4	6. 3
1½	12	13	15
2	24	28	44
2½	49	66	161
3	102	164	740
3½	220	435	4, 298
4	483	1, 210	31, 500
4½	1080	3, 520	294, 000
5	2470	10, 650	3, 488, 000

(or a younger one who is destined to make his mark in the art) could, without too much difficulty, identify the cryptogram for what it is.³⁴

c. The importance of evaluating distributions and repetitive phenomena cannot be overstressed. Let us take as an example the case of 40 messages in a certain unknown system that was under study. The text groups, after the discriminants and indicators were deleted, totalled 9717 letters with the following distribution:

A 356	G 403	L 361	Q 334	V 372
B 347	H 398	M 381	R 395	W 306
C 318	I 347	N 421	S 484	X 372
D 369	J 325	O 401	T 409	Y 418
E 386	K 379	P 313	U 359	Z 375
F 388				

We have also observed 91 repeated tetragraphs and 5 repeated pentagraphs in the traffic, which strikes us as being probably considerably above the random expectations; there are no other longer repetitions.

The  $\delta$  I.C. here is  $\frac{26(3,659,986)}{9717 \times 9716} = 1.0079$ , certainly "flat-looking." But we must not forget that the

significance of the  $\delta$  I.C. is tied to the sample size, so we should go ahead and compute the sigmage. The standard deviation for this example is  $\frac{\sqrt{2(26-1)}}{\sqrt{9717 \times 9716}}$ , which for all practical purposes becomes  $\frac{7.0711}{9717} =$

.00073. Therefore the sigmage is  $\frac{.0079}{.00073} = 10.8\sigma$ —and we revise our estimate of the relative flatness of

the distribution. As for the polygraphic repetitions, it would be wise to take a closer look at them. In arriving at the Poisson probability, we first compute  $a = Np$  (where  $N$  is the sample size and  $p$  is the probability of the item under investigation), so for tetragraphs  $a = \frac{9717}{26^4} = .0213$ , rounded off to .02 for

looking up in the tables, and for pentagraphs  $a = \frac{9717}{26^5} = .00082$ , rounded off to .001. Under the entry of

$a = .02$  we find the probability of .0001960 for a two-fold occurrence (i.e., a repetition) of a tetragraph, and we multiply this probability by  $26^4$  to obtain the number of tetragraphs expected at random in a sample of this size; under the entry of  $a = .001$  we find the probability of .0000005 for a repeated pentagraph, and we multiply this probability by  $26^5$  to obtain the number of pentaglyphs expected at random. Our findings are summarized below:

Tetragraphs:  $a = \frac{9717}{26^4} = .0213$  ( $\approx .02$ ); Poisson probability = .0001960

Expected at random = .0001960( $26^4$ ) = 89.6; observed = 91

Pentaglyphs:  $a = \frac{9717}{26^5} = .00082$  ( $\approx .001$ ); Poisson probability = .0000005

Expected at random = .0000005( $26^5$ ) = 5.5; observed = 5

Random on the nose. Statistics *are* useful. This means that, if the system is to be eventually solved, it will not be solved on the basis of its polygraphic repetitions.

d. We have already stated, not in so many words, that the distribution of the  $\delta$  I.C. is asymptotic to the chi-square distribution with  $c-1$  degrees of freedom; in plain English, this means that the distribution of the  $\delta$  I.C. is approximated (and thus may be interpreted) by the  $\chi^2$  distribution. The  $\xi$  I.C.,

³⁴ A practice message, consisting of random typing of 5-letter groups on a typewriter. Note groups of the text, typical of typewriter random, composed of keyboard sequences and patterns (such as ASDFK, LPOIU, and QWERP, alternating hand patterns (such as FOROF, GHTYU, and QPWOL), and one-hand patterns (such as DRFTG, KIOLK, and REDFS).

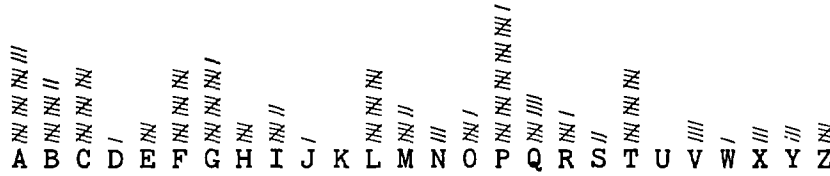
however, is approximately Normally distributed, and thus has different formulas for standard deviation and sigmage, as shown below: ³⁵

(1) The  $\xi$  I.C. has the formula  $\xi = \frac{c \sum f_1 f_2}{N_1 N_2}$ , where  $c$  is the number of categories,  $\sum f_1 f_2$  the sum of the cross products of the corresponding frequencies, and  $N_1$  and  $N_2$  the sizes of the two distributions being compared. If we recall the formula for the  $\gamma$  I.C. (see footnote 22 on p. 345),  $\gamma = \frac{c \sum f^2}{N^2}$ . Now if we compute the  $\gamma$  I.C. for each of the two distributions being matched, the standard deviation of the  $\xi$  I.C. is given by the formula  $\sigma = \frac{\sqrt{(\gamma_1 - 1)(\gamma_2 - 1)}}{\sqrt{c - 1}}$ . The sigmage of the  $\xi$  I.C. is then given by the formula  $S = \frac{\xi - 1}{\sigma}$  or, in another form,  $S = \frac{(\xi - 1)\sqrt{c - 1}}{\sqrt{(\gamma_1 - 1)(\gamma_2 - 1)}}$ .

(2) As an example of the use of these formulas, let us take the  $\xi$  I.C. of the following two distributions

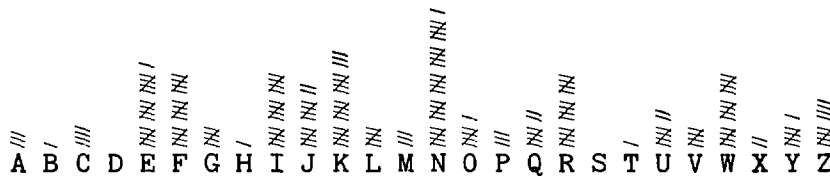
1.	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	N=57	
	≡	≡	≡	≡	≡	≡	≡	≡	≡	≡	≡	≡	≡	≡	≡	≡	≡	≡	≡	≡	≡	≡	≡	≡	≡	≡	≡	
						</																						

we diagnose it immediately as that of a direct standard alphabet encipherment, since what we have is the normal profile displaced by three positions ( $A_p=D_c$ ). Likewise, the profile

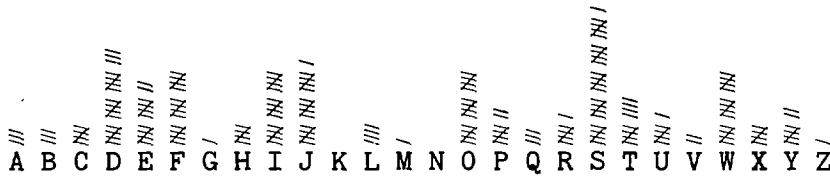


reveals itself as that of a reversed standard alphabet encipherment, since it can be recognized that it is the reversed normal profile, at a slide of  $-6(A_p=T_c)$ .

(2) Although Porta systems³⁶ are rarely encountered, nevertheless we should still know enough to recognize immediately distributions arising from encipherment by a Porta table. In the normal Porta, if we draw a vertical line between the M and N of the distribution, we can fit a cyclic permutation of the first half (A-M) of the normal sequence in the *right* half of the distribution, and we can fit a cyclic permutation of the last half (N-Z) of the normal sequence in the *left* half of the distribution; moreover, since Porta encipherment is reciprocal, establishing an identity in one half of the distribution automatically establishes an identity in the other half. For example, in the theoretical distribution below,

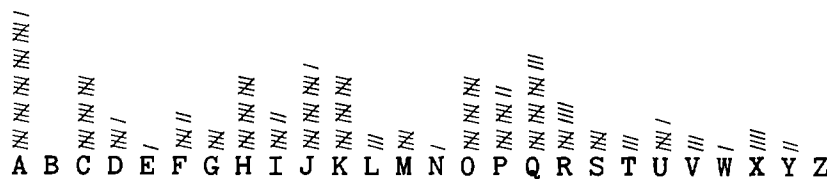


it is clear that the plaintext sequence A . . . E . . . I is at cipher W . . . N . . . R, and that the plaintext sequence RST is at cipher IJK; furthermore, establishing one letter, say  $N_c=E_p$ , then the reciprocal value  $N_p=E_c$  must obtain. In complementary Porta (in which the A-M sequence of the table runs in the opposite direction from the N-Z sequence) the direction of fitting the plaintext sequences to the cipher must be reversed, as in the following example:



Here the plaintext sequence A . . . E . . . I is at cipher W . . . S . . . O, and the plaintext sequence RST is at cipher FED.

(3) A monoalphabetic distribution is recognized by its roughness, which will be that of the underlying text. For English, the expected  $\delta$  I.C. is 1.73, and a 200-letter distribution involving a mixed alphabet might look as follows:



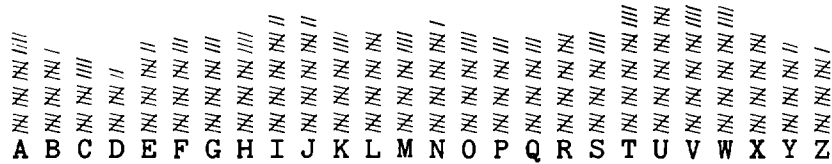
³⁶ Cf. par. 23 (on pp. 45-47) of *Military Cryptanalytics, Part II*.

The monographic roughness will prevail not only in monoalphabetic substitution, but also in polyalphabetic substitution after the ciphertext letters have been properly allocated into the respective cipher alphabets to which they belong, since this has the effect of reducing the polyalphabetic text to monoalphabetic terms. If this step has not been correctly performed, the resultant distributions will be a merger of two or more monoalphabetic distributions; and if the distributions which were merged are of equal size, the expected  $\delta$  I.C. is 1.00 plus  $1/m$  of the bulge of the I.C. of the underlying text, where  $m$  is the number of distributions that were merged. Thus, if a 300-letter periodic polyalphabetic cipher of a period of 30 were incorrectly assumed to have a period of 15, the expected I.C. of the distributions (and therefore also that of the over-all width write-out) would be  $1.00 + \frac{.73}{2} = 1.37$ ; or if the period were mistakenly assumed to be 10, the expected I.C. would be  $1.00 + \frac{.73}{3} = 1.24$ . Such indices can therefore be a guide to what is happening, because if we had written out our cipher text on a width of 10 and obtained an I.C. of 1.24, on observing that this has one-third the bulge expected for English plain text we might have suspected that the true period is 30 and not 10 as assumed.

(4) The Gronsfeld system,³⁷ in which each plaintext letter has as its cipher equivalent either itself or one of the nine letters following it in the normal alphabetical sequence, has a characteristic frequency distribution even (or especially so) if the source of key is a large book of random digits. The theoretical relative frequencies are shown below, for English underlying text:

A 3.84	G 3.56	L 3.96	Q 3.58	V 4.80
B 3.18	H 3.85	M 3.90	R 4.00	W 4.71
C 2.88	I 4.40	N 4.28	S 3.88	X 3.96
D 2.38	J 4.40	O 3.73	T 4.78	Y 3.40
E 3.42	K 3.70	P 3.71	U 5.01	Z <u>3.14</u>
F 3.55				100.00

The  $\gamma$  I.C. of this distribution (multiplying the entries above by 100) is  $\frac{26(3,940,534)}{(10,000)^2} = 1.0245$ , which is the characteristic roughness expected of a Gronsfeld cipher.³⁸ The distributional profile is the following (on a base of 500):



³⁷ Cf. par. 24 (on pp. 47-48) of *Military Cryptanalytics, Part II*.

³⁸ We use the  $\gamma$  I.C. here because we are assuming the composition of the universe or total population.

A quick test for identifying a Gronsfeld cipher is as follows: the four highest cipher letters (T, U, V, W) have a combined theoretical frequency of 19.3%, and the two lowest cipher letters (C and D) have a combined frequency of 5.26%, so the ratio  $\frac{TUVW}{CD}$  of the cipher letters is  $\frac{19.3}{5.26} = 3.67$ , as compared with the ratio  $\frac{4/26}{2/26} = 2$  for a random (i.e., equiprobable) population. This index, 3.67, may be used as an expected value in a suspected case of Gronsfeld encipherment. As an example, let us consider the following distribution derived from an intercepted 1100-letter message:

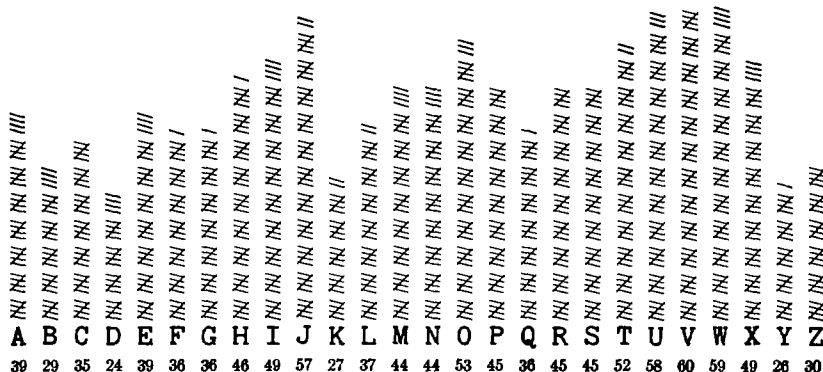


FIGURE 172

The  $\delta$  I.C. is  $\frac{26(48,218)}{1100(1099)} = 1.037$ ; the standard deviation is  $\frac{7.0711}{1100} = .0064$ ; and the sigmage is  $\frac{.037}{.0064} =$

$5.8\sigma$ . The Gronsfeld index of  $\frac{TUVW}{CD}$  is  $\frac{229}{59} = 3.88$ , supporting the hypothesis that this is a case of Gronsfeld encipherment.

(5) In complex noncrashing systems (e.g., Enigma machine systems) wherein a plaintext letter cannot be enciphered by itself, the 25 cipher equivalents of any plaintext letter are equiprobable, leading to the following theoretical relative ciphertext frequencies for English underlying text:

A 3.70	G 3.94	L 3.86	Q 3.99	V 3.94
B 3.96	H 3.86	M 3.90	R 3.70	W 3.94
C 3.88	I 3.70	N 3.68	S 3.76	X 3.98
D 3.83	J 3.99	O 3.70	T 3.63	Y 3.92
E 3.48	K 3.99	P 3.89	U 3.90	Z 4.00
F 3.88				<u>100.00</u>

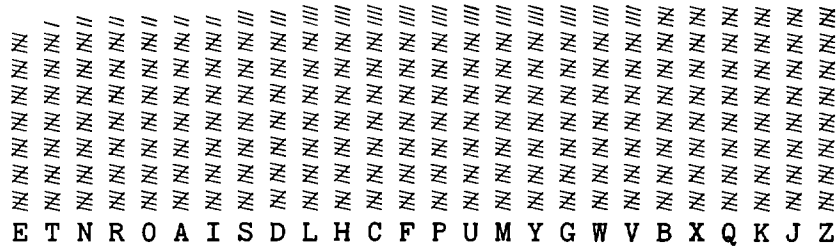
The  $\gamma$  I.C. of the cipher text is most easily computed by the formula  $\gamma_c = 1 + \frac{\beta_p}{(c-1)^2}$ , where  $\beta_p$  is the bulge

of the I.C. of the plain (i.e.,  $\gamma_p - 1.00$ ) and  $c$  is the number of categories; therefore  $\gamma = 1 + \frac{.73}{(26-1)^2} = 1.0012$ .

A property of such systems is that, if the distribution of the cipher letters is made in the descending frequency order of the *plaintext* letters of the language, the slope of frequencies of the ciphertext letters will be that of a gradual ascent; thus:

E 3.48	I 3.70	C 3.88	Y 3.92	X 3.98
T 3.63	S 3.76	F 3.88	G 3.94	Q 3.99
N 3.68	D 3.83	P 3.89	W 3.94	K 3.99
R 3.70	L 3.86	U 3.90	V 3.94	J 3.99
O 3.70	H 3.86	M 3.90	B 3.96	Z 4.00
A 3.70				<u>100.00</u>

Or, in tally-mark form (to a base of 1000 letters):



The slope is so gradual that usually about 8000 letters are required for a positive determination. As an example, let us study the following combined frequency distribution of a number of messages, totalling 4306 letters:

167	171	189	152	141	159	194	152	146	162	154	167	165	137	150	182	189	138	172	187	163	172	159	179	174	185
A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z

The  $\delta$  I.C. is  $\frac{26(715,628)}{4306 \times 4305} = 1.0037$ ; the standard deviation is  $\frac{7.0711}{4306} = .00164$ ; and the sigmage is  $\frac{.0037}{.0016} = 2.3\sigma$ . On the hypothesis that this might possibly be a noncrashing encipherment of English plain text, we construct the distribution in the descending frequency order of English plaintext letters; this is shown by the bar graph in Fig. 173, below. Since the distributional sample is small, we try to smooth the rough bar graph by averaging every pair of letters; this is shown in the figure by the line composed of dashes. Then, in order further to improve matters, we average pairs of averages—we're trying very hard to make things come out the way we wish—and this plotting (shown by the line composed of dots) now displays a gradual ascent from left to right, so we have proved our point.

(6) In plaintext autokey systems, and also in other systems in which the key is literal plain text derived from a book or other source, the expected I.C. will show a measurable departure from random.

The bulge of the I.C. (i.e., the excess over random) may be calculated by the formula  $\beta_c = \frac{\beta_k \times \beta_p}{c-1}$ , where

$\beta_c$  is the bulge of the cipher text,  $\beta_p$  the bulge of the plain text (for English, .73),  $\beta_k$  the bulge of the key (which, since the key text is plain text, is also .73), and  $c$  is the number of categories (in this case, 26). Thus the expected bulge of this type of traffic, without regard to the identity of the components involved, is  $\frac{.73 \times .73}{25} = .0213$ , so the expected I.C. is 1.02 in the general case. When the components are

known sequences, the theoretical distribution for the ciphertext letters may be computed, as well as the I.C. of the specific case. For example, where the components are direct standard alphabets, the relative frequencies are the following (reduced to a base of 1000 letters):

A 40.6	G 45.9	L 41.5	Q 30.9	V 51.7
B 35.3	H 41.8	M 43.5	R 47.2	W 47.3
C 31.6	I 50.5	N 30.1	S 42.2	X 40.9
D 25.0	J 30.1	O 28.0	T 41.5	Y 31.5
E 47.5	K 35.9	P 34.3	U 30.4	Z 35.5
F 39.3				<u>1000.0</u>

The kappa or repeat rate (i.e., the sum of the squares of the probabilities of the cipher letters) is found to be .0398; therefore the theoretical I.C. for direct standard alphabets is  $26(.0398) = 1.0348$ . Where the components are reversed standard alphabets, the relative frequencies are the following (to a base of 1000 letters):

A 66.9	G 34.8	L 45.4	Q 37.7	V 34.4
B 39.9	H 33.9	M 37.4	R 38.1	W 44.1
C 34.1	I 31.3	N 46.7	S 31.3	X 32.1
D 32.1	J 38.1	O 37.4	T 33.9	Y 34.1
E 44.1	K 37.7	P 45.4	U 34.8	Z 39.9
F 34.4				<u>1000.0</u>



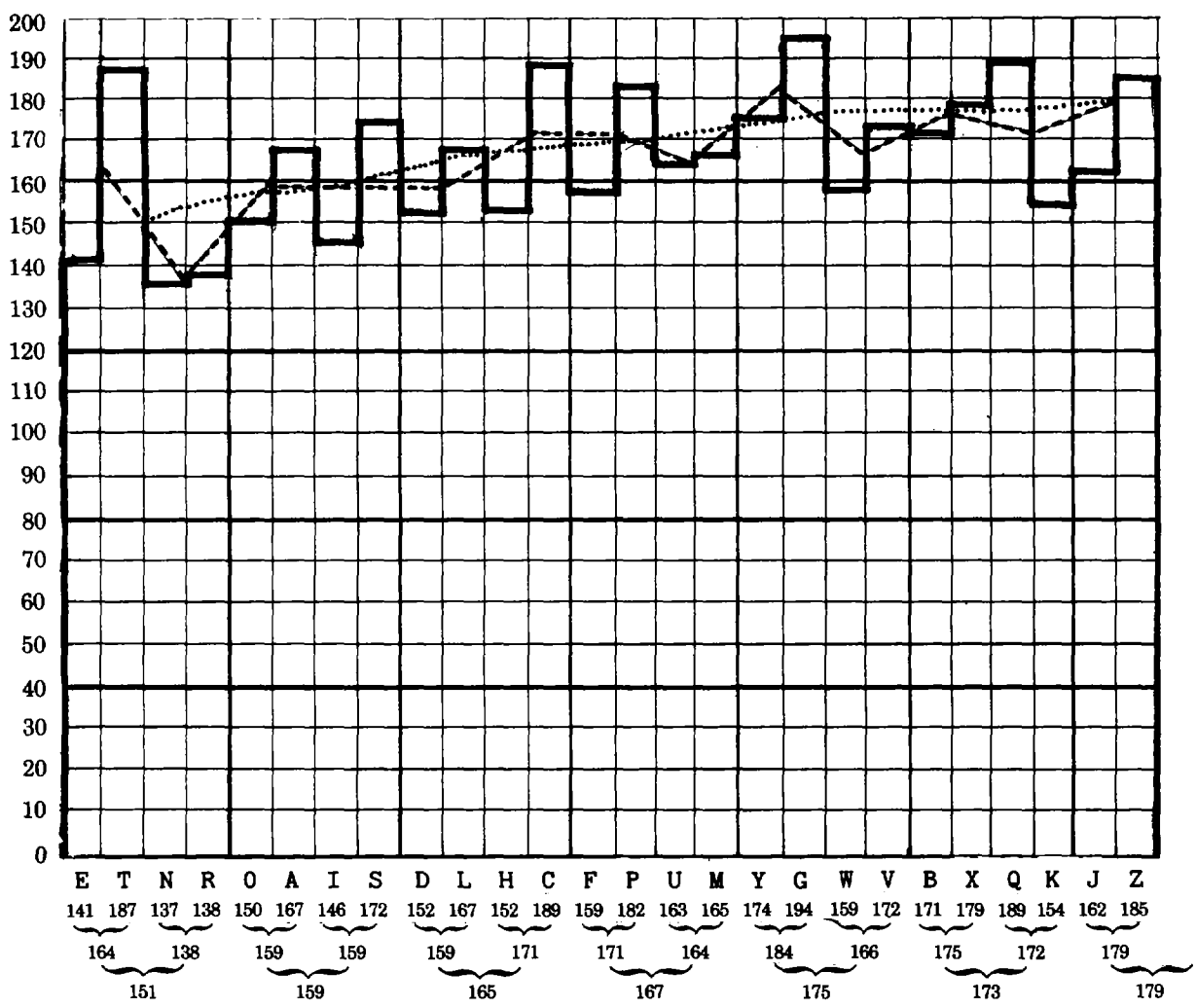


FIGURE 173

The kappa here too is .0398, so the theoretical I.C. for reversed standard alphabets happens to be the same as that for direct standard alphabets, namely, 1.0348. (Note in particular a striking property of this distribution: not only is the frequency of A_e outstanding, about twice that of the average of the other letters, but the distribution is symmetrical about A_e, so that the frequency of B_e=Z_e, C_e=Y_e, D_e=X_e, etc.) For a quick test to determine whether direct standard alphabets have been used, under the assumption

of plaintext keying, we take the ratio  $\frac{VIER}{JNOD} = \frac{197}{113} = 1.7$ ; and, for testing for reversed standard alphabets,

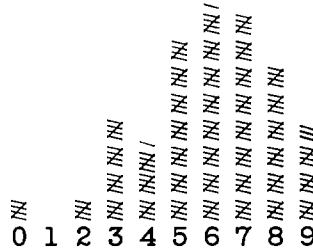
we take the ratio  $\frac{ANLP}{DXIS} = \frac{204}{127} = 1.6$ . (The expected value for random in both cases is of course 1.0.) More

precise measurement would involve the use of the chi-square test of a sample against the theoretical distribution of the assumed population.

(7) In numerical cryptosystems, one of the most striking distributional profiles is that of the classic Nihilist system,³⁹ which involves encipherment (usually periodic) by an additive key which is derived from plain text, applied to intermediate text produced by a 5×5 bipartite square with the row- and column coordinates consisting of the digits 1-5 in normal order, the interior of the square containing the

³⁹ Cf. par. 81 (on pp. 208-218) of *Military Cryptanalytics, Part II*.

letters A-Z inscribed in straight horizontals (with I and J in the same cell). The following distribution of a 210-digit cryptogram is typical:



The virtual absence of the digit 1, the low frequency of 0 and 2, and the characteristic curve of the digits 3-9 are earmarks of this system, without regard to the length of the additive key. Certain other numerical systems, especially those used without superencipherment, also have distinctive profiles; among the most common of these are monome-dinome systems,⁴⁰ particularly those having two or three medium- or low-frequency letters in the top row of the enciphering matrix. Two typical distributions are shown in Figs. 174a and b, below:

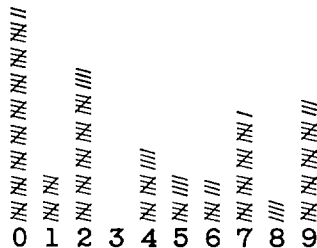


FIGURE 174a

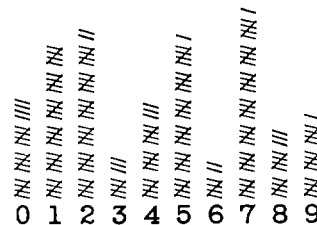


FIGURE 174b

The row coordinates of monome-dinome matrices will be found among the digits of highest frequency: in Fig. 174a, they are 0 and 2; in Fig. 174b they happen to be 1, 5, and 7. The I.C.'s of the matrices will vary, from the lowest possible I.C. of 1.002 to those above 2.00, but in operational cases encountered wherein the top row consists of a key word, the I.C.'s of matrices with two numbered rows are usually in the vicinity of 1.30 to 1.50.⁴¹

(8) The criterion of 40% vowels should not be the sole basis for the identification of a transposition cipher, because there exist substitution systems in which the vowels are abnormally high in the cipher text. For example, (a) 5-letter codes in which two of the letters in each group are vowels, and (b) certain manual and machine cryptosystems (e.g., the "transpositeur à permutations secrètes," a French commercial cipher device⁴²) in which vowels are enciphered by vowels, consonants by consonants. In the former case, the 5-letter code with 2 vowels in each group would be instantly recognized for what it is; if, however, the code groups were further enciphered by a transposition system the phenomena of the individual code groups would be lost, but the over-all text would still contain exactly 40% vowels—in fact, the figure of *exactly* 40%, if consistent in several messages, would be sufficient cause for suspicion.

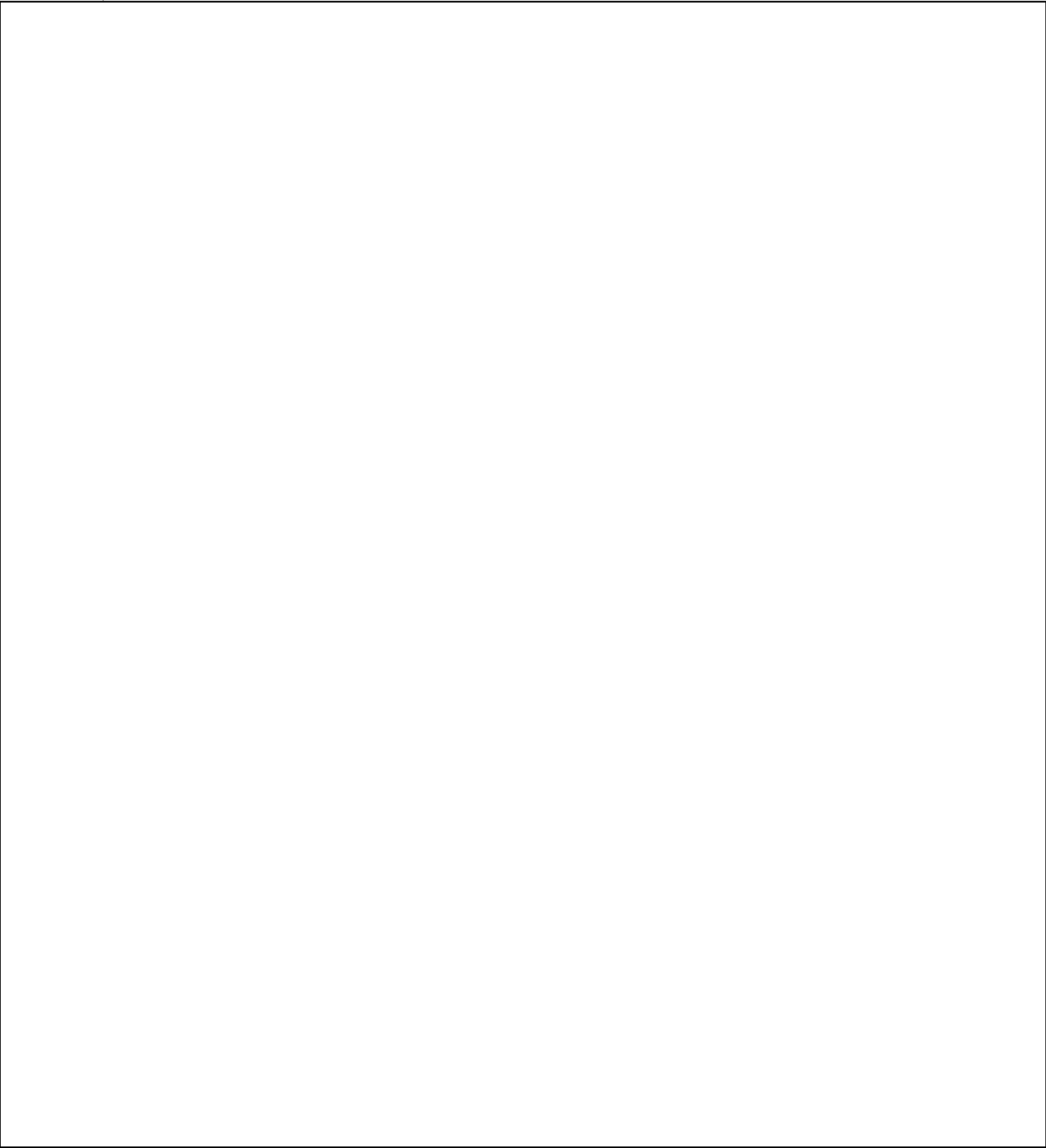
(9) There have been instances of combined substitution-transposition systems involving standard-alphabet monoalphabetic substitution and single columnar transposition. The frequency distribution would reveal the standard-alphabet encipherment, which when removed would leave as a residue the transposition which can then be easily solved. In those cases involving transposition followed by periodic polyalphabetic substitution with standard alphabets, the period may be determined by writing out the text on various widths, with confirmation by the average  $\delta$  I.C. of the columns of the correct width.

⁴⁰ Cf. Chapter X, *Military Cryptanalytics, Part I*.

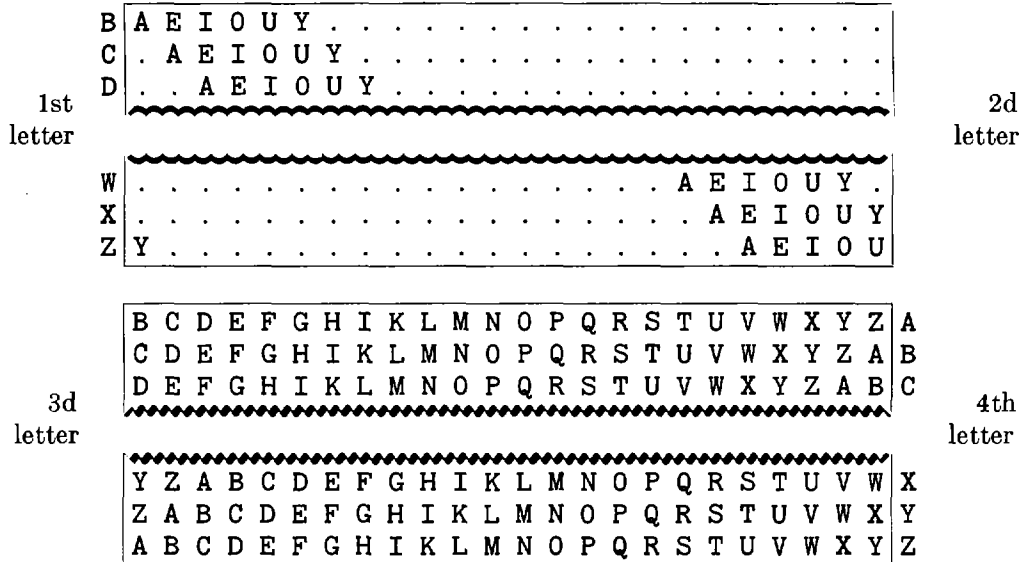
⁴¹ For a discussion of the I.C.'s of different matrices, see par. 89 (on pp. 261-263) of *Military Cryptanalytics, Part II*.

⁴² Cf. par. 76 (on pp. 190-197) of *Military Cryptanalytics, Part II*.





(b) (1)  
(b) (3) -18 USC 798  
(b) (3) -50 USC 3024(i)  
(b) (3) -P.L. 86-36



Only a few messages in this system were intercepted and the code was never broken; the only observation of any importance was that every message contained the group COVQ at least once. It now looks as if Message "A" is a monoalphabetic substitution of a message in this code, and Message "B" a transposition of the basic code text.

(2) In each of the two distributions the frequencies of 10, 9, 7, and 5 occur only once; therefore in Message "A" we can make the decipherments  $D_c=C_p$ ,  $C_c=I_p$ ,  $W_c=X_p$ , and  $F_c=L_p$ , as shown in the work sheet below:

	1	2	3	4	5	6	7
A	D A W S	D C F L	M S U M	W X Z H	F A A S	P S O W	T X I F
C	X	C I L		X	L	X	L
B	B S K D	J C F W	B A S G	<u>I C K U</u>	W H R E	F X P R	<u>I C K U</u>
		C I L X		I	X	L	I
C	J A M D	Q A X L	D K D W	E C Q C	R C X Q	Q C D E	I X Z K
		C	C C X	I I	I	I C	
D	J H K D	D K T N	D A E L	W A C K			
		C C	C	X I			

The crib COVQ has only two possible placements, at D2 or D3; the frequencies of the cipher letters K, T, and N match exactly the frequencies of the plaintext letters O, V, and Q in Message "B", so these decipherments may be made. Furthermore, in the six vowel equivalents (A, C, H, K, S, X) of Message "A" we can identify  $H_c=A_p$  by comparing the frequency distributions of the two messages; and since  $K_c$  (which has a frequency of 8) has already been identified as  $O_p$  from the COVQ crib, then the only other remaining cipher letter with a frequency of 8,  $A_c$ , must therefore represent  $E_p$ . Our work sheet will now look as follows:

	1	2	3	4	5	6	7
A	D A W S	D C F L	M S U M	X W Z H	F A A S	P S O W	T X I F
	C E X	C I		X Y A	E E		X V Y
B	B S K D	J C F W	B A S G	<u>I C K U</u>	W H R E	F X P R	<u>I C K U</u>
	O C	I X	E	I O	X A	Y	I O
C	J A M D	Q A X L	D K D W	E C Q C	R C X Q	Q C D E	I X Z K
	E C	E Y	C O C X	I I	I Y	I C	Y O
D	J H K D	D K T N	D A E L	W A C K			
	A O C	C O V Q	C E	X E I O			

(3) From here on the solution of Message "A" is automatic. The partially recovered groups CEX-, XY-A, and -AOC can now be completed as CEXU, XYZA, and NAOC by means of the permutation table, and these decipherments will snowball into a complete reconstruction of the plain code message:

```

C E X U C I L G P U F P X Y Z A L E E U S U R X V Y H L
J U O C N I L X J E U M H I O F X A D K L Y S D H I O F
N E P C T E Y G C O C X K I T I D I Y T T I C K H Y Z O
N A O C C O V Q C E K G X E I O
    
```

The substitution alphabet, which should have been compiled concurrently with the reconstruction of the plain text,⁴⁷ is found to be as follows:

```

P: A B C D E F G H I J K L M N O P Q R S T U V W X Y Z
C: H Y D R A U L I C B E F G J K M N O P Q S T V W X Z
    
```

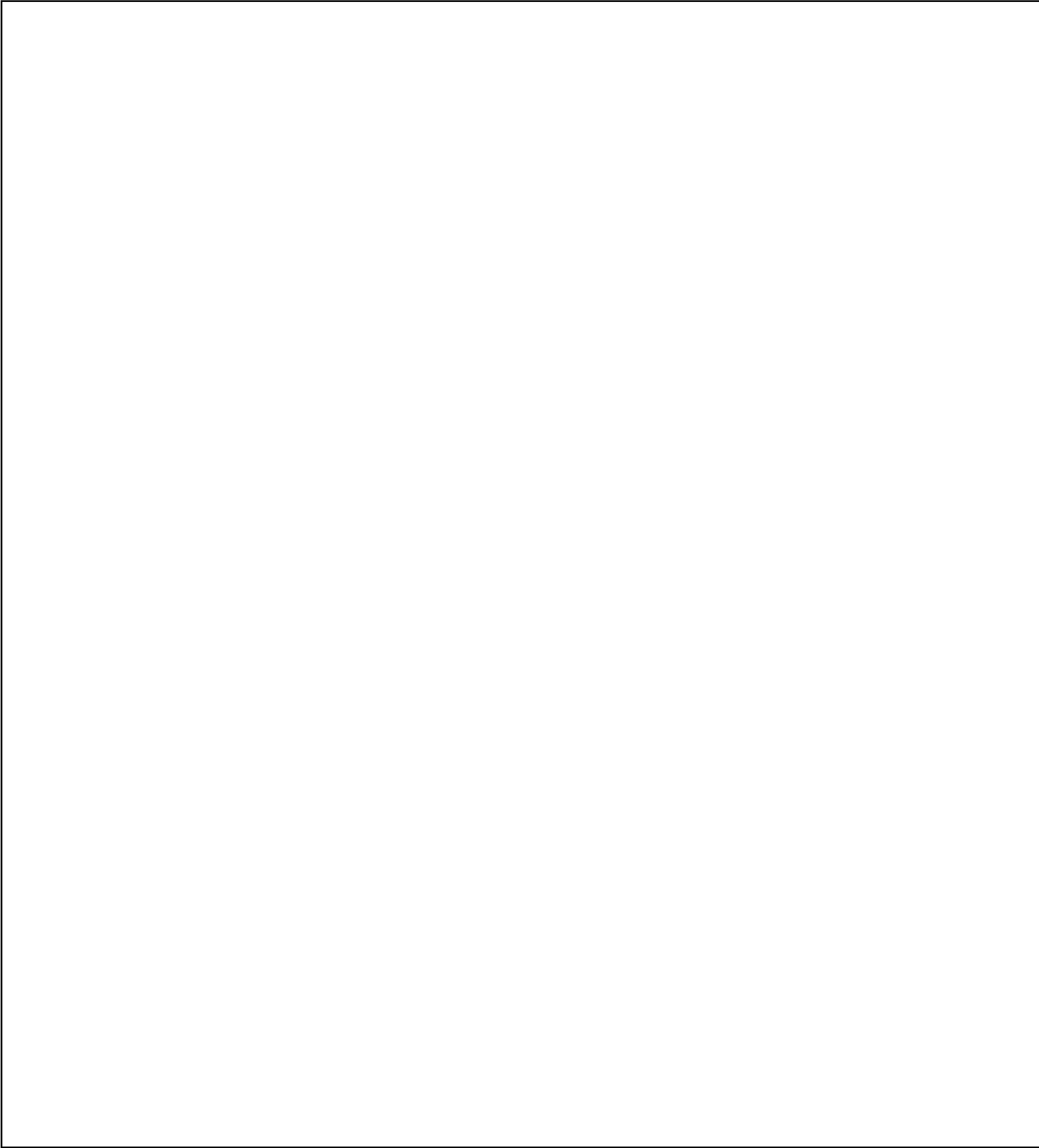
Having reconstructed the underlying plain code of Messages "A" and "B", we can now recover the transposition rectangle used to encipher Message "B", together with the numerical key:⁴⁸

21	13	10	18	6	5	16	19	1	20	7	17	14	9	2	12	8	15	11	4	3
C	E	X	U	C	I	L	G		P	U	F	P	X		Y	Z	A	L	E	
E	U	S	U			R	X	V	Y	H	L	J	U	O	C	N	I	L		X
J	E	U	M	H	I	O	F	X	A		D	K		L	Y		S	D	H	I
O	F		N	E	P	C	T	E	Y	G	C	O	C	X		K	I		T	I
D		I	Y	T	T	I	C	K	H	Y	Z		O	N	A	O		C	C	O
V	Q	C		E	K		G	X	E	I		O								

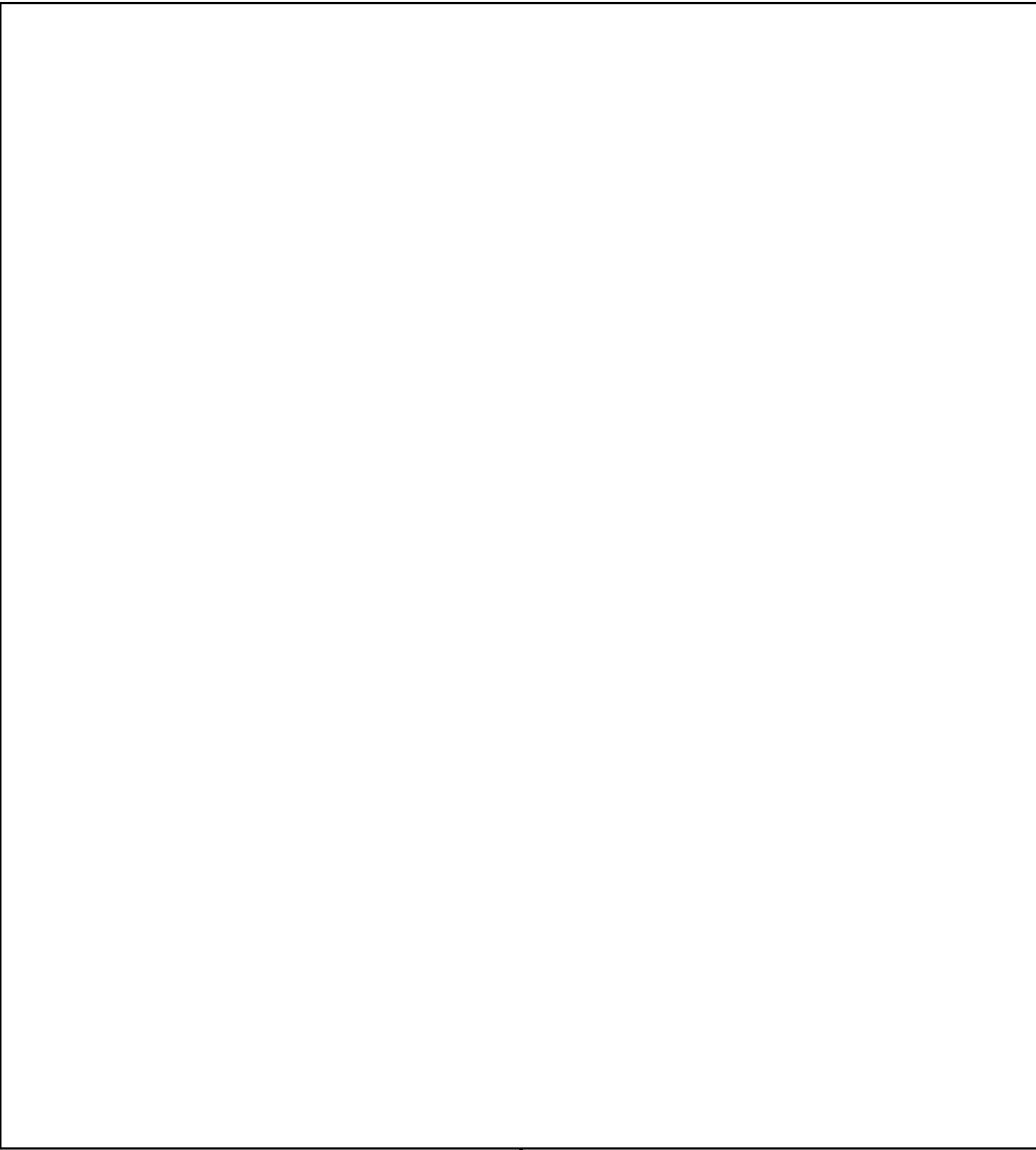
It will be observed that the blank cells in the matrix are systematically placed: in the first row, at key positions 1, 2, and 3; in the second row, at 4, 5, and 6; and so forth, with perhaps blanks in a possible seventh row at positions 19, 20, and 21 for this particular key. The blanks in the matrix vitiate any attempts at anagramming the columns, which would have been possible with the COVQ crib had there been no blanks. Thus neither message is solvable individually, but they are vulnerable when taken together.

⁴⁷ This sin of omission was purposely committed in this example so that the more general technique of solution, which would not rest on the systematic construction of the enciphering alphabet, could be demonstrated.

⁴⁸ The reader might like to recover the literal key from which this numerical key was derived. See in this connection pp. 427-429 of *Military Cryptanalytics, Part II*.

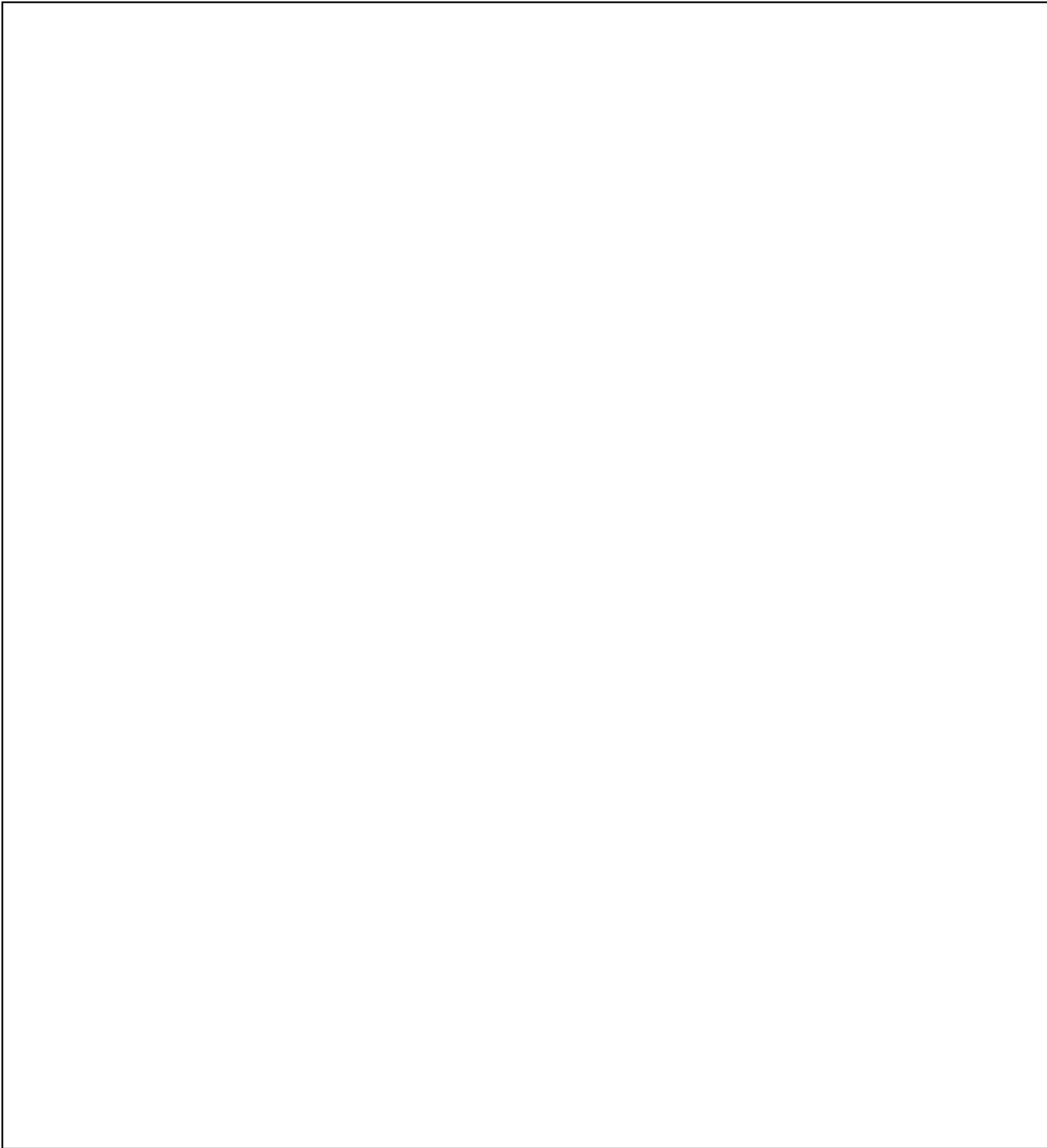


(b) (1)  
(b) (3)-18 USC 798  
(b) (3)-50 USC 3024(i)  
(b) (3)-P.L. 86-36

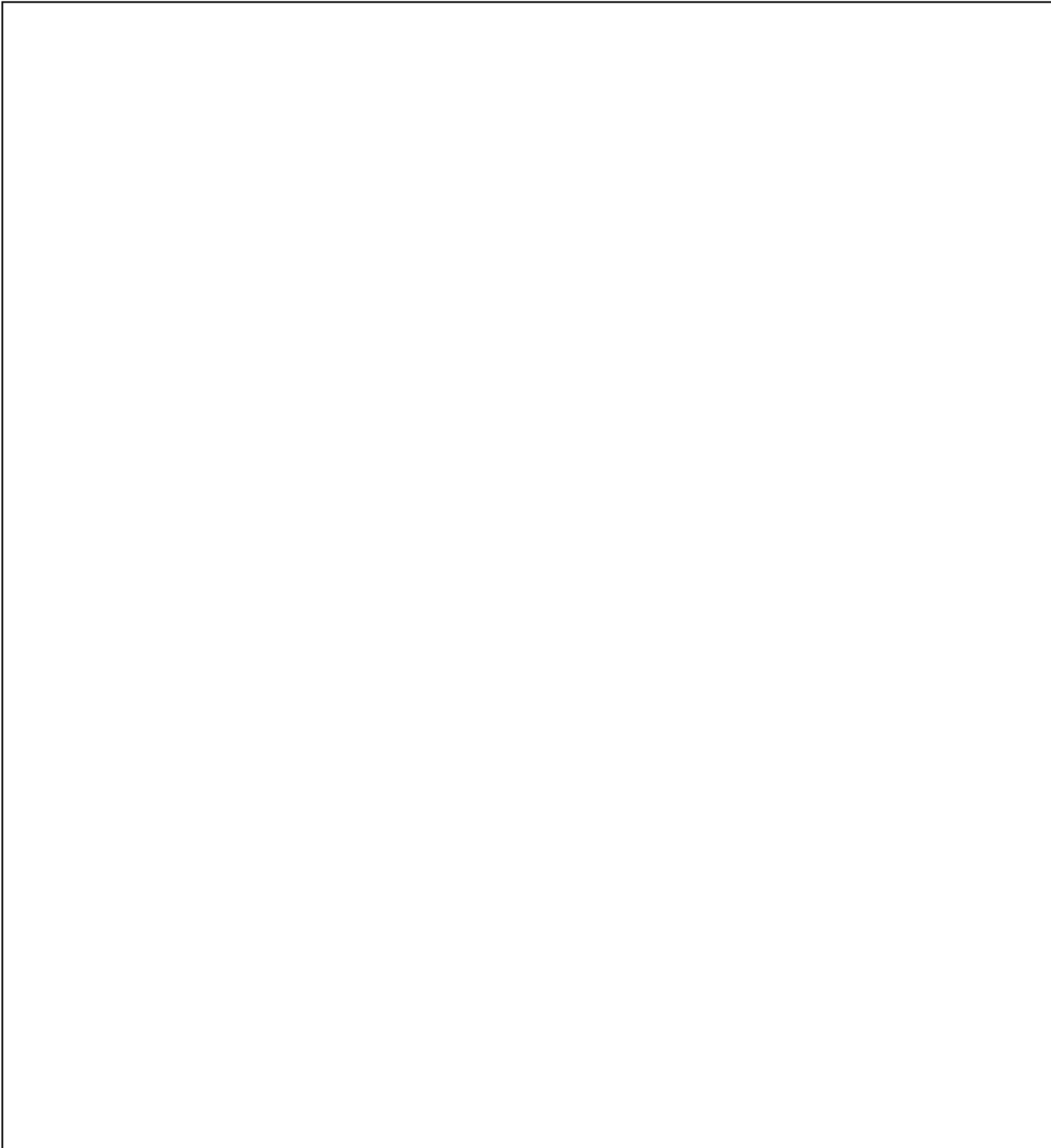


(b) (1)  
(b) (3)-18 USC 798  
(b) (3)-50 USC 3024(i)  
(b) (3)-P.L. 86-36



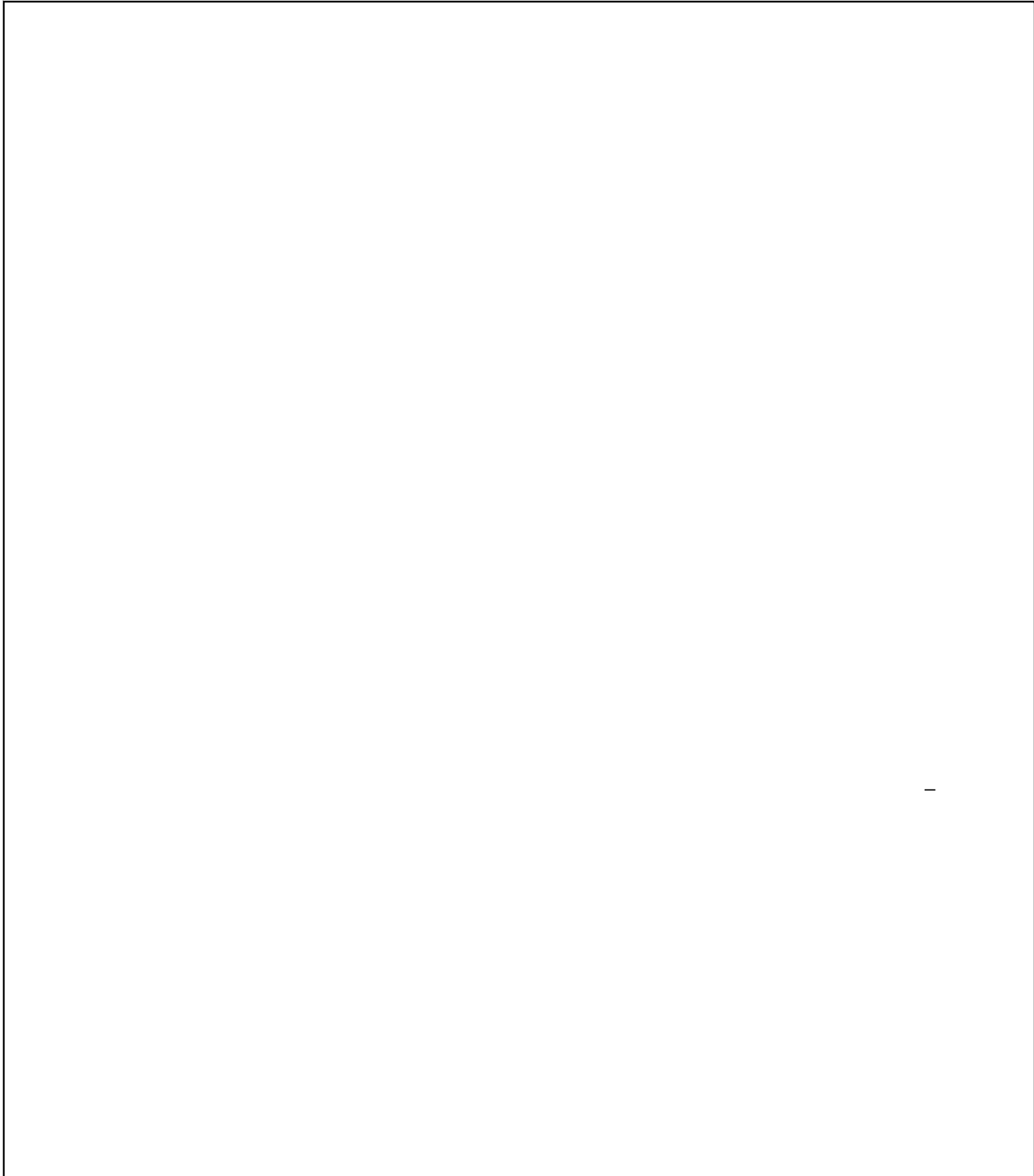


(b) (1)  
(b) (3)-18 USC 798  
(b) (3)-50 USC 3024(i)  
(b) (3)-P.L. 86-36



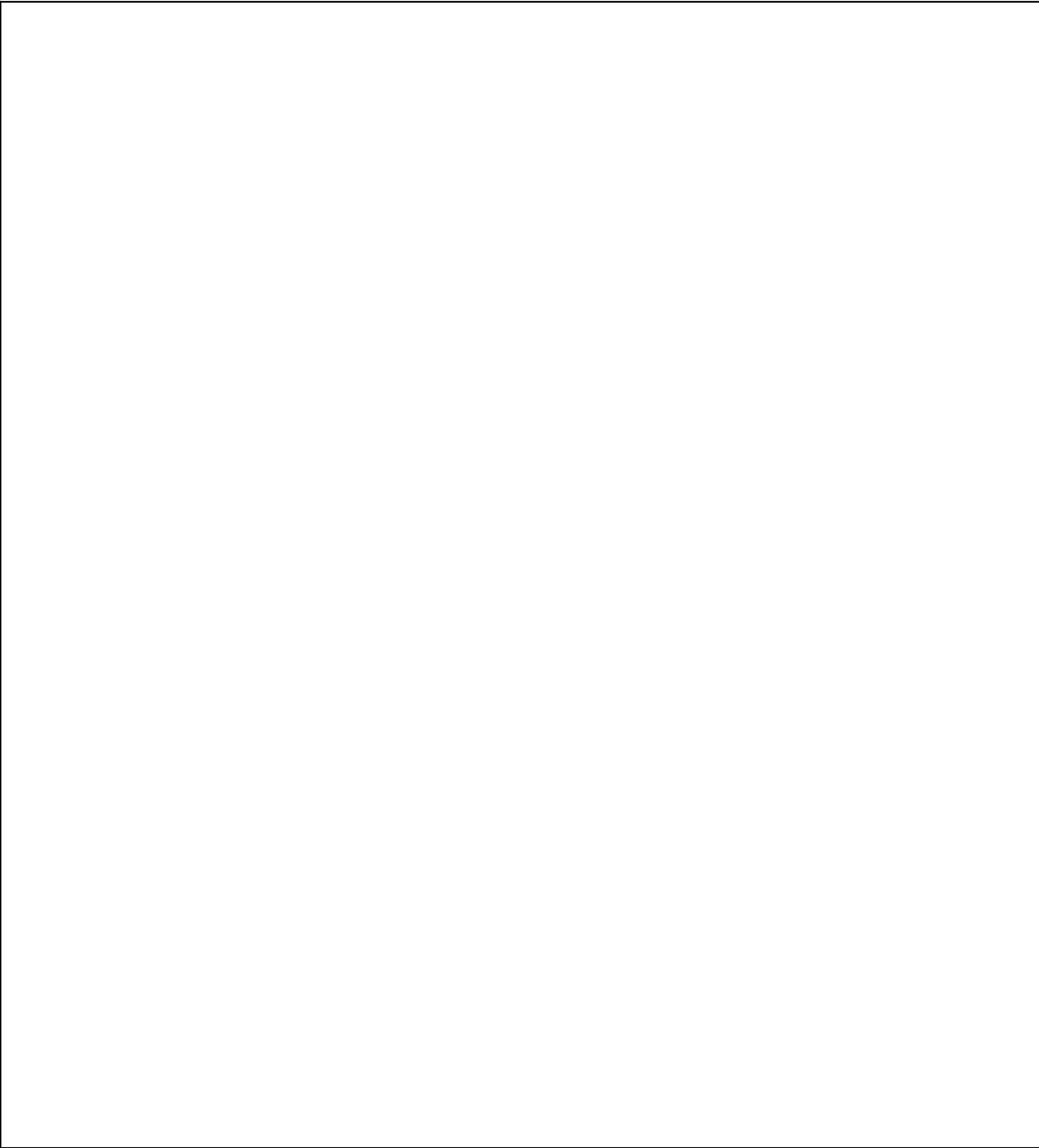
(b) (1)  
(b) (3)-18 USC 798  
(b) (3)-50 USC 3024 (i)  
(b) (3)-P.L. 86-36

(b) (1)  
(b) (3)-18 USC 798  
(b) (3)-50 USC 3024(i)  
(b) (3)-P.L. 86-36



(b) (1)  
(b) (3) -18 USC 798  
(b) (3) -50 USC 3024(i)  
(b) (3) -P.L. 86-36

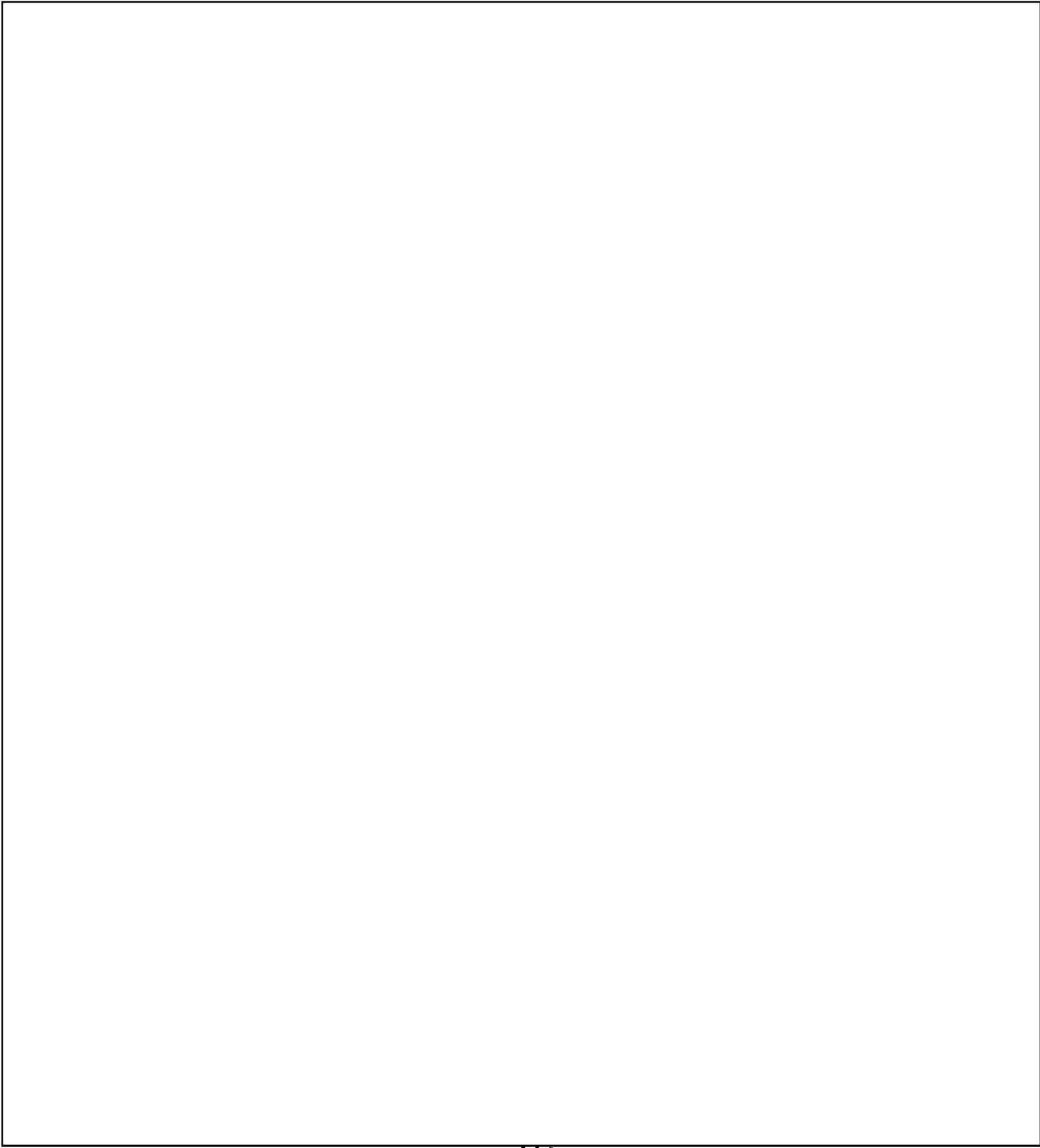
(b) (1)  
(b) (3)-18 USC 798  
(b) (3)-50 USC 3024(i)  
(b) (3)-P.L. 86-36



(b) (1)  
(b) (3)-18 USC 798  
(b) (3)-50 USC 3024(i)  
(b) (3)-P.L. 86-36



(b) (1)  
(b) (3)-18 USC 798  
(b) (3)-50 USC 3024(i)  
(b) (3)-P.L. 86-36

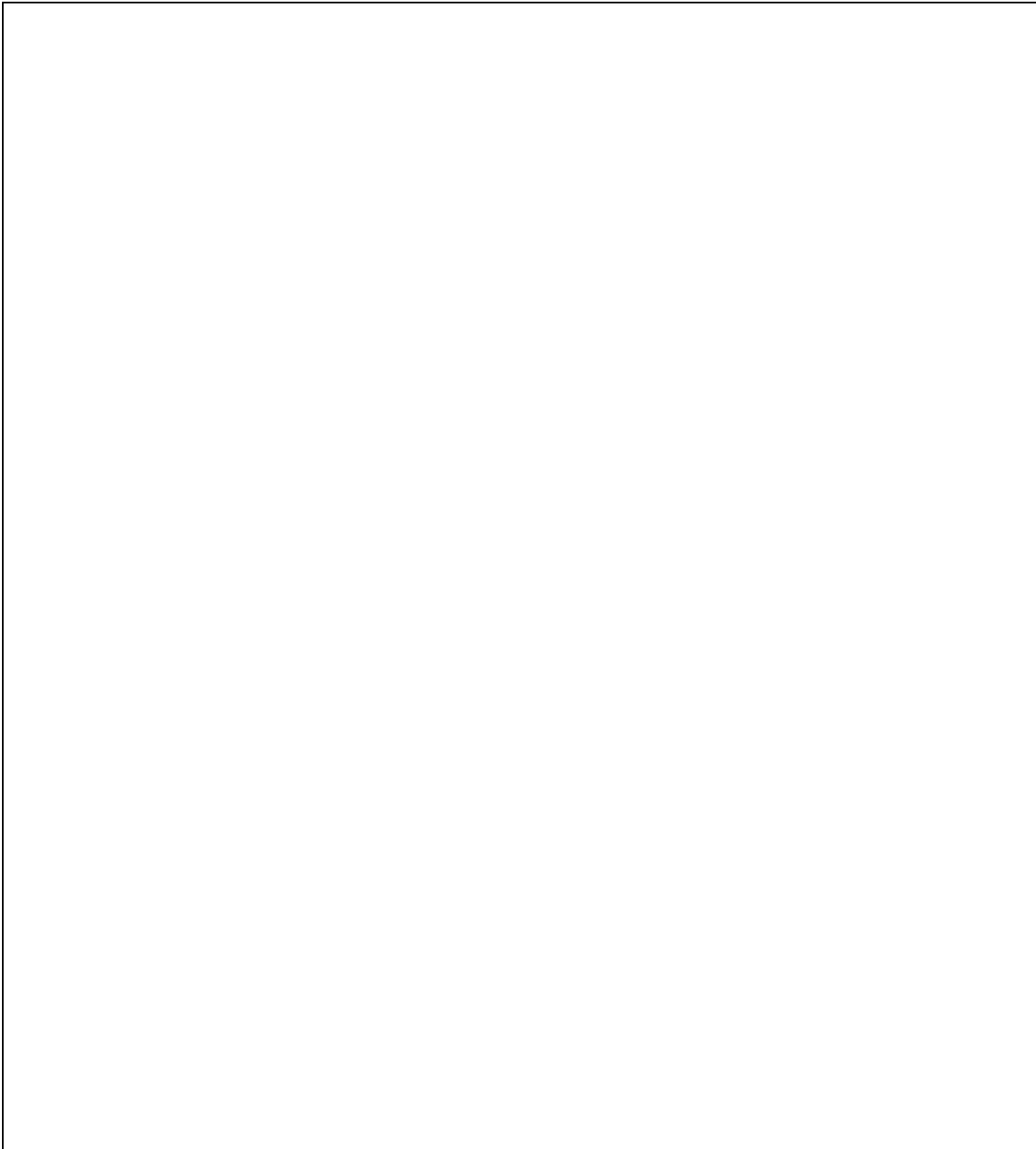


(b) (1)  
(b) (3)-18 USC 798  
(b) (3)-50 USC 3024(i)  
(b) (3)-P.L. 86-36





(b) (1)  
(b) (3)-18 USC 798  
(b) (3)-50 USC 3024(i)  
(b) (3)-P.L. 86-36

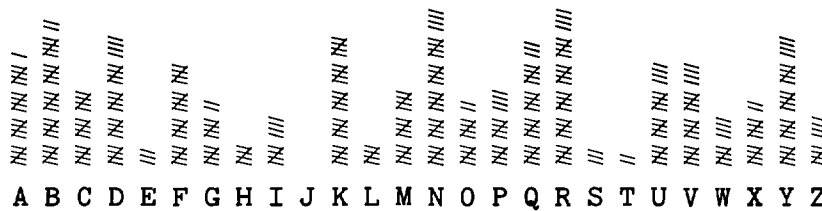


(b) (1)  
(b) (3)-18 USC 798  
(b) (3)-50 USC 3024(i)  
(b) (3)-P.L. 86-36

(b) (1)  
(b) (3)-18 USC 798  
(b) (3)-50 USC 3024 (i)  
(b) (3)-P.L. 86-36

(6) Distributional properties, limitations, and associations provide valuable insights into an unknown cryptosystem. Let us study the following message and its accompanying uniliteral distribution:

B D A U B U A R A D L D Z R B C K Q F N F M Q V B R Z D N B  
 Y Q Z U R B M W Z C C E N A E U D A L G B N N Z L U F P E M  
 R X Q A K C N K V D K G K D U F W U B Q D Z R Z P Y R K G Y  
 C Y W G Z N B P B N A M Y N D W T C K P A Q R V A N A G G K  
 X N F Q N B D B M F I M D K X D Q Y A M D Y K C P S F R Y U  
 Q V V R R I U W Q Y M S F U Q X K P Y D V N M A R Y B Q W N  
 G W C K O Y Y R X U K R U A C B G L A D R B N Y O B P B N V  
 O V K O K R F U M H A Q K N I Q N A M V A U N I B D O K G B  
 Z R F M D X B R F O X R C B D V R F I G B P F N Q I A R V D  
 V Q V R P X A N F D I N Y P K N Y C O W Q K Y O Q B V M K M  
 V N V Q H Q R X Y C Y Q F R V U X N U V U L Y G U T I P W D  
 K D B C F D N K V O N F Q F C K P B R A P K O H Y R B G R Y  
 H O R K N X H M A C S U I R F Q Y P Y N D F B O X



(b) (1)  
 (b) (3) -18 USC 798  
 (b) (3) -50 USC 3024(i)  
 (b) (3) -P.L. 86-36

An interesting profile, no J, a  $\delta$  I.C. of 1.28 representing a deviation of  $15\sigma$ . Digraphic distributions are now made, on and off the cut; these are shown in Figs. 176a and b on the next page. The digraphic I.C. of the on-cut distribution (fig. 176a) is  $\frac{625(92)}{192 \times 191} = 1.57$ , while that of the off-cut distribution (Fig. 176b) is  $\frac{625(80)}{192 \times 191} = 1.36$ . Although  $\frac{192}{25} = 7.7$  doublets are expected if the 25 letters present were equiprobable, and even more in the case at hand with such a rough uniliteral distribution, Fig. 176b has only 5 doublets whereas Fig. 176a has none whatsoever. Furthermore, Fig. 176a shows some striking properties in the physical appearance of the distribution, displaying affinities of some letters for others, and apparent matching propensities among the rows and columns of the distribution; moreover, since there is an apparent symmetry about the main diagonal (from upper left to lower right), this means that the matching of rows also corresponds to identical matching of the columns. Since this now bespeaks a biliteral system with a commutative matrix, we divide the text into digraphs

BD AU BU AR AD LD ZR BX KQ FN FM QV BR ZD NB . . .

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	--	1	2	--	1	--	--	--	--	2	2	--	2	2	--	2	--	2	--	--	--	--	--	--	--	--
B	--	2	2	--	1	--	--	--	--	--	2	1	2	2	2	--	1	--	--	--	--	--	--	--	--	--
C	--	2	--	1	--	--	--	2	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	1	--
D	1	1	--	--	1	--	--	--	1	--	--	--	--	--	--	--	--	--	--	--	1	1	1	1	1	1
E	--	--	--	--	--	--	--	--	--	1	--	--	--	--	--	--	--	--	--	--	1	--	--	--	--	--
F	--	--	2	--	--	--	--	--	--	--	2	2	1	1	2	2	--	2	--	--	--	--	--	--	--	--
G	--	1	--	--	--	--	--	--	1	1	--	--	--	--	--	--	--	--	--	--	1	1	--	--	--	--
H	--	--	--	--	--	--	--	--	1	1	1	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--
I	--	--	--	--	1	--	--	--	1	1	1	1	1	--	--	--	--	--	--	--	--	--	--	--	--	--
J	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--
K	--	2	2	--	1	--	--	--	--	1	2	1	2	1	2	--	--	--	--	--	--	--	--	--	--	--
L	--	--	1	--	1	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	1	--	--	--	--	--
M	1	--	--	--	1	1	--	--	--	--	--	--	--	--	--	--	1	--	1	1	--	--	--	--	--	--
N	2	2	--	--	1	--	1	2	--	--	--	--	--	--	--	--	--	--	--	--	1	1	1	1	1	1
O	--	1	--	--	--	1	--	1	--	--	--	--	--	--	--	--	--	--	--	--	1	1	1	1	1	1
P	--	2	--	--	--	--	--	--	1	--	--	--	--	--	--	--	1	--	--	--	--	--	1	1	1	1
Q	1	1	--	--	1	--	1	1	--	--	--	--	--	--	--	--	--	--	--	--	2	1	2	1	2	1
R	1	2	--	--	1	--	1	2	--	--	--	--	--	--	--	--	--	--	--	--	1	2	2	1	2	1
S	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	1	--	--	--	--	--
T	--	1	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--
U	1	--	--	1	--	--	--	1	--	--	--	--	--	--	--	--	1	--	1	1	--	--	--	--	--	--
V	--	--	2	--	--	--	--	--	1	2	1	2	2	--	1	--	--	--	--	--	1	--	--	--	--	--
W	--	--	1	--	1	--	--	--	1	--	--	--	--	--	--	--	--	--	--	--	1	--	--	--	--	--
X	--	--	1	--	--	--	--	--	2	--	--	1	--	--	1	--	--	--	--	--	1	--	--	--	--	--
Y	--	2	1	--	1	--	--	--	--	2	1	2	2	2	--	1	--	--	--	--	--	1	--	--	--	--
Z	--	1	1	--	--	--	--	--	--	1	--	--	2	--	1	--	--	--	--	--	--	1	--	--	--	--

FIGURE 176a

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	--	1	1	--	--	--	--	1	1	1	--	1	1	--	1	1	--	--	--	--	--	--	--	--	--	--
B	--	--	2	--	1	--	--	--	--	2	2	1	1	--	1	1	--	--	1	--	1	--	1	1	1	1
C	--	1	--	1	--	--	--	2	--	1	1	1	--	1	--	1	--	--	--	--	1	--	--	--	--	--
D	1	1	--	--	--	--	1	2	1	2	1	1	1	--	1	2	--	--	--	--	1	2	--	--	--	1
E	--	--	--	--	--	--	--	--	--	1	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--
F	--	1	1	--	--	--	2	--	--	--	--	--	--	--	1	--	--	--	--	--	1	--	--	--	--	--
G	--	2	--	--	--	1	--	--	1	--	--	--	--	--	1	--	1	--	1	--	--	1	--	--	1	1
H	1	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	1	1
I	1	1	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	1	--	--	--	--	--	--
J	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--
K	--	--	--	--	2	--	--	--	--	1	2	1	--	--	--	--	--	--	2	--	2	1	--	--	--	--
L	1	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	1	1
M	1	--	3	--	--	--	--	1	--	--	--	--	1	1	--	1	--	--	1	--	1	--	1	--	--	1
N	2	1	2	--	3	1	--	1	--	--	1	1	--	1	--	1	--	--	1	1	--	1	--	2	--	2
O	--	--	--	--	--	--	--	1	--	1	--	1	1	--	1	1	--	--	--	--	2	--	--	--	--	--
P	1	1	--	1	1	--	--	1	--	--	--	--	--	--	--	--	--	--	--	--	1	--	2	--	--	--
Q	--	--	1	--	2	--	1	--	1	--	2	--	--	2	--	--	--	--	--	--	1	1	--	1	1	1
R	1	2	1	--	4	--	--	--	--	--	--	--	--	--	1	1	--	1	1	--	1	2	--	1	1	1
S	--	--	--	--	2	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--
T	--	--	--	--	--	--	1	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--
U	1	2	--	1	--	1	--	1	1	1	1	--	2	1	--	--	--	--	--	--	1	--	--	--	--	--
V	2	1	--	--	--	--	--	1	--	--	1	--	1	--	1	--	--	--	--	--	1	1	--	--	--	--
W	--	1	--	--	--	--	--	--	--	--	--	--	--	--	2	--	1	--	--	--	1	--	--	--	--	--
X	1	1	--	--	--	1	--	1	--	--	--	--	--	--	1	--	--	--	--	--	1	--	--	--	--	--
Y	1	1	1	--	--	--	1	--	1	--	1	1	--	1	--	1	--	--	--	--	1	--	--	1	1	1
Z	--	--	--	--	--	--	--	--	1	--	--	1	--	1	--	1	--	--	--	--	--	--	--	--	--	--

FIGURE 176b

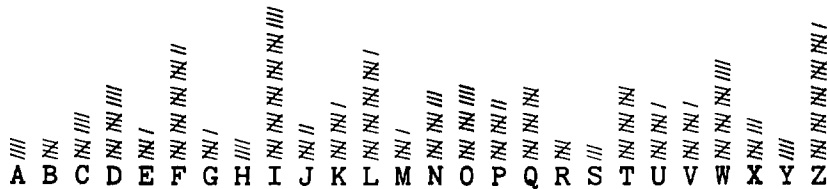
and proceed to establish the two families of letters in the manner illustrated in subpar. *f*(10), above, arriving at the following groupings of 15 and 10 letters:

A B E F H I K L S T V W X Y Z | C D G M N O P Q R U

From the distribution in Fig. 176a we see that the A, F, and V rows match (and also these columns), and we may continue the matching process until we reconstruct the 15 variant row coordinates and the 10 variant column coordinates of what becomes a 5 x 5 matrix. Then, using an arbitrary A-Z sequence within the square, we may reduce the biliteral cipher text to monoalphabetic terms. If slight errors are made in the matching, these can be caught and corrected during the recovery of the plain text.⁶¹

(7) In the next case to be studied, we have the following cryptogram and its accompanying distribution:

<u>C</u>	<u>W</u>	<u>I</u>	<u>E</u>	<u>L</u>	X	G	Q	Z	B	W	E	L	V	A	E	D	N	L	Q	O	I	F	P	Z	O	K	W	Z	M
W	I	F	V	F	Q	I	F	T	B	X	E	G	Q	L	P	Z	I	K	W	C	P	E	J	V	I	D	V	I	D
Q	L	W	Z	K	Q	U	L	T	F	W	<u>C</u>	<u>W</u>	<u>I</u>	<u>E</u>	<u>L</u>	V	F	Q	Z	U	J	T	Z	C	P	F	N	I	I
D	Q	F	R	O	<u>K</u>	<u>N</u>	<u>D</u>	<u>T</u>	<u>I</u>	B	T	Z	J	N	U	K	T	D	N	U	F	S	O	K	W	C	V	Z	O
F	P	Z	O	L	W	I	K	P	O	M	R	I	B	R	Z	L	T	I	D	X	U	L	N	F	W	G	T	Z	F
V	O	M	P	Z	M	X	I	F	N	U	Z	C	S	O	<u>K</u>	<u>N</u>	<u>D</u>	<u>T</u>	<u>I</u>	H	R	G	Y	Z	L	Q	L	Y	U
Z	I	O	C	V	C	W	F	Q	Z	C	N	O	F	X	I	Z	L	S	U	A	D	Q	H	X	I	B	X	M	Y
Z	L	W	J	Q	F	T	I	I	Z	G	X	<u>I</u>	<u>L</u>	<u>T</u>	<u>U</u>	<u>Z</u>	<u>G</u>	<u>R</u>	<u>I</u>	<u>L</u>	<u>T</u>	<u>U</u>	<u>Z</u>	D	P	O	L	V	F
P	O	D	W	J	V	H	N	Z	A	F	N	J	P	I	K	Q	L	W	D	T	M	W	Z	F	N	I	D	Y	A
I	L	V	L	W	Z	L	N	I	O	D	Q	J	T	U	F	T	H	W	I	K	P	I	K	W	F	Q	F	P	Z



Another interesting profile, with an I.C. of 1.28 representing a deviation of  $12\sigma$ . The one hexagraphic repetition present is at an interval of 70, and the two pentagraphic repetitions are at intervals of 71 and 7, so no common factor is involved. Digraphic distributions are now made, on and off the cut, and since these show considerable similarity it means that the cut makes no difference; the two distributions are therefore combined, as shown in Fig. 177, below. There seems to be a remarkable affinity for the letters A-M to contact letters in the last half of the alphabet and vice versa, with the exception of the vowels A, E, I, O, and U; the letter Z also seems not to fit the pattern (note the appearance of the last column of the distribution). In examining the cipher text more closely, it is seen that consonants are clustered in pairs (if we exclude Z), and that these pairs always consist of a letter from the first half of the alphabet followed by a letter from the last half (Y here behaves as a member of the consonant family). No property is discernible among the vowels, other than the fact that they are reluctant to contact each other—there are only 10 such contacts among the 64 vowels AEIOU present; furthermore, the only doublets in the cipher text are the two occurrences of the digraph II. We now conclude that what we have is a uniliteral-biliteral system. We note that the message contains 64 vowels and 105 consonant digraph elements, making a total of 169 underlying plaintext elements. If the cipher vowels actually represent plaintext vowels (say some arrangement of A, E, I, O, and U), and the consonant cipher digraphs represent plaintext consonants (with variants), the ratio of 64:169 is a percentage of 37.9%, which would be acceptable under this hypothesis. Furthermore, the Z_c which might have been assumed to be a null may now be considered, not only from its spacing throughout the cipher text but also from its frequency of 26 out of the 169 plaintext elements (=15.4%) to be a word separator. (The long stretch of 23 cipher letters between the Z's in the last line of the cipher represents only 14 plaintext letters, so that the assumption of a word separator is quite plausible.) The completion of the solution is again left to the reader as an instructive exercise.

⁶¹ Completion of the solution is left to the reader as an exercise.

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	-	-	-	1	1	1	-	-	1	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
B	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	1	-	1	-	-	1	2	-	-	-
C	-	-	-	-	-	-	-	-	-	-	-	-	1	-	2	-	-	1	-	-	2	3	-	-	-	-
D	-	-	-	-	-	-	-	-	-	-	-	2	-	1	4	-	-	3	-	1	1	1	1	-	-	-
E	-	-	1	-	-	1	-	-	1	-	3	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
F	-	-	-	-	-	-	-	-	-	-	-	4	-	4	4	1	1	3	-	2	2	1	-	-	-	-
G	-	-	-	-	-	-	-	-	-	-	-	-	-	-	2	1	-	1	-	-	-	1	1	-	-	-
H	-	-	-	-	-	-	-	-	-	-	1	-	-	1	-	-	-	-	-	1	1	-	-	-	-	-
I	-	3	-	5	2	4	-	1	2	-	5	3	-	-	2	-	-	-	-	-	-	-	-	-	-	2
J	-	-	-	-	-	-	-	-	-	-	-	-	1	-	1	1	-	-	2	-	2	-	-	-	-	-
K	-	-	-	-	-	-	-	-	-	-	-	2	-	2	2	-	-	1	-	-	4	-	-	-	-	-
L	-	-	-	-	-	-	-	-	-	-	-	2	-	1	2	-	1	4	-	4	5	1	1	-	-	-
M	-	-	-	-	-	-	-	-	-	-	-	-	-	1	-	1	-	-	-	-	2	1	1	-	-	-
N	-	-	2	-	1	-	-	3	1	-	1	-	-	1	-	-	-	-	-	3	-	-	-	-	-	1
O	-	-	1	2	-	2	-	-	1	-	4	2	2	-	-	-	-	-	-	-	-	-	-	-	-	-
P	-	-	-	1	1	-	-	2	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	5
Q	-	-	-	-	3	-	1	1	1	-	4	-	-	1	-	-	-	-	-	1	-	-	-	-	-	3
R	-	-	-	-	-	1	-	2	-	-	-	-	-	1	-	-	-	-	-	-	-	-	-	-	-	1
S	-	-	-	-	-	-	-	-	-	-	-	-	2	-	-	-	-	-	-	-	1	-	-	-	-	-
T	-	1	-	1	-	1	-	1	4	-	-	1	-	-	-	-	-	-	-	3	-	-	-	-	-	3
U	1	-	-	-	2	-	-	-	1	1	2	-	-	-	-	-	-	-	-	-	-	-	-	-	-	4
V	1	-	1	-	-	3	-	1	2	-	-	1	-	-	1	-	-	-	-	-	-	-	-	-	-	1
W	-	-	3	1	1	2	1	-	5	2	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	4
X	-	-	-	1	-	1	-	4	-	-	-	1	-	-	-	-	-	-	-	-	1	-	-	-	-	-
Y	1	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	1	-	-	-	-	2
Z	1	1	3	1	-	2	2	-	2	1	1	5	2	-	3	-	-	-	-	-	1	-	-	-	-	-

FIGURE 177

(8) As a final admonition on the recognition of variant phenomena, let us consider an aspect that might escape our notice. We have at hand the following four message beginnings:

- (a) 77790 26062 54876 06579 10093 44420 90978 84898 08236 . . .
- (b) 95743 42558 03993 11928 74140 29556 30307 92815 00311 . . .
- (c) 88521 84625 51975 71358 47204 07600 39699 59667 68331 . . .
- (d) 69674 03906 14939 22790 85401 91774 89689 43339 45359 . . .

Nothing out of the ordinary is seen, until we divide the texts into trinomes:

- (a) 777 902 606 254 876 065 791 009 344 420 909 788 489 808 236 . . .
- (b) 957 434 255 803 993 119 287 414 029 556 303 079 281 500 311 . . .
- (c) 885 218 462 551 975 713 584 720 407 600 396 995 966 768 331 . . .
- (d) 696 740 390 614 939 227 908 540 191 774 896 894 333 945 359 . . .

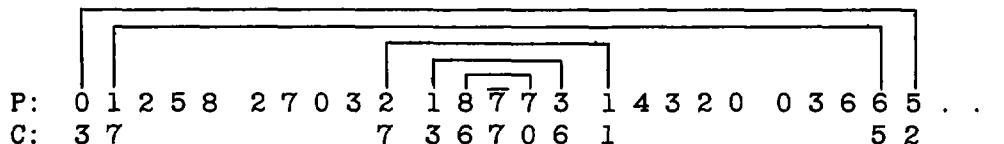
Just when we are about to let this go by, too, we suddenly note that the trinomes in the first column all sum to 21, and that all those in the second column sum to 11; in fact, each of the first 9 columns has trinomes summing to a fixed number. The system is now identified as a summing-trinome system, in which each plaintext letter is assigned a unique value of 1 to 26; this value is then expressed as a trinome, the digits of which sum to the designated value of the letter. The idiomorphic pattern of the stereotyped initial 9-letter word reveals itself as REFERENCE, and the message beginnings are now read with ease and all keys recovered.







From the appearance of these repetitions, after no doubt a considerable amount of study, we may conjecture (a) that the method of encryption encompasses five groups at a time; (b) that similar beginnings are present, involving in the main the first four groups; and (c) that, as a result of observing the predominantly symmetrically placed hits with the A3 group as the center, the manner of encryption involves dinomic substitution starting with elements of the central group, fanning outward until elements of the first and last groups (i.e., the A1 and A5) are combined. This will be clarified by studying the following example of the encryption of a message beginning, using the dinome substitution table shown below:



	0	1	2	3	4	5	6	7	8	9
0	31	67	58	24	90	32	18	84	45	97
1	42	82	50	36	53	29	75	23	06	73
2	62	71	88	17	03	93	30	28	27	15
3	26	00	05	91	79	54	13	41	59	56
4	99	37	10	65	86	08	80	94	61	77
5	12	98	81	14	35	96	39	72	02	38
6	87	48	20	83	92	43	69	01	74	66
7	76	21	57	19	68	16	70	49	95	34
8	46	52	11	63	07	89	44	60	22	85
9	04	33	64	25	47	78	55	09	51	40

The central digit of the A3 is left unenciphered, the *b* and *d* digits (8, 7) are enciphered dinomically as (6, 0) and replaced in the corresponding positions, and the *a* and *e* digits (1, 3) are enciphered as (3, 6). This process is continued in gradually expanding dinomic treatment until the *b* digit (1) of the A1 is combined with the *d* digit (6) of the A5 group to yield the dinome (7, 5), and finally the *a* digit (0) of A1 is combined with the *e* digit (5) of A5 to yield the dinome (3, 2). The feature of reciprocal dinomic substitution incorporated in the table avoids the possible cipher clerk's error of using the deciphering table for encipherment. As an anticlimatic revelation, the system on which this example is based was not solved cryptanalytically, nor for that matter even diagnosed, but instead was read as a result of adroit tachydaetylurgy: light-fingered techniques applied to the enemy's wastebasket. The cryptanalyst is never too proud to accept help from whatever quarter—and even Faust turned the tables on Mephistopheles in the end.

h. We have already shown a number of examples of the application of mathematics in recognizing phenomena. One of the useful mathematical tools for evaluating distributions, i.e., testing for "goodness of fit" against an assumed statistical population, is the  $\chi^2$  (chi square) test. The value of  $\chi^2$  is calculated by the formula  $\chi^2 = \sum \frac{(f_i - a_i)^2}{a_i}$ , where  $f_i$  is the observed frequency of each category and  $a_i$  is the expected frequency of each category in a distribution. The  $\chi^2$  value and the appropriate number of "degrees of freedom" (symbolized by the Greek letter  $\nu$ , nu) are then looked up in a table and translated into a probability statement. The number of degrees of freedom is usually  $c - 1$ : thus for digital text  $\nu = 9$ ; for 26-letter text,  $\nu = 25$ ; and for teleprinter text,  $\nu = 31$ . In Fig. 178 is illustrated an abridged chi-square table that will be found generally useful in estimating the orders of magnitudes of probabilities.

(1) As an example of the application of the  $\chi^2$  test, let us assume that we are to evaluate a distribution of 180 digits of supposedly random text, i.e., from an equiprobable population; ⁶⁴ this distribution is shown in the column labeled  $f_i$  of the diagram below:

	$f_i$	$a_i$	$f_i - a_i$	$(f_i - a_i)^2$
0	22	18	4	16
1	14	18	-4	16
2	13	18	-5	25
3	18	18	0	0
4	18	18	0	0
5	17	18	-1	1
6	16	18	-2	4
7	18	18	0	0
8	17	18	-1	1
9	27	18	9	81
	—	—	—	—
	180	180	0	144

The sum (144) of the squares of the differences, divided by the expected number (18), gives a  $\chi^2$  value of 8; this figure, looked up in the table on the row for 9 degrees of freedom, is found to represent a probability of something greater than 0.5. This means that if we were to examine 100 samples of 10-category random text (the sample size is for all practical purposes immaterial), slightly more than half of them would be as rough as or rougher than the distribution just studied—in other words, this distribution is indistinguishable from a random one. Had the  $\chi^2$  value for a distribution of digits turned out to be, say, 28, looking this up in the row for 9 degrees of freedom gives us a probability of .001; i.e., in 1000 samples of random text, only one of them would be expected to be as rough as or rougher than the case at hand.

⁶⁴ The sample is taken from the four message beginnings given in subpar. *g*(8), above.

CHI-SQUARE TABLE

Probability

$\nu$	0.5	0.1	.05	.01	.005	.001	.0001	.00001	.000001	$\nu$
1	0.5	2.7	3.8	6.6	7.9	10.8	15.1	19.5	23.9	1
2	1.4	4.6	6.0	9.2	10.6	13.8	18.4	23.0	27.6	2
3	2.4	6.2	7.8	11.3	12.8	16.3	21.1	25.9	30.7	3
4	3.4	7.8	9.5	13.3	14.9	18.5	23.5	28.5	33.4	4
5	4.4	9.2	11.1	15.1	16.8	20.5	25.7	30.9	35.9	5
6	5.3	10.6	12.6	16.8	18.5	22.5	27.9	33.1	38.3	6
7	6.3	12.0	14.1	18.5	20.3	24.3	29.9	35.3	40.5	7
8	7.3	13.4	15.5	20.1	22.0	26.1	31.8	37.3	42.7	8
9	8.3	14.7	16.9	21.7	23.6	27.9	33.7	39.3	44.8	9
10	9.3	16.0	18.3	23.2	25.2	29.6	35.6	41.3	46.9	10
11	10.3	17.3	19.7	24.7	26.8	31.3	37.4	43.2	48.9	11
12	11.3	18.6	21.0	26.2	28.3	32.9	39.1	45.1	50.8	12
13	12.3	19.8	22.4	27.7	29.8	34.5	40.9	46.9	52.8	13
14	13.3	21.1	23.7	29.1	31.3	36.1	42.6	48.7	54.6	14
15	14.3	22.3	25.0	30.6	32.8	37.7	44.3	50.5	56.5	15
16	15.3	23.5	26.3	32.0	34.3	39.3	45.9	52.2	58.3	16
17	16.3	24.8	27.6	33.4	35.7	40.8	47.6	54.0	60.1	17
18	17.3	26.0	28.9	34.8	37.2	42.3	49.2	55.7	61.9	18
19	18.3	27.2	30.1	36.2	38.6	43.8	50.8	57.4	63.7	19
20	19.3	28.4	31.4	37.6	40.0	45.3	52.4	59.0	65.4	20
21	20.3	29.6	32.7	38.9	41.4	46.8	54.0	60.7	67.1	21
22	21.3	30.8	33.9	40.3	42.8	48.3	55.5	62.3	68.9	22
23	22.3	32.0	35.2	41.6	44.2	49.7	57.1	64.0	70.6	23
24	23.3	33.2	36.4	43.0	45.6	51.2	58.6	65.6	72.2	24
25	24.3	34.4	37.7	44.3	46.9	52.6	60.1	67.2	73.9	25
26	25.3	35.6	38.9	45.6	48.3	54.1	61.7	68.8	75.6	26
27	26.3	36.7	40.1	47.0	49.6	55.5	63.2	70.4	77.2	27
28	27.3	37.9	41.3	48.3	51.0	56.9	64.7	71.9	78.8	28
29	28.3	39.1	42.6	49.6	52.3	58.3	66.2	73.5	80.4	29
30	29.3	40.3	43.8	50.9	53.7	59.7	67.6	75.0	82.0	30
31	30.3	41.4	45.0	52.2	55.0	61.1	69.1	76.6	83.6	31
32	31.3	42.6	46.2	53.5	56.3	62.5	70.6	78.1	85.2	32
33	32.3	43.8	47.4	54.8	57.7	63.9	72.0	79.6	86.8	33
34	33.3	44.9	48.6	56.1	59.0	65.3	73.5	81.1	88.4	34
35	34.3	46.1	49.8	57.3	60.3	66.6	74.9	82.6	90.0	35
48	47.3	60.9	65.2	73.7	77.0	84.0	93.2	101.7	109.7	48
49	48.3	62.0	66.3	74.9	78.2	85.4	94.6	103.1	111.1	49
63	62.3	77.8	82.5	92.0	95.7	103.4	113.5	122.7	131.4	63
80	79.3	96.6	101.9	112.3	116.3	124.8	135.8	145.8	155.1	80
99	98.3	117.4	123.2	134.6	139.0	148.2	160.1	170.8	180.8	99

FIGURE 178

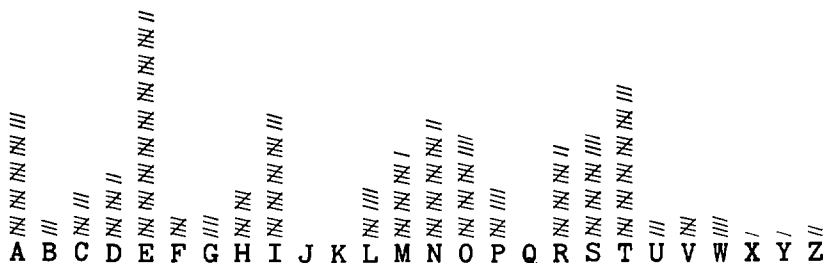
(2) Where the expected frequencies in each category are equal, it is preferable to use an equivalent formula for  $\chi^2$ . This formula, especially advantageous when a desk calculator is handy, is  $\chi^2 = \frac{c}{N} \sum f_i^2 - N$ ; thus, in the previous example wherein the sum of the squares of the frequencies is 3384,  $\chi^2 = \frac{10}{180} (3384) - 180 = 8$ , as before.⁶⁵ In a similar situation involving 26-letter text, we have the following distribution to be tested on the hypothesis of an equiprobable universe:

A 167	G 194	L 167	Q 189	V 172
B 171	H 152	M 165	R 138	W 159
C 189	I 146	N 137	S 172	X 179
D 152	J 162	O 150	T 187	Y 174
E 141	K 154	P 182	U 163	Z <u>185</u>
F 159				<u>4306</u>

The expected (average) frequency for each letter is  $\frac{4306}{26}$  or 165.62, rounded off to the nearest hundredth, and the squaring of the  $(f_i - a_i)$  differences would be a little clumsy. Instead, we calculate the sum (719,934) of the squares of the frequencies, and compute  $\chi^2 = \frac{26}{4306} (719,934) - 4306 = 41.0$  which, as may be seen in the table (in the row of 25 degrees of freedom), roughly interpolating by eye between 37.7 and 44.3, means a probability of about .02, i.e., only one random sample in 50 will have a score as large as or larger than 41.0.

(3) We shall now treat a case wherein the expected frequencies are not equal. Let us assume that the following cryptogram has been recognized as being a transposition cipher, but that the language of the underlying text is unknown, perhaps either English or German:

ITANM IETNA ICTGV IRCHN PESMS LECNE EDAST LDEIM ROSWD RAMEM  
 SNPEO ETTEP VENA E WHNNI TEONO TESWD SAAED EMEMT MPOTA RRTOT  
 EXEDE WNEAF GMAEN NRBEA EIFTR RDNFA ELEAB HAOIE URIOF DPDSO  
 PLMHR IAODM MIPFM THIZA ERRTC AERLT EAISS IATAN SSNTY SEOET  
 CTEIH TSALO ONUVI EDIRV NIIIL THNDO CHTCN ZOLEE NTTIR BEPAE  
 ERTIS MNCTS LRHVG GMSSE IMNOE OOSOA EUTHP



The expected frequencies for a given language are obtained by multiplying the probability of each letter by the sample size; thus, if in English the letter A_p has a probability of .0737, then we should expect .0737 × 285 or 21.00 A's in our sample, and so on. In Fig. 179, below, are listed the computational steps in testing the distribution under the hypothesis that the cryptogram is transposed English plain text, and in Fig. 180 are these steps under the hypothesis that it is transposed German plain text; the "Sq"

⁶⁵ The most convenient sequence of operations for obtaining the values for  $\chi^2$  and  $\delta$  I.C., when a desk calculator is available, is to derive the  $\gamma$  I.C. first, as follows:

- (1)  $\gamma = \frac{c \sum f_i^2}{N^2}$
- (2)  $\chi^2 = N(\gamma - 1)$
- (3)  $\delta = 1 + \frac{\chi^2 + 1 - c}{N - 1}$ , or  $\frac{\chi^2 + N - c}{N - 1}$

in the column headings means of course  $(f_i - a_i)^2$ . The  $\chi^2$  of 34.69 with 25 degrees of freedom for the English hypothesis, representing a probability of 0.1 is not a bad fit, while the value of 105.54 shows that German plain text is astronomically out of the question. We must, however, take another look at our computations. The test is prone to error when the expected frequencies in some categories are too small (look in particular at the contribution of 10.57 for Z in Fig. 179). What we should do is lump together these categories which fall below a preselected level, adjusting the number of degrees of freedom accordingly; here we shall combine the probabilities and observed frequencies of those letters whose expected frequencies are less than 2.00:

	P(E)	$f_i$	$a_i$		P(G)	$f_i$	$a_i$
J	.0016	—	(0.46)	J	.0032	—	(0.91)
K	.0030	—	(0.86)	Q	.0001	—	(0.03)
Q	.0035	—	(1.00)	X	.0002	1	(0.06)
X	.0046	1	(1.31)	Y	.0004	1	(0.11)
Z	.0010	2	(0.29)		.0039	2	
	<u>.0137</u>	<u>3</u>					

These combined entries are now substituted in the calculations, as shown in Figs. 179a and 180a in the lines labelled "&". It is seen that the value of 22.43 (now with 21 degrees of freedom) for the hypothesis of English plain text is much improved (probability of 0.5), and it can be shown (with more extensive  $\chi^2$  tables) that even the  $\chi^2$  of 83.49 with 22 degrees of freedom has been improved by a factor of 1000 to a still useless 0.0000001. (Note, by the way, the high score contributed by the letter M: there happens to be an inordinate number of M's in the plain text, many more than would be expected in an average sample of the language.)

	P(E)	$f_i$	$a_i$	$f_i - a_i$	Sq	$\frac{Sq}{a_i}$
A	.0737	23	21.00	2.00	4.00	0.19
B	.0097	3	2.76	0.24	0.06	0.02
C	.0307	8	8.75	-0.75	0.56	0.06
D	.0424	12	12.08	-0.08	0.01	0.00
E	.1300	42	37.05	4.95	24.50	0.66
F	.0283	5	8.07	-3.07	9.42	1.17
G	.0164	4	4.67	-0.67	0.45	0.10
H	.0339	10	9.66	0.34	0.12	0.01
I	.0735	23	20.95	2.05	4.20	0.20
J	.0016	—	0.46	-0.46	0.21	0.46
K	.0030	—	0.86	-0.86	0.74	0.86
L	.0364	9	10.37	-1.37	1.88	0.18
M	.0247	16	7.04	8.96	80.28	11.40
N	.0795	22	22.66	-0.66	0.44	0.02
O	.0753	19	21.46	-2.46	6.05	0.28
P	.0267	9	7.61	1.39	1.93	0.25
Q	.0035	—	1.00	-1.00	1.00	1.00
R	.0758	17	21.60	-4.60	21.16	0.98
S	.0612	19	17.44	1.56	2.43	0.14
T	.0919	28	26.19	1.81	3.28	0.13
U	.0260	3	7.41	-4.41	19.45	2.62
V	.0153	5	4.36	0.64	0.41	0.09
W	.0156	4	4.45	-0.45	0.20	0.04
X	.0046	1	1.31	-0.31	0.10	0.08
Y	.0193	1	5.50	-4.50	20.25	3.68
Z	.0010	2	0.29	1.71	2.92	10.07
	1.0000	285	285.00	0.00		34.69

FIGURE 179

	P(G)	$f_i$	$a_i$	$f_i - a_i$	Sq	$\frac{Sq}{a_i}$
A	.0600	23	17.10	5.90	34.81	2.04
B	.0170	3	4.85	-1.85	3.42	0.71
C	.0270	8	7.70	0.30	0.09	0.01
D	.0541	12	15.42	-3.42	11.70	0.76
E	.1795	42	51.16	-9.16	83.91	1.64
F	.0160	5	4.56	0.44	0.19	0.04
G	.0320	4	9.12	-5.12	26.21	2.87
H	.0413	10	11.77	-1.77	3.13	0.27
I	.0813	23	23.17	-0.17	0.03	0.00
J	.0032	—	0.91	-0.91	0.83	0.91
K	.0124	—	3.53	-3.53	12.46	3.53
L	.0331	9	9.43	-0.43	0.18	0.02
M	.0226	16	6.44	9.56	91.39	14.19
N	.1055	22	30.07	-8.07	65.12	2.17
O	.0272	19	7.75	11.25	126.56	16.33
P	.0083	9	2.37	6.63	43.96	18.55
Q	.0001	—	0.03	-0.03	0.00	0.00
R	.0723	17	20.61	-3.61	13.03	0.63
S	.0687	19	19.58	-0.58	0.34	0.02
T	.0574	28	16.36	11.64	135.49	8.28
U	.0458	3	13.05	-10.05	101.00	7.74
V	.0087	5	2.48	2.52	6.35	2.56
W	.0150	4	4.28	-0.28	0.08	0.02
X	.0002	1	0.06	0.94	0.88	14.67
Y	.0004	1	0.11	0.89	0.79	7.18
Z	.0109	2	3.11	-1.11	1.23	0.40
	1.0000	285	285.02	0.02		105.54

FIGURE 180

	P(E)	$f_i$	$a_i$	$f_i - a_i$	Sq	$\frac{Sq}{a_i}$
A	.0737	23	21.00	2.00	4.00	0.19
B	.0097	3	2.76	0.24	0.06	0.02
C	.0307	8	8.75	-0.75	0.56	0.06
D	.0424	12	12.08	-0.08	0.01	0.00
E	.1300	42	37.05	4.95	24.50	0.66
F	.0283	5	8.07	-3.07	9.42	1.17
G	.0164	4	4.67	-0.67	0.45	0.10
H	.0339	10	9.66	0.34	0.12	0.01
I	.0735	23	20.95	2.05	4.20	0.20
J	.0016	—				
K	.0030	—				
L	.0364	9	10.37	-1.37	1.88	0.18
M	.0247	16	7.04	8.96	80.28	11.40
N	.0795	22	22.66	-0.66	0.44	0.02
O	.0753	19	21.46	-2.46	6.05	0.28
P	.0267	9	7.61	1.39	1.93	0.25
Q	.0035	—				
R	.0758	17	21.60	-4.60	21.16	0.98
S	.0612	19	17.44	1.56	2.43	0.14
F	.0919	28	26.19	1.81	3.28	0.13
U	.0260	3	7.41	-4.41	19.45	2.62
V	.0153	5	4.36	0.64	0.41	0.09
W	.0156	4	4.45	-0.45	0.20	0.04
X	.0046	(1)				
Y	.0193	1	5.50	-4.50	20.25	3.68
Z	.0010	(2)				
&	.0137	3	3.90	-0.90	0.81	0.21
	1.0000	285	284.98	0.02		22.43

FIGURE 179a

	P(G)	$f_i$	$a_i$	$f_i - a_i$	Sq	$\frac{Sq}{a_i}$
A	.0600	23	17.10	5.90	34.81	2.04
B	.0170	3	4.85	-1.85	3.42	0.71
C	.0270	8	7.70	0.30	0.09	0.01
D	.0541	12	15.42	-3.42	11.70	0.76
E	.1795	42	51.16	-9.16	83.91	1.64
F	.0160	5	4.56	0.44	0.19	0.04
G	.0320	4	9.12	-5.12	26.21	2.87
H	.0413	10	11.77	-1.77	3.13	0.27
I	.0813	23	23.17	-0.17	0.03	0.00
J	.0032	—				
K	.0124	—	3.53	-3.53	12.46	3.53
L	.0331	9	9.43	-0.43	0.18	0.02
M	.0226	16	6.44	9.56	91.39	14.19
N	.1055	22	30.07	-8.07	65.12	2.17
O	.0272	19	7.75	11.25	126.56	16.33
P	.0083	9	2.37	6.63	43.96	18.55
Q	.0001	—				
R	.0723	17	20.61	-3.61	13.03	0.63
S	.0687	19	19.58	-0.58	0.34	0.02
T	.0574	28	16.36	11.64	135.49	8.28
U	.0458	3	13.05	-10.05	101.00	7.74
V	.0087	5	2.48	2.52	6.35	2.56
W	.0150	4	4.28	-0.28	0.08	0.02
X	.0002	(1)				
Y	.0004	(1)				
Z	.0109	2	3.11	-1.11	1.23	0.40
&	.0039	2	1.11	0.89	0.79	0.71
	1.0000	285	285.02	-0.02		83.49

FIGURE 180a



(4) One more example might be apropos at this point. If we wished to test the distribution of the 4306 letters given in subpar. (2), above, for the possibility of a complex noncrashing encipherment, we will have the following computational steps:⁶⁶

	P	f _i	a _i	f _i -a _i	(f _i -a _i ) ²	$\frac{(f_i - a_i)^2}{a_i}$
A	.0370	167	159.32	7.68	58.98	0.37
B	.0396	171	170.52	0.48	0.23	0.00
C	.0388	189	167.07	21.93	480.92	2.88
D	.0383	152	164.92	-12.92	166.93	1.01
E	.0348	141	149.85	-8.85	78.32	0.52
F	.0388	159	167.07	-8.07	65.12	0.39
G	.0394	194	169.66	24.34	592.44	3.49
H	.0386	152	165.21	-14.21	201.92	1.21
I	.0370	146	159.32	-13.32	177.42	1.11
J	.0399	162	171.81	-9.81	96.24	0.56
K	.0399	154	171.81	-17.81	317.20	1.85
L	.0386	167	166.21	0.79	0.62	0.00
M	.0390	165	167.93	-2.93	8.58	0.05
N	.0368	137	158.46	-21.46	460.53	2.91
O	.0370	150	159.32	-9.32	86.86	0.55
P	.0389	182	167.50	14.50	210.25	1.26
Q	.0399	189	171.81	17.19	295.50	1.72
R	.0370	138	159.32	-21.32	454.54	2.85
S	.0376	172	161.91	10.09	101.81	0.63
T	.0363	187	156.31	30.69	941.88	6.03
U	.0390	163	167.93	-4.93	24.30	0.14
V	.0394	172	169.66	2.34	5.48	0.03
W	.0394	159	169.66	-10.66	113.64	0.67
X	.0398	179	171.38	7.62	58.06	0.34
Y	.0392	174	168.80	5.20	27.04	0.16
Z	.0400	185	172.24	12.76	162.82	0.95
	<u>1.0000</u>	<u>4306</u>	<u>4306.00</u>	<u>0.00</u>		<u>31.68</u>

Interpolating in the  $\chi^2$  table for 25 degrees of freedom, we find that the value 31.68 represents a probability of about 0.2; in other words, this is a good fit for the hypothesis of noncrashing encipherment.

(5) We cannot leave this discussion without an admonishment on the application of mathematical tools. High scores in significance tests are regarded by the experienced cryptanalyst as indicative of a probability of a particular hypothesis, and not proof of the matter. Take for example the following 440-character cryptogram sent by an enemy known to be using cyclic additive keys of lengths between 20 and 40 digits:

```

90723 78168 94849 15771 16844 17454 66220 88312 87103 45436
51844 80725 95351 25207 71062 43897 67340 60921 05986 85348
28147 15733 58293 45515 05206 88337 34666 19895 67818 09150
66954 13321 61791 75797 51414 31979 86210 85627 71095 58825
20894 16966 09087 59634 80149 82880 81862 77470 01320 13674
11794 57837 24849 06800 00520 19613 90147 16045 20150 35129
06260 72364 91991 17821 62194 36516 06329 85610 90458 05395
55013 35800 92354 04365 92886 96225 20858 05926 00264 38137
81653 45991 26864 97686 06029 44327 74662 65027

```

⁶⁶ The probabilities here are those given on p. 363, and have been calculated by the formula  $P_i = \frac{1-p_i}{c-1}$ , where  $P_i$  is the probability of the cipher letter,  $p_i$  the probability of the plaintext letter in the language, and  $c$  the number of categories. Thus, since E_p in English has a probability of .1300, the probability of E in the cipher text is  $\frac{1-.1300}{25} = .0348$ .

The frequency distribution of the cipher text written out on a width of 20 is the following:

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	
0	4	6	1	2	4	5	1	1	2	3	5	3	4	3	1	1	1	3			
1	1	3	5	2	2	5	2	1	2	1	7	1	2	1	5	1	2	4	3		
2	4	2	3	3	1	2	1	4	2	1	3	3	3			1	7	1			
3		4	3	1	1	5	3	1	1	1		1	2	4	2	3	3	1			
4	1	1	6	4	3	2	2	1	3	3	1	2	6	2	1	1	1				
5	2	5		8	1	2	3	4	2	1	2	1	3	7	1	5					
6	4	4	1	1	1	1	4	2	4	4	2	4	2	6	3	1	1	4	1		
7	3	2	2	3	1	2	1	5	3	1	1	1	4	2	3	4					
8	4	1	5	3	3	2	2	1	1	1	1	5	3	4	3	6	1	1			
9	5		3	3	1	4	3	3	1	3	4	2	2	3	1	2	2				
	68	58	60	66	46	58	74	42	40	52	48	68	46	60	52	54	68	52	68	46	=1126

The  $\delta$  I.C. here is  $\frac{10(1126)}{20(22 \cdot 21)} = 1.22$ , and its sigmage is  $\frac{440(1.22-1.00)}{\sqrt{2(20 \cdot 9)}} = 5.1\sigma$ .

This sigmage, which can be interpreted by the  $\chi^2$  distribution with  $20 \times 9$  or 180 degrees of freedom, turns out to have a probability of 0.000005 of having occurred by chance in a random sample of this size.⁶⁷ This shows that we are *certainly on the right track, but it doesn't prove that we necessarily have the right answer*. If we should write the cipher text on a width of 30, however, we will have the following distributional diagram:

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	
0	9	3	2	1	5	1			1	1	3	2	1	1	2	1	2	1	3	1	2	3	1	2	3	2	2	4			
1	1	1	1	3	2	3	1	1	6	4	2	5							3	1	3	2	3	2	1	2	2	1			
2	1	5	6	1	1	1	3	1	1	2	2	1	1	4	5	1	1	1													
3	4	1	1	2	7	3	1	1	2	1	1	3	1	1	1	3	1	1													
4		3	1	2	1	3	2	1	4	1	3	1	1	1	1	1	1	1													
5	3	1	3	1	4	1																									
6	2	6	2	2	5	3	1	3	3	2	1	2	1	3	2	2	1	3	2	2	1	3	1	1	4						
7	1	1	2	1	5	3	1	2	2	1	2	1	1	4	2																
8	1	2	5	4	2	3	1	2	1	1	1	1	6	1	1	1	8	2	1	2	1										
9	3	1	2	2	2	5	1	4	2	1	1	3	5																		
	80	42	36	40	30	28	30	64	24	28	32	40	24	32	12	28	24	38	38	38	38	16	58	28	36	20	26	20	20	28	=1020

The  $\delta$  I.C. here is  $\frac{10(1020)}{20(15 \cdot 14) + 10(14 \cdot 13)} = 1.69$ , while the sigmage is  $\frac{440(1.69-1.00)}{\sqrt{2(30 \cdot 9)}} = 13.06\sigma$ . This

sigmage, on the  $\chi^2$  distribution with  $30 \times 9$  or 270 degrees of freedom, can be interpreted and shown to have a probability of less than  $10^{-23}$  of occurring by chance. The explanation is that a cyclic 30-digit additive sequence was actually used with underlying monome-dinome text of a theoretical I.C. of approximately 1.69; on a width of 20, however, each column of the distribution diagram is composed not of a random sampling of ciphertext digits, but instead represents a merger of three monoalphabetic distributions, as is in fact suggested by the average I.C. of 1.22 for this array—almost exactly one-third the bulge of the underlying plain text.

⁶⁷ The manner of this computation, a bit complicated, is outlined here for the interested reader. Since the distribution of the  $\delta$  I.C. is asymptotically related to the  $\chi^2$  distribution, the latter may be used to evaluate the  $\delta$  I.C. The mean of any  $\chi^2$  distribution is equal to  $\nu$ , and the variance ( $\sigma^2$ ) is equal to  $2\nu$ , which in this case is 360; the standard deviation ( $\sigma$ ), being equal to the square root of the variance, is in this case  $\sqrt{360}$  or 19.0. The sum of the mean (180) plus the product  $5.1 \times 19.0$  gives the equivalent  $\chi^2$  score of 276.9. Now the probability that a  $\chi^2$  score equal to or greater than  $k$  will occur is given by 1 minus the Poisson cumulative entry for  $\frac{\nu}{2}$ , where  $\frac{a}{2}$  is expected. Thus, in this particular case, we look up  $a = \frac{276.9}{2}$  (rounded off to 138) in the Poisson cumulative tables, and opposite the expected value  $\frac{180}{2}$  or 90 we find the entry .999995, which when subtracted from 1 gives the answer 0.000005.

(6) A typical example of the use of log weights in substitution ciphers has been treated in subpar. 76q(4) in connection with the selection of generatrices. Log weights are also useful in the solution of transposition ciphers, as will be shown by the subsequent discussion. Let us suppose that we have at hand the transposition cipher given in subpar. h(3), above, and that it has been recognized that the underlying language is English. The message length, 285 letters, suggests the possibility of a completely filled rectangular matrix, either 15×19 or 19×15. If this assumption is correct and if the usual form of keyed columnar transposition is involved, we can determine the size of the matrix actually used. This we do by inscribing the cipher text into the matrices by columns from left to right, counting the vowels in the rows and noting the deviations from the expected. The correct matrix size will exhibit a consistency of smaller deviations from the expected 40% vowels; the sum of the deviations, divided by the column lengths, gives a convenient index pointing to the correct matrix from among several possibilities—the correct matrix will be the one with the smallest index. In Fig. 181, below, the expected number of vowels in each row is  $.40 \times 15 = 6.0$  and the index is  $\frac{27.0}{19} = 1.4$ , whereas in Fig. 182 the expected number is  $.40 \times 19 = 7.6$  and the index is  $\frac{15.0}{15} = 1.0$ ; it is obvious that Fig. 182 is the correct matrix.

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	V	D
I	N	I	T	E	R	N	A	M	R	S	O	D	P	M	5	1.0	
T	P	M	E	S	R	N	B	H	R	S	O	O	A	S	4	2.0	
A	E	R	P	W	T	R	H	R	T	N	N	C	E	S	3	3.0	
N	S	O	V	D	O	B	A	I	C	T	U	H	E	E	7	1.0	
M	M	S	E	S	T	E	O	A	A	Y	V	T	R	I	7	1.0	
I	S	W	N	A	E	A	I	O	E	S	I	C	T	M	8	2.0	
E	L	D	A	A	X	E	E	D	R	E	E	N	I	N	8	2.0	
T	E	R	E	E	E	I	U	M	L	O	D	Z	S	O	8	2.0	
N	C	A	W	D	D	F	R	M	T	E	I	O	M	E	5	1.0	
A	N	M	H	E	E	T	I	I	E	T	R	L	N	O	7	1.0	
I	E	E	N	M	W	R	O	P	A	C	V	E	C	O	7	1.0	
C	E	M	N	E	N	R	F	F	I	T	N	E	T	S	4	2.0	
T	D	S	I	M	E	D	D	M	S	E	I	N	S	O	5	1.0	
G	A	N	T	T	A	N	P	T	S	I	I	T	L	A	5	1.0	
V	S	P	E	M	F	F	D	H	I	H	I	T	R	E	4	2.0	
I	T	E	O	P	G	A	S	I	A	T	L	I	H	U	8	2.0	
R	L	O	N	O	M	E	O	Z	T	S	T	R	V	T	4	2.0	
C	D	E	O	T	A	L	P	A	A	A	H	B	G	H	6	0.0	
H	E	T	T	A	E	E	L	E	N	L	N	E	G	P	6	0.0	
																<u>6</u>	<u>0.0</u>
																111	27.0

FIGURE 181

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	V	D
I	I	E	R	V	T	M	W	E	H	P	T	E	S	O	T	N	M	I		7	.6
T	R	D	A	E	E	P	N	I	A	L	H	A	E	N	H	T	N	M		7	.6
A	C	A	M	N	S	O	E	F	O	M	I	I	O	U	N	T	C	N		9	1.4
N	H	S	E	A	W	T	A	T	I	H	Z	S	E	V	D	I	T	O		7	.6
M	N	T	M	E	D	A	F	R	E	R	A	S	T	I	O	R	S	E		7	.6
I	P	L	S	W	S	R	G	R	U	I	E	I	C	E	C	B	L	O		7	.6
E	E	D	N	H	A	R	M	D	R	A	R	A	T	D	H	E	R	O		7	.6
T	S	E	P	N	A	T	A	N	I	O	R	T	E	I	T	P	H	S		7	.6
N	M	I	E	N	E	O	E	F	O	D	T	A	I	R	C	A	V	O		10	2.4
A	S	M	O	I	D	T	N	A	F	M	C	N	H	V	N	E	G	A		6	1.6
I	L	R	E	T	E	E	N	E	D	M	A	S	T	N	Z	E	G	E		8	.4
C	E	O	T	E	M	X	R	L	P	I	E	S	S	I	O	R	M	U		8	.4
T	C	S	T	O	E	E	B	E	D	P	R	N	A	I	L	T	S	T		6	1.6
G	N	W	E	N	M	D	E	A	S	F	L	T	L	I	E	I	S	H		6	1.6
V	E	D	P	O	T	E	A	B	O	M	T	Y	O	L	E	S	E	P		9	1.4
																				111	15.0

FIGURE 182

The columns of the matrix of Fig. 182 are correct; only their order remains to be determined. Unless col. 1 is the last column of the matrix, it must be followed by one of the other columns, which may be determined by considering the sum of the log weights of the digraphs formed by the 18 pairings shown below:⁶⁸

12	13	14	15	16	17	18	19	110
II --	IE 59	IR 73	IV 72	IT 73	IM 53	IW --	IE 59	IH --
TR 64	TD 45	TA 74	TE 91	TE 91	TP 25	TN 48	TI 82	TA 74
AC 61	AA 33	AM 61	AN 89	AS 80	AO 25	AE 13	AF 38	AO 25
NH 38	NS 71	NE 87	NA 72	NW 33	NT 93	NA 72	NT 93	NI 51
MN --	MT 25	MM 59	ME 72	MD 13	MA 78	MF 13	MR 25	ME 72
IP 48	IL 70	IS 78	IW --	IS 78	IR 73	IG 67	IR 73	IU --
EE 81	ED 88	EN 99	EH 48	EA 78	ER 94	EM 61	ED 88	ER 94
TS 67	TE 91	TP 25	TN 48	TA 74	TT 67	TA 74	TN 48	TI 82
NM 42	NI 75	NE 87	NN 51	NE 87	NO 66	NE 87	NF 53	NO 66
AS 80	AM 61	AO 25	AI 64	AD 73	AT 83	AN 89	AA 33	AF 38
IL 70	IR 73	IE 59	IT 73	IE 59	IE 59	IN 92	IE 59	ID 45
CE 76	CO 80	CT 61	CE 76	CM 13	CX --	CR 38	CL 42	CP --
TC 45	TS 67	TT 67	TO 84	TE 91	TE 91	TB 33	TE 91	TD 45
GN 33	GW 13	GE 61	GN 33	GM 13	GD 13	GE 61	GA 48	GS 33
VE <u>87</u>	VD <u>--</u>	VP <u>--</u>	VO <u>13</u>	VT <u>13</u>	VE <u>87</u>	VA <u>45</u>	VB <u>--</u>	VO <u>13</u>
792	851	916	886	869	907	793	832	638

⁶⁸ The weights used here are the digraphic weights (to the base 224) given in Table 15 of Appendix 2, *Military Cryptanalytics, Part I*.

1 11	1 12	1 13	1 14	1 15	1 16	1 17	1 18	1 19	
IP 48	IT 73	IE 59	IS 78	IO 80	IT 73	IN 92	IM 53	II --	
TL 42	TH 92	TA 74	TE 91	TN 48	TH 92	TT 67	TN 48	TM 45	
AM 61	AI 64	AI 64	AO 25	AU 59	AN 89	AT 83	AC 61	AN 89	
NH 38	NZ --	NS 71	NE 87	NV 33	ND 85	NI 75	NT 93	NO 66	
MR 25	MA 78	MS 38	MT 25	MI 53	MO 55	MR 25	MS 38	ME 72	
II --	IE 59	II --	IC 69	IE 59	IC 69	IB 25	IL 70	IO 80	
EA 78	ER 94	EA 78	ET 79	ED 88	EH 48	EE 81	ER 94	EO 58	
TO 84	TR 64	TT 67	TE 91	TI 82	TT 67	TP 25	TH 92	TS 67	
ND 85	NT 51	NA 72	NI 75	NR 38	NC 67	NA 72	NV 33	NO 66	
AM 61	AC 61	AN 89	AH 25	AV 48	AN 89	AE 13	AG 45	AA 33	
IM 53	IA 51	IS 78	IT 73	IN 92	IZ 25	IE 59	IG 67	IE 59	
CI 48	CE 76	CS 13	CS 13	CI 48	CO 80	CR 38	CM 13	CU 38	
TP 25	TR 64	TN 48	TA 74	TI 82	TL 42	TT 67	TS 67	TT 67	
GF 25	GL 25	GT 38	GL 25	GI 42	GE 61	GI 42	GS 33	GH 67	
VM --	VT 13	VY --	VO 13	VL --	VE 87	VS --	VE 87	VP --	
673	865	789	843	852	1029	764	894	807	

The high score of 1029 for the pairing of cols. 1-16 shows that these columns are correctly juxtaposed. We could now continue the process, finding which column should be to the left of col. 1, and which column is to the right of col. 16, and in the end we would establish the order of all the columns, even if we had but a minimum background in the language.⁶⁹

i. As a final word on the recognition of nonrandom phenomena, it must be stressed that diagnostic examination in the initial phases should rely heavily on powers of *observation*, rather than calculation; in particular, the spotting of bust messages and other errors, which has often been the crux of the first entry into a new cryptosystem, is more readily done by eye than by statistical analysis or machine methods. Nevertheless, machine aids can and do make valuable contributions to diagnosis, especially in performing much of the clerical and statistical work incidental to the study of a new cryptosystem. One of the basic exploratory (or so-called "diagnostic") machine programs is called the STETHOSCOPE program, for obvious reasons. The particular computer on which it is run may change as time goes on, but in essence the program presents a variety of fundamental information about a single message (or a single stretch of key) under study, as follows:

- a. The uniliteral frequency distribution, the monographic I.C., and its sigmage.
- b. The over-all digraphic I.C., as well as the digraphic I.C.'s on cut "A" and cut "B" and their sigmages.
- c. The over-all trigraphic I.C., and the trigraphic I.C.'s on cuts "A", "B", and "C" and their sigmages.
- d. The local roughness (in terms of the observed and expected number of hits, and sigmage), when the message is offset against itself at offsets of 1 to 33.
- e. Width tests, giving average columnar I.C.'s and sigmages of the message if it were written out on widths from 2 to 51.
- f. The observed and expected number of tetragraphic and pentagraphic repetitions, and their I.C.'s and sigmages.
- g. A listing of polygraphic repetitions of length 4 or longer.
- h. If desired, the same categories of statistical information on the delta stream.

The STETHOSCOPE program exists in several versions, including one in which several messages may be treated together; its general purpose remains the same, as in a doctor's first examination of a patient.⁷⁰

⁶⁹ A modification of this general procedure is adapted in machine methods for the solution of transposition ciphers with incompletely filled matrices, whether or not the number of columns of the matrix is known.

⁷⁰ The reader might be interested in examining a work entitled "Cryptanalytic Diagnosis with the Aid of a Computer—a Collection of 147 STETHOSCOPE Listings" which I prepared for use in my *Intensive Study Program in General Cryptanalysis*. This anthology is derived from cryptographic examples embracing a wide variety of manual and machine cryptosystems, many of which are diagnosable from the STETHOSCOPE listing.

78. Third step: interpreting the phenomena.—a. The third step in diagnosis, that of explaining the nonrandom characteristics or manifestations once they are recognized, is the most crucial step in the diagnostic process; as indicated in subpar. 72b, this takes experience and imagination, and, in addition, *intelligence*. In some cases interpretation will be practically synonymous with recognition: a striking roughness in a literal cryptogram, together with the presence of a plethora of polygraphic repetitions whose lengths look not unlike those expected for plain text, identify the message as simple substitution. Even in a more complicated system, interpretation may follow directly on the heels of recognition. In the following example from a pre-World War II course in cryptanalysis, it is given that the plain text is a message famous in English history:

253 269 863 261 471 958 220 370 4 21 20 25

Although very short, the message can be easily and quickly solved by inspection, and the nature of the cryptosystem determined.

b. Specific guidelines for the interpretation of nonrandom phenomena cannot be formulated: the cerebral gifts with which the analyst has been endowed will have to suffice—and the pooling of such gifts, especially in a particularly difficult problem, is to be encouraged and indeed may be absolutely necessary. Nevertheless, there are some generalities which bear restating. Certain distributional profiles can be easily identified for what they are (cf. subpar. 77e on pp. 360–367), and their interpretative exploitation may follow. Even when a rough distributional profile itself cannot be interpreted, nevertheless when there are changes in the distributional profile this signifies a key change, i.e., it denotes the beginning of a new cryptoperiod. Phenomena connected with certain bust or isolog situations may likewise be easily interpretable. The presence of depths shows that the key is not influenced by the plain or cipher text during the course of encipherment, and the presence of polygraphic repetitions in excess of those expected at random automatically excludes certain major classes of systems.⁷¹ The presence of isomorphs which exhibit properties of indirect symmetry of position and which can be chained out to yield a complete sequence, identifies the system as one involving sliding components and Vigenère properties.

c. The absence of certain letters may yield interpretable information. An absent J may be indicative of a small-matrix digraphic system, or it may be another 25-letter system such as a 5×5 fractionating system, or a code in which there is no J in the code groups. If a missing letter is K, Q, W, X, or Z, this may point to a code (especially a commercial code) since permutation tables for codes have been constructed with one of these letters missing. On the other hand, messages containing, say, only the letters A through O merely mean that 15 letters have been employed, just that: the system might be a code system, or some type of multiliteral cipher. If the cipher text consisted only of consonants, without the 6 vowels, the system could be either a code or a multiliteral cipher—but even a digraphic system could not be excluded (cf. the system illustrated on pp. 387–391 of *Military Cryptanalytics, Part I*.)

d. Certain types of aberrations, isologs, and other special situations in transposition ciphers lend themselves to facile interpretation, as will be shown by the examples below.

(1) For the first case, let us study the following message:

A R A R U L O S E F E S O O T U L O C O M E N A T F M T V Z  
N V D W L H A R W C L M E I E O P I N O E S N D G O T T E I  
F W R O F R T N O W T P T I T C G A M H E E J I C N E T O S  
L L M T V Z N V D E L R T E F

The presence of a 7-letter ciphertext repetition, and the *location* of these segments in the message, point to an error involving a *repeated column* of the matrix in a keyed columnar transposition cipher. The column lengths involved are 7 and 6: there are 7 letters in the repeated column; there are 6 letters following the second occurrence of the repetition; and there are 26 letters ( $26 = 2 \times 7 + 2 \times 6$ ) preceding the first occurrence of the repetition. Furthermore, since the interval between the two repetitions is 59, the only sum of integral multiples of 7 and 6 possible is  $5 \times 7 + 4 \times 6$ ; thus there must be a total of 9 long columns and 7 short columns in the matrix of 16 columns.

⁷¹ Careful judgment must be exercised in arriving at conclusions: as an illustration, the presence of long polygraphic repetitions in the cipher text of messages would not exclude, for example, one-time key based upon running plain text from a book.

(2) For the next example, the following two messages are to be studied:

Message "A"

H I N D R W O M S M A C P E G E A B I R E L T A N I L W F B  
S E A P O C T R U H N O T L F I P N E A T A L F D O T V C S  
N I E E T L E B L L L I T E O

Message "B"

H I N D R W O M S M A C P E G E A B I R E L T A N I L W F B  
S E A P O C T R U H N O T L F I P N E A T A L F D O ( G F E E  
E N T M Y N ) T V C S N I E E T L E B L L L I T E O

The two messages are identical except for the insertion of 10 letters in Message "B" starting at the 57th position. Had these 10 letters been in two complete groups, it could have merely signified that these groups were inadvertently dropped in Message "A" by the transmitting operator; but in this context, it shows an *omitted column* of the transposition diagram, and that one column length must be 10. The 19 letters following the interpolated segment in Message "B" shows that there must be one long column of 10 and one short column of 9 letters there; and the 56 letters ( $56=2\times 10+4\times 9$ ) prior to the interpolated segment must consist of two long columns and four short columns, making a matrix of 9 columns, four of them long and five of them short.

(3) For the third example we have the following pair of messages isolated for study:

Message "A"

T T O T E O T P L G F S D R R R U S N H A J W L A E U B F B  
T O M T H N M T E R A G A R O O I Y E H E H M E Y S N R E R  
U H N O S I R E A R

Message "B"

O M T H N M T P L G F S D R R R U S N H A J W L A E U B F B  
T T T O T E O T E R A G A R O O I Y E H E H M E Y S N R E R  
U H N O S I R E A R

This is clearly a case of a pair of *transposed columns* in a keyed columnar transposition cipher, and the number of letters between the two underlined segments, 24, points either to four columns of 6 letters each, or three columns of 8 letters each; but the number of letters after the second underlined column, 32, points to the latter case; thus in the matrix of 9 columns there are seven long columns of 8 letters, and two short columns of 7 letters.

(4) The next case deals with the repetitive phenomena present in the following two messages:

Message "A"

N O S M O B O O O I T E A R S P R D E O E P O O L G N T I F  
E U U N S I L A T T A T O D O L Y I B R A R L I M C T I M C  
← T T R S E E M E A A Y E N C O F B P I O N Y I I C N D S R Y  
C C F A D T U G S E

Message "B"

N O S E A C L I T C O I T F D N L E A I N D E O I L L W E C  
S D G N T I L A L N E K N S I T E T S T E F E T O D O M L S  
B S G O A R L C T T E R T O R M C T F I B T P R E J M E A E  
A A I O A S U O F B P M N U E E O R I C N V Y E I D A I C F  
← A E E O A R P R I

These manifestations are the result of *similar beginnings* in a columnar transposition system. There are 12 segments initiated by the underlined polygraphs, indicating 12 columns of the matrix; in Message "A" the column lengths are 9 and 8, while in Message "B" the column lengths are 11 and 10. Since the column breaks are known, anagramming of the texts is a trivial matter.

(5) In this next example the manifestations admittedly would be hard to detect in a volume of traffic, but on detailed examination it is found that there is a large number of polygraphic repetitions in common between the two messages, spaced at a more-or-less uniform distance apart, but not preserving the same order of these repetitions in the two messages:

Message "A"

C Y M R S T U H I T O O A N B E O D H E D Y T S D E T E O V  
 ← S B E R H E A V U E E O I E D D D C R E I A L E N S R L O G  
 M S R F H R E N A S U R A P N N A G I E S F E H N R I C N C

Message "B"

M T I U S R L R O M I H E A E N P J S U R Y S N S R E I E E  
 O N A G R B T T O I E E M D N R F H H E E O C N C S C V I F  
 ← E H F F G S T S D E R O T O V S N E U S O O A I I P O D H N  
 N O R S T

These are the manifestations of a pair of messages in columnar transposition with *similar endings*, relatively offset in the bottom rows of the two matrices. Although the segments delineated by the repetitions could be anagrammed as in the case of similar beginnings, we are able by a special method of solution to derive the transposition key directly, without recourse to anagramming (see pp. 425-427 of *Military Cryptanalytics, Part II*, for the solution of this example).

(6) In another example of the interpretation of phenomena in transposition ciphers, let us study the following pair of messages:

Message "A"

C N S D O M E D U T D M F L T F A L S E A D O S I N A L E O  
 N U T V C E T I G O A F I L S H W O A N E D A A T P A S N T  
 L A U O I M F L E E T L E R L C I I Y V N T N O I R R T M C  
 N F S R G I P E L P R O I U C E E S N L T E B S E A S I C F

Message "B"

C N S D O L E I T M F L T A P I T G D O S W O C H N U T E T  
 F I O A L E T A I O A N P B A E N A S N A I E D M F L E N U  
 O M H C I K N F N O I R R T I P T T G I P L R V O I U B T N  
 I T T E B S R O E G

Although the repetitive phenomena present are reminiscent of similar beginnings in columnar transposition ciphers, the lengths (2, 3, 4, 5, and 6) of the polygraphic repetitions in common are puzzling at first glance, since we expect them to be of lengths  $n$  and  $(n+1)$ , barring accidental contacts which might cause an occasional fluke longer repetition. Furthermore, the column lengths of Message "A" appear to be from 7 through 10 letters, inclusive, and those of Message "B" appear to be from 5 through 10 letters. A little thought on the subject, however, will lead us to the hypothesis that what is involved is a matrix with blank cells incorporated, and that these blank cells are placed near the *beginnings* of the columns (thus giving rise to the different-length repetitions). Solution of this case, then, would proceed by anagramming the *ends* of the 13 columns delineated by the repetitions.



(7) For the last example, let us consider a case which, although rarely encountered, serves to illustrate certain interpretative considerations. The following message is being studied:

TOROE REVST ENFOS RAIUO OSADY ODIYP ESDTE IXPOS MOTOH BRGGA  
 FGOVC RRSSI REFOI GPSIN NSPLP OESOA LANTL EVERE NSHEI LATST  
 EAWIS ENDIN IVASL BEDOP TOLLA SASFO EATOE MATFI NEGIU RHTWI  
 OFNOI ETLEV RRSTN ESSST ENENV IRWOA NIRZU RNSEE OONI OUPDE  
 INDTO LMEMI SELLF ERTSW OCENI VONYO IOIVT RDIIT PSEWT NTEPW  
 VEFCA KESIN REEDO STRXF ITSFU RVIOS TOONG HECTO WPROO PTHEM  
 LLARD SSEER

From its uniliteral frequency distribution, it has been determined that the message is an English-language transposition cipher, but initial efforts to anagram the text on the basis of single columnar transposition have proved fruitless. In further study of the cryptogram, we make a digraphic distribution on the cut

and find the digraphic  $\phi$  to be 178, so the digraphic  $\delta$  I.C. is  $\frac{676(178)}{155 \cdot 154} = 5.04$ ; the digraphic  $\phi$  off the cut,

however is 110, so the digraphic  $\delta$  I.C. for this latter case is  $\frac{676(110)}{154 \cdot 153} = 3.12$ . The situation is now clear:

what we have is a case of *digraphic transposition*, in which each cell of the matrix contains a digraph instead of a single letter. The digraphic kappa plain constant for English is .0069, so the expected digraphic I.C. is  $676(.0069) = 4.66$ ; on the other hand, the I.C. of digraphs composed of *disconnected* letters from an English-language population, thus destroying the digraphic cohesion of the language, is  $676(.0667)^2 = 3.01$ . On cut, then, this message displays the characteristics of English plaintext digraphs. Once the nature of the system is deduced, anagramming is much simpler than in the case of monographic transposition since we are dealing with larger units.

(8) The foregoing discussion has been confined to manifestations in cases of monophase (i.e., single) transposition. The phenomena in double transposition are much obscured, and each case presents a very special case. In spite of casual references to the alleged existence of a test to be able to distinguish single columnar transposition from double, the truth of the matter is that no practical test exists.⁷² The best way of distinguishing single columnar transposition from double is this: if it's single, you solve it with ease.

*e.* Proforma systems consisting of stereotyped messages in which the order and nature of the successive elements are determined by prearrangement (as for example, weather messages) are identified as such by their very appearance. The specific type of proforma system may have to be determined through patent characteristics associated with certain types of traffic or through collateral information. Sometimes the problem of interpretation is simple enough to be solved without any extraneous information, as in

⁷² This test is based on sliding the first several letters of a cipher message (i.e., those presumed to come from col. 1, the first numbered column of the matrix) and the last several letters of the message (i.e., those presumed to come from the last column of the matrix) throughout the remainder of the cipher text, and evaluating the digraphs thus formed, using log weights in a procedure similar to that illustrated in subpar. 77h(6); if the cryptogram is a single transposition, a certain mean score of four sets of log weights should be attained—but by this time we would already have *solved* the cryptogram.

the case of the following 14 messages given in their entirety, together with the intercept information enclosed in parentheses:

1. (MIH DE FSE 1030 16 DEC) 04941 45401 02124 44464 44149 42401
2. (MIH DE FSE 1044 16 DEC) 04942 48421 53625 46424 94244 46411
3. (MIH DE FSE 1055 16 DEC) 04944 49421 53625 46424 94244 47411
4. (MIH DE FSE 1119 16 DEC) 04040 40401 02124 44464 44149 41401
5. (MIH DE FSE 1135 16 DEC) 04042 40401 02124 44464 44149 45411
6. (MIH DE FSE 1154 16 DEC) 04043 46471 14724 44464 44047 42401
7. (MIH DE FSE 1205 16 DEC) 04044 49421 53625 46424 94244 47411
8. (MIH DE FSE 1229 16 DEC) 04141 42401 02124 44464 44149 42401
9. (MIH DE FSE 1252 16 DEC) 04143 45471 14724 44464 44047 44401
10. (MIH DE FSE 1307 16 DEC) 04249 40471 14724 44464 44047 43401
11. (MIH DE FSE 1314 16 DEC) 04249 47401 02124 44464 44149 41401
12. (MIH DE FSE 1323 16 DEC) 04240 46421 53625 46424 94949 43421
13. (MIH DE FSE 1342 16 DEC) 04242 45492 61215 46424 94241 42401
14. (MIH DE FSE 1355 16 DEC) 04243 47471 14724 44464 44048 49421

This example, based upon a situation encountered during World War II in the Pacific Theater of Operations, is capable of being solved in its entirety, in spite of the brevity of the messages and the small amount of traffic.

f. We shall now take up the interpretation of phenomena in connection with indicators, and we shall use as an example one which may be considered typical of the approaches in such problems.

(1) Let us study the following collection of A1 and Z0 groups (known to be the indicator and indicator-check groups) of 40 messages in an unknown cryptosystem:

	<u>A1</u>	<u>Z0</u>		<u>A1</u>	<u>Z0</u>
1.	T X N E A	X G F K H	21.	D P G I M	T H P C K
2.	R F C W P	G N G L V	22.	R C Y F W	N O Z V D
3.	A K P L M	I Z V R K	23.	G S T B C	P Y I Z E
4.	S G W F T	I N N E Z	24.	K Z H U X	D O Q B A
5.	Z E R O M	H W X G S	25.	P A G S V	E L P K G
6.	Q I F W E	G O O H M	26.	M I Y E Q	H C Z H T
7.	C O K R Z	L A R U E	27.	E A T M R	A I I X G
8.	L M D K G	P A A I Z	28.	M W Q Z G	M A M Z W
9.	A Q X B I	T L D M D	29.	G E B O D	X U L C P
10.	T G Z V E	C E B P M	30.	N B F H Z	S M O K B
11.	W M I U R	D F H W Z	31.	Y S K L Q	I Y R Y Z
12.	B W U G E	C P W N Z	32.	C O L T S	B H S U E
13.	Y A V L E	V S E D Z	33.	H B X S N	O B D S T
14.	R Y K Z E	G S R L D	34.	S H L D O	U X S O X
15.	C R E B X	K S C D V	35.	U N A Z O	W S K F W
16.	L X U Y P	C B W R S	36.	F D M X U	O D T R U
17.	K Y M C A	D G T B D	37.	D T B W C	G U L Q K
18.	V W E Y M	Q Z C F G	38.	X U R C A	D G X O D
19.	O M T R D	A X I H W	39.	V N O D U	Y C U F P
20.	E L D F T	I N A S V	40.	O V S H L	S I Y E F

(2) The following information has been gleaned from an initial study of the traffic:

- a. The messages have flat counts, and polygraphic repetitions within messages are no more than those expected for random; but a high hit rate between certain pairs of messages proves that the cryptosystem is one in which depths are possible.
- b. The texts of message nos. 16 and 18 are in flush depth.
- c. Message no. 38 is offset 30 positions to the right of message no. 15; and message no. 28 is offset 30 positions to the right of message no. 14.
- d. Message no. 37 is offset 60 positions to the right of message no. 31; and message no. 30 is offset 60 positions to the right of message no. 33.
- e. Message no. 6 is offset 90 positions to the right of message no. 3; message no. 16 is offset

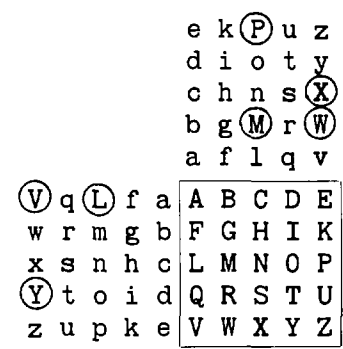
90 positions to the right of message no. 39; and message no. 5 is offset 90 positions to the right of message no. 25.

f. Message nos. 6, 13, 28, 30, 32, 34, and 35 have been determined from traffic analysis to be high-precedence messages.

(3) It has been observed that there are no J's present in any of the indicator groups, although there are J's in the cipher texts of the messages. The A1 group always consists of a set of five different letters; the over-all I.C.'s of the A1 groups (0.97) and the Z0 groups (1.01) are flat, as are the ten individual columnar counts except for the Z0e which has an I.C. of 1.47. The only doublets present in the Z0 groups are in the bc position. Several instances of apparent digraphic relationships are seen between the A1 and Z0 groups (e.g., note the LM's in the A1 groups of message nos. 3 and 8 associated with IZ's in the Z0 groups), and it is observed that these relationships are reversible (e.g., note the CR in message no. 15 and the RC in message no. 22 associated with DV and VD). It is further noted that these digraphic relationships are confined to the first and last digraphs of the two indicator groups; it is therefore conjectured that the last digraph of Z0 represents an encipherment of the first digraph of A1, and that the first digraph of Z0 represents an encipherment of the last digraph of A1, leaving the c position of Z0 perhaps a monographic encipherment of the c position of A1. The absence of the letter J, the lack of doublets in the Z0ab and de positions, together with the reversibility feature, suggests Playfair; but encipherments such as the AK_p=RK_c in message no. 3 seem to require that the Z0 groups be read *in reverse* before establishing equivalencies with the A1 groups. The Playfair hypothesis is quickly proved with the reconstruction of the square and the derivation of a key word on which it is based, and it is found that the c position of A1 is enciphered with the square by taking the letter to its immediate right in the row in which it is located.

(4) The A1c position of the high-precedence messages consists of one of the letters A, F, L, Q, or V; these letters are 5 apart on the normal sequence (if J is omitted), and we might even conjecture that these letters come from the first column of a 5x5 square into which has been inscribed the normal sequence, less J. Is it possible that the A1c represents the precedence, and that the latter is based on the identity of the particular one of five columns (of such a square) in which the letter is found? Message nos. 16 and 18 which are in flush depth have the A1 groups LXUYP and VWEYM; and since the indicators in a flush depth situation may be presumed to represent identical information, the letters in the c position, U and E, *could* come from the fifth column EKPuz of our putative 5x5 square. These manifestations in the c position may either be encipherments, or perhaps even more likely, some type of *variants*.

(5) The existence of depths composed of pairs of messages offset at intervals of 30, 60, and 90 suggests that the keying sequence is in multiples of 30 (i.e., if a key book is involved, the pages contain lines of 30 letters each), and that therefore the indicators designate the starting line used. If this hypothesis is correct, then the ab and de digraphs of A1 could indicate the page and line, probably in that order. Then from message nos. 16 and 18 in flush depth with A1's of LXUYP and VWEYM, it should follow that LX=VW, and YP=YM. The suggestion of variants is still strong, so perhaps A1ab and de are digraphs representing *single letters* indicating page and line in a key book: thus the book might contain 25 pages of 25 lines each. If the interior of a 5x5 square is inscribed with the normal sequence, perhaps the row and column coordinates of the bipartite variant square also consist of the normal sequence following some prearranged route. The urge is very strong to hypothesize the following coordinate configuration, in which the elements LX=VW and YP=YM are shown in ringed capital letters, the lower-case letters being the completion of the assumed order of coordinate letters:



In order to test what may seem to be a bold assumption, we consider a pair of messages, nos. 15 and 38, which are in offset depth 30 intervals apart on the keying sequence, with A1 groups CREBX and XURCA: sure enough, CR=XU on the diagram above, and we find that BX and CA represent sequent positions (=30 letters in the keying sequence). A second test is in order, so we pick messages nos. 31 and 37 which are in offset depth 60 intervals apart, with A1 groups YSKLQ and DTBWC: again on the diagram above YS=DT, and LQ and WC are two positions apart. We shall make one final test to be triply sure, so we examine messages nos. 3 and 6 which are in offset depth 90 intervals apart, with A1 groups AKPLM and QIFWE: AK=QI in the diagram, and LM is separated by three positions from WE. All the messages may now be correctly superimposed with respect to the keying sequence of  $25 \times 25 \times 30 = 18,750$  letters, keeping in mind the two possibilities that when the bottom of a key page is reached, the key is continued (a) from the top of the same page, or (b) from the top of the next page (perhaps with a proviso in the cryptographic instructions that a message should not be enciphered with keys starting past, let us say, the middle of page Z, the last page).

(6) This example, although artificial, nevertheless contains complexities similar in nature to those of certain complicated indicator systems encountered in actual operations. Without sufficient material for study, and without the element of luck which is all too often essential to success, we might not have been able to complete the solution. Sometimes we are able to solve a problem in spite of errors in thought or procedure, and at other times we are able to reach a solution *because* of such errors.⁷³ As a demonstration, we assumed in subpar. (4), above, that the indicators LXUYP and VWEYM must represent identical information, because the messages to which they appertained were in flush depth, and, encouraged by our findings, we went ahead and solved our problem. This is faulty reasoning, because the *c* position of the indicator (which happens to be a *precedence* symbol) bears no relation to the page and line keys used in the encipherment, and thus the two messages in depth would not necessarily have the same precedence. Had the letters in the *c* position of the two groups been, say U and O, we might have argued ourselves out of the hypothesis being postulated and thus either delayed the solution, or missed it completely. Furthermore, although in the preceding subparagraph it was conjectured that A1*ab* and *de* were digraphs representing *single* letters for the page and line indicators, these digraphs could just as well have represented as many as  $25^2$  pages and some number greater than 25 (say, 50, 75, or 100, with a variant usage) for the line designator.

(7) As an epilogue to the discussion of interpretation of indicator phenomena, we should keep in mind certain situations which have arisen in operational practice. We must not overlook the possibility of *cleartext indicators* in various contexts with which we may be familiar, and extrapolations from familiar contexts. The situation in subpar. 76f(3) may be cited as an example, that of Hagelin C-38 indicators in the clear which were interpretable at once from the five columnar distributions of the *a-e* positions of the indicator groups. If these indicators had been enciphered by five different direct or reversed standard cipher alphabets, recognition and interpretation would hardly have been delayed. And even if the encipherment had been accomplished by five mixed alphabets, the severe limitation in the indicator positions representing the last two wheels would still enable easy recognition and interpretation. In connection with cleartext indicators, we should also be on the lookout for an indicator in the clear every *n* groups of the cipher text (as in a case in which every 40th group was such an indicator for purposes of check on the encipherment). *Tailing indicators* are often easily interpretable under apparent or assumed rules of motion when the rules are not too complex, such as in certain pin-wheel devices or in certain varieties of notch control in wired-wheel systems. Null letters in indicators may be identified as such by finding indicators of messages known to be in flush depth, with a discrepancy in one of the positions; e.g., indicators of the form LDPCX and LDPCY in a machine cipher system could

⁷³ The most striking example that comes to mind of incorrect reasoning making solution possible occurred many years ago during World War II, before the advent of computers, in a very complex teleprinter cipher system about which nothing was known. A long sequence of key was recovered from reading a depth, and, because of a totally unwarranted conjecture of the apparent limitation of two of the indicator positions to 23 and 25 letters, the key levels were written out on a width of the product of these numbers, 575. In this write-out, some long polygraphic repetitions were observed on successive rows, but displaced one position to the left, indicating a significant period of 574, not 575. Since  $574 = 14 \times 41$ , the key levels were written on the prime width of 41; more polygraphic repetitions were found on this width, proving that the cycle of 41 played a part in the machine. Had it not been for the totally erroneous interpretation of the indicator phenomena, it is possible that the machine would not have been solved.

suggest the possibility of four wheels and a null position.⁷⁴ Finally, literal systems have been encountered which have an underlying *numerical base*, such as in the simple scheme of A=1, B=2 . . . J=0, or as in the case of the three pairs of indicators and indicator-check groups shown below:

	<u>A1</u>	<u>A2</u>
1.	M A N U S	C U D K I
2.	B G K H R	V Q A R H
3.	Z U Q M G	P A G W Q

These could have come from the variant values of the following diagram:

	<u>1</u>	<u>2</u>	<u>3</u>	<u>4</u>	<u>5</u>	<u>6</u>	<u>7</u>	<u>8</u>	<u>9</u>	<u>0</u>
A	B	C	D	E	F	G	H	I	J	
K	L	M	N	O	P	Q	R	S	T	
U	V	W	X	Y	Z					

Furthermore, given the order 1-0 for the digits in the top line, it is seen that the A1 and A2 are both sum-checking groups, confirming this order.

**79. The treatment: hypothesis formulation and testing.**—*a.* In modern practice, cryptodiagnosis may be thought of as embracing hypothesis formulation and hypothesis testing. The establishment of a hypothesis is followed by a particular diagnostic test or set of tests, and their outcome will determine the validity of the hypothesis and the subsequent road to be followed.

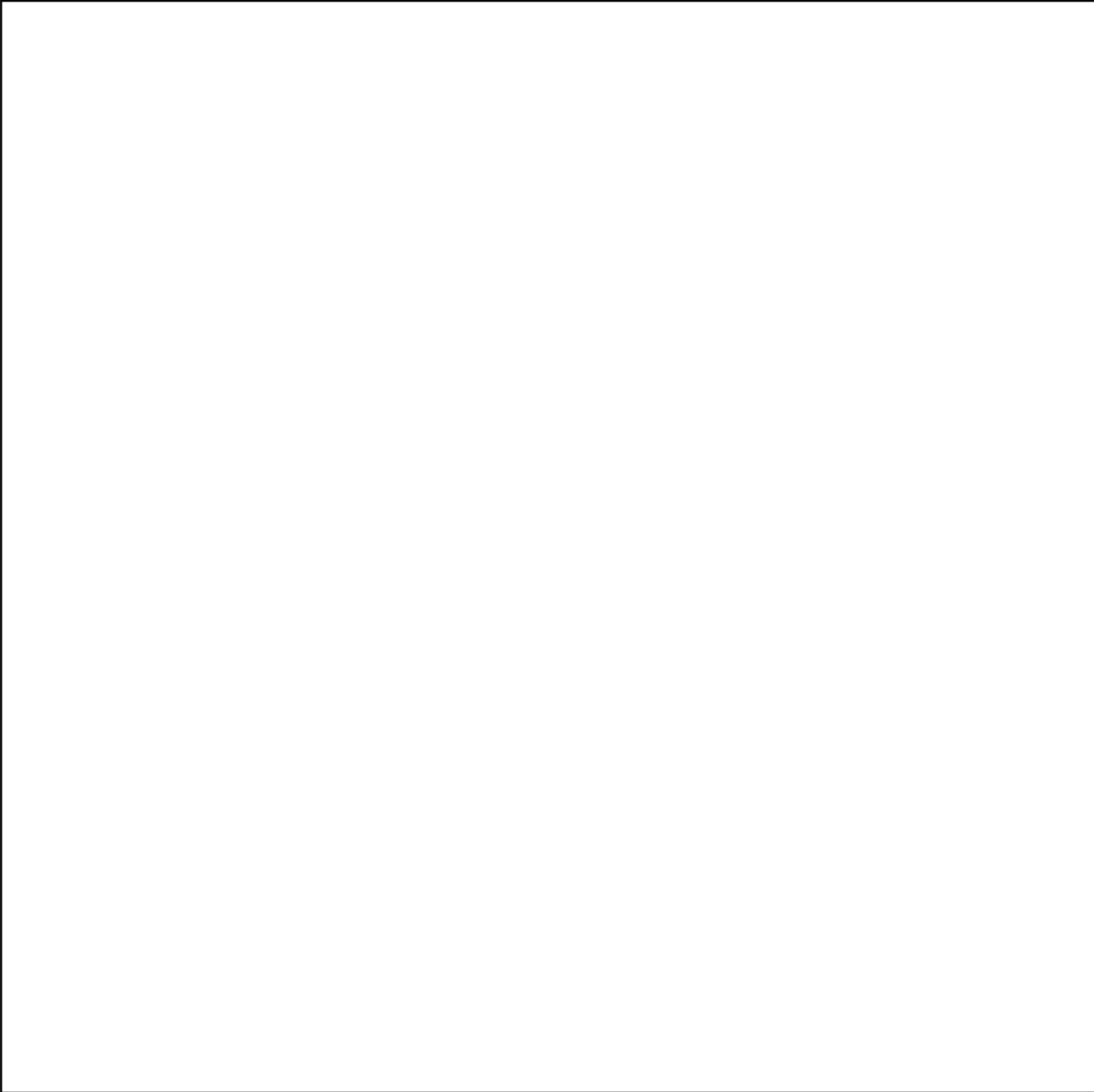
*b.* As an elementary example, in studying the 385-letter cryptogram given in subpar 77g(6) with its accompanying on-the-cut digraphic distribution as shown below,

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	-	-	1	2	-	-	1	-	-	-	-	-	2	2	-	-	2	2	-	2	-	2	-	-	-	-
B	-	-	2	2	-	-	1	-	-	-	-	-	2	1	2	2	2	-	-	1	-	-	-	-	-	-
C	-	2	-	-	1	-	-	-	-	-	2	-	-	-	-	-	-	-	-	-	-	-	-	-	1	-
D	1	1	-	-	1	-	-	-	-	1	-	-	-	-	-	-	-	-	-	-	-	1	1	1	1	1
E	-	-	-	-	-	-	-	-	-	-	1	-	-	-	-	-	-	-	-	-	1	-	-	-	-	-
F	-	-	-	2	-	-	-	-	-	-	-	2	2	-	-	2	2	-	-	2	-	2	-	-	-	-
G	-	1	-	-	-	-	-	-	-	1	1	-	-	-	-	-	-	-	-	-	-	1	1	-	-	-
H	-	-	-	-	-	-	-	-	-	-	1	1	-	1	-	1	-	-	-	-	-	-	-	-	-	-
I	-	-	-	-	-	1	-	-	-	-	1	1	-	1	1	1	-	-	-	-	-	-	-	-	-	-
J	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
K	-	-	2	2	-	-	1	-	-	-	-	1	2	1	2	1	2	-	-	-	-	-	-	-	-	-
L	-	-	-	1	-	-	1	-	-	-	-	-	-	-	-	-	-	-	-	-	1	-	-	-	-	-
M	1	-	-	-	1	-	1	-	-	-	-	-	-	-	-	-	-	-	1	-	1	1	-	-	-	-
N	2	2	-	-	1	-	1	-	2	-	-	-	-	-	-	-	-	-	-	-	1	-	1	1	1	1
O	-	1	-	-	-	-	1	-	1	-	-	-	-	-	-	-	-	-	-	-	1	1	-	1	-	-
P	-	2	-	-	-	-	-	-	-	1	-	-	-	-	-	-	-	-	1	-	-	-	1	1	-	-
Q	1	1	-	-	1	-	1	-	1	-	-	-	-	-	-	-	-	-	-	-	2	-	1	2	-	-
R	1	2	-	-	1	-	1	-	2	-	-	-	-	-	-	-	-	-	-	-	1	-	2	2	1	-
S	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	1	-	-	-	-	-
T	-	-	1	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
U	1	-	-	-	1	-	-	-	-	1	-	-	-	-	-	-	-	-	-	-	1	-	1	1	-	-
V	-	-	-	2	-	-	-	-	-	-	1	2	1	-	2	2	-	-	1	-	-	-	-	-	-	-
W	-	-	-	1	-	-	1	-	-	-	-	1	-	-	-	-	-	-	-	-	1	-	-	-	-	-
X	-	-	-	1	-	-	-	-	-	-	2	-	-	-	1	-	-	-	1	-	-	1	-	-	-	-
Y	-	-	2	1	-	-	1	-	-	-	-	2	1	2	2	2	-	-	1	-	-	-	-	-	-	-
Z	-	-	1	1	-	-	-	-	-	-	1	-	-	-	2	-	-	1	-	-	-	-	-	-	-	-

⁷⁴ The possibility of *variants* should of course not be overlooked; one must also keep in mind that an apparent null or dummy position may not always be what it seems—it may be information extraneous to the keying, as was the case in the example in subpar. (4), above. For that matter, each indicator letter may control more than one keying element, so that each of the first four letters LDPC in the example above might be used to set a pair of wheels in a 8-wheel machine.

we were struck by (a) the absence of the letter J, (b) the lack of doublets, (c) the apparent matching propensities among the rows and columns of the distribution, and (d) the symmetry about the main diagonal. These characteristics lead us to the hypothesis of a bipartite system with a commutative matrix, and under this hypothesis we amalgamate the variant rows and columns of a  $5 \times 5$  square, reducing the text to uniliteral, monoalphabetic terms with a satisfactory over-all  $\delta$  I.C., following which the plain text is recovered, proving the hypothesis.

c. In another elementary example, if we have identified a cipher as being digraphic substitution and we wish to test it for the possibility of its being enciphered with an *inverse four-square system*,⁷⁵ all we have to do is to convert the cipher text with an arbitrary four-square matrix containing the normal sequence in the *ciphertext* sections and, if the hypothesis is correct, the distributions of the initial letters and of the final letters of the converted digraphs should exhibit the characteristics of monoalphabeticity.⁷⁶



(b) (1)  
(b) (3)-18 USC 798  
(b) (3)-50 USC 3024(i)  
(b) (3)-P.L. 86-36

**80. Post mortem.**—*a.* After a system has been solved (or for that matter, just as important, even if a system has *not* been solved), the diagnostic steps taken and a résumé of the work done on the problem should be properly documented. Technical reporting is all too often inadequate, in spite of the fact that it should be a major facet of cryptanalytic operations if the reports are to be of benefit to technicians, particularly the newer personnel.⁷⁷ In those cases wherein a system has not been solved, it is important to record the work which has been done, in order to evaluate the steps already taken, and to avoid unnecessary duplication if the problem is restudied later. In Fig. 183 is illustrated a suggested reporting form for unsolved systems which contains on a single sheet of paper a convenient résumé of the system.

*b.* As mentioned in subpar. 74*f*, it is important that the cryptanalyst have readily available the salient cryptolinguistic data in the languages with which he is working. Among these data, the indispensable items are the following:⁷⁸

1. The frequencies of single letters, the monographic kappa plain constant, and the monographic I.C.
2. The frequencies of digraphs, the digraphic kappa plain constant, and the digraphic I.C.
3. The frequencies of initial letters of words.
4. The frequencies of initial digraphs of words.
5. A listing of the most frequent trigraphs, with their frequencies.
6. A listing of the most frequent initial trigraphs of words, with their frequencies.
7. A listing of the most frequent tetragraphs, with their frequencies.
8. The average length of words.

In addition to the foregoing, we should also have lists of frequent words and common phrases expected to be in the traffic, as well as a collection of representative samples of different types of messages.

---

⁷⁷ For suggestions on technical report writing, and for a model of a technical report, see pp. 386–391 of *Military Cryptanalytics, Part I*.

⁷⁸ See in this connection the compilation I prepared in 1956 entitled *Letter Frequency Data, Foreign Languages*, which contains the indispensable cryptolinguistic data, through tetragraphs in the following 20 languages: Albanian, Arabic, Bulgarian, Czech, Dutch, French, German, Greek, Hungarian, Indonesian, Italian, Persian, Polish, Portuguese, Romanian, Russian, Serbo-Croat, Slovak, Spanish, and Turkish.

Reporting Form for Unsolved Systems

* * * * *

- 1. Short Title: _____ 2. Service Description: _____
- 3. Time element covered: _____ to _____
- 4. Message volume: _____ per week; _____ per month; _____ total on hand
- 5. Msgs sent in _____ -letter groups; _____ -digit groups. Missing chars.: _____
- 6. Discriminant: _____; Indicator(s): _____
- 7. Other nontextual groups: _____
- 8. Possible indicator explanation: _____
- 9. Evidence of tailing, trailing, or flush starts: _____
- 10. Remainder test on _____ msgs: _____
- 11. Frequency counts:

Msg No.	No. of chars.	Mono I.C.	Dig I.C.	Dig Cut A	Dig Cut B
_____	_____	_____	_____	_____	_____
_____	_____	_____	_____	_____	_____
_____	_____	_____	_____	_____	_____
_____	_____	_____	_____	_____	_____
_____	_____	_____	_____	_____	_____

- 12. Width tests:
    - Msg No. _____; width _____; av. depth _____; av. I.C. _____
    - Msg No. _____; width _____; av. depth _____; av. I.C. _____
    - Msg No. _____; width _____; av. depth _____; av. I.C. _____
    - Msg No. _____; width _____; av. depth _____; av. I.C. _____
  - 13. Evidence of local roughness: _____
  - 14. Positional roughness, _____ group: 1 _____ 2 _____ 3 _____ 4 _____ 5 _____
  - 15. Phenomena in delta stream: _____
  - 16. Polygraphic repeats within msgs _____; between msgs _____; at beginnings _____; at endings _____; in body of text _____
  - 17. Evidence of isomorphism: _____
  - 18. No. of flush depths _____; offset depths _____; maximum depth _____ deep.
  - 19. Bust msgs: _____
  - 20. Analysts most familiar with system: _____
  - 21. Additional remarks (coded to item nos. above); related facts, collateral information (e.g., predecessor systems, probable type of system, traffic analysis observations): _____
- Date: _____ 19____ Reported by: _____ Org. _____

FIGURE 183

c. There is nothing like live traffic in an unknown cryptosystem to test one's assimilation and understanding of diagnostic principles and techniques. If the traffic is in a low- or medium-grade system, diagnosis and solution should be a matter of course, given a sufficient amount of material for study. But even if the traffic is in a high-grade system, something can often be discovered in fairly short order, even if the magnitude of the discovery is not particularly startling—after all, a jigsaw puzzle consists of many pieces. For example, (a) the identification of buried indicator groups in certain positions of the messages, or (b) the recognition of probable machine-cipher traffic (implied by the level of correspondents and the volume of traffic passed) as Enigma from the over-all uniliteral frequency distribution typical of a noncrashing system, should be made quite early in the cryptanalytic game. In the meantime, or perhaps even as a concurrent exercise, the analyst would derive benefit and gain experience from participation in the Zendian Problem ⁷⁹ (especially if he worked as a member of a team ⁸⁰), which provides considerable

⁷⁹ Cf. Appendix 8 ("The Zendian Problem: An Exercise in Communication Intelligence Operations"), *Military Cryptanalytics, Part II*.

⁸⁰ For example, as do the students in my *Intensive Study Program in General Cryptanalysis*.



practice both in traffic analysis and in the diagnosis and solution of the low-, medium- and high-grade systems contained therein.

*d. This chapter began with a definition; it is therefore fitting that we also end it with a definition:*

*"diagnostician, n. An experienced cryptanalyst of ability, just before retirement age."*

This is but a gentle reminder to the reader of an aphorism of Hippocrates, as translated by Chaucer: "The lyf so short, the craft so long to lerne."⁸¹

---

⁸¹ What Hippocrates actually said was *ὁ βίος βραχύς, ἡ δὲ τέχνη μακρή*.



These squares, used sequentially, would yield periodic polyalphabetic substitution with a period of 25 digraphs; but the band of squares may be used in various ways to produce aperiodic encipherment. For example, in a plaintext interruptor system with E_p as the interruptor letter, whenever E_p occurs as the *first* letter of a digraph,³ a double skip in the otherwise normal key progression could take place. In the illustrative encipherment below, we have used the foregoing Playfair band, starting in square no. 1 with E_p as the plaintext interruptor:

Square no.:	1	3	5	6	7	8	9	10	11	12	13	14	16	17	18
Plain:	EN	EM	YP	AT	RO	LS	AC	TI	VE	IN	AR	EA	WE	ST	OF . . .
Cipher:	NT	ZU	WH	WA	EN	UD	CI	NE	AB	DX	HA	BT	LV	HD	GU

Or, in a plaintext autokey variation, the *second* letter of the plaintext digraph could designate the particular square (identified by the letter in the upper left-hand corner of the square) for the next encipherment; e.g., the "A" square is square no. 3, the "B" square is no. 8, and so on. This is illustrated in the following example:

Square no.:	1	9	19	10	12	20	11	23	7	17	9	25	3	17	12
Plain:	EN	EM	YP	AT	RO	LS	AC	TI	VE	IN	AR	EA	WE	ST	OF . . .
Cipher:	NT	AE	PD	OE	CL	OW	OT	PE	HV	FQ	ET	FE	LX	HD	QA

Ciphertext interruption and ciphertext autokey could be accomplished in a similar manner. An added complication would be to predicate the keying, not on a single letter, but on the mod-25 sum (as measured on the normal A-Z sequence, less J) of *both* letters of the keying digraph. Thus, in the example below, the second digraph is enciphered in square no. (E+N=5+13=18), the third digraph is square no. (E+M=5+12=17), the fourth digraph in square no. (Y+P=24+15=14), and so on:

Square no.:	1	18	17	14	20	6	4	4	3	1	22	18	6	2	12
Plain:	EN	EM	YP	AT	RO	LS	AC	TI	VE	IN	AR	EA	WE	ST	OF . . .
Cipher:	NT	OE	PD	TP	SR	ZL	DY	CO	GV	UP	GZ	OW	SM	LP	QA

This latter scheme could yield ciphers of considerable complexity, as would the use of a very long literal key (with J either being ignored, or combined with I), such as in the following example:

Square:	W	H	E	N	I	N	T	H	E	C	O	U	R	S	E
Plain:	EN	EM	YP	AT	RO	LS	AC	TI	VE	IN	AR	EA	WE	ST	OF . . .
Cipher:	XP	FE	PD	CA	EN	SX	OT	WU	GV	UP	US	QS	TG	NP	NU

c. Many types of aperiodic substitution systems initially appear very complicated or difficult in their cryptanalysis, but, as we have seen from our studies thus far, methods for their solution become readily available or demonstrable.⁴ Even in apparently more abstruse cryptographic cases, methods for their solution can readily be postulated. We shall now take up two illustrative special cases.

**82. Analysis and solution of a first case.**—a. For the first example of what at first blush appears to be a complex case of aperiodic encipherment, we shall treat a cryptosystem that once occurred to the author in a dream after a particularly sumptuous meal.⁵ In that dream there came to us the principle for

³ For that matter, an E_p in *either* position of a digraph could be used to govern the key interruption.

⁴ In this connection, the following quotation may provide some food for thought:

"It has been said, with regard to musical problems, that musicians generally give the correct answers supported by illogical argument, but mathematicians arrive at incorrect answers through a process of irrefutable reasoning."

—A. L. Leigh Silver, in *The American Mathematical Monthly*, Vol. 78, No. 4, April 1971.

From this can be extrapolated that the intuitive cryptanalyst may hit upon a solution for reasons that are entirely irrelevant, whereas a mathematician may correctly define the steps in a problem, predicated however on initial assumptions that later prove to be invalid.

⁵ This story, including complete details of the meal which gave rise to the dream, is written up in an article entitled "A Cryptanalyst's Nightmare: An Oneirotic Problem and Its Solution," appearing in the *NSA Technical Journal*, Vol. XVI, No. 4, Fall 1971.

a cipher machine, a principle startling in its simplicity and yet apparently devilishly difficult in its cryptanalytic aspects—a machine incorporating sliding components with both plaintext *and* ciphertext autokeying in its cryptography. In this system, the first letter of the message plain text is enciphered by a key letter designated by an indicator; after that, every subsequent plaintext letter is enciphered by a key letter which is the mod-26 sum of the immediately preceding plaintext letter and its ciphertext equivalent. Thus the system would embrace all of the nasty features of plaintext and ciphertext autokeying, and none of their [for the cryptanalyst] welcome attributes: polygraphic repetitions, which are plentiful in plaintext autokey, are here drastically reduced; and isomorphs, which arise in ciphertext autokey, should here be nonexistent. If the introductory key consists of several letters, there is no statistical way of determining its length, and other mathematical techniques applicable in autokey systems are fruitless here. A veritable cryptanalyst's nightmare!

b. But let us approach the subject calmly: after all, there must be *some* solution, albeit for a special situation. Let us consider the trivial case of known components and examine what happens in the following message enciphered with direct standard alphabets:

```

      6 21 22 9 26 11 8 11 26 9 14 23 6 17 26 1 14 19 22 7 24 11 2 5
K:  M F U V I Z K H K Z I N W F Q Z A N S V G X K B E
P:  W H A T I S Y O U R P R E S E N T P O S I T I O N
C:  I M U O Q R I V E Q X E A X U M T C G N O Q S P R

```

The first plaintext letter,  $W_p$ , enciphered in the initial key of  $M_k$  yields  $I_c$  as the cipher equivalent. The second plaintext letter,  $H_p$ , is enciphered by the mod-26 sum ( $\equiv 6 = F_k$ ) of the preceding  $W_p$  and  $I_c$ , yielding  $M_c$  as the result. The third plaintext letter,  $A_p$ , is enciphered by the mod-26 sum ( $\equiv 21 = U_k$ ) of the preceding  $H_p$  and  $M_c$ , yielding  $O_c$ . And so on.

c. Now if all we had were the ciphertext message and a knowledge of the general system, we could make trial decipherments on the basis of direct standard cipher alphabets. In the three diagrams below, we have assumed that the first plaintext letter is A, B, and C, in turn, and we have deciphered the first five letters accordingly:

```

      10 17 26 5           11 16 1 4           12 15 2 3
K:    J Q Z E           K P A D           L O B C
C:    I M U O Q       I M U O Q       I M U O Q
P:    A D E P M       B C F O N       C B G N O

```

Noting the alternation of progression of the 1st, 2d, 3d . . . letters of the decipherments, we construct from the first "decipherment" a generatrix diagram in which the sequence in the even columns runs in the opposite direction from that of the odd columns, as follows:

	<u>I</u>	<u>M</u>	<u>U</u>	<u>O</u>	<u>Q</u>
	A	D	E	P	M
	B	C	F	O	N
	C	B	G	N	O
	D	A	H	M	P
	E	Z	I	L	Q
	F	Y	J	K	R
	G	X	K	J	S
	H	W	L	I	T
	I	V	M	H	U
	J	U	N	G	V
	K	T	O	F	W
	L	S	P	E	X
	M	R	Q	D	Y
	N	Q	R	C	Z
	O	P	S	B	A
	P	O	T	A	B
	Q	N	U	Z	C
	R	M	V	Y	D
	S	L	W	X	E
	T	K	X	W	F
	U	J	Y	V	G
	V	I	Z	U	H
	*W	H	A	T	I
	X	G	B	S	J
	Y	F	C	R	K
	Z	E	D	Q	L

The message plain text comes out on one generatrix, as is indicated by the asterisked row.

d. The foregoing case was patently trivial, the components being known. If, however, the components were *unknown*, it would seem that the only practical solutions must be predicated on either a huge sample of cipher text (correctly assuming—without foundation—the length of the introductory key) for the possible application of Fourier techniques and other palpable mathematical approaches, or a sizeable quantity of matched plain and cipher text—if we are to call these practical solutions. In the next case to be examined, let us assume a knowledge of the general system, and let us further assume that the plain and cipher are unknown mixed sequences but that the sequence for the keying (i.e., for performing the modular arithmetic) is the normal sequence. Therefore if we had available some matched plain and cipher, we would also be privy to the *keys* involved. Let us now study the two message beginnings given below:

			5		10		15		20		25																	
		21	20	14	10																							
	K:	U	T	N	J	Z	B	U	T	Z	F	G	J	Z	R	P	Y	L	M	I	F	B	R	J	X	E		
1.	P:	R	E	F	E	R	E	N	C	E	Y	O	U	R	M	E	S	S	A	G	E	N	U	M	B	E	R	. . .
	C:	C	O	H	E	H	W	G	Q	U	G	R	O	H	E	K	F	S	L	B	A	N	W	W	V	Z	W	
				12	7	17	24																					
	K:	L	G	Q	X	H	A	N	P	W	M	S	V	K	L	G	B	G	H	N	J	S	V	T	H	A		
2.	P:	R	E	F	E	R	E	N	C	E	Y	O	U	R	M	E	S	S	A	G	E	N	U	M	B	E	R	. . .
	C:	T	B	K	S	P	V	Z	M	R	N	D	A	S	Y	B	I	N	G	G	E	E	A	G	F	V	O	

If the keying sequence is the normal sequence, then in Message No. 1 the sum  $R_p + C_c = 21 = U$  will be the key for enciphering the second plaintext letter, and the sum  $E_p + O_c = 20 = T$  will be the key for enciphering the third plaintext letter, and so on. The 50 key-plain-cipher relationships derivable from the foregoing diagram are inserted in a reconstruction matrix, as shown in Fig. 184, below.

Plain

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A														Z				O								
B														G				N			W					
C																										
D																					W					
E																										
F															N	R										
G	G						K													I		O				
H				V			G																			
I				A																						
J		V												E					H							
K													Y													
L	L			B																						
M							B								D											
N			M	E																						
O																										
P					R														F							
Q					S																					
R					K								W													
S																										
T		F			U	H																A				
U		Q		O																						
V														G					S							
W																									N	
X					Z														P							
Y																			S							
Z					W								E												G	

FIGURE 184

Noting in the A column that  $G_c$  and  $L_c$  are opposite  $G_k$  and  $L_k$ , we capitalize on this implication and chain our cipher letters to the  $\emptyset$  column outside the matrix. The partial chains are the following:

- Cols.  $\emptyset$ -B: JV TF
- $\emptyset$ -C: NM UQ
- $\emptyset$ -E: HV IA LB NE PRK QS TUO XZW
- $\emptyset$ -F: GK TH
- $\emptyset$ -G: HG MB
- $\emptyset$ -M: KY RW VG ZE
- $\emptyset$ -N: AZ BG FN JE
- $\emptyset$ -O: FR MD
- $\emptyset$ -R: AO EW JH VS XP
- $\emptyset$ -S: BN GI PF YS
- $\emptyset$ -U: BW GO SA
- $\emptyset$ -Y: WN ZG

From these chains the following equivalent primary cipher component can easily be reconstructed:

X Z W Y T U O Q S P R K L B F J D G N E M C I A H V

This sequence is then decimated at various trial intervals, and when the decimation of -7 is reached, it will be discovered that the original cipher component is based upon the diagram below:

6 1 2 4 5 7 3  
M A C H I N E  
B D F G J K L  
O P Q R S T U  
V W X Y Z

The plain component can now be recovered by juxtaposing a blank strip against the known cipher component, designating an arbitrary cell as the index position against which to set the key letter, and filling in the plaintext values at the various positionings of the sliding cipher component. This yields the following sequence:

A G . S . . B . O U . E F . . . M . N . Y R C . . .

Although there are only 13 different plaintext letters in our component, the recovered sequence can be put together as in the diagram below, revealing the key word DREAM:

2 5 3 1 4  
. R E A M  
B C F G .  
. . . . N  
O . . S .  
U . . . Y

e. For the third case, we have the following matched plain and cipher beginnings of three messages:

- 1.                    ⁵                    ¹⁰                    ¹⁵                    ²⁰                    ²⁵  
R E F E R E N C E Y O U R M E S S A G E N U M B E R . . .  
O B P X S V P U Z L J A L F A X X E H X V H E F P L
- 2. R E F E R E N C E Y O U R M E S S A G E N U M B E R . . .  
A T F O B K F C L D E G D M G O O H S O K S H M F D
- 3. R E F E R E N C E Y O U R M E S S A G E N U M B E R . . .  
D E K L J O K B U C F I C R I L L M Q L O Q M R K C

To our utter astonishment, isomorphism has appeared in a system we could have sworn could not possibly yield isomorphs, since *plaintext* autokey is one of the features involved in the encipherment! Nevertheless, doing what comes naturally, we derive the following sets of partial chains from the foregoing beginnings:

Msgs 1-2: XOAG JEHSBT PFM VK UC ZLD  
Msgs 1-3: VOD ZUBEM PK XLC SJFR AI HQ  
Msgs 2-3: ADCBJ TEFKOLU GI HMR SQ

These partial chains are quickly put together into the following cipher-component sequence, J E H S B T . U C . Z L D I X O A G V K R . P F M Q, and upon trial decimation we discover that at the interval of -5 we can recover the original key word upon which the sequence is based:

7 5 3 4 9 6 1 8 2  
. I G H T M A R E  
B C D F J K L O P  
Q S U V . X . Z

The plain component is found to be identical to the cipher component, as is also the keying sequence. The isomorphism is a result of identical cipher and keying sequences, the constitution of the plain component being irrelevant.

f(1). For the last case, we shall examine the matched plain and cipher of the following eight message beginnings:

- |    |   |    |    |    |    |    |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |
|----|---|----|----|----|----|----|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
|    | 5 | 10 | 15 | 20 | 25 | 30 |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |
| 1. | R | E  | F  | E  | R  | E  | N | C | E | Y | O | U | R | M | E | S | S | A | G | E | N | U | M | B | E | R | . | . | . |   |   |   |   |   |
|    | F | A  | O  | N  | A  | G  | C | Z | M | K | W | V | B | D | K | K | U | U | U | V | B | F | B | F | Q | D | . | . | . |   |   |   |   |   |
| 2. | R | E  | F  | E  | R  | E  | N | C | E | Y | O | U | R | M | E | S | S | A | G | E | N | U | M | B | E | R | . | . | . |   |   |   |   |   |
|    | H | Q  | K  | H  | S  | S  | O | H | V | J | T | Q | T | A | E | H | T | T | N | H | W | S | T | V | F | X | . | . | . |   |   |   |   |   |
| 3. | R | E  | F  | E  | R  | E  | N | C | E | Y | O | U | R | M | E | S | S | A | G | E | N | U | M | B | E | R | . | . | . |   |   |   |   |   |
|    | A | G  | X  | X  | V  | L  | N | M | S | T | V | D | D | G | R | P | X | X | B | U | X | Q | F | E | O | H | . | . | . |   |   |   |   |   |
| 4. | T | O  | C  | O  | M  | M  | A | N | D | I | N | G | O | F | F | I | C | E | R | S | A | L | L | U | N | I | T | S | . | . | . |   |   |   |
|    | R | N  | H  | S  | A  | I  | Y | Z | L | L | O | B | J | Q | Z | X | U | K | C | A | A | V | X | N | H | I | O | I | . | . | . |   |   |   |
| 5. | T | O  | C  | O  | M  | M  | A | N | D | I | N | G | O | F | F | I | C | E | R | S | A | L | L | U | N | I | T | S | . | . | . |   |   |   |
|    | V | T  | G  | Z  | J  | H  | Q | C | B | D | D | H | E | J | H | Y | X | W | J | J | J | U | R | G | B | Q | N | S | . | . | . |   |   |   |
| 6. | T | O  | C  | O  | M  | M  | A | N | D | I | N | G | O | F | F | I | C | E | R | S | A | L | L | U | N | I | T | S | . | . | . |   |   |   |
|    | M | F  | C  | L  | T  | T  | U | A | S | O | E | J | O | S | O | M | A | C | Z | L | L | W | C | T | G | J | M | H | . | . | . |   |   |   |
| 7. | R | E  | C  | O  | N  | N  | A | I | S | S | A | N | C | E | R | E | R | E | P | O | R | T | S | I | N | D | I | C | A | T | E | . | . | . |
|    | T | K  | J  | I  | E  | L  | K | E | Q | A | A | N | M | S | Y | O | K | A | C | W | K | G | A | S | O | V | L | Y | C | . | . | . |   |   |
| 8. | R | E  | C  | O  | N  | N  | A | I | S | S | A | N | C | E | R | E | R | E | P | O | R | T | S | I | N | D | I | C | A | T | E | . | . | . |
|    | J | E  | R  | J  | A  | Y  | Q | I | B | G | G | T | N | G | L | Y | R | B | A | H | F | D | D | I | E | L | S | N | I | . | . | . |   |   |

We begin by indexing the vertical plain-cipher digraphs and, in the hope that commutative keying (i.e., involving only one keying sequence) is present, we index the first four vertical digraphs of Msg No. 1 as FR, AE, FO, and EN. From this index we list the key digraphs occurring two or more times together with the plain-cipher equivalencies which directly follow them:

	<u>Key</u>	<u>P-C</u>	<u>equivalents</u>		<u>Key</u>	<u>P-C</u>	<u>equivalents</u>
1.	AA	LV	NN	24.	EQ	RD	FK
2.	AL	LW	TY	25.	ES	NO	YT RY
3.	AM	EE	MI	26.	EV	NB	YJ
4.	AN	DS	NY	27.	FO	EN	IM CC
5.	AQ	NC	II	28.	FS	FO	ID
6.	AR	EG	TH	29.	GN	EH	IJ
7.	AS	AA	TN	30.	GU	EV	NB
8.	AU	GU	NA	31.	II	TO	SB
9.	BG	EU	OJ	32.	IM	AY	CA
10.	BN	UF	IQ	33.	IO	NE	CV
11.	CH	EV	OS	34.	JO	FQ	NA
12.	CL	UT	AS	35.	JR	SJ	EE
13.	CN	CZ	DB EG	36.	KS	SU	IG
14.	CR	SA	TW OJ	37.	LR	UG	EY
15.	DI	ND	IE	38.	MT	BV	MT AU SH OF
16.	DN	GH	DI	39.	NO	CH	GB
17.	EE	SH	CR	40.	NT	CN	SS EI
18.	EG	FX	NC RL	41.	OT	UQ	SI CG
19.	EH	RS	NW	42.	QU	RT	MF
20.	EI	SQ	CL	43.	RT	MA	ON EK
21.	EK	SK	RC CJ	44.	SU	AU	MT
22.	EN	RA	GJ NL	45.	TY	OV	EC
23.	EO	RH	FJ PK				



The foregoing plain-cipher equivalents are now indexed in order to equate *key* equivalents. It is discovered that the plain-cipher equivalents AU, EE, EG, EV, MT, NA, NB, NC, OJ, and SH have occurred twice each, so we are able to arrive at the diagram of equivalencies shown in Fig. 185, below:

	<u>Keys</u>		<u>P-C equivalencies</u>							<u>Keys</u>		<u>P-C equivalencies</u>					
1.	BG	CR	TW	OJ	EU	SA			19.	EN	RA	GJ	NL				
2.			CL	AS	UT				20.	EO	RH	FJ	PK				
3.	EE	SU	MT	AU	BV	MT	SH	OF	CR	21.	EQ	RD	FK				
4.		JR	AM	EE	MI	SJ				22.	ES	NO	YT	RY			
5.		CN	AR	EG	TH	CZ	DB			23.	FO	EN	IM	CC			
6.	EV	GU	CH	EV	OS	NB	YJ			24.	FS	FO	ID				
7.		JO	AU	NA	GU	FQ				25.	GN	EH	IJ				
8.		EG	AQ	NC	II	FX	RL			26.	II	TO	SB				
9.			AA	LV	NN					27.	IM	AY	CA				
10.			AL	LW	TY					28.	IO	NE	CV				
11.			AN	DS	NY					29.	KS	SU	IG				
12.			AS	AA	TN					30.	LR	UG	EY				
13.			BN	UF	IQ					31.	NO	CH	GB				
14.			DI	ND	IE					32.	NT	CN	SS	EI			
15.			DN	GH	DI					33.	OT	UQ	SI	CG			
16.			EH	RS	NW					34.	QU	RT	MF				
17.			EI	SQ	CL					35.	RT	MA	ON	EK			
18.			EK	SK	RC	CJ				36.	TY	OV	EC				

FIGURE 185

The values of the plain-cipher equivalencies are inserted into a reconstruction matrix, as shown in Fig. 186, below:

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
1				U						J									A	W						
2	S																									T
3	U	V	R															T	F					H		
4				E																					J	
5			Z	B	G																					H
6				V															B	S						J
7					Q	U														A						
8					X			I												C					L	
9													V							N						
10													W												Y	
	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
11				S																Y						
12	A																								N	
13										Q																F
14										E										D						
15			I				H																			
16																				W					S	
17			L																						Q	
18			J																						C	K
19																									A	
20							J													L					K	H
	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
21																										
22																										
23			C		N																					
24																										
25																										
26																										
27	Y		A																							
28			V																							
29																										
30																										
	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
31			H																							
32			N		I																					
33			G																							
34																										
35																										
36																										

FIGURE 186

The following chains are derived from the foregoing matrix:

1- 3:	JF AH	4-32:	EI JS	8-24:	XO ID
1- 4:	UE AJ	4-35:	EK IA	16-19:	WL SA
1- 5:	UG WH	5-23:	ZC GN	16-22:	WO SY
1- 6:	UV JS	5-32:	ZN GI	17-18:	LJ QK
1-26:	AB WO	6-22:	BO JT	17-32:	LN QS
1-32:	UI AS	6-35:	VK SN	17-33:	LG QI
1-35:	UK JN	6-36:	SVC	18-32:	JN KS
1-36:	UC JV	7- 8:	QX AC	18-33:	JG KI
3- 4:	TI HJ	7-19:	UJ AL	19-22:	LO AY
3-17:	RL HQ	8-14:	IE CD	20-21:	JK HD
3-18:	RJ HK	8-16:	CW LS	23-25:	NH MJ
3-27:	UY RA	8-19:	CLA	23-32:	CNI
3-32:	RN HS	8-20:	XJ LH	32-33:	NG SI
3-33:	RG HI	8-21:	XK LD	35-36:	KC NV
3-35:	TA FN	8-22:	CO LY		

These chains may now be combined into the following cipher-component sequence:

S V C L A X F Q P E O Y G R T B I H Z J U D N K M W

When decimated at an interval of -9, it can be analyzed and found that this sequence is derived from the following diagram:

```

6 1 2 4 5 7 3
M A C H I N E
B D)
F G J)
K L O P Q R S)
T U V W)
X Y Z   )

```

(2) We now place our recovered cipher component in juxtaposition against a blank plain-component strip and, referring to line 1 of Fig. 186, we write an E_p over the U_c and O_p over the J_c, an S_p over the A_c, and a T_p over the W_c. We then slide F_c under the O_p, and, referring to line 3, we write A_p over the U_c, B_p over the V_c, C_p over the R_c, and so forth for all entries of line 3. Continuing in this vein, we recover the entire plain component and find that it is based upon the following diagram:

```

2 5 3 1 4
D R E A M
B C F G)
H)
I J K)
L N O P Q)
S T)
U V W X)
Y)
Z   )

```



The top row (the 0 row) in conjunction with one of the other rows shows that the expressed equivalencies have identical modular sums: that is, in rows 0-1, the combinations AM and JR sum to the same number, mod 26. Since we have already proved that there is commutative keying in the cryptosystem, the MA and RJ must also sum to the same number with AM and JR; therefore we may insert these reciprocal values into the matrix, as shown by the lower-case letters. Chains are then derived from this matrix, as shown below:

1- 2: MR JA	3- 8: NS OAG	7-11: TE OY
1- 3: MN JT	3- 9: IK AD	7-14: TJ ON
1-13: RM AJ	3-10: IH AO SN TL	9-10: KH CR DO
2- 3: RN CAT	3-11: IO SE RY	9-13: CN DL
2- 5: NR AC	3-12: ISF OE	10-11: HO NE
2- 8: RS CG	3-14: AT SJ RN	10-12: HS NF
2- 9: NL CD	4- 5: EB AS	10-13: RN OL
2-10: CO AL	4- 8: QS EN	10-14: OT NJ
3- 4: NQ IG	5- 8: BN QA	11-12: OS EF
3- 5: TC OQ	6- 9: IN EK	11-14: EJ YN
3- 6: IED RM	6-11: EO MY	13-14: MO LT
3- 7: NL ST RO	7-10: AR TN	

These partial chains can now be amalgamated into a single chain with six blanks, as follows:

A J Y . O . Q R M I E D T H C S L . . N K F G . . B

This sequence is either the original keying sequence or, more likely, a decimation thereof. Referring now to the matched plain and cipher of Message No. 1,

R E F E R E N C E Y O U R M E S S A G E N U M B E R . . .  
F A O N A G C Z M K W V B D K K U U U V B F B F Q D

and by using our recovered plain and cipher components, we can determine that if  $E_p = A_c$  at position 2, the key letter must be  $H_k$  (under the assumption of  $A_p$  as the index letter). If the commutative keying is expressed as a strip sliding against itself, the mod-26 sum of  $R+F=H$  at position 1 can be represented on the keying strips as follows:

- (1) A J Y . O . Q R M I E D T H C S L . . N K **(F)** G . . B
- (2) . N K F G . . B A J Y . O . Q **(R)** M I E D T **(H)** C S L .

which means that the first element (R) of the equation  $R+F=H$  is under S as an index. At position 3,  $F_p = O_c$  with our sliding strips means a key of  $F_k$ , so the alignment of the keying strips for the mod-26 sum of  $E+A=F$  must be

- (1) **(A)** J Y . O . Q R M I E D T H C S L . . N K F G . . B
- (2) **(F)** G . . B A J Y . O . Q R M I **(E)** D T H C S L . . N K

and again the index letter in the upper strip is seen to be S. By using the data in the message beginnings, we can recover the entire keying strip as follows:

A J Y Z O U Q R M I E D T H C S L V W N K F G X P B

Even though this is a decimation of the original keying sequence, it nevertheless will suffice for the cryptographic operations of the system, which has now been laid completely bare.

g. These solutions teach us a lesson we are sometimes prone to forget. The original cryptoprinciple of the machine appeared at the outset to be extremely complicated in analysis, and as we learned more about it, at each step we were temporarily beset by insurmountable obstacles that we speedily managed to surmount. In the end, all the approaches to solution appeared quite straightforward and obvious.

83. Analysis and solution of a second case.—a. For the second example of an apparently complex case of aperiodic encipherment which yielded to facile attack we shall quote verbatim an article by William Lutwiniak which appeared in the *NSA Technical Journal*, Vol. I, No. 3, October 1956:

SOLUTION OF A POLYALPHABETIC MONOME DINOME SYSTEM

By William Lutwiniak

An interesting use of monome-dinome matrix encipherment has been suggested by Mr. L. D. Callimahos. His scheme calls for 10 matrices, used successively, to encipher the plain text. The ten matrices are generated from one basic matrix by systematically displacing the coordinate sequence one position at a time. By way of example, if the basic matrix is the first one shown below,

4 5 1 7 0 6 2 8 3 9 - S E - R A T I O - N 1 B C D F G H J K L M 3 P Q U V W X Y Z . ,	5 1 7 0 6 2 8 3 9 4 - S E - R A T I O - N 7 B C D F G H J K L M 9 P Q U V W X Y Z . ,	1 7 0 6 2 8 3 9 4 5 - S E - R A T I O - N 0 B C D F G H J K L M 4 P Q U V W X Y Z . ,
Matrix 1	Matrix 2	Matrix 3
9 4 5 1 7 0 6 2 8 3 - S E - R A T I O - N 5 B C D F G H J K L M 8 P Q U V W X Y Z . ,		
Matrix 10		

then the 2d, 3d . . . 10th are generated as indicated. Plain text THE if started in the first matrix, would be enciphered as 6727. Note that the row coordinates are slides of the column coordinates. The first row is successively 1, 7, 0, . . . 5 and the second 3, 9, 4, . . . 8. The distance between the pair of row coordinates for a given matrix, measured on the sequence of the column coordinates, is fixed by the position of the blanks on the monomic row; this distance is the same for all ten matrices.

The system gives rise to some interesting properties. The original plain language has a rigid cycle of 10, but the average cipher cycle equals 10 plus the relative frequency of the letters enciphered by dinomes. In general, these frequencies vary between 33% and 60%, depending on the number and relative frequencies of the monomes composing the top row. In the example given above, the eight monomes are the eight most frequent letters in English, which normally make up 66% of plain text. The cycle of the cipher would thus average 13.3%; this, however, is a purely statistical cycle, and the cipher text would give the appearance of being aperiodic.

One other feature is that the cipher text is guaranteed to be monomically flat. Each digit is used in turn for all columns and rows; hence whatever inherent bias exists monomically in the basic matrix will be systematically and equally distributed over all 10 digits.

Mr. Callimahos submitted for consideration a 925-digit message as a test problem. All that was known was that the encipherment proceeded as indicated above, by systematically displacing the horizontal coordinate one position; the locations of the blanks on the monome row determine the successive row coordinates. The number of the row coordinates is unknown, as is the underlying language. The first 210 digits of the message are given below:

1 0 4 4 9	0 7 9 7 5	1 7 3 8 5	2 2 1 0 5	6 6 9 1 7	5 9 4 3 9
3 4 6 0 9	2 5 0 6 8	4 5 3 9 0	4 1 7 0 8	1 0 8 5 3	8 8 2 4 4
7 7 0 7 5	5 6 8 1 3	6 4 9 0 7	5 3 2 1 9	8 1 5 1 2	1 0 7 4 7
6 7 9 9 5	8 5 5 5 9	4 2 2 3 9	9 7 9 6 0	9 9 5 8 8	9 8 8 1 5
6 7 0 8 1	4 6 0 0 1	3 6 0 6 8	4 6 8 5 8	2 3 9 1 8	4 6 2 5 6
2 9 0 2 2	7 1 3 5 4	9 0 8 6 2	9 3 8 2 3	0 7 7 7 8	0 3 2 1 8
1 1 5 0 1	6 3 7 5 8	4 0 1 1 6	1 8 2 9 2	7 0 3 5 2	2 9 2 5 0 . . .

A STETHOSCOPE run on the material elicited the following facts:

- Monomic delta I.C.: 0.999 (As anticipated, flat)
- Dinomic delta I.C.: 1.07 (4.6 sigmas)
- Trinomic delta I.C.: 1.29 (6 sigmas)

The repeat rates at distances 1 to 10 were not significant. The following polymeric repeats, all occurring twice, were listed:

Size	Number of pairs
5	5
6	6
7	4
8	1
10	1
11	1

The distances between these repeats, as expected, gave every indication of being aperiodic; the shorter intervals involved were 24, 51 (twice), 63, 69, 75, and 82. It had been hoped that the statistical cycle could be inferred from the shorter intervals between repeats, but the observed data are insufficient. A count of repeats at distances from 1 to 20 should peak at the statistical cycle; however, an attack was devised that did not require this information.

Referring to the sample matrices at the beginning of this article, the following are the 10 successive encipherments of GETTYSBURG:

Plain	
	G E T T Y S B U R G
1	1 0 1 8 3 1 4 6 3 2 6 9 5 5 7
2	7 6 7 3 9 7 5 2 9 8 2 4 1 1 0
3	0 2 0 9 4 0 1 8 4 3 8 5 7 7 6
4	6 8 6 4 5 6 7 3 5 9 3 1 0 0 2
5	2 3 2 5 1 2 0 9 1 4 9 7 6 6 8
6	8 9 8 1 7 8 6 4 7 5 4 0 2 2 3
7	3 4 3 7 0 3 2 5 0 1 5 6 8 8 9
8	9 5 9 0 6 9 8 1 6 7 1 2 3 3 4
9	4 1 4 6 2 4 3 7 2 0 7 8 9 9 5
10	5 7 5 2 8 5 9 0 8 6 0 3 4 4 1
Pattern:	A B A C D A E F D G F H I I J

It will be noted that all versions are isomorphic to each other, since all have the pattern ABACDAEFDGFHIIJ. Further, each of the 15 columns is a slide of the actual horizontal coordinates. At first glance, it seems a little strange that the row coordinates behave no differently from the column coordinates: all are slides of the basic sequence. However, it is readily apparent that the designations for each row are determined by the fixed location of the blanks in the monomic portion of the matrix, and hence must be slides of the basic sequence. What is not known is the distance (as measured on the basic sequence) between the blanks, and there is no information derivable from the isomorphs that bears on this question.

Consideration of the encipherment scheme makes the reason for isomorphism quite clear: the location of the plain values in the matrix is invariant; only the coordinate values designating the plain vary, and these values progress regularly one position at a time. Each individual plaintext repeat must be associated with the isomorph caused by invariant plain positions in the matrix, regardless of where the repeat starts in the sequence of 10 matrices. A ciphertext repeat is merely a special case of isomorphism; i.e., a plaintext repeat which starts at the same point in the 10-matrix sequence.

This suggests a simple, straightforward attack based on this phenomenon: locate long isomorphs; then reconstruct the basic coordinate sequence by the principles of indirect symmetry. It is true that this reconstructed coordinate sequence may be a decimation of the true one; but there is a procedure for selecting the correct one from among the possibilities.

In order to avoid a tedious isomorphic search, the longer hits located by STETHOSCOPE were listed and patterned as follows:

Repeat	Pattern
2 3 7 9 9 3 5 8 9 7 7	A B C D D B E F D C C
8 1 3 6 4 9 0 7 5 3	A B C D E F G H I C
2 8 5 0 9 5 7 0	A B C D E C F D
<u>6 8 0 4 6 5 5</u>	<u>A B C D A E E</u>
4 7 2 2 3 2 1	A B C C D C E
<u>2 7 8 5 2 3 3</u>	<u>A B C D A E E</u>
8 5 2 2 1 0 5	A B C C D E B

Fortunately, there is an isomorphic repeat with patterns ABCDAEE among these repeats. This pattern was searched for elsewhere in the message; since it already indicated a plaintext group occurring four times, it was expected that there might be other occurrences. The following possibilities, including the original pair, were found:

	A	B	C	D	A	E	E
(1)	6	8	0	4	6	5	5
(2)	2	7	8	5	2	3	3
(3)	3	0	9	2	3	4	4
(4)	9	3	5	8	9	7	7
(5)	1	5	4	0	1	8	8
(6)	7	5	2	3	7	9	9
(7)	7	0	8	4	7	2	2

If the members of the original pair (1) and (2) are taken as correct, (7) cannot be right, since there is a repeated digit (8) in column C of the pattern. The mechanics of the system demands that between a pair of isomorphs, the corresponding digits must either all be different or all be identical. The other conflict remaining, after eliminating (7), is that both (5) and (6) cannot be correct: there is a clash in column B. This clears up quickly when it is noted that (4) is contained in the 11-digit repeat, and that (6) involves the beginning of this repeat—23799. The fact that one of the 7-digit isomorphs was contained in the 11-digit repeat led to testing the 4 digits preceding the remaining 7-digit isomorphs, and the following was built up:

	A	B	C	D	D	B	E	F	D	C	C
(1)	1	8	5	6	6	8	0	4	6	5	5
(2)	9	7	3	2	2	7	8	5	2	3	3
(3)	7	0	4	3	3	0	9	2	3	4	4
(4)	2	3	7	9	9	3	5	8	9	7	7
(5)					1	5	4	0	1	8	8

The principles of indirect symmetry were applied, and the following equivalent sequence reconstructed: 9306827415. This is either the true basic sequence or a decimation of the true sequence at intervals 3, 7, or 9. (Had the true sequence been such that even decimations, or a decimation of 5, produced either 2 sets of 5 or 5 sets of 2, all relationships obtained from the isomorphs would have had these properties and hence an unbroken sequence, as reconstructed automatically, eliminates the even decimations and the one at distance 5.)

Before attempting to select the correct decimation from the four possibilities, let us consider the properties of a monome-dinome matrix. The numbered rows, in the least favorable case (where 8 monomes represent ETNROAIS), must contain 33% of the plain text. This percentage increases with fewer and/or less frequent monomes. Thus, there is often a tendency for dinomes to follow one another sufficiently often to be distinguished from the random case. In the system under consideration, an "A-A" dinome count (in the sequence ABCDE . . . , A-A dinomes are AC, BD, CE, etc.) will cover a situation where a dinome from a particular row is followed by another dinome from that same row. However, in this respect, we cannot distinguish one row from another: each time a dinome from any given row is followed by a dinome from that same row it will be reflected in the A-A dinome count, since each row is a slide of the basic sequence starting at a different point. We do lose the information when a dinome from a given row is followed by a dinome from some other row.

The following is the A-A dinome distribution:

		$\theta_c^2$									
		0	1	2	3	4	5	6	7	8	9
$\theta_c^{-1}$	0	4	13	9	9	10	11	9	9	8	10
	1	8	10	9	8	4	11	15	5	10	6
	2	16	5	6	13	7	3	6	11	11	15
	3	10	12	6	4	11	5	4	9	10	5
	4	14	5	10	6	4	11	7	11	13	7
	5	10	2	9	8	12	9	5	10	13	13
	6	6	12	7	1	6	8	8	4	9	14
	7	7	7	8	11	6	13	12	9	12	10
	8	11	10	13	10	13	10	10	11	8	11
	9	5	6	14	8	12	14	4	17	13	9





Herewith are the first 60 digits of the message, with the plain component sequence completed down the columns:

```

(1 0) 4 4 9 0 7 9 7 5 1 7 3 8 (5) 2 2 1 0 5 6 6 9 1 7 5 9 4 (3) 9
2 5 8 8 4 5 6 4 6 7 2 6 (1 3) 7 0 0 2 5 7 9 9 4 2 6 7 4 (8) 1 4
0 7 3 3 8 7 9 8 9 6 0 (9) 2 1 6 5 5 0 7 6 4 4 8 0 9 (6 8) 3 2 8
5 6 1 1 3 6 4 3 4 9 (5) 4 0 2 9 7 7 5 6 9 8 8 3 5 (4) 9 3 1 0 3
7 9 2 2 1 9 8 1 8 (4) 7 8 5 0 4 6 6 7 9 4 3 3 (1 7) 8 4 1 2 5 1
6 4 0 0 2 4 3 2 (3) 8 6 3 7 5 8 9 9 6 4 8 (1 1) 2 6 3 8 2 0 7 2
9 8 5 5 0 8 (1 0) 1 3 9 1 6 7 3 4 4 9 8 (3) 2 2 0 9 1 3 0 5 6 0
4 3 7 7 5 (3) 2 5 2 1 4 2 9 6 1 8 8 4 (3) 1 0 0 5 4 2 1 5 7 9 5
8 1 6 (6 7) 1 0 7 0 2 8 0 4 9 2 3 3 (8) 1 2 5 5 7 8 0 2 7 6 4 7
3 2 (9) 9 6 2 5 6 5 0 3 5 8 4 0 (1 1) 3 2 0 7 7 6 3 5 0 6 9 8 (6)

3 4 6 0 9 2 5 0 6 8 4 5 (3) 9 0 4 1 7 0 8 1 0 8 5 3 8 (8) 2 4 4
1 8 9 5 4 0 7 5 9 3 8 (7) 1 4 5 8 2 6 5 3 2 5 3 7 1 (3) 3 0 8 8
2 3 4 7 8 5 6 7 4 (1 3) 6 2 8 7 3 0 9 7 1 0 7 1 (6 2) 1 1 5 3 3
0 1 8 6 3 7 9 (6 8) 2 1 9 0 3 6 1 5 4 6 2 5 (6 2) 9 0 2 2 7 1 1
5 2 3 9 1 6 (4) 9 3 0 2 4 5 1 9 2 7 8 9 0 (7) 9 0 4 5 0 0 6 2 2
7 0 1 4 2 (9) 8 4 1 5 0 8 7 2 4 0 6 3 4 (5) 6 4 5 8 7 5 5 9 0 0
6 5 2 8 (0) 4 3 8 2 7 5 3 6 0 8 5 9 1 (8) 7 9 8 7 3 6 7 7 4 5 5
9 7 0 (3) 5 8 1 3 0 6 7 1 9 5 3 7 4 (2) 3 6 4 3 6 1 9 6 6 8 7 7
4 (6 5) 1 7 3 2 1 5 9 6 2 4 7 1 (6 8) 0 1 9 8 1 9 2 4 9 9 3 6 (6)
8) 9 7 2 6 1 0 2 7 4 9 0 8 (6 2) 9 3 5 2 4 3 2 4 0 8 4 4 (1 9) 9

```

In testing the ten possible starting points on the completed plain component, the rule is to read on the same generatrix one position for a monome, or two for a dinome, and then ascend one generatrix for the matrix. The reverse would be true had the basic sequence been recovered as a right-to-left progression. In the actual case at hand, it is necessary to test for only five assumptions. The positions of the blanks (five apart) gives 5 sets of 2; thus (2, 9) is identical with (9, 2) insofar as reading the generatrices is concerned.

The five streams (derived from the foregoing diagram) representing the ten possibilities for the first 60 digits of the message follow; all start with the initial digit of cipher text. The fraction following each stream is the monome-to-dinome ratio of the stream. The introductory dinomes are the two row coordinates associated with the particular matrix under consideration.

```

9, 2   1 29 6 5 8 3 1 4 6 26 3 4 23 8 98 8 3 8 8 26
and    5 6 6 95 6 0 3 6 8 0 5 27 96 1 6 24 27 4 7 3
2, 9   1 24 24 6 7 90 2-
                                           33
                                           14

4, 0   1 2 6 7 08 3 1 49 09 1 8 01 3 43 3 1 3 3 09 7
and    9 9 47 9 5 1 9 3 5 7 06 49 2 9 08 06 8 6 1 2
0, 4   08 08 9 6 45 0-
                                           31
                                           15

8, 5   1 2 6 7 0 4 81 4 6 2 7 84 2 88 9 4 4 88 80 6
and    59 9 4 59 52 4 1 7 6 59 84 0 4 53 59 3 9 2 0 53
5, 8   53 4 9 87 5-
                                           29
                                           16

3, 7   1 2 6 75 8 32 8 9 0 6 38 0 33 4 8 8 33 35 9 74
and    4 8 74 70 8 2 6 9 74 38 5 8 71 74 1 4 0 5 71 71
7, 3   8 4 36 7-
                                           27
                                           17

1, 6   10 9 67 3 10 3 4 5 9 13 5 11 8 3 3 11 17 4 68 8
and    3 68 65 3 0 9 4 68 13 7 3 62 68 2 8 5 7 62 62 3
6, 1   8 19 6-
                                           25
                                           18

```

The (1, 6) possibility looks the best from the standpoint of monome-to-dinome ratio, and, in fact, is correct. In the actual solution, 250 digits were examined on the basis of the five possibilities, and the (1, 6) possibility was outstandingly the correct one. The following matrix was recovered quickly:

```

      8 3 1 2 0 5 7 6 9 4
- R E - A C T I - O N
1 B F H K M Q U W Y
6 D G J L P S V X Z

```

The key word is obviously REACTION, and the following is the basic format:

	9	4	8	3	1	2	0	5	7	6
-	O	N	R	E	-	A	C	T	I	-
6	Z		D	G	J	L	P	S	V	X
1	Y		B	F	H	K	M	Q	U	W

The sequence of column coordinates is found to be the numerical key derived from the internal key word expanded to ten letters, i.e., REACTIONRE; the message plain text begins with the words "MOVEMENT OF THREE HUNDRED. . ."

Thus, what at first glance appears to be a rather complicated system yields to a straightforward attack which derives largely from simple cryptanalytic fundamentals. The attack depends in the main on the principles of indirect symmetry of related alphabets, and the fact that in this instance these principles were applied to digits rather than letters merely underscores the fundamental importance of the principles. This is just one more illustration of the desirability of every cryptanalyst's having a complete grasp of cryptanalytic fundamentals: one never knows where they may be applied next.

The basic system itself was assumed to be known, but the attack would probably have proceeded as above, albeit less directly, had nothing been known about the cryptosystem. Thus, aperiodic, causal ciphertext repeats would have been observed. Sooner or later isomorphism would be noticed among these repeats and the principles of indirect symmetry applied to yield the basic sequence. Once the fact was ascertained that 10 digital related alphabets were involved, an attempt would be made to determine what caused the aperiodicity. Eventually these investigations would lead to the fact that the 10 alphabets were used in order, and a statistical period determined. Among the hypotheses which might account for such a statistical period would be monome-dinome substitution.

Under a long additive for a superencipherment, the system would afford considerable security. It could, however, be solved, if sufficient depth were available to permit entry via the classic repeated differences attack, at which point the stripped text would be treated as above. The selection could be controlled by a key word, expressed as digits through the basic matrix, each digit selecting a matrix in turn. This would render part of the attack outlined above ineffective, but the entry via isomorphs would still obtain. Also, selection other than cyclical would no longer ensure monome flatness, and the roughness thus exhibited might suggest specific attacks. Isologs would be extremely vulnerable; indeed, most of the variations on related alphabet systems and the appropriate attacks relating to them are applicable to the basic system set forth here, with the modifications necessitated by the peculiarities of monome-dinome encipherment. A nasty version of this system would embrace a matrix with coordinate sequences selected from the ten rows of a Latin square, superenciphered by a long additive—we reserve judgment on this one.

b. The final paragraph in the article above mentions some of the "if's, and's, and but's," variations possible in the system. In any cryptosystem if the cryptography is too complicated, cipher clerks' errors are bound to arise, and it is often through these messages and their subsequent correction that entries may be made, particularly in a difficult system.

84. **Final remarks.**—a. Unlike the preceding two texts, because of space considerations this volume does not contain a glossary as one of its appendices. It is assumed that the reader has already acquired a basic technical vocabulary from a study of the first two texts; furthermore, new terms in this volume have been defined on their first occurrence and therefore should be absorbed during the course of systematic study. The reader may wish to resort to the NSA *Basic Cryptologic Glossary* (June 1971) to refresh his memory.

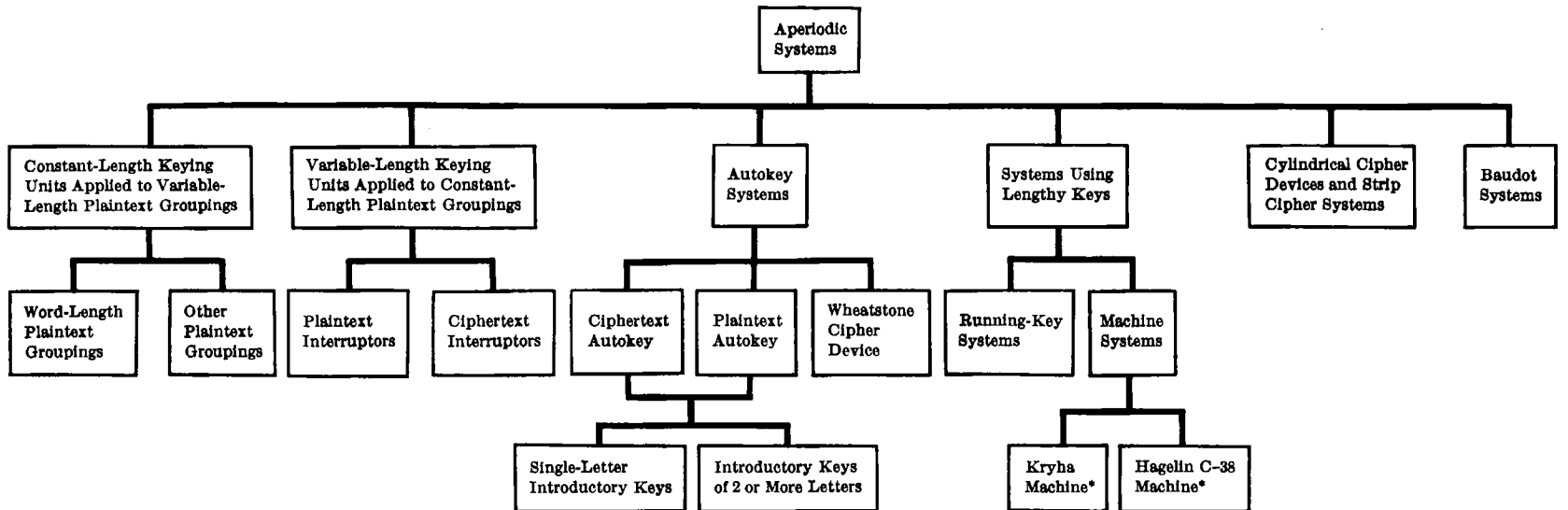
b. Four of the appendices have been included in order to enhance the usefulness of this volume as an operational reference manual. Appendix 3, "Tables of the Poisson distribution," and Appendix 4, "Table of the Binomial distribution for  $p = 1/10$ ," are of service in evaluating probabilities; Appendix 5, "Plain-text and random material for sampling purposes," will be found useful in certain experimenting and testing situations; and Appendix 6, "Basic letter frequency data, 24 foreign languages," shows the cryptolinguistic similarities and differences among monographic and digraphic frequencies of some major languages.

c. As was the case with the previous texts, mere reading of the methods of solution of the various types of cryptosystems covered in this volume is not enough to ensure complete understanding of the principles and techniques presented. It is therefore strongly recommended that the reader solve the problems contained in Appendix 7, "Problems—Military Cryptanalytics, Part III," as a means of acquiring facility and adroitness in the solution of aperiodic ciphers.

d. The formal portion of this text will be closed with a synoptic chart of cryptography found on the next page, continuing the series of charts established in the first volume, showing the relationships among the various cryptosystems treated in *Military Cryptanalytics, Part III*. This chart is a continuation of the chart on p. 318 of *Military Cryptanalytics Part II*, if we consider the present chart as an amplification of the box labelled "Aperiodic" in the previous chart.

---

FKUPK JYZVB NCJNC RCAVP XIIAI P



434

*Strictly speaking, these are periodic systems; but this classification is academic, since they are solved as if they were aperiodic systems.

Synoptic chart of cryptography for *Military Cryptanalytics, Part III*.

## APPENDICES

APPENDIX	Page
1. De Profundis; or the ABC of depth reading.....	437
2. Synoptic tables, Cipher Device M-94.....	447
3. Tables of the Poisson distribution.....	463
4. Table of the Binomial distribution for $p = 1/10$ .....	537
5. Plaintext and random material for sampling purposes.....	553
6. Basic letter frequency data, 24 foreign languages.....	561
7. Problems—Military Cryptanalytics, Part III.....	611
INDEX.....	653

## APPENDIX 1

**DE PROFUNDIS; OR THE ABC OF DEPTH READING**

This article, reprinted here with minor emendations, first appeared in the *NSA Technical Journal*, Vol. 2, No. 1. It is included here not only because it is a self-contained, concise explanation of the principles of depth reading in alphabetical, digital, and Baudot systems, but also because it is a particularly instructive example and model of how to write a lucid technical paper calculated to reach a majority of readers, especially including those who may not be versed in a subject under discussion.

DE PROFUNDIS; OR  
THE ABC OF DEPTH READING

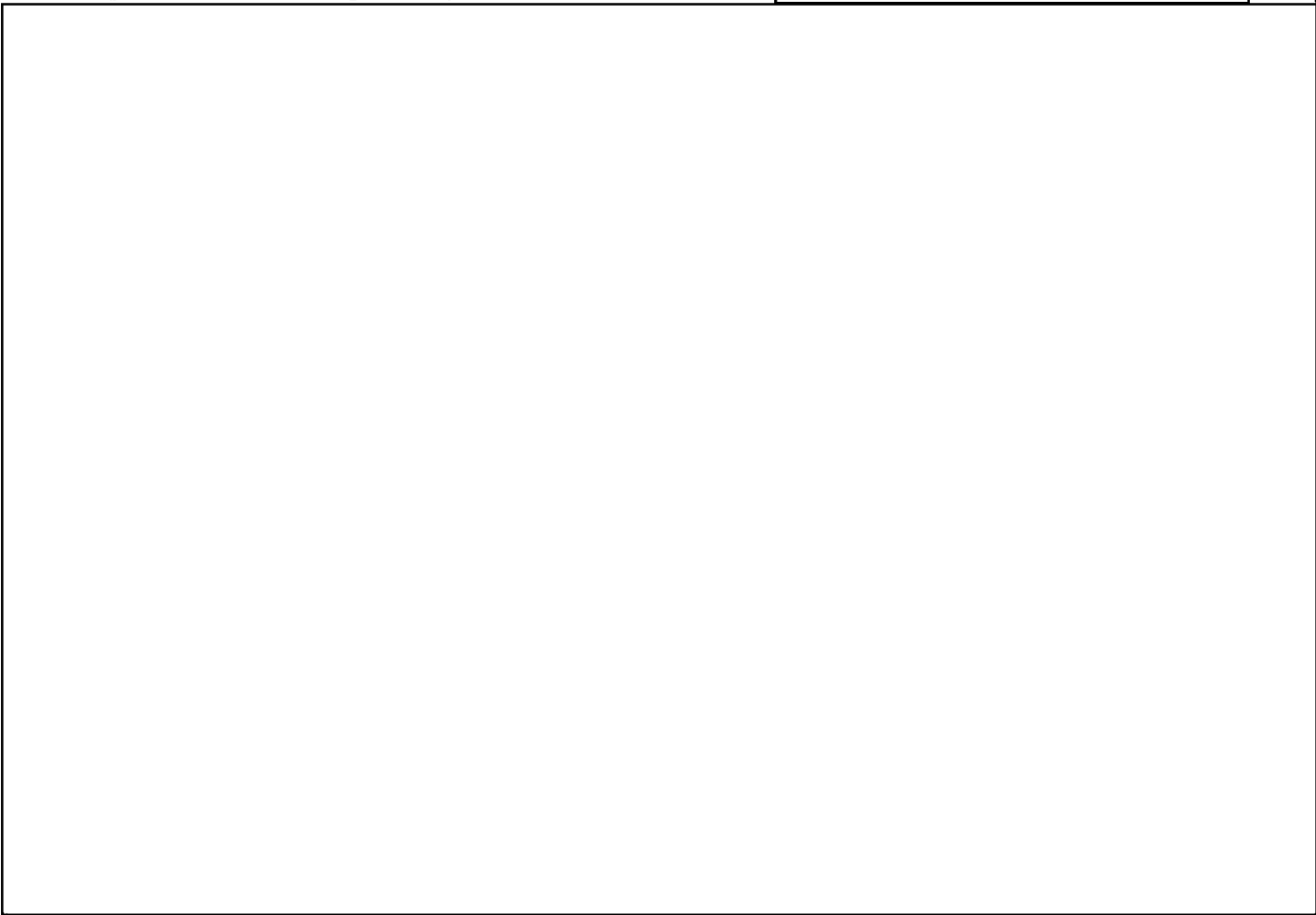
By Lambros D. Callimahos

(b) (1)  
(b) (3) -18 USC 798  
(b) (3) -50 USC 3024 (i)  
(b) (3) -P.L. 86-36

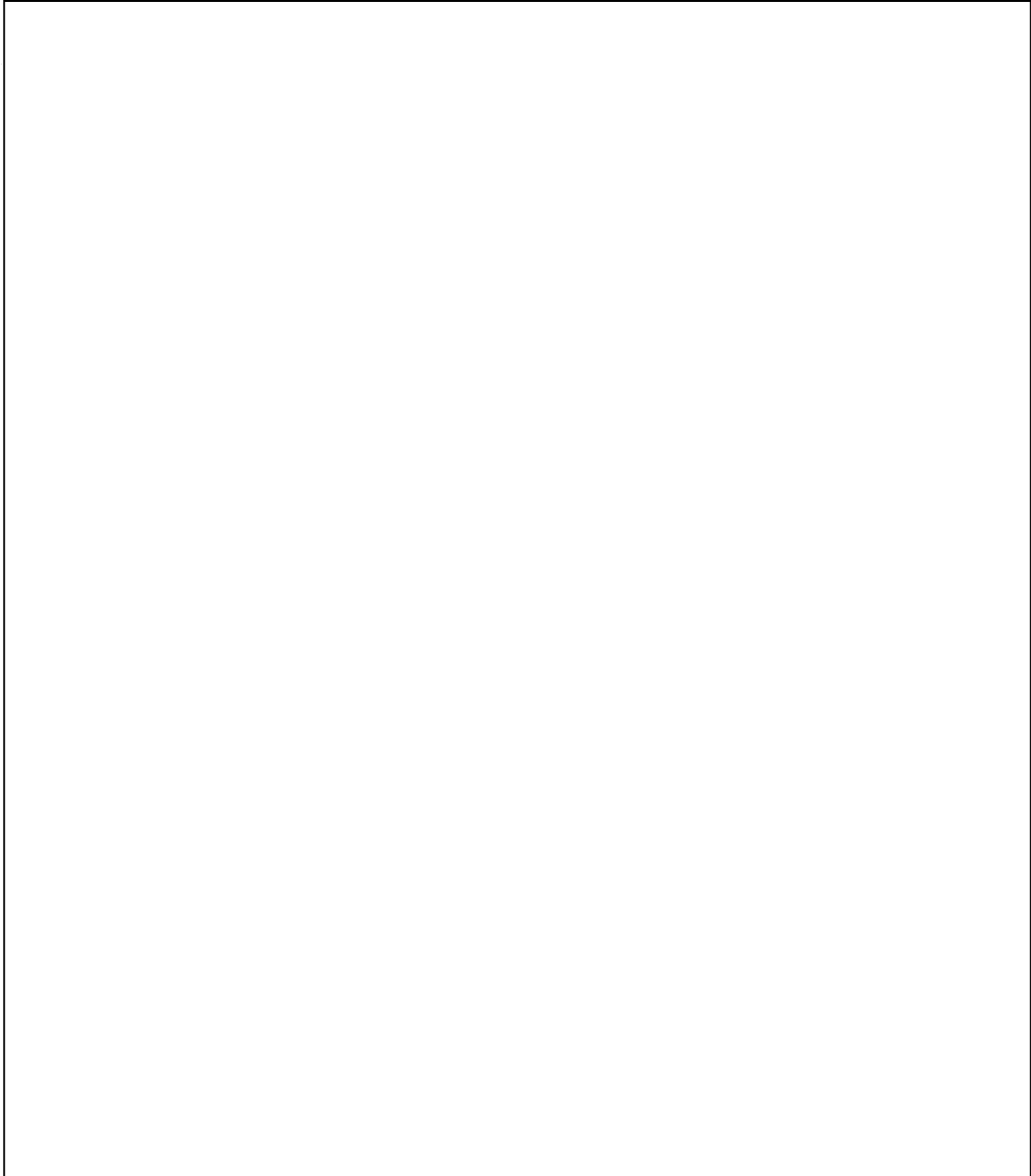
(A concise explanation of the principles of depth reading in alphabetical, digital, and Baudot systems.)

The Editor [of the *Technical Journal*] informs us that he is perpetually trying to cajole our engineers to write the ABC of this or that, in a fashion calculated to explain to the *nonengineer* the mysteries of black boxes; that is, produce articles intended to be basic introductions to something or other, explaining the obvious for the benefit of those of us to whom it is *not* obvious. Much to the Editor's surprise, one of these engineers buttonholed him, saying: "How about an article explaining what [redacted] Most engineers don't know." The Editor approached the writer; the writer, tit for tatting, borrowed the title from the engineers; what follows is, we hope, an answer to this request.

It is assumed that the reader has some idea of the concepts of letter frequencies of plain text.¹ We know that, for instance, the letters of English text have greatly varying frequencies, ranging from an E of 13% and a T of 9% to the group of letters JKQXZ whose combined individual frequencies sum to 1.4 per cent.² If English plain text is subjected to a simple monoalphabetic substitution, the ratios between the frequencies are not changed—only the *identities* of the letters; [redacted]

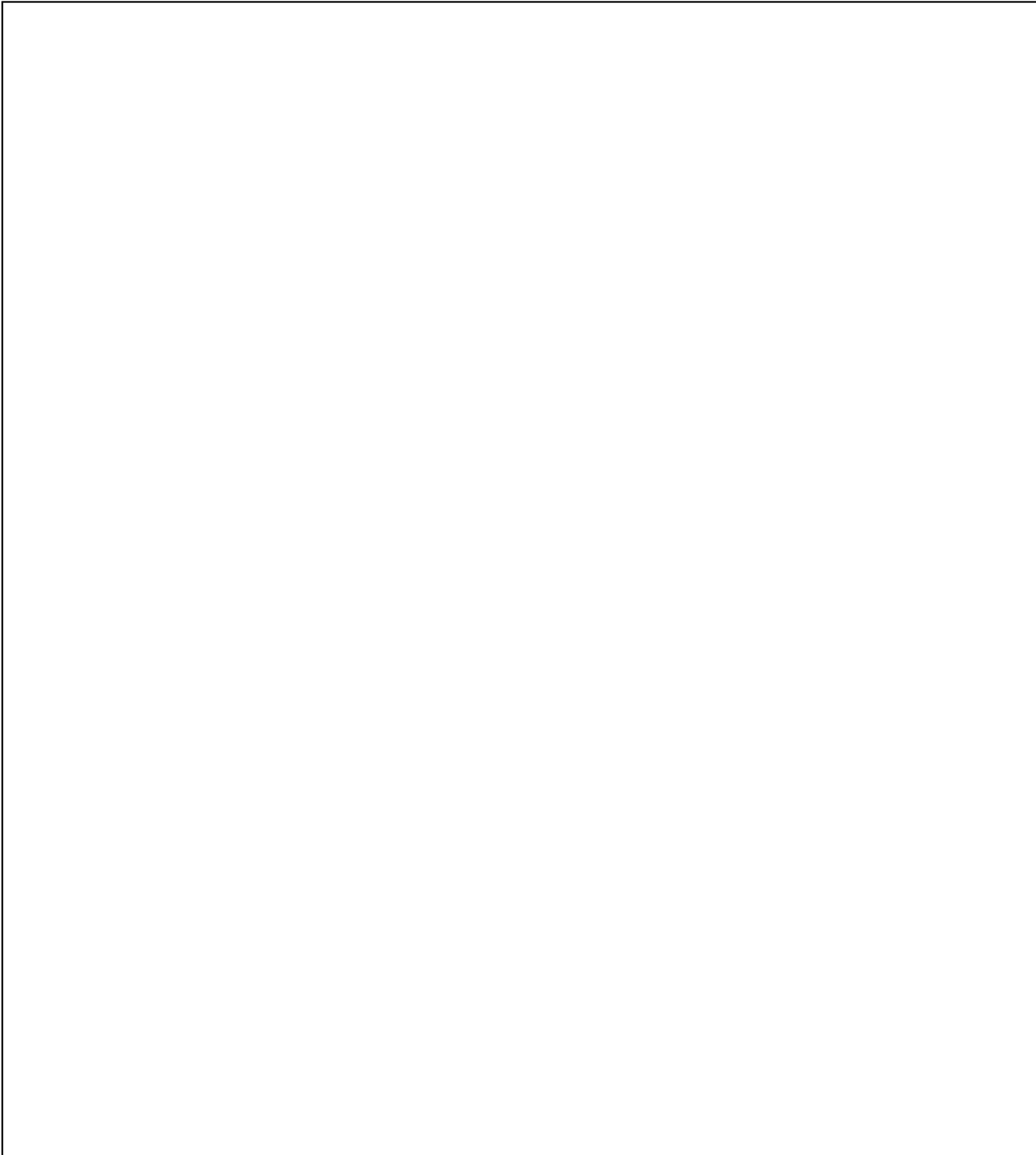






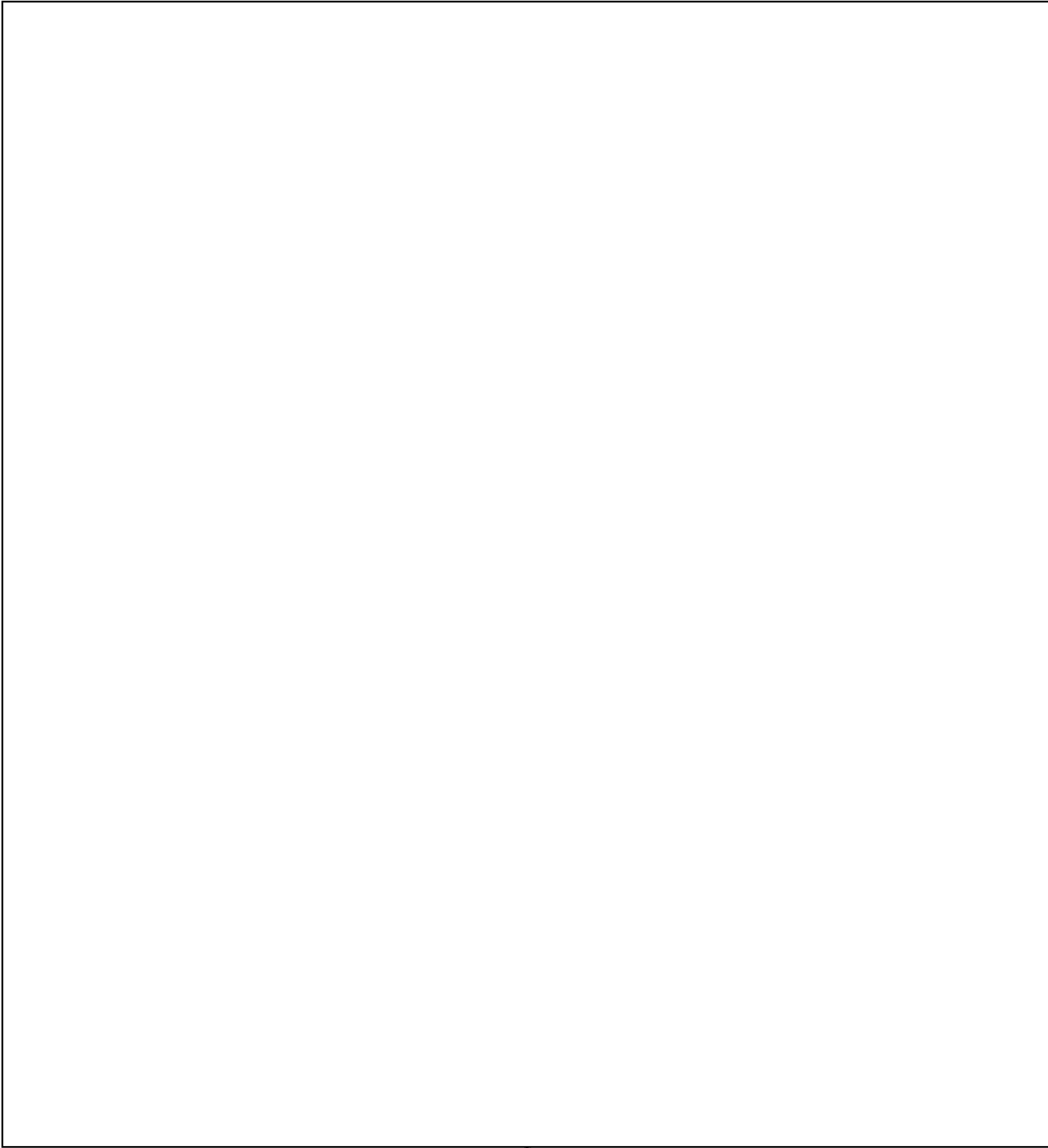
(b) (1)  
(b) (3)-18 USC 798  
(b) (3)-50 USC 3024(i)  
(b) (3)-P.L. 86-36

(b) (1)  
(b) (3)-18 USC 798  
(b) (3)-50 USC 3024(i)  
(b) (3)-P.L. 86-36

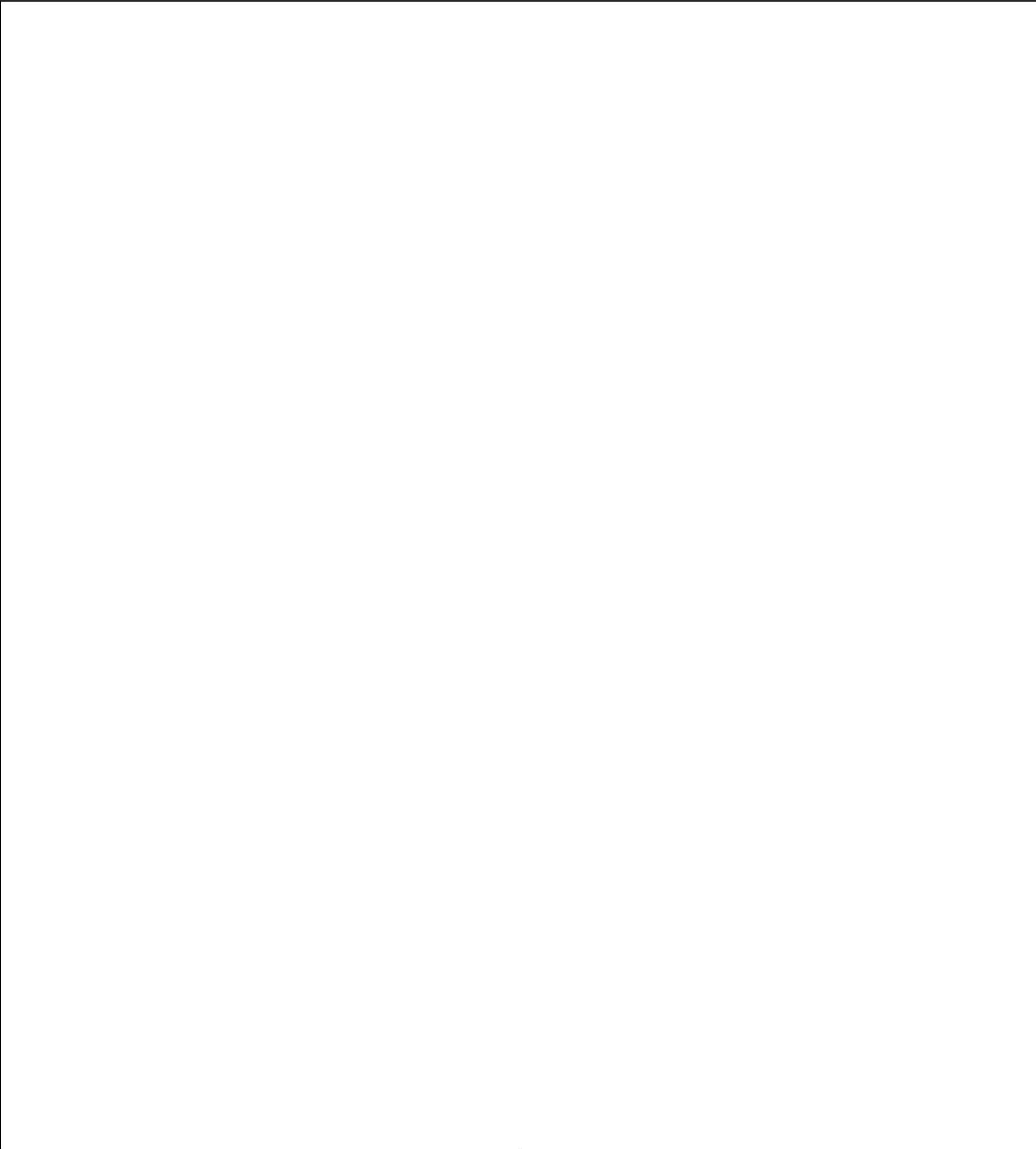


(b) (1)  
(b) (3)-18 USC 798  
(b) (3)-50 USC 3024(i)  
(b) (3)-P.L. 86-36

(b) (1)  
(b) (3)-18 USC 798  
(b) (3)-50 USC 3024 (i)  
(b) (3)-P.L. 86-36



(b) (1)  
(b) (3)-18 USC 798  
(b) (3)-50 USC 3024(i)  
(b) (3)-P.L. 86-36



(b) (1)  
(b) (3)-18 USC 798  
(b) (3)-50 USC 3024(i)  
(b) (3)-P.L. 86-36

-

APPENDIX 2  
**SYNOPTIC TABLES, CIPHER DEVICES M-94**

Synoptic Table for A

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25
0	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A
1	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
2	C	D	K	D	N	P	X	H	D	E	T	N	C	D	B	J	M	D	O	T	N	V	K	J	D
3	E	E	O	C	Q	O	J	P	S	L	M	F	J	W	V	N	Y	M	J	R	K	S	W	P	N
4	I	H	M	B	U	C	E	J	K	B	S	L	I	P	H	U	O	C	Y	Z	H	F	R	X	B
5	G	F	J	I	K	I	Z	O	Q	D	X	H	L	K	I	B	F	N	L	X	R	D	E	M	U
6	D	I	U	F	D	X	B	B	O	F	V	Q	D	J	Y	T	T	E	F	Q	G	L	V	V	H
7	J	J	B	G	O	L	N	W	I	J	Q	G	H	V	K	G	H	Q	X	L	O	I	D	K	Y
8	F	K	G	J	P	U	I	K	V	G	P	C	B	I	S	I	E	B	N	Y	X	E	T	B	F
9	V	T	E	H	I	R	K	C	T	H	N	U	M	U	G	M	U	O	G	I	E	B	U	Q	W
10	U	L	P	L	T	N	P	V	Z	O	O	J	K	Q	U	W	S	Z	W	O	Y	H	F	W	J
11	Y	M	H	K	J	D	V	F	E	N	H	T	G	H	E	Z	Z	P	H	V	B	K	O	U	L
12	M	O	S	M	B	Y	R	Z	F	M	U	B	X	Z	N	R	J	L	V	B	F	N	Y	G	V
13	H	U	C	R	R	Z	O	L	H	T	W	Y	U	C	T	V	X	G	C	P	S	R	H	L	G
14	T	V	Z	U	H	H	G	Q	G	P	D	P	Z	T	C	L	D	V	M	E	J	J	M	O	R
15	Q	Y	I	O	C	W	S	E	Y	R	I	Z	T	X	X	X	P	J	I	S	M	Q	L	S	C
16	K	G	N	Q	Y	B	Y	R	U	Q	Z	K	S	B	O	C	C	R	R	N	U	Z	S	T	Q
17	Z	Z	X	V	S	J	D	Y	N	S	Y	X	W	L	W	S	W	K	B	H	D	G	I	E	M
18	O	N	F	P	L	S	U	N	L	V	C	I	Q	E	F	H	G	Y	S	J	Q	M	Q	C	P
19	L	P	Y	T	W	Q	L	S	P	Z	G	S	Y	G	Q	D	Q	T	E	W	C	X	N	H	S
20	R	Q	Q	N	E	F	C	U	M	U	K	R	V	N	D	E	I	F	K	M	L	P	J	N	O
21	X	X	R	W	M	K	F	M	B	X	R	D	O	Y	R	O	B	U	U	D	Z	U	C	Z	E
22	S	R	T	Y	Z	V	M	G	X	Y	F	V	R	R	L	K	K	I	P	G	W	C	P	F	X
23	P	W	V	X	V	M	Q	T	W	W	B	E	P	S	J	F	L	W	D	F	T	O	G	R	T
24	W	S	W	Z	X	E	T	D	C	I	E	W	F	M	Z	P	N	X	Z	C	I	T	B	I	K
25	N	B	L	S	G	T	W	X	R	C	J	O	E	F	M	Y	V	H	Q	K	P	Y	Z	D	I

Synoptic Table for B

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25
0	B	B	B	B	B	B	B	B	B	B	B	B	B	B	B	B	B	B	B	B	B	B	B	B	B
1	C	A	G	I	R	J	N	W	X	D	E	Y	M	L	V	T	K	O	S	P	F	H	Z	Q	U
2	E	C	E	F	H	S	I	K	W	F	J	P	K	E	H	G	L	Z	E	E	S	K	A	W	H
3	I	D	P	G	C	Q	K	C	J	A	Z	G	G	I	I	N	P	K	S	J	N	X	U	Y	
4	G	E	H	J	Y	F	P	V	R	G	L	K	X	N	Y	M	V	L	U	N	M	R	K	G	F
5	D	H	S	H	S	K	V	F	A	H	T	X	U	Y	K	W	A	G	P	H	U	J	W	L	W
6	J	F	C	L	L	V	R	Z	J	O	M	I	Z	R	S	Z	R	V	D	J	D	Q	R	O	J
7	F	I	Z	K	W	M	O	L	D	N	S	S	T	S	G	R	M	J	Z	W	Q	Z	E	S	L
8	V	J	I	M	E	E	G	Q	S	M	X	R	S	M	U	V	Y	R	Q	M	C	G	V	T	V
9	U	K	N	R	M	T	S	E	K	T	V	D	W	F	E	L	O	K	A	D	L	M	D	E	G
10	Y	T	X	U	Z	A	Y	R	Q	P	Q	V	Q	A	N	X	F	Y	T	G	Z	X	T	C	R
11	M	L	F	O	V	G	D	Y	O	R	P	E	Y	O	T	C	T	T	O	F	W	P	U	H	C
12	H	M	Y	Q	X	P	U	N	I	Q	N	W	V	D	C	S	H	F	J	C	T	U	F	N	Q
13	T	O	Q	V	G	O	L	S	V	S	O	O	O	W	X	H	E	U	Y	K	I	C	O	Z	M
14	Q	U	R	P	A	C	C	U	T	V	H	A	R	P	O	D	U	I	L	A	P	O	Y	F	P
15	K	V	T	T	F	I	F	M	Z	Z	U	M	P	K	W	E	S	W	F	U	A	T	H	R	S
16	Z	Y	V	N	N	X	M	G	E	U	W	N	F	J	F	O	Z	X	X	T	V	Y	M	I	O
17	O	G	W	W	Q	L	Q	T	F	X	D	F	E	V	Q	K	J	H	N	R	N	A	L	D	E
18	L	Z	L	Y	U	U	T	D	H	Y	I	L	A	I	D	F	X	A	G	Z	K	W	S	A	X
19	R	N	A	X	K	R	W	X	G	W	Z	H	N	U	R	P	D	S	W	X	H	V	I	Y	T
20	X	P	D	Z	D	N	A	A	Y	I	Y	Q	C	Q	L	Y	P	D	H	Q	R	S	Q	J	K
21	S	Q	K	S	O	D	H	I	U	C	C	G	J	H	J	A	C	M	V	L	G	F	N	P	I
22	P	X	O	A	P	Y	X	H	N	A	G	C	I	Z	Z	Q	W	C	C	Y	O	D	J	X	A
23	W	R	M	E	I	Z	J	P	L	K	K	U	L	C	M	J	G	N	M	I	X	L	C	M	Z
24	N	W	J	D	T	H	E	J	P	E	R	J	D	T	A	N	Q	E	I	O	E	I	P	V	D
25	A	S	U	C	J	W	Z	O	M	L	F	T	H	X	P	U	I	Q	R	V	Y	E	G	K	N



Synoptic Table for C

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25
0	C	C	C	C	C	C	C	C	C	C	C	C	C	C	C	C	C	C	C	C	C	C	C	C	C
1	E	D	Z	B	Y	I	F	V	R	A	G	U	J	T	X	S	W	N	M	K	L	O	P	H	Q
2	I	E	I	I	S	X	M	F	A	K	K	J	I	X	O	H	G	E	I	A	Z	T	G	N	M
3	G	H	N	F	L	L	Q	Z	J	E	R	T	L	B	W	D	Q	Q	R	U	W	Y	B	Z	P
4	D	F	X	G	W	U	T	L	D	L	F	B	D	L	F	E	I	B	B	T	T	A	Z	F	S
5	J	I	F	J	E	R	W	Q	S	B	B	Y	H	E	Q	O	B	O	S	R	I	W	A	R	O
6	F	J	Y	H	M	N	A	E	K	D	E	P	B	G	D	K	K	Z	E	Z	P	V	X	I	E
7	V	K	Q	L	Z	D	H	R	Q	F	J	Z	M	N	R	F	L	P	K	X	A	S	K	D	X
8	U	T	R	K	V	Y	X	Y	O	J	A	K	K	Y	L	P	N	L	U	Q	V	F	W	A	T
9	Y	L	T	M	X	Z	J	N	I	G	L	X	G	R	J	Y	V	G	P	L	N	D	R	Y	K
10	M	M	V	R	G	H	E	S	V	H	T	I	X	S	Z	A	A	V	D	Y	K	L	E	J	I
11	H	O	W	U	A	W	Z	U	T	O	M	S	U	M	M	Q	R	J	Z	I	H	I	V	P	A
12	T	U	L	O	F	B	B	M	Z	N	S	R	Z	F	A	J	M	R	Q	O	R	E	D	X	Z
13	Q	V	A	Q	N	J	N	G	E	M	X	D	T	A	P	N	Y	K	A	V	G	B	T	M	D
14	K	Y	D	V	Q	S	I	T	F	T	V	V	S	O	B	U	O	Y	T	B	O	H	U	V	N
15	Z	G	K	P	U	Q	K	D	H	P	Q	E	W	D	V	B	F	T	O	P	X	K	F	K	B
16	O	Z	O	T	K	F	P	X	G	R	P	W	Q	W	H	T	T	F	J	E	E	N	O	B	U
17	L	N	M	N	D	K	V	A	Y	Q	N	O	Y	P	I	G	H	U	Y	S	Y	R	Y	Q	H
18	R	P	J	W	O	V	R	I	U	S	O	A	V	K	Y	I	E	I	L	N	B	J	H	W	Y
19	X	Q	U	Y	P	M	O	H	N	V	H	M	O	J	K	M	U	W	F	H	F	Q	M	U	F
20	S	X	B	X	I	E	G	P	L	Z	U	N	R	V	S	W	S	X	X	J	S	Z	L	G	W
21	P	R	G	Z	T	T	S	J	P	U	W	F	P	I	G	Z	Z	H	N	W	J	G	S	L	J
22	W	W	E	S	J	A	Y	O	M	X	D	L	F	U	U	R	J	A	G	M	M	M	I	O	L
23	N	S	P	A	B	G	D	B	B	Y	I	H	E	Q	E	V	X	S	W	D	U	X	Q	S	V
24	A	B	H	E	R	P	U	W	X	W	Z	Q	A	H	N	L	D	D	H	G	D	P	N	T	G
25	B	A	S	D	H	O	L	K	W	I	Y	G	N	Z	T	X	P	M	V	F	Q	U	J	E	R

Synoptic Table for D

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25
0	D	D	D	D	D	D	D	D	D	D	D	D	D	D	D	D	D	D	D	D	D	D	D	D	D
1	J	E	K	C	O	Y	U	X	S	F	I	V	H	W	R	E	P	M	Z	G	Q	L	T	A	N
2	F	H	O	B	P	Z	L	A	K	J	Z	E	B	P	L	O	C	C	Q	F	C	I	U	Y	B
3	V	F	M	I	I	H	C	I	Q	G	Y	W	M	K	J	K	W	N	A	C	L	E	F	J	U
4	U	I	J	F	T	W	F	H	O	H	C	O	K	J	Z	F	G	E	T	K	Z	B	O	P	H
5	Y	J	U	G	J	B	M	P	I	O	G	A	G	V	M	P	Q	Q	O	A	W	H	Y	X	Y
6	M	K	B	J	B	J	Q	J	V	N	K	M	X	I	A	Y	I	B	J	U	T	K	H	M	F
7	H	T	G	H	R	S	T	O	T	M	R	N	U	U	P	A	B	O	Y	T	I	N	M	V	W
8	T	L	E	L	H	Q	W	B	Z	T	F	F	Z	Q	B	Q	K	Z	L	R	P	R	L	K	J
9	Q	M	P	K	C	F	A	W	E	P	B	L	T	H	V	J	L	P	F	Z	A	J	S	B	L
10	K	O	H	M	Y	K	H	K	F	R	E	H	S	Z	H	N	N	L	X	X	V	Q	I	Q	V
11	Z	U	S	R	S	V	X	C	H	Q	J	Q	W	C	I	U	V	G	N	Q	N	Z	Q	W	G
12	O	V	C	U	L	M	J	V	G	S	A	G	Q	T	Y	B	A	V	G	L	K	G	N	U	R
13	L	Y	Z	O	W	E	E	F	Y	V	L	C	Y	X	K	T	R	J	W	Y	H	M	J	G	C
14	R	G	I	Q	E	T	Z	Z	U	Z	T	U	V	B	S	G	M	R	H	I	R	X	C	L	Q
15	X	Z	N	V	M	A	B	L	N	U	M	J	O	L	G	I	Y	K	V	O	G	P	P	O	M
16	S	N	X	P	Z	G	N	Q	L	X	S	T	R	E	U	M	O	Y	C	V	O	U	G	S	P
17	P	P	F	T	V	P	I	E	P	Y	X	B	P	G	E	W	F	T	M	B	X	C	B	T	S
18	W	Q	Y	N	X	O	K	R	M	W	V	Y	F	N	N	Z	T	F	I	P	E	O	Z	E	O
19	N	X	Q	W	G	C	P	Y	B	I	Q	P	E	Y	T	R	H	U	R	E	Y	T	A	C	E
20	A	R	R	Y	A	I	V	N	X	C	P	Z	A	R	C	V	E	I	B	S	B	Y	X	H	X
21	B	W	T	X	F	X	R	S	W	A	N	K	N	S	X	L	U	W	S	N	F	A	K	N	T
22	C	S	V	Z	N	L	O	U	C	K	O	X	C	M	O	X	S	X	E	H	S	W	W	Z	K
23	E	B	V	S	Q	U	G	M	R	E	H	I	J	F	W	C	Z	H	K	J	J	V	R	F	I
24	I	A	L	A	U	R	S	G	A	L	U	S	I	A	F	S	J	A	U	W	M	S	E	R	A
25	G	C	A	E	K	N	Y	T	J	B	W	R	L	O	Q	H	X	S	P	M	U	F	V	I	Z

Synoptic Table for E

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25
0	E	E	E	E	E	E	E	E	E	E	E	E	E	E	E	E	E	E	E	E	E	E	E	E	E
1	I	H	P	D	M	T	Z	R	F	L	J	W	A	G	N	O	U	Q	K	S	Y	B	V	C	X
2	G	F	H	C	Z	A	B	Y	H	B	A	O	N	N	T	K	S	B	U	N	B	H	D	H	T
3	D	I	S	B	V	G	N	N	G	D	L	A	C	Y	C	F	Z	O	P	H	F	K	T	N	K
4	J	J	C	I	X	P	I	S	Y	F	T	M	J	R	X	P	J	Z	D	J	S	N	U	Z	I
5	F	K	Z	F	G	O	K	U	U	J	M	N	I	S	O	Y	X	P	Z	W	J	R	F	F	A
6	V	T	I	G	A	C	P	M	N	G	S	F	L	M	W	A	D	L	Q	M	M	J	O	R	Z
7	U	L	N	J	F	I	V	G	L	H	X	L	D	F	F	Q	P	G	A	D	U	Q	Y	I	D
8	Y	M	X	H	N	X	R	T	P	O	V	H	H	A	Q	J	C	V	T	G	D	Z	H	D	N
9	M	O	F	L	Q	L	O	D	M	N	Q	Q	B	O	D	N	W	J	O	F	Q	G	M	A	B
10	H	U	Y	K	U	G	X	B	M	P	G	M	D	R	U	G	R	J	C	C	M	L	Y	U	
11	T	V	Q	M	K	R	S	A	X	T	N	C	K	W	L	B	Q	K	Y	K	L	X	S	J	H
12	Q	Y	R	R	D	N	Y	I	W	P	O	U	G	P	J	T	I	Y	L	A	Z	P	I	P	Y
13	K	G	T	U	O	D	D	H	C	R	H	J	X	K	Z	G	B	T	F	U	W	U	Q	X	F
14	Z	Z	V	O	P	Y	U	P	R	Q	U	T	U	J	M	I	K	F	X	T	T	C	N	M	W
15	O	N	W	Q	I	Z	L	J	A	S	W	B	Z	V	A	M	L	U	N	R	I	O	J	V	J
16	L	P	L	V	T	H	C	O	J	V	D	Y	T	I	P	W	N	I	G	Z	P	T	C	K	L
17	R	Q	A	P	J	W	F	B	D	Z	I	P	S	U	B	Z	V	W	W	X	A	Y	P	B	V
18	X	X	D	T	B	B	M	W	S	U	Z	Z	W	Q	V	R	A	X	H	Q	V	A	G	Q	G
19	S	R	K	N	R	J	Q	K	K	X	Y	K	Q	H	H	V	R	H	V	L	N	W	B	W	R
20	P	W	O	W	H	S	T	C	Q	Y	C	X	Y	Z	I	L	M	A	C	Y	K	V	Z	U	C
21	P	S	M	Y	C	Q	W	V	O	W	G	I	V	C	Y	X	Y	S	M	I	H	S	A	G	Q
22	N	B	J	X	Y	F	A	F	I	I	K	S	O	T	K	C	O	D	I	O	R	F	X	L	M
23	A	A	U	Z	S	K	H	Z	V	C	R	R	R	X	S	S	F	M	R	V	G	D	K	O	P
24	B	C	B	S	L	V	X	L	T	A	F	D	P	B	G	H	T	C	B	B	O	L	W	S	S
25	C	D	G	A	W	M	J	Q	Z	K	B	V	F	L	U	D	H	N	S	P	X	I	R	T	O

Synoptic Table for F

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	
0	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	
1	V	I	Y	G	N	K	M	Z	H	J	B	L	E	A	Q	P	T	U	X	C	S	D	O	R	W	
2	U	J	Q	J	Q	V	Q	L	G	G	E	H	A	O	D	Y	H	I	N	K	J	L	Y	I	J	
3	Y	K	R	H	U	M	T	Q	Y	H	J	Q	N	D	R	A	E	W	G	A	M	I	H	D	L	
4	M	T	T	L	K	E	W	E	U	O	A	G	C	W	L	Q	U	X	W	U	U	E	M	A	V	
5	H	L	V	K	D	T	A	R	N	N	L	C	J	P	J	J	S	H	H	T	D	B	L	Y	G	
6	T	M	W	M	O	A	H	Y	L	M	T	U	I	K	Z	N	Z	A	V	R	Q	H	S	J	R	
7	Q	O	L	R	P	G	X	N	P	T	M	J	L	J	M	U	J	S	C	Z	C	K	I	P	C	
8	K	U	A	U	I	P	J	S	M	P	S	T	D	V	A	B	X	D	M	X	L	N	Q	X	Q	
9	Z	V	D	O	T	O	E	U	B	R	X	B	H	I	P	T	D	M	I	Q	Z	R	N	M	M	
10	O	Y	K	Q	J	C	Z	M	X	Q	V	Y	B	U	B	G	P	C	R	L	W	J	J	V	P	
11	L	G	O	V	B	I	B	G	W	S	Q	P	M	Q	V	I	C	N	B	Y	T	Q	C	K	S	
12	R	Z	M	P	R	X	N	T	C	V	P	Z	K	H	H	M	W	E	S	I	I	Z	P	B	O	
13	X	N	J	T	H	L	I	D	R	Z	N	K	G	Z	I	W	G	Q	E	O	P	G	G	Q	E	
14	S	P	U	N	C	U	K	X	A	U	O	X	X	C	Y	Z	Q	B	K	V	A	M	B	W	X	
15	P	Q	B	W	Y	R	P	A	J	X	H	I	U	T	K	R	I	O	U	B	V	X	Z	U	T	
16	W	X	G	Y	S	N	V	I	D	Y	U	S	Z	X	S	V	B	Z	P	P	N	P	A	G	K	
17	N	R	E	X	L	D	R	H	S	W	W	R	T	B	G	L	K	P	D	E	K	U	X	L	I	
18	A	W	P	Z	W	Y	O	P	K	I	D	D	S	L	U	X	L	L	Z	S	H	C	K	O	A	
19	B	S	H	S	E	Z	G	J	Q	C	I	V	W	E	E	C	N	G	Q	N	R	O	W	S	Z	
20	C	B	S	A	M	H	S	O	O	A	Z	E	Q	G	N	S	V	V	A	H	G	T	R	T	D	
21	E	A	C	E	Z	W	Y	B	I	K	Y	W	Y	N	T	H	A	J	T	J	O	Y	E	E	N	
22	I	C	Z	D	V	B	D	W	V	E	C	O	V	Y	C	D	R	R	O	W	X	A	V	C	B	
23	G	D	I	C	X	J	U	K	T	L	G	A	O	R	X	E	M	K	J	M	E	W	D	H	U	
24	D	E	N	B	G	S	L	C	Z	B	K	M	R	S	O	O	Y	Y	D	Y	D	Y	V	T	N	H
25	J	H	X	I	A	Q	C	V	E	D	R	N	P	M	W	K	O	T	L	G	B	S	U	Z	Y	

Synoptic Table for G

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25
0	G	G	G	G	G	G	G	G	G	G	G	G	G	G	G	G	G	G	G	G	G	G	G	G	G
1	D	Z	E	J	A	P	S	T	Y	H	K	C	X	N	U	I	Q	V	W	F	O	M	B	L	R
2	J	N	P	H	F	O	Y	D	U	O	R	U	U	Y	E	M	I	J	H	C	X	X	Z	O	C
3	F	P	H	L	N	C	D	X	N	N	F	J	Z	R	N	W	B	R	V	K	E	P	A	S	Q
4	V	Q	S	K	Q	I	U	A	L	M	B	T	T	S	T	Z	K	K	C	A	Y	U	X	T	M
5	U	X	C	M	U	X	L	I	P	T	E	B	S	M	C	R	L	Y	M	U	B	C	K	E	P
6	Y	R	Z	R	K	L	C	H	M	P	J	Y	W	F	X	V	N	T	I	T	F	O	W	C	S
7	M	W	I	U	D	U	F	P	B	R	A	P	Q	A	O	L	V	F	R	R	S	T	R	H	O
8	H	S	N	O	O	R	M	J	X	Q	L	Z	Y	O	W	X	A	U	B	Z	J	Y	E	N	E
9	T	B	X	Q	P	N	Q	O	W	S	T	K	V	D	F	C	R	I	S	X	M	A	V	Z	X
10	Q	A	F	V	I	D	T	B	C	V	M	X	O	W	Q	S	M	W	E	Q	U	W	D	F	T
11	K	C	Y	P	T	Y	W	W	R	Z	S	I	R	P	D	H	Y	X	K	L	D	V	T	R	K
12	Z	D	Q	T	J	Z	A	K	A	U	X	S	P	K	R	D	O	H	U	Y	Q	S	U	I	I
13	O	E	R	N	B	H	H	C	J	X	V	R	F	J	L	E	F	A	P	I	C	F	F	D	A
14	L	H	T	W	R	W	X	V	D	Y	Q	D	E	V	J	O	T	S	D	O	L	D	O	A	Z
15	R	F	V	Y	H	B	J	F	S	W	P	V	A	I	Z	K	H	D	Z	V	Z	L	Y	Y	D
16	X	I	W	X	C	J	E	Z	K	I	N	E	N	U	M	F	E	M	Q	B	W	I	H	J	N
17	S	J	L	Z	Y	S	Z	L	Q	C	O	W	C	Q	A	P	U	C	A	P	T	E	M	P	B
18	P	K	A	S	S	Q	B	Q	O	A	H	O	J	H	P	Y	S	N	T	E	I	B	L	X	U
19	W	T	D	A	L	F	N	E	I	K	U	A	I	Z	B	A	Z	E	O	S	P	H	S	M	H
20	N	L	K	E	W	K	I	R	V	E	W	M	L	C	V	Q	J	Q	J	N	A	K	I	V	Y
21	A	M	O	D	E	V	K	Y	T	L	D	N	D	T	H	J	X	B	Y	H	V	N	Q	K	F
22	B	O	M	C	M	M	P	N	Z	B	I	F	H	X	I	N	D	O	L	J	N	R	N	B	W
23	C	U	J	B	Z	E	V	S	E	D	Z	L	B	B	Y	U	P	Z	F	W	K	J	J	Q	J
24	E	V	U	I	V	T	R	U	F	F	Y	H	M	L	K	B	C	P	X	M	H	Q	C	W	L
25	I	Y	B	F	X	A	O	M	H	J	C	Q	K	E	S	T	W	L	N	D	R	Z	P	U	V

Synoptic Table for H

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25
0	H	H	H	H	H	H	H	H	H	H	H	H	H	H	H	H	H	H	H	H	H	H	H	H	H
1	T	F	S	L	C	W	X	P	G	O	U	Q	B	Z	I	D	E	A	V	J	R	K	M	N	Y
2	Q	I	C	K	Y	B	J	J	Y	N	W	G	M	C	Y	E	U	S	C	W	G	N	L	Z	F
3	K	J	Z	M	S	J	E	O	U	M	D	C	K	T	K	O	S	D	M	M	O	R	S	F	W
4	Z	K	I	R	L	S	Z	B	N	T	I	U	G	X	S	K	Z	M	I	D	X	J	I	R	J
5	O	T	N	U	W	Q	B	W	L	P	Z	J	X	B	G	F	J	C	R	G	E	Q	Q	I	L
6	L	L	X	O	E	F	N	K	P	R	Y	T	U	L	U	P	X	N	B	F	Y	Z	N	D	V
7	R	M	F	Q	M	K	I	C	M	Q	C	B	Z	E	E	Y	D	E	S	C	B	G	J	A	G
8	X	O	Y	V	Z	V	K	V	B	S	G	Y	T	G	N	A	P	Q	E	K	F	M	C	Y	R
9	S	U	Q	P	V	M	P	F	X	V	K	P	S	N	T	Q	C	B	K	A	S	X	P	J	C
10	P	V	R	T	X	E	V	Z	W	Z	R	Z	W	Y	C	J	W	O	U	U	J	P	G	P	Q
11	W	Y	T	N	G	T	R	L	C	U	F	K	Q	R	X	N	G	Z	P	T	M	U	B	X	M
12	N	G	V	W	A	A	O	Q	R	X	B	X	Y	S	O	U	Q	P	D	R	U	C	Z	M	P
13	A	Z	W	Y	F	G	G	E	A	Y	E	I	V	M	W	B	I	L	Z	Z	D	O	A	V	S
14	B	N	L	X	N	P	S	R	J	W	J	S	O	F	F	T	B	G	Q	X	Q	T	X	K	O
15	C	P	A	Z	Q	O	Y	Y	D	I	A	R	R	A	Q	G	K	V	A	Q	C	Y	K	B	E
16	E	Q	D	S	U	C	D	N	S	C	L	D	P	O	D	I	L	J	T	L	L	A	W	Q	X
17	I	X	K	A	K	I	U	S	K	A	T	V	F	D	R	M	N	R	O	Y	Z	W	R	W	T
18	G	R	O	E	D	X	L	U	Q	K	M	E	E	W	L	W	V	K	J	I	W	V	E	U	K
19	D	W	M	D	O	L	C	M	O	E	S	W	A	P	J	Z	A	Y	Y	O	T	S	V	G	I
20	J	S	J	C	P	U	F	G	I	L	X	O	N	K	Z	R	R	T	L	V	I	F	D	L	A
21	F	B	U	B	I	R	M	T	V	B	V	A	C	J	M	V	M	F	F	B	P	D	T	O	Z
22	V	A	B	I	T	N	Q	D	T	D	Q	M	J	V	A	L	Y	U	X	P	A	L	U	S	D
23	U	C	G	F	J	D	T	X	Z	F	P	N	I	I	P	X	O	I	N	E	V	I	F	T	N
24	Y	D	E	G	B	Y	W	A	E	J	N	F	L	U	B	C	F	W	G	S	N	E	O	E	B
25	M	E	P	J	R	Z	A	I	F	G	O	L	D	Q	V	S	T	X	W	N	K	B	Y	C	U

Synoptic Table for I

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25
0	I	I	I	I	I	I	I	I	I	I	I	I	I	I	I	I	I	I	I	I	I	I	I	I	I
1	G	J	N	F	T	X	K	H	V	C	Z	S	L	U	Y	M	B	W	R	O	P	E	Q	D	A
2	D	K	X	G	J	L	P	P	T	A	Y	R	D	Q	K	W	K	X	B	V	A	B	N	A	Z
3	J	T	F	J	B	U	V	J	Z	K	C	D	H	H	S	Z	L	H	S	B	V	H	J	Y	D
4	F	L	Y	H	R	R	R	O	E	E	G	V	B	Z	G	R	N	A	E	P	N	K	C	J	N
5	V	M	Q	L	H	N	O	B	F	L	K	E	M	C	U	V	V	S	K	E	K	N	P	P	B
6	U	O	R	K	C	D	G	W	H	B	R	W	K	T	E	L	A	D	U	S	H	R	G	X	U
7	Y	U	T	M	Y	Y	S	K	G	D	F	O	G	X	N	X	R	M	P	N	R	J	B	M	H
8	M	V	V	R	S	Z	Y	C	Y	F	B	A	X	B	T	C	M	C	D	H	G	Q	Z	V	Y
9	H	Y	W	U	L	H	D	V	U	J	E	M	U	L	C	S	Y	N	Z	J	O	Z	A	K	F
10	T	G	L	O	W	W	U	F	N	G	J	N	Z	E	X	H	O	E	Q	W	X	G	X	B	W
11	Q	Z	A	Q	E	B	L	Z	L	H	A	F	T	G	O	D	F	Q	A	M	E	M	K	Q	J
12	K	N	D	V	M	J	C	L	P	O	L	L	S	N	W	E	T	B	T	D	Y	X	W	W	L
13	Z	P	K	P	Z	S	F	Q	M	N	T	H	W	Y	F	O	H	O	O	G	B	P	R	U	V
14	O	Q	O	T	V	Q	M	E	B	M	M	Q	Q	R	Q	K	E	Z	J	F	F	U	E	G	G
15	L	X	M	N	X	F	Q	R	X	T	S	G	Y	S	D	F	U	P	Y	C	S	C	V	L	R
16	R	R	J	W	G	K	T	Y	W	P	X	C	V	M	R	P	S	L	L	K	J	O	D	O	C
17	X	W	U	Y	A	V	W	N	C	R	V	U	O	F	L	Y	Z	G	F	A	M	T	T	S	Q
18	S	S	B	X	F	M	A	S	R	Q	Q	J	R	A	J	A	J	V	X	U	U	Y	U	T	M
19	P	B	G	Z	N	E	H	U	A	S	P	T	P	O	Z	Q	X	J	N	T	D	A	F	E	P
20	W	A	E	S	Q	T	X	M	J	V	N	B	F	D	M	J	D	R	G	R	Q	W	O	C	S
21	N	C	P	A	U	A	J	G	D	Z	O	Y	E	W	A	N	P	K	W	Z	C	V	Y	H	O
22	A	D	H	E	K	G	E	T	S	U	H	P	A	P	P	U	C	Y	H	X	L	S	H	N	E
23	B	E	S	D	D	P	Z	D	K	X	U	Z	N	K	B	B	W	T	V	Q	Z	F	M	Z	X
24	C	H	C	C	O	O	B	X	Q	Y	W	K	C	J	V	T	G	F	C	L	W	D	L	F	T
25	E	F	Z	B	P	C	N	A	O	W	D	X	J	V	H	G	Q	U	M	Y	T	L	S	R	K

Synoptic Table for J

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25
0	J	J	J	J	J	J	J	J	J	J	J	J	J	J	J	J	J	J	J	J	J	J	J	J	J
1	F	K	U	H	B	S	E	O	D	G	A	T	I	V	Z	N	X	R	Y	W	M	Q	C	P	L
2	V	T	B	L	R	Q	Z	B	S	H	L	B	L	I	M	U	D	K	L	M	U	Z	P	X	V
3	U	L	G	K	H	F	B	W	K	O	T	Y	D	U	A	B	P	Y	F	D	D	G	G	M	G
4	Y	M	E	M	C	K	N	K	Q	N	M	P	H	Q	P	T	C	T	X	G	Q	M	B	V	R
5	M	O	P	R	Y	V	I	C	O	M	S	Z	B	H	B	G	W	F	N	F	C	X	Z	K	C
6	H	U	H	Y	S	M	K	V	I	T	X	K	M	Z	V	I	G	U	G	C	L	P	A	B	Q
7	T	V	S	O	L	E	P	F	V	P	V	X	K	C	H	M	Q	I	W	K	Z	U	X	Q	M
8	Q	Y	C	Q	W	T	V	Z	T	R	Q	I	G	T	I	W	I	W	H	A	W	C	K	W	P
9	K	G	Z	V	E	A	R	L	Z	Q	P	S	X	Y	Z	B	X	V	U	T	O	W	U	S	
10	Z	Z	I	P	M	G	O	Q	E	S	N	R	U	B	K	R	K	H	C	T	I	T	R	G	O
11	O	N	N	T	Z	P	G	E	F	V	O	D	Z	L	S	V	L	A	M	R	P	Y	E	L	E
12	L	P	X	N	V	O	S	R	H	Z	H	V	T	E	G	L	N	S	I	Z	A	A	V	O	X
13	R	Q	F	W	X	C	Y	Y	G	U	U	E	S	G	U	X	V	D	R	X	V	W	D	S	T
14	X	X	Y	Y	G	I	D	N	Y	X	W	W	N	E	C	A	M	B	Q	N	V	T	T	K	
15	S	R	Q	X	A	X	U	S	U	Y	D	O	Q	Y	N	S	R	C	S	L	K	S	U	E	I
16	P	W	R	Z	F	L	L	U	N	W	I	A	Y	R	T	H	M	N	E	Y	H	F	F	C	A
17	W	S	T	S	N	U	C	M	L	I	Z	M	V	S	C	D	Y	E	K	I	R	D	O	H	Z
18	N	B	V	A	Q	R	F	G	P	C	Y	N	O	M	X	E	O	Q	U	O	G	L	Y	N	D
19	A	A	W	E	U	N	M	T	M	A	C	F	R	F	O	O	F	B	P	V	O	I	H	Z	N
20	B	C	L	D	K	D	Q	D	B	K	G	L	P	A	W	K	T	O	D	B	X	E	M	F	B
21	C	D	A	C	D	Y	T	X	X	E	K	H	F	O	F	F	H	Z	Z	P	E	B	L	R	U
22	E	E	D	B	O	Z	W	A	W	L	R	Q	E	D	Q	P	E	P	Q	E	Y	H	S	I	H
23	I	H	K	I	P	H	A	I	C	B	F	G	A	W	D	Y	U	L	A	S	B	K	I	D	Y
24	G	F	O	F	I	W	H	H	R	D	B	C	N	P	R	A	S	G	T	N	F	N	Q	A	F
25	D	I	M	G	T	B	X	P	A	F	E	U	C	K	L	Q	Z	V	O	H	S	R	N	Y	W

Synoptic Table for K

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25
0	K	K	K	K	K	K	K	K	K	K	K	K	K	K	K	K	K	K	K	K	K	K	K	K	K
1	Z	T	O	M	D	V	P	C	Q	E	R	X	G	J	S	F	L	Y	U	A	H	N	W	B	I
2	O	L	M	R	O	M	V	V	O	L	F	I	X	V	G	P	N	T	P	U	R	R	R	Q	A
3	L	M	J	U	P	E	R	F	I	B	B	S	U	I	U	Y	V	F	D	T	G	J	E	W	Z
4	R	O	U	O	I	T	O	Z	V	D	E	R	Z	U	E	A	A	U	Z	R	O	Q	V	U	D
5	X	U	B	Q	T	A	G	L	T	F	J	D	T	Q	N	Q	R	I	Q	Z	X	Z	D	G	N
6	S	V	G	V	J	G	S	Q	Z	J	A	V	S	H	T	J	M	W	A	X	E	G	T	L	B
7	P	Y	E	P	B	P	Y	E	E	G	L	E	W	Z	C	N	Y	X	T	Q	Y	M	U	O	U
8	W	G	P	T	R	O	D	R	F	H	T	W	Q	C	X	U	O	H	O	L	B	X	F	S	H
9	N	Z	H	N	H	C	U	Y	H	O	M	O	Y	T	O	B	F	A	J	Y	F	P	O	T	Y
10	A	N	S	W	C	I	L	N	G	N	S	A	V	X	W	T	T	S	Y	I	S	U	Y	E	F
11	B	P	C	Y	Y	X	C	S	Y	M	X	M	O	B	F	G	H	D	L	O	J	C	H	C	W
12	C	Q	Z	X	S	L	F	U	U	T	V	N	R	L	Q	I	E	M	F	V	M	O	M	H	J
13	E	X	I	Z	L	U	M	M	N	P	Q	F	P	E	D	M	U	C	X	B	U	T	L	N	L
14	I	R	N	S	W	R	Q	G	L	R	P	L	F	G	R	W	S	N	N	P	D	Y	S	Z	V
15	G	W	X	A	E	N	T	T	P	Q	N	H	E	N	L	Z	Z	E	G	E	Q	A	I	F	G
16	D	S	F	E	M	D	W	D	M	S	O	Q	A	Y	J	R	J	Q	W	S	C	W	Q	R	R
17	J	B	Y	D	Z	Y	A	X	B	V	H	G	N	R	Z	V	X	B	H	N	L	V	N	I	C
18	F	A	Q	C	V	Z	H	A	X	Z	U	C	C	S	M	L	D	O	V	H	Z	S	J	D	Q
19	V	C	R	B	X	H	X	I	W	U	W	U	J	M	A	X	P	Z	C	J	W	F	C	A	M
20	U	D	T	I	G	W	J	H	C	X	D	J	I	F	P	C	C	P	M	W	T	D	P	Y	P
21	Y	E	V	F	A	B	E	P	R	Y	I	T	L	A	B	S	W	L	I	M	I	L	G	J	S
22	M	H	W	G	F	J	Z	J	A	W	Z	B	D	O	V	H	G	G	R	D	P	I	B	P	O
23	H	F	L	J	N	S	B	O	J	I	Y	Y	H	D	H	D	Q	V	B	G	A	E	Z	X	E
24	T	I	A	H	Q	Q	N	B	D	C	C	P	B	W	I	E	I	J	S	F	V	B	A	M	X
25	Q	J	D	L	U	F	I	W	S	A	G	Z	M	P	Y	O	B	R	E	C	N	H	X	V	T

Synoptic Table for L

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25
0	L	L	L	L	L	L	L	L	L	L	L	L	L	L	L	L	L	L	L	L	L	L	L	L	L
1	R	M	A	K	W	U	C	Q	P	B	T	H	D	E	J	X	N	G	F	Y	Z	I	S	O	V
2	X	O	D	M	E	R	F	E	M	D	M	Q	H	G	Z	C	V	V	X	I	W	E	I	S	G
3	S	U	K	R	M	N	M	R	B	F	S	G	B	N	M	S	A	J	N	O	T	B	Q	T	R
4	P	V	O	U	Z	D	Q	Y	X	J	X	C	M	Y	A	H	R	R	G	V	I	H	N	E	C
5	W	Y	M	O	V	Y	T	N	W	G	V	U	K	R	P	D	M	K	W	B	P	K	J	C	Q
6	N	G	J	Q	X	Z	W	S	C	H	Q	J	G	S	B	E	Y	Y	H	P	A	N	C	H	M
7	A	Z	U	V	G	H	A	U	R	O	P	T	X	M	V	O	O	T	V	E	V	R	P	N	P
8	B	N	B	P	A	W	H	M	A	N	N	B	U	F	H	K	F	F	C	S	N	J	G	Z	S
9	C	P	G	T	F	B	X	G	J	M	O	Y	Z	A	I	F	T	U	M	N	K	Q	B	F	O
10	E	Q	E	N	N	J	J	T	D	T	H	P	T	O	Y	P	H	I	I	H	H	Z	Z	R	E
11	I	X	P	W	Q	S	E	D	S	P	U	Z	S	D	K	Y	E	W	R	J	R	G	A	I	X
12	G	R	H	Y	U	Q	Z	X	K	R	W	K	W	W	S	A	U	X	B	W	G	M	X	D	T
13	D	W	S	X	K	F	B	A	Q	Q	D	X	Q	P	G	Q	S	H	S	M	O	X	K	A	K
14	J	S	C	Z	D	K	N	I	O	S	I	I	Y	K	U	J	Z	A	E	D	X	P	W	Y	I
15	F	B	Z	S	O	V	I	H	I	V	Z	S	V	J	E	N	J	S	K	G	E	U	R	J	A
16	V	A	I	A	P	M	K	P	V	Z	Y	R	O	V	N	U	X	D	U	F	Y	C	E	P	Z
17	Y	C	N	E	I	E	P	J	T	U	C	D	R	I	T	B	D	M	P	C	B	O	V	X	D
18	Y	D	X	D	T	T	V	O	Z	X	G	V	P	U	C	T	P	C	D	K	F	T	D	M	N
19	M	E	F	C	J	A	R	B	E	Y	K	E	F	Q	X	G	C	N	Z	A	S	Y	T	V	B
20	H	H	Y	B	B	G	O	W	F	W	R	W	E	H	O	I	W	E	Q	U	J	A	U	K	U
21	T	F	Q	I	R	P	G	K	H	I	F	O	A	Z	W	M	G	Q	A	T	M	W	F	B	H
22	Q	I	R	F	H	O	S	C	G	C	B	A	N	C	F	W	Q	B	T	R	U	V	O	Q	Y
23	K	J	T	G	C	C	Y	V	Y	A	E	M	C	T	Q	Z	I	O	O	Z	D	S	Y	W	F
24	Z	K	V	J	Y	I	D	F	U	K	J	N	J	X	D	R	B	Z	J	X	Q	F	H	U	W
25	O	T	W	H	S	X	U	Z	N	E	A	F	I	B	R	V	K	P	Y	Q	C	D	M	G	J

Synoptic Table for M

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25
0	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M
1	H	O	J	R	Z	E	Q	G	B	T	S	N	K	F	A	W	Y	C	I	D	U	X	L	V	P
2	T	U	U	V	T	T	T	X	P	X	F	G	A	P	Z	O	N	R	G	D	P	S	K	S	S
3	Q	V	B	O	X	A	W	D	W	R	V	L	X	O	B	R	F	E	B	F	Q	U	I	B	O
4	K	Y	G	Q	G	G	A	X	C	Q	Q	H	U	D	V	V	T	Q	S	C	C	C	Q	Q	E
5	Z	G	E	V	A	P	H	A	R	S	P	Q	Z	W	H	L	H	B	E	K	L	O	N	W	X
6	O	Z	P	P	F	O	X	I	A	V	N	G	T	P	I	X	E	O	K	A	Z	T	J	U	T
7	L	N	H	T	N	C	J	H	J	Z	O	C	S	K	Y	C	U	Z	U	U	W	Y	C	G	K
8	R	P	S	N	Q	I	E	P	D	U	H	U	W	J	K	S	S	P	T	T	A	P	L	I	I
9	X	Q	C	W	U	X	Z	J	S	X	U	J	Q	V	S	H	Z	L	D	R	I	W	G	O	A
10	S	X	Z	Y	K	L	B	O	K	Y	W	T	Y	I	G	D	J	G	Z	Z	P	V	B	S	Z
11	P	R	I	X	D	U	N	B	Q	W	D	B	V	U	E	X	V	Q	X	A	S	Z	T	D	D
12	W	W	N	Z	O	R	I	W	O	I	I	Y	O	Q	E	O	D	J	A	Q	V	F	A	E	N
13	N	S	X	S	P	N	K	K	I	C	Z	P	R	H	N	K	P	R	T	L	N	D	X	C	B
14	A	B	F	A	I	D	P	C	V	A	Y	Z	P	Z	T	F	C	K	O	Y	K	L	K	H	U
15	B	A	Y	E	T	Y	V	V	T	K	C	K	F	C	C	P	W	Y	J	I	H	I	W	N	H
16	C	C	Q	D	J	Z	R	F	Z	E	G	X	E	T	X	Y	G	T	Y	O	R	E	R	Z	Y
17	E	D	R	C	B	H	O	Z	E	L	K	I	A	X	O	A	Q	F	L	V	G	B	E	F	F
18	I	E	T	B	R	W	G	L	F	B	R	S	N	B	W	Q	I	U	F	B	O	H	V	R	W
19	G	H	V	I	H	B	S	Q	H	D	F	R	C	L	F	J	B	I	X	P	X	K	D	I	J
20	D	F	W	F	C	J	Y	E	G	F	B	D	J	E	Q	N	K	W	N	E	E	N	T	D	L
21	J	I	L	G	Y	S	D	R	Y	J	E	V	I	G	D	U	L	X	G	S	Y	R	U	A	V
22	F	J	A	J	S	Q	U	Y	U	G	J	E	L	N	R	B	N	H	W	N	B	J	F	Y	G
23	V	K	D	H	L	F	L	N	N	H	A	W	D	Y	L	T	V	A	H	H	F	Q	O	J	R
24	U	T	K	L	W	K	C	S	L	O	L	O	H	R	J	G	A	S	V	J	S	Z	Y	P	C
25	Y	L	O	K	E	V	F	U	P	N	T	A	B	S	Z	I	R	D	C	W	J	G	H	X	Q

Synoptic Table for N

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25
0	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N
1	A	P	X	W	Q	D	I	S	L	M	O	F	C	Y	T	U	V	E	G	H	K	R	J	Z	B
2	B	Q	F	Y	U	Y	K	U	P	T	H	L	J	R	C	B	A	Q	W	J	H	J	C	F	U
3	C	X	Y	X	K	Z	P	M	P	U	H	I	S	X	T	R	B	H	W	R	Q	P	R	H	H
4	E	R	Q	Z	D	H	V	G	B	R	W	Q	L	M	O	G	M	O	V	M	G	Z	G	I	Y
5	I	W	R	S	O	W	R	T	X	Q	D	G	D	F	W	I	Y	Z	C	D	O	G	B	D	F
6	G	S	T	A	P	B	O	D	W	S	I	C	H	A	F	M	O	P	M	G	X	M	Z	A	W
7	D	B	V	E	I	J	G	X	C	V	Z	U	B	O	Q	W	F	L	I	F	E	X	A	Y	J
8	J	A	W	D	T	S	S	A	R	Z	Y	J	M	D	D	Z	T	G	R	C	Y	P	X	J	L
9	F	C	L	C	J	Q	Y	I	A	U	C	T	K	W	R	R	H	V	B	K	B	U	K	P	V
10	V	D	A	B	B	F	D	H	J	X	G	B	G	P	L	V	E	J	S	A	F	C	W	X	G
11	U	E	D	I	R	K	U	P	D	Y	K	Y	X	K	J	L	U	R	E	U	S	O	R	M	R
12	Y	H	K	F	H	V	L	J	S	W	R	P	U	J	Z	X	S	K	K	T	J	T	E	V	C
13	M	F	O	G	C	M	C	O	K	I	F	Z	Z	V	M	C	Z	Y	U	R	M	Y	V	K	Q
14	H	I	M	J	Y	E	F	B	Q	C	B	K	T	I	A	S	J	T	P	Z	U	A	D	B	M
15	T	J	J	H	S	T	M	W	O	A	E	X	S	U	P	H	X	F	D	X	D	W	T	Q	P
16	Q	K	U	L	L	A	Q	K	I	K	J	I	W	Q	B	D	D	U	Z	Q	Q	V	U	W	S
17	K	T	B	K	W	G	T	C	V	E	A	S	Q	H	V	E	P	I	Q	L	C	S	F	U	O
18	Z	L	G	M	E	P	W	V	T	L	L	R	Y	Z	H	O	C	W	A	Y	L	F	O	G	E
19	O	M	E	R	M	O	A	F	Z	B	T	D	V	C	I	K	W	X	T	I	Z	D	Y	L	X
20	L	O	P	U	Z	C	H	Z	E	D	M	V	O	T	Y	F	G	H	O	O	W	L	H	O	T
21	R	U	H	O	V	I	X	L	F	F	S	E	R	X	K	P	Q	A	J	V	T	I	M	S	K
22	X	V	S	Q	X	X	J	Q	H	J	X	W	P	B	S	Y	I	S	Y	B	I	E	L	T	I
23	S	Y	C	V	G	L	E	E	G	G	V	O	F	L	G	A	B	D	L	P	P	B	S	E	A
24	P	G	Z	P	A	U	Z	R	Y	H	Q	A	E	E	U	Q	K	M	F	E	A	H	I	C	Z
25	W	Z	I	T	F	R	B	Y	U	O	P	M	A	G	E	J	L	C	X	S	V	K	Q	H	D

Synoptic Table for O

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25
0	O	O	O	O	O	O	O	O	O	O	O	O	O	O	O	O	O	O	O	O	O	O	O	O	O
1	L	U	M	Q	P	C	G	B	I	N	H	A	R	D	W	K	F	Z	J	V	X	T	Y	S	E
2	R	V	J	V	I	I	S	W	V	M	U	M	P	W	F	F	T	P	Y	B	E	Y	H	T	X
3	X	Y	U	P	T	X	Y	K	T	T	W	N	F	P	Q	P	H	L	L	P	Y	A	M	E	T
4	S	G	B	T	J	L	D	C	Z	P	D	F	E	K	D	Y	E	G	F	E	B	W	L	C	K
5	P	Z	G	N	B	U	V	E	R	I	L	A	J	R	A	U	V	X	S	F	V	S	H	I	
6	W	N	E	W	R	R	L	F	F	Q	Z	H	N	V	L	Q	S	J	N	N	S	S	I	N	A
7	N	P	P	Y	H	N	C	Z	H	S	Y	Q	C	I	J	J	Z	R	G	H	J	F	Q	Z	Z
8	A	Q	H	X	C	D	F	L	G	V	C	G	J	U	Z	N	J	K	W	J	M	D	N	F	D
9	B	X	S	Z	Y	M	Q	Y	Z	G	C	I	Q	M	U	X	Y	H	W	U	L	J	R	N	
10	C	R	C	S	S	Z	Q	E	U	U	K	U	L	H	A	B	D	T	V	M	D	I	C	I	B
11	E	W	Z	A	L	H	T	R	N	X	R	J	D	Z	P	T	P	F	C	D	Q	E	P	D	U
12	I	S	I	E	W	W	Y	L	Y	F	T	H	C	B	G	C	U	M	G	C	B	G	A	H	
13	G	B	N	D	E	B	A	N	P	W	B	B	B	T	V	I	W	I	I	F	L	H	B	Y	Y
14	D	A	X	C	M	J	H	S	M	I	E	Y	M	X	H	M	G	W	R	C	Z	K	Z	J	F
15	J	C	F	B	Z	S	X	U	B	C	J	P	K	B	I	W	Q	X	B	K	W	N	A	P	W
16	F	D	Y	I	V	Q	J	M	X	A	A	Z	G	L	Y	Z	I	H	S	A	T	R	X	X	J
17	V	E	Q	F	X	F	E	G	W	K	L	K	X	E	K	R	B	A	E	U	I	J	K	M	L
18	U	H	R	G	G	K	Z	T	C	E	T	X	U	G	S	V	K	S	K	T	P	Q	W	V	V
19	Y	F	T	J	A	V	B	D	R	L	M	I	Z	N	G	L	L	D	U	R	A	Z	R	K	G
20	M	I	V	H	F	M	N	X	A	B	S	S	T	Y	U	X	N	M	P	Z	V	G	E	B	R
21	H	J	W	L	N	E	I	A	J	D	X	R	S	R	E	C	V	C	D	X	N	M	V	Q	C
22	T	K	L	K	Q	T	K	I	D	F	V	D	W	S	N	S	A	N	Z	Q	K	X	D	W	Q
23	Q	T	A	M	U	A	P	H	S	J	Q	V	Q	M	T	H	R	E	Q	L	H	P	T	U	M
24	K	L	D	R	K	G	V	P	K	G	P	E	Y	F	C	D	M	Q	A	Y	R	U	U	G	P
25	Z	M	K	U	D	P	R	J	Q	H	N	W	V	A	X	E	Y	B	T	I	G	C	F	L	S

Synoptic Table for P

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25
0	P	P	P	P	P	P	P	P	P	P	P	P	P	P	P	P	P	P	P	P	P	P	P	P	P
1	W	Q	H	T	I	O	V	J	M	R	N	Z	F	K	B	Y	C	L	D	E	A	U	G	X	S
2	N	X	S	N	T	C	R	O	B	Q	O	K	E	J	V	A	W	G	Z	S	V	C	B	M	O
3	A	R	C	W	J	I	O	B	X	S	H	X	A	V	H	Q	G	V	Q	N	N	O	Z	V	E
4	B	W	Z	Y	B	X	G	W	W	V	U	I	N	I	I	J	Q	J	A	H	K	T	A	K	X
5	C	S	I	X	R	L	S	K	C	Z	W	S	C	U	Y	N	I	R	T	J	H	Y	X	B	T
6	E	B	N	Z	H	U	Y	C	R	U	D	R	J	Q	K	U	B	K	O	W	R	A	K	Q	K
7	I	A	X	S	C	R	D	V	A	X	I	D	I	H	S	B	K	Y	J	M	G	W	W	W	I
8	G	C	F	A	Y	N	U	F	J	Y	Z	V	L	Z	G	T	L	T	Y	D	O	V	R	U	A
9	D	D	Y	E	S	D	L	Z	D	W	Y	E	D	C	U	G	N	F	L	G	X	S	E	G	Z
10	J	E	Q	D	L	Y	C	L	S	I	C	W	H	T	E	I	V	U	F	F	E	F	V	L	D
11	F	H	R	C	W	Z	F	Q	K	C	G	O	B	X	N	M	A	I	X	C	Y	D	D	O	N
12	V	F	T	B	E	H	M	E	Q	A	K	A	M	B	T	W	R	W	N	K	B	L	T	S	B
13	U	I	V	I	M	W	Q	R	O	K	R	M	K	L	C	Z	M	X	G	A	F	I	U	T	U
14	Y	J	W	F	Z	B	T	Y	I	E	F	N	G	E	X	R	Y	H	W	U	S	E	F	E	H
15	M	K	L	G	V	J	W	N	V	L	B	F	X	G	O	V	O	A	H	T	J	B	O	C	Y
16	H	T	A	J	X	S	A	S	T	B	E	L	U	N	W	L	F	S	V	R	M	H	Y	H	F
17	T	L	D	H	G	Q	H	U	Z	D	J	H	Z	Y	F	X	T	D	C	Z	U	K	H	N	W
18	Q	M	K	L	A	F	X	M	E	F	A	Q	T	R	Q	C	H	M	M	X	D	N	M	Z	J
19	K	O	O	K	F	K	J	G	F	J	L	G	S	S	D	S	E	C	I	Q	Q	R	L	F	L
20	Z	U	M	M	N	V	E	T	H	G	T	C	W	M	R	H	U	N	R	L	C	J	S	R	V
21	O	V	J	R	Q	M	Z	D	G	H	M	U	Q	F	L	D	S	E	B	Y	L	Q	I	I	G
22	L	Y	U	U	U	E	B	X	Y	O	S	J	Y	A	J	E	Z	Q	S	I	Z	Z	Q	D	R
23	R	G	B	O	K	T	N	A	U	N	X	T	V	O	Z	O	J	B	E	O	W	G	N	A	C
24	X	Z	G	Q	D	A	I	I	N	M	V	B	O	D	M	K	X	O	K	V	T	M	J	Y	Q
25	S	N	E	V	O	G	K	H	L	T	Q	Y	R	W	A	F	D	Z	U	B	I	X	C	J	M

Synoptic Table for Q

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25
0	Q	Q	Q	Q	Q	Q	Q	Q	Q	Q	Q	Q	Q	Q	Q	Q	Q	Q	Q	Q	Q	Q	Q	Q	Q
1	K	X	R	V	U	F	T	E	O	S	P	G	Y	H	D	J	I	B	A	L	C	Z	N	W	M
2	Z	R	T	P	K	K	W	R	I	V	N	C	V	Z	R	N	B	O	T	Y	L	G	J	U	P
3	O	W	V	T	D	V	A	Y	V	Z	O	U	O	C	L	U	K	Z	O	I	Z	M	C	G	S
4	L	S	W	N	O	M	H	N	T	U	H	J	R	T	J	B	L	P	J	O	W	X	P	L	O
5	R	B	L	W	P	E	X	S	Z	X	U	T	P	X	Z	T	N	L	Y	V	T	P	G	O	E
6	X	A	A	Y	I	T	J	U	E	Y	W	B	F	B	M	G	V	G	L	B	I	U	B	S	X
7	S	C	D	X	T	A	E	M	F	W	D	Y	E	L	A	I	A	V	F	P	P	C	Z	T	T
8	P	D	K	Z	J	G	Z	G	H	I	I	P	A	E	P	M	R	J	X	E	A	O	A	E	K
9	W	E	O	S	B	P	B	T	G	C	Z	Z	N	G	B	W	M	R	N	S	V	T	X	C	I
10	N	H	M	A	R	O	N	D	Y	A	Y	K	C	N	V	Z	Y	K	G	N	N	Y	K	H	A
11	A	F	J	E	H	C	I	X	U	K	C	X	J	Y	H	R	O	Y	W	H	K	A	W	N	Z
12	B	I	U	D	C	I	K	A	N	E	G	I	I	R	I	V	F	T	H	J	H	W	R	Z	D
13	C	J	B	C	Y	X	P	I	L	L	K	S	L	S	Y	L	T	F	V	W	R	V	E	F	N
14	E	K	G	B	S	L	V	H	P	B	R	R	D	M	K	X	H	U	C	M	G	S	V	R	B
15	I	T	E	I	L	U	R	P	M	D	F	D	H	F	S	C	E	I	M	D	O	F	D	I	U
16	G	L	P	F	W	R	O	J	B	F	B	V	B	A	G	S	U	W	I	G	X	D	T	D	H
17	D	M	H	G	E	N	G	O	X	J	E	E	M	O	U	H	S	X	R	F	E	L	U	A	Y
18	J	O	S	J	M	D	S	B	W	G	J	W	K	D	E	D	Z	H	B	C	Y	I	F	Y	F
19	F	U	C	H	Z	Y	Y	W	C	H	A	O	G	W	N	E	J	A	S	K	B	E	O	J	W
20	V	V	Z	L	V	Z	D	K	R	O	L	A	X	P	T	O	X	S	E	A	F	B	Y	P	J
21	U	Y	I	K	X	H	U	C	A	N	T	M	U	K	C	K	D	D	K	U	S	H	H	X	L
22	Y	G	N	M	G	W	L	V	J	M	M	N	Z	J	X	F	P	M	U	T	J	K	M	M	V
23	M	Z	X	R	A	B	C	F	D	T	S	F	T	V	O	P	C	C	P	R	M	N	L	V	G
24	H	N	F	U	F	J	F	Z	S	P	X	L	S	I	W	Y	W	N	D	Z	U	R	S	K	R
25	T	P	Y	O	N	S	M	L	K	R	V	H	W	U	F	A	G	E	Z	X	D	J	I	B	C

Synoptic Table for R

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	
0	R	R	R	R	R	R	R	R	R	R	R	R	R	R	R	R	R	R	R	R	R	R	R	R	R	
1	X	W	T	U	H	N	O	Y	A	Q	F	D	P	S	L	V	M	K	B	Z	G	J	E	I	C	
2	S	S	V	O	C	D	G	N	J	S	B	V	F	M	J	L	Y	Y	S	X	O	Q	V	D	Q	
3	P	B	W	Q	Y	Y	S	S	D	V	E	E	E	F	Z	X	O	T	E	Q	X	Z	D	A	M	
4	W	A	L	V	S	Z	Y	U	S	Z	J	W	A	A	M	C	F	F	K	L	E	G	T	Y	P	
5	N	C	A	P	L	H	D	M	K	U	A	O	N	O	A	S	T	U	U	Y	Y	M	U	J	S	
6	A	D	D	T	W	W	U	G	Q	X	L	A	C	D	P	H	H	I	P	I	B	X	F	P	O	
7	B	E	K	N	E	B	L	T	O	Y	T	M	J	W	B	D	E	W	D	O	F	P	O	X	E	
8	C	H	O	W	M	J	C	D	I	W	M	N	I	P	V	E	U	X	Z	V	S	U	Y	M	X	
9	E	F	M	Y	Z	S	F	X	V	I	S	F	L	K	H	O	S	H	Q	B	J	C	H	V	T	
10	I	I	J	X	V	Q	M	A	T	C	X	L	D	J	I	K	Z	A	A	P	M	O	M	K	K	
11	G	J	U	Z	X	F	Q	I	Z	A	V	H	H	V	Y	F	J	S	T	E	U	T	L	B	I	
12	D	K	B	S	G	K	T	H	E	K	Q	Q	B	I	K	P	X	D	O	S	D	Y	S	Q	A	
13	J	T	G	A	A	V	W	P	F	E	P	G	M	U	S	Y	D	M	J	N	Q	A	I	W	Z	
14	F	L	E	E	F	M	A	J	H	L	N	C	K	Q	G	A	P	C	Y	H	C	W	Q	U	D	
15	V	M	P	D	N	E	H	O	G	B	O	U	G	H	U	Q	C	N	L	J	L	V	N	G	N	
16	U	O	H	C	Q	T	X	B	Y	D	H	J	X	Z	E	J	W	E	F	W	Z	S	J	L	B	
17	Y	U	S	B	U	A	J	W	U	F	U	T	U	C	N	N	G	Q	X	M	W	F	C	O	U	
18	M	V	C	I	K	A	G	E	K	N	J	W	B	Z	T	T	U	Q	B	N	D	T	D	P	S	H
19	H	Y	Z	F	D	P	Z	C	L	G	D	Y	T	X	C	B	I	O	G	G	I	L	G	T	Y	
20	T	G	I	G	O	O	B	V	P	H	I	P	S	B	X	T	B	Z	W	F	P	I	B	E	F	
21	Q	Z	N	J	P	C	N	F	M	O	Z	Z	W	L	O	G	K	P	H	C	A	E	Z	C	W	
22	K	N	X	H	I	I	I	Z	B	N	Y	K	Q	E	W	I	L	L	V	K	V	B	A	H	J	
23	Z	P	F	L	T	X	K	L	X	M	C	X	Y	G	F	M	N	G	C	A	N	H	X	N	L	
24	O	Q	Y	K	J	L	P	Q	W	T	G	I	V	N	Q	W	V	V	M	U	K	K	K	Z	V	
25	L	X	Q	M	B	U	V	E	C	P	K	S	O	Y	D	Z	A	J	I	T	H	N	W	F	G	



Synoptic Table for S

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25
0	S	S	S	S	S	S	S	S	S	S	S	S	S	S	S	S	S	S	S	S	S	S	S	S	S
1	P	B	C	A	L	Q	Y	U	K	V	X	R	W	M	G	H	Z	D	E	N	J	F	I	T	O
2	W	A	Z	E	W	F	D	M	Q	Z	V	D	Q	F	U	D	J	M	K	H	M	D	Q	E	E
3	N	C	I	D	E	K	U	G	O	U	Q	V	Y	A	E	E	X	C	U	J	U	L	N	C	X
4	A	D	N	C	M	V	L	T	I	X	P	E	V	O	N	O	D	N	P	W	D	I	J	H	T
5	B	E	X	B	Z	M	C	D	V	Y	N	W	O	D	T	K	P	E	D	M	Q	E	C	N	K
6	C	H	F	I	V	E	F	X	T	W	O	O	R	W	C	F	C	Q	Z	D	C	B	P	Z	I
7	E	F	Y	F	X	T	M	A	Z	I	H	A	P	P	X	P	W	B	Q	G	L	H	G	F	A
8	I	I	Q	G	G	A	Q	I	E	C	U	M	F	K	O	Y	G	O	A	F	Z	K	B	R	Z
9	G	J	R	J	A	G	T	H	F	A	W	N	E	J	W	A	Q	Z	T	C	W	N	Z	I	D
10	D	K	T	H	F	P	W	P	H	K	D	F	A	V	F	Q	I	P	O	K	T	R	A	D	N
11	J	T	V	L	N	O	A	J	G	E	I	L	N	I	Q	J	B	L	J	A	I	J	X	A	B
12	F	L	W	K	Q	C	H	O	Y	L	Z	H	C	U	D	N	K	G	Y	U	P	Q	K	Y	U
13	V	M	L	M	U	I	X	B	U	B	Y	Q	J	Q	R	U	L	V	L	T	A	Z	W	J	H
14	U	O	A	R	K	X	J	W	N	D	C	G	I	H	L	B	N	J	F	R	V	G	R	P	Y
15	Y	U	D	U	D	L	E	K	L	F	G	C	L	Z	J	T	V	R	X	Z	N	M	E	X	F
16	M	V	K	O	O	U	Z	C	P	J	K	U	D	C	Z	G	A	K	N	X	K	X	V	M	W
17	H	Y	O	Q	P	R	B	V	M	G	R	J	H	T	M	I	R	Y	G	Q	H	P	D	V	J
18	T	G	M	V	I	N	N	F	B	H	F	T	B	X	A	M	M	T	W	L	R	U	T	K	L
19	Q	Z	J	P	T	D	I	Z	X	O	B	B	M	B	P	W	Y	F	H	Y	G	C	U	B	V
20	K	N	U	T	J	Y	K	L	W	N	E	Y	K	L	B	Z	O	U	V	I	O	O	F	Q	G
21	Z	P	B	N	B	Z	P	Q	C	M	J	P	G	E	V	R	F	I	C	O	X	T	O	W	R
22	O	Q	G	W	R	H	V	E	R	T	A	Z	X	G	H	V	T	W	M	V	E	Y	Y	U	C
23	L	X	E	Y	H	W	R	R	A	P	L	K	U	N	I	L	H	X	I	B	Y	A	H	G	Q
24	R	R	P	X	C	B	O	Y	J	R	T	X	Z	Y	Y	X	E	H	R	P	B	W	M	L	M
25	X	W	H	Z	Y	J	G	N	D	Q	M	I	T	R	K	C	U	A	B	E	F	V	L	O	P

Synoptic Table for T

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25
0	T	T	T	T	T	T	T	T	T	T	T	T	T	T	T	T	T	T	T	T	T	T	T	T	T
1	Q	L	V	N	J	A	W	D	Z	P	M	B	S	X	C	G	H	F	O	R	I	Y	U	E	K
2	K	M	W	W	B	G	A	X	E	R	S	Y	W	B	X	I	E	U	J	Z	P	A	F	C	I
3	Z	O	L	Y	R	P	H	A	F	Q	X	P	Q	L	O	M	U	I	Y	X	A	W	O	H	A
4	O	U	A	X	H	O	X	I	H	S	V	Z	Y	E	W	W	S	W	L	Q	V	V	Y	N	Z
5	L	V	D	Z	C	C	J	H	G	V	Q	K	V	G	F	Z	Z	X	F	L	N	S	H	Z	D
6	R	Y	K	S	Y	I	E	P	Y	Z	P	X	O	N	Q	R	J	H	X	Y	K	F	M	F	N
7	X	G	O	A	S	X	Z	J	U	N	I	R	Y	D	V	X	A	N	I	H	D	L	R	B	
8	S	Z	M	E	L	L	B	O	N	X	O	S	P	R	R	L	D	S	G	O	R	L	S	I	U
9	P	N	J	D	W	U	N	B	L	Y	H	R	F	S	L	X	P	D	W	V	G	I	I	D	H
10	W	P	U	C	E	R	I	W	P	W	U	D	E	M	J	C	C	M	H	B	O	E	Q	A	Y
11	N	Q	B	B	M	N	K	K	M	I	W	V	A	F	Z	S	W	C	V	P	X	B	N	Y	F
12	A	X	G	I	Z	D	P	C	B	C	D	E	N	A	M	H	G	N	C	E	E	H	J	J	W
13	B	R	E	F	V	Y	V	V	X	A	I	W	C	O	A	D	Q	E	M	S	Y	K	C	P	J
14	C	W	P	G	X	Z	R	F	W	K	Z	O	J	D	P	E	I	Q	I	N	B	N	P	X	L
15	E	S	H	J	G	H	O	Z	C	E	Y	A	I	W	B	O	B	B	R	H	F	R	G	M	V
16	I	B	S	H	A	W	G	L	R	L	C	M	L	P	V	K	K	O	B	J	S	J	B	V	G
17	G	A	C	L	F	B	S	Q	A	B	G	N	D	K	H	F	L	Z	S	W	J	Q	Z	K	R
18	D	C	Z	K	N	J	Y	E	J	D	K	F	H	J	I	P	N	P	E	M	M	Z	A	B	C
19	J	D	I	M	Q	S	D	R	D	F	R	L	B	V	Y	Y	V	L	K	D	U	G	X	Q	Q
20	F	E	N	R	U	Q	U	Y	S	J	F	H	M	I	K	A	A	G	U	G	D	M	K	W	M
21	V	H	X	U	K	F	L	N	K	G	B	Q	K	U	S	Q	R	V	P	F	Q	X	W	U	P
22	U	F	F	O	D	K	C	S	Q	H	E	G	G	Q	G	J	M	J	D	C	C	P	R	G	S
23	Y	I	Y	Q	O	V	F	U	O	O	J	C	X	H	U	N	Y	R	Z	K	L	U	E	L	O
24	M	J	Q	V	P	M	M	I	N	A	U	U	Z	E	U	O	K	Q	A	Z	C	V	O	E	
25	H	K	R	P	I	E	Q	G	V	M	L	J	Z	C	N	B	F	Y	A	U	W	O	D	S	X

Synoptic Table for U

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25
0	U	U	U	U	U	U	U	U	U	U	U	U	U	U	U	U	U	U	U	U	U	U	U	U	U
1	Y	V	B	O	K	R	L	M	N	X	W	J	Z	Q	E	B	S	I	P	T	D	C	F	G	H
2	M	Y	G	Q	D	N	C	G	L	Y	D	T	T	H	N	T	Z	W	D	R	Q	O	O	L	Y
3	H	G	E	V	O	D	F	T	P	W	I	B	S	Z	T	G	J	X	Z	Z	C	T	Y	O	F
4	T	Z	P	P	P	Y	M	D	M	I	Z	Y	W	C	C	I	X	H	Q	X	L	Y	H	S	W
5	Q	N	H	T	I	Z	Q	X	B	C	Y	P	Q	T	X	M	D	A	A	Q	Z	A	M	T	J
6	K	P	S	N	T	H	T	A	X	A	C	Z	Y	X	O	W	P	S	T	L	W	W	L	E	L
7	Z	Q	C	W	J	W	W	I	W	K	G	K	V	B	W	Z	C	D	O	Y	T	V	S	C	V
8	O	X	Z	Y	B	B	A	H	C	E	K	X	O	L	F	R	W	M	J	I	I	S	I	H	G
9	L	R	I	X	R	J	H	P	R	L	R	I	R	E	Q	V	G	C	Y	O	P	F	Q	N	R
10	R	W	N	Z	H	S	X	J	A	B	F	S	P	G	D	L	Q	N	L	V	A	D	N	Z	C
11	X	S	X	S	C	Q	J	O	J	D	B	R	F	N	R	X	I	E	F	B	V	L	J	F	Q
12	S	B	F	A	Y	F	E	B	D	F	E	D	E	Y	L	C	B	Q	X	P	N	I	C	R	M
13	P	A	Y	E	S	K	Z	W	S	J	J	V	A	R	J	S	K	B	N	E	K	E	P	I	P
14	W	C	Q	D	L	V	B	K	K	G	A	E	N	S	Z	H	L	O	G	S	H	B	G	D	S
15	N	D	R	C	W	M	N	C	Q	H	L	W	C	M	M	D	N	Z	W	N	R	H	B	A	O
16	A	E	T	B	E	E	I	V	O	O	T	O	J	F	A	E	V	P	H	H	G	K	Z	Y	E
17	B	H	V	I	M	T	K	F	I	N	M	A	I	A	P	O	A	L	V	J	O	N	A	J	X
18	C	F	W	F	Z	A	P	Z	V	M	S	M	L	O	B	K	R	G	C	W	X	R	X	P	T
19	E	I	L	G	V	G	V	L	T	T	X	N	D	D	V	F	M	V	M	M	E	J	K	X	K
20	I	J	A	J	X	P	R	Q	Z	P	V	F	H	W	H	P	Y	J	I	D	Y	Q	W	M	I
21	G	K	D	H	G	O	O	E	E	R	Q	L	B	P	I	Y	O	R	R	G	B	Z	R	V	A
22	D	T	K	L	A	C	G	R	F	Q	P	H	M	K	Y	A	F	K	B	F	F	G	E	K	Z
23	J	L	O	K	F	I	S	Y	H	S	N	Q	K	J	K	Q	T	Y	S	C	S	M	V	B	D
24	F	M	M	M	N	X	Y	N	G	V	O	G	G	V	S	J	H	T	E	K	J	X	D	Q	N
25	V	O	J	R	Q	L	D	S	Y	Z	H	C	X	I	G	N	E	F	K	A	M	P	T	W	B

Synoptic Table for V

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	
0	V	V	V	V	V	V	V	V	V	V	V	V	V	V	V	V	V	V	V	V	V	V	V	V	V	V
1	U	Y	W	P	X	M	R	F	T	Z	Q	E	O	I	H	L	A	J	C	B	N	S	D	K	G	
2	Y	G	L	T	G	E	O	Z	Z	U	P	W	R	U	I	X	R	R	M	P	K	F	T	B	R	
3	M	Z	A	N	A	T	G	L	E	X	N	O	P	Q	Y	C	M	K	I	E	H	D	U	Q	C	
4	H	N	D	W	F	A	S	Q	F	Y	O	A	F	H	K	S	Y	Y	R	S	R	L	F	W	Q	
5	T	P	K	Y	N	G	Y	E	H	W	H	M	E	Z	S	H	O	T	B	N	G	I	O	U	M	
6	Q	Q	O	X	Q	P	D	R	G	I	U	N	A	C	G	D	F	F	S	H	O	E	Y	G	P	
7	K	X	M	Z	U	O	U	Y	Y	C	W	F	N	T	U	E	T	U	E	J	X	B	H	L	S	
8	Z	R	J	S	K	C	L	N	U	A	D	L	C	X	E	O	H	I	K	W	E	H	M	O	O	
9	O	W	U	A	D	I	C	S	N	K	I	H	J	B	N	K	E	W	U	M	Y	K	L	S	E	
10	L	S	B	E	O	X	F	U	L	E	Z	Q	I	L	T	F	U	X	P	D	B	N	S	T	X	
11	R	B	G	D	P	L	M	M	P	L	Y	G	L	E	C	P	S	H	D	G	F	R	I	E	T	
12	X	A	E	C	I	U	Q	G	M	B	C	C	D	G	X	Y	Z	A	Z	F	S	J	Q	C	K	
13	S	C	P	B	T	R	T	T	B	D	G	U	H	N	O	A	J	S	Q	C	J	Q	N	H	I	
14	P	D	H	I	J	N	W	D	X	F	K	J	B	Y	W	Q	X	D	A	K	M	Z	J	N	A	
15	W	E	S	F	B	D	A	X	W	J	R	T	M	R	F	J	D	M	T	A	U	G	C	Z	Z	
16	N	H	C	G	R	Y	H	A	C	G	F	B	K	S	Q	N	P	C	O	U	D	M	P	F	D	
17	A	F	Z	J	H	Z	X	I	R	H	B	Y	G	M	D	U	C	N	J	T	Q	X	G	R	N	
18	B	I	I	H	C	H	J	H	A	O	E	P	X	F	R	B	W	E	Y	R	C	P	B	I	B	
19	C	J	N	L	Y	W	E	P	J	N	J	Z	U	A	L	T	G	Q	L	Z	L	U	Z	D	U	
20	E	K	X	K	S	B	Z	J	D	M	A	K	Z	O	J	G	Q	B	F	X	Z	C	A	A	H	
21	I	T	F	M	L	J	B	O	S	T	L	X	T	D	Z	I	I	O	X	Q	W	O	X	Y	Y	
22	G	L	Y	R	W	S	N	B	K	P	T	I	S	W	M	M	B	Z	N	L	T	T	K	J	F	
23	D	M	Q	U	E	Q	I	W	Q	R	M	S	W	P	A	W	K	P	G	Y	I	Y	W	P	W	
24	J	O	R	O	M	F	K	K	O	Q	S	R	Q	K	P	R	L	L	W	I	P	A	R	X	J	
25	F	U	T	Q	Z	K	P	C	I	S	X	D	Y	J	B	R	N	G	H	O	A	W	E	M	L	

Synoptic Table for W

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25
0	W	W	W	W	W	W	W	W	W	W	W	W	W	W	W	W	W	W	W	W	W	W	W	W	W
1	N	S	L	Y	E	B	A	K	C	I	D	O	Q	P	F	Z	G	X	H	M	T	V	R	U	J
2	A	B	A	X	M	J	H	C	R	C	I	A	Y	K	Q	R	Q	H	V	D	I	S	E	G	L
3	B	A	D	Z	Z	S	X	V	A	A	Z	M	V	J	D	V	I	A	C	G	P	F	V	L	V
4	C	C	K	S	V	Q	J	F	J	K	Y	N	O	V	R	L	B	S	M	F	A	D	D	O	G
5	E	D	O	A	X	F	E	Z	D	E	C	F	R	I	L	X	K	D	I	C	V	L	T	S	R
6	I	E	M	E	G	K	Z	L	S	L	G	L	P	U	J	C	L	M	R	K	N	I	U	T	C
7	G	H	J	D	A	V	B	Q	K	B	K	H	F	Q	Z	S	N	C	B	A	K	E	F	E	Q
8	D	F	U	C	F	M	N	E	Q	D	R	Q	E	H	M	H	V	N	S	U	H	B	O	C	M
9	J	I	B	N	E	I	R	O	F	F	G	A	Z	A	D	A	E	E	T	R	H	Y	H	P	
10	F	J	G	I	Q	T	K	Y	I	J	B	C	N	C	P	E	R	Q	K	R	G	K	H	N	S
11	V	K	E	F	U	A	P	N	V	G	E	U	C	T	B	O	M	B	U	Z	O	N	M	Z	O
12	U	T	P	G	K	G	V	S	T	H	J	J	J	X	V	K	Y	O	P	X	X	R	L	F	E
13	Y	L	H	J	D	P	R	U	Z	O	A	T	I	B	H	F	O	Z	D	Q	E	J	S	R	X
14	M	M	S	H	O	O	O	M	E	N	L	B	L	L	I	P	F	P	Z	L	Y	Q	I	I	T
15	H	O	C	L	P	C	G	G	F	M	T	Y	D	E	Y	Y	T	L	Q	Y	B	Z	Q	D	K
16	T	U	Z	K	I	I	S	T	H	T	M	P	H	G	K	A	H	G	A	I	F	G	N	A	I
17	Q	V	I	M	T	X	Y	D	G	P	S	Z	B	N	S	Q	E	V	T	O	S	M	J	Y	A
18	K	Y	N	R	J	L	D	X	Y	R	X	K	M	Y	G	J	U	J	O	V	J	X	C	J	Z
19	Z	G	X	U	B	U	U	A	U	Q	V	X	K	R	U	N	S	R	J	B	M	P	P	P	D
20	O	Z	F	O	R	R	L	I	N	S	Q	I	G	S	E	U	Z	K	Y	P	U	U	G	X	N
21	L	N	Y	Q	H	N	C	H	L	V	P	S	X	M	N	B	J	Y	L	E	D	C	B	M	B
22	R	P	Q	V	C	D	F	P	P	Z	N	R	U	F	T	T	X	T	F	S	Q	O	Z	V	U
23	X	Q	R	P	Y	Y	M	J	M	U	O	D	Z	A	C	G	D	F	X	N	C	T	A	K	H
24	S	X	T	T	S	Z	Q	O	B	X	H	V	T	O	X	I	P	U	N	H	L	Y	X	B	Y
25	P	R	V	N	L	H	T	B	X	Y	U	E	S	D	O	M	C	I	G	J	Z	A	K	Q	F

Synoptic Table for X

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25
0	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
1	S	R	F	Z	G	L	J	A	W	Y	V	I	U	B	O	C	D	H	N	Q	E	P	K	M	T
2	P	W	Y	S	A	U	E	I	C	W	Q	S	Z	L	W	S	P	A	G	L	Y	U	W	V	K
3	W	S	Q	A	F	R	Z	H	R	I	P	R	T	E	F	H	C	S	W	Y	B	C	R	K	I
4	N	B	R	E	N	N	B	P	A	C	N	D	S	G	Q	D	W	D	H	I	F	O	E	B	A
5	A	A	T	D	Q	D	N	J	J	A	O	V	W	N	D	E	G	M	V	O	S	T	V	Q	Z
6	B	C	V	C	U	Y	I	O	D	K	H	E	Q	Y	R	O	Q	C	C	V	J	Y	D	W	D
7	C	D	W	B	K	Z	K	B	S	E	U	W	Y	R	L	K	I	N	M	B	M	A	T	U	N
8	E	E	L	I	D	H	P	W	K	L	W	O	V	S	J	F	B	E	I	P	U	W	U	G	B
9	I	H	A	F	O	W	V	K	Q	B	D	A	O	M	Z	P	K	Q	R	E	D	V	F	L	U
10	G	F	D	G	P	B	R	C	O	D	I	M	R	F	M	Y	L	B	B	S	Q	S	O	O	H
11	D	I	K	J	I	J	O	V	I	F	Z	N	P	A	A	A	N	O	S	N	C	F	Y	S	Y
12	J	J	O	H	T	S	G	F	V	J	Y	F	F	O	P	Q	V	Z	E	H	L	D	H	T	F
13	F	K	M	L	J	Q	S	Z	T	G	C	L	E	D	B	J	A	P	K	J	Z	L	M	E	W
14	V	T	J	K	B	F	Y	L	Z	H	G	H	A	W	V	N	R	L	U	W	W	I	L	C	J
15	U	L	U	M	R	K	D	Q	E	O	K	Q	N	P	H	U	M	G	P	M	T	E	S	H	L
16	Y	M	B	R	H	V	U	E	F	N	R	G	C	K	I	B	Y	V	D	D	I	B	I	N	V
17	M	O	G	U	C	M	L	R	H	M	F	C	J	J	Y	T	O	J	Z	G	P	H	Q	Z	G
18	H	U	E	O	Y	E	C	Y	G	T	B	U	I	V	K	G	F	R	Q	F	A	K	N	F	R
19	T	V	P	Q	S	T	F	N	Y	P	E	J	L	I	S	I	T	K	A	C	V	N	J	R	C
20	Q	Y	H	V	L	A	M	S	U	R	J	T	D	U	G	M	H	Y	T	K	N	R	C	I	Q
21	K	G	S	P	W	G	Q	U	N	Q	A	B	H	Q	U	W	E	T	O	A	K	J	P	D	M
22	Z	Z	C	T	E	P	T	M	L	S	L	Y	B	H	E	Z	U	F	J	U	H	Q	G	A	P
23	O	N	Z	N	M	O	W	G	P	V	T	P	M	Z	N	R	S	U	Y	T	R	Z	B	Y	S
24	L	P	I	W	Z	C	A	T	M	Z	M	Z	K	C	T	V	Z	I	L	R	G	G	Z	J	O
25	R	Q	N	Y	V	I	H	D	B	U	S	K	G	T	C	L	J	W	F	Z	O	M	A	P	E

Synoptic Table for Y

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25
0	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
1	M	G	Q	X	S	Z	D	N	U	W	C	P	V	R	K	A	O	T	L	I	B	A	H	J	F
2	H	Z	R	Z	L	H	U	S	N	I	G	Z	O	S	S	Q	F	F	F	O	F	W	M	P	W
3	T	N	T	S	W	W	L	U	L	C	K	K	R	M	G	J	T	U	X	V	S	V	L	X	J
4	Q	P	V	A	E	B	C	M	P	A	R	X	P	F	U	N	H	I	N	B	J	S	S	M	L
5	K	Q	W	E	M	J	F	G	M	K	F	I	F	A	E	U	E	W	G	P	M	F	I	V	V
6	Z	X	L	D	Z	S	M	T	B	E	B	S	E	O	N	B	U	X	W	E	U	D	Q	K	G
7	O	R	A	C	V	Q	Q	D	X	L	E	R	A	D	T	T	S	H	H	S	D	L	N	B	R
8	L	W	D	B	X	F	T	X	W	B	J	D	N	W	C	G	Z	A	V	N	Q	I	J	Q	C
9	R	S	K	I	G	K	W	A	C	D	A	V	C	P	X	I	J	S	C	H	C	E	C	W	Q
10	X	B	O	F	A	V	A	I	R	F	L	E	J	K	O	M	X	D	M	J	L	B	P	U	M
11	S	A	M	G	F	M	H	H	A	J	T	W	I	J	W	W	D	M	I	W	Z	H	G	G	P
12	P	C	J	J	N	E	X	P	J	G	M	O	L	V	F	Z	P	C	R	M	W	K	B	L	S
13	W	D	U	H	Q	T	J	J	D	H	S	A	D	I	Q	R	C	N	B	D	T	N	Z	O	O
14	N	E	B	L	U	A	E	O	S	O	X	M	H	U	D	V	W	E	S	G	I	R	A	S	E
15	A	H	G	K	K	G	Z	B	K	N	V	N	B	Q	R	L	G	Q	E	F	P	J	X	T	X
16	B	F	E	M	D	P	B	W	Q	M	Q	F	M	H	L	X	Q	B	K	C	A	Q	K	E	T
17	C	I	P	R	O	O	N	K	O	T	P	L	K	Z	J	C	I	O	U	K	V	Z	W	C	K
18	E	J	H	U	P	C	I	C	I	P	N	H	G	C	Z	S	B	Z	P	A	N	G	R	H	I
19	I	K	S	O	I	I	K	V	V	R	O	Q	X	T	M	H	K	P	D	U	K	M	E	N	A
20	G	T	C	Q	T	X	P	F	T	Q	H	G	U	X	A	D	L	L	Z	T	H	X	V	Z	Z
21	D	L	Z	V	J	L	V	Z	Z	S	U	C	Z	B	P	E	N	G	Q	R	R	P	D	F	D
22	J	M	I	P	B	U	R	L	E	V	W	U	T	L	B	O	V	V	A	Z	G	U	T	R	N
23	F	O	N	T	R	R	O	Q	F	Z	D	J	S	E	V	K	A	J	T	X	O	C	U	I	B
24	V	U	X	N	H	N	G	E	H	U	I	T	W	G	H	F	R	R	O	Q	X	O	F	D	U
25	U	V	F	W	C	D	S	R	G	X	Z	B	Q	N	I	P	M	K	J	L	E	T	O	A	H

Synoptic Table for Z

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25
0	Z	Z	Z	Z	Z	Z	Z	Z	Z	Z	Z	Z	Z	Z	Z	Z	Z	Z	Z	Z	Z	Z	Z	Z	Z
1	O	N	I	S	V	H	B	L	E	U	Y	K	T	C	M	R	J	P	Q	X	W	G	A	F	D
2	L	P	N	A	X	W	N	Q	F	X	C	X	S	T	A	V	X	L	A	Q	T	M	X	R	N
3	R	Q	X	E	G	B	I	E	H	Y	G	I	W	X	P	L	D	G	T	L	I	X	K	I	B
4	X	X	F	D	A	J	K	R	G	W	K	S	Q	B	B	X	P	V	O	Y	P	P	W	D	U
5	S	R	Y	C	F	S	P	Y	Y	I	R	R	Y	L	V	C	C	J	J	I	A	U	R	A	H
6	P	W	Q	B	N	Q	V	N	U	C	F	D	V	E	H	S	W	R	Y	O	V	C	E	Y	Y
7	W	S	R	I	Q	F	R	S	N	A	B	V	O	G	I	H	G	K	L	V	N	O	B	J	F
8	N	B	T	F	U	K	O	U	L	K	E	E	R	N	Y	D	Q	Y	F	B	K	T	D	P	W
9	A	A	V	G	K	V	G	M	P	E	J	W	P	Y	K	E	I	T	X	P	H	Y	T	X	J
10	B	C	W	J	D	M	S	G	M	L	A	O	F	R	S	O	B	F	N	E	R	A	U	M	L
11	C	D	L	H	O	E	Y	T	B	B	L	A	E	S	G	K	K	U	G	S	G	W	F	V	V
12	E	E	A	L	P	T	D	D	X	D	T	M	A	M	U	F	L	I	W	N	O	V	O	K	G
13	I	H	D	K	I	A	U	X	W	F	M	N	N	F	E	P	N	W	H	H	X	S	Y	B	R
14	G	F	K	M	T	G	L	A	C	J	S	F	C	A	N	Y	V	X	V	J	E	F	H	Q	C
15	D	I	O	R	J	P	C	I	R	G	X	L	J	O	T	A	A	H	C	W	Y	D	M	W	Q
16	J	J	M	U	B	O	F	H	A	H	V	H	I	D	C	Q	R	A	M	M	B	L	L	U	M
17	F	K	J	O	R	C	M	P	J	O	Q	Q	L	W	X	J	M	S	I	D	F	I	S	G	P
18	V	T	U	Q	H	I	Q	J	D	N	P	G	D	P	O	N	Y	D	R	G	S	E	I	L	S
19	U	L	B	V	C	X	T	O	S	M	N	C	H	K	W	U	O	M	B	F	J	B	Q	O	O
20	Y	M	G	P	Y	L	W	B	K	T	O	U	B	J	F	B	F	C	S	C	M	H	N	S	E
21	M	O	E	T	S	U	A	W	Q	P	H	J	M	V	Q	T	T	N	E	K	U	K	J	T	X
22	H	U	P	N	L	R	H	K	O	R	U	T	K	I	D	G	H	E	K	A	D	N	C	E	T
23	T	V	H	W	W	N	X	C	I	Q	W	B	G	U	R	I	E	Q	U	U	Q	R	P	C	K
24	Q	Y	S	Y	E	D	J	V	V	S	D	Y	X	Q	L	M	U	B	P	T	C	J	G	H	I
25	K	G	C	X	M	Y	E	F	T	V	I	P	U	H	J	W	S	O	D	R	L	Q	B	N	A

APPENDIX 3  
**TABLES OF THE POISSON DISTRIBUTION**  
(Individual and cumulative terms)

## TABLES OF THE POISSON DISTRIBUTION

(Individual and cumulative terms)

### I. INTRODUCTION

1. The importance of the phenomena of repetitions in cryptanalysis is very well known. When the cryptanalyst has at hand a sample of encrypted text, it is often necessary or desirable to determine whether or not the observed repetitions are *causal* repetitions (e.g., produced by the action of identical keying sequences upon identical portions of plain text), or *random* repetitions, (i.e., produced purely by "accident" or "chance"). The number of random repetitions to be expected in a sample of text of a given length may be calculated, and this calculation serves as a criterion for the evaluation of the phenomena present in the sample.

2. If each of the  $n$  possible elements (where  $n=10, 26, 100, 676$ , etc., for single digits, single letters, dinomes, digraphs, etc.) has the same chance of occurrence, the probability,  $P$ , that an element will occur *exactly*  $x$  times (where  $x=0, 1, 2 \dots N$ ) in a sample of size  $N$  is given by the formula

$$P_x = C_x^N (1-p)^{N-x} p^x$$

where  $C_x^N$  has its usual meaning (i.e., the number of combinations of  $N$  things taken  $x$  at a time), and  $p = \frac{1}{n}$ . The Poisson Tables, so called because they are derived from the Poisson exponential formula  $\frac{a^x e^{-a}}{x!}$  where  $a = Np$ , give an approximation to this probability that is sufficiently accurate for values of  $n$  when  $n$  is equal to or greater than 26.¹

3. In order to use the Poisson Tables it is necessary to determine  $a = Np$ , i.e., the average or mean number² of occurrences of each of the elements in a given sample of size  $N$ . Table I (Individual Terms) gives for values of  $a$  the probabilities for  $x$ -fold repetitions (i.e., *exactly* 0, 1, 2 . . .  $N$  times). The expected number of  $x$ -fold repetitions is computed from the Table by multiplying the entries in the Table by  $n$ . This number,  $nP$ , is then compared with the sample under study. Table II (Cumulative Terms) gives the probabilities of repetitions of multiplicity  $c$  or greater, where  $c$  is the sum of all entries in Table I for  $x \geq c$ . The expected number of repetitions occurring  $c$  or more times is here also computed by multiplying the entries in Table II by  $n$ .

4. Samples of random text may exhibit repetitions which vary considerably from the expected number. The percentage deviation may be quite large in cases where the number of available elements (letters or digits) is small. Only if the deviation is too great, in a given sample under investigation, to be due to fluctuations from sample to sample should this circumstance be attributed to causal factors. In using Table I, a practical guide that has been found useful for measuring excessive deviation is to compare the deviation from the expected with  $2\frac{1}{2}$  times the square root of the expected number. For example, if 72 3-fold repetitions are expected in a certain sample, then the deviation in random samples may be  $\pm 2\frac{1}{2}\sqrt{72} = \pm 2\frac{1}{2}(8.5) = \pm 21$ , and therefore the observed number will usually lie between 51 and 93. Only if the observed number is outside these limits should the repetitions be considered as manifestations causal to the nature of the cryptographic system.

¹ For cases where  $n$  is considerably less than 26, the Poisson distribution becomes increasingly inaccurate and therefore the Binomial distribution should be used. Appendix 4, "Table of the Binomial distribution for  $p=1/10$ ," for ranges of  $N$  between 10 and 1200, gives accurate probability statements for digital cases.

² The average number is usually represented by a small  $a$  but, for convenience in printing, the tables have this element denoted by a capital  $A$ .

5. The Table below will assist the analyst in interpreting the deviations from the expected. The statistical quantity called "standard deviation" (represented by  $\sigma$ ) is in this case approximated by the square root of the expected number of x-fold repetitions.

Expected number plus 1 $\sigma$ will be equalled or exceeded once every	6.3 times
Expected number plus $1\frac{1}{2}\sigma$ will be equalled or exceeded once every	15 times
Expected number plus 2 $\sigma$ will be equalled or exceeded once every	44 times
Expected number plus $2\frac{1}{2}\sigma$ will be equalled or exceeded once every	161 times
Expected number plus 3 $\sigma$ will be equalled or exceeded once every	740 times
Expected number plus $3\frac{1}{2}\sigma$ will be equalled or exceeded once every	4,310 times
Expected number plus 4 $\sigma$ will be equalled or exceeded once every	31,500 times
Expected number plus $4\frac{1}{2}\sigma$ will be equalled or exceeded once every	294,000 times
Expected number plus 5 $\sigma$ will be equalled or exceeded once every	3,480,000 times

## II. EXAMPLES OF USE OF THE TABLES

1. Two samples of 40 letters each are under study, and the x-fold repetitions of single letters are recorded under A and B respectively in the diagram below. The expected numbers of x-fold repetitions have been entered in the last column, and were obtained thus: since  $n=26$  and  $N=40$ , then  $a=\frac{40}{26}=1.54$ . The entries under 1.5 (the value for  $a$  in the Table closest to 1.54) in Table I were then multiplied by 26.

x	Sample A	Sample B	Expected
0	5	9	5.8
1	8	8	8.7
2	7	2	6.5
3	6	5	3.3
4	—	—	1.2
5	—	—	.37
6	—	1	.09
7	—	1	.02

The interpretation of the meaning of the decimal fractions in the last column may be given as follows. Out of 100 samples of random text of size  $N=40$ , 37 of them would have one 5-fold repetition, 9 would have one 6-fold repetition, and 2 would have one 7-fold repetition.

Variation from the expected is usual even for random text. In sample A six letters occur 3 times each where only three letters are expected to occur 3 times each. However, there are no occurrences of 4-fold or 5-fold repetitions, although there is a slight expectancy of their occurrence in these cases; this deviation therefore is not sufficient to imply that the repetitions in sample A are other than accidental. In sample B the variations from the expected number are considerable. Note the comparatively great number of blanks (0-fold repetitions) which would rarely occur in a sample of random text; but of much greater significance is the occurrence of 6- and 7-fold repetitions, which have a combined expectancy of only .11. From these phenomena it may be safely inferred that sample B is definitely not a random assortment of letters. Actually, sample A was enciphered with 25 non-related alphabets, whereas sample B is a monoalphabetic substitution cipher.

The individual variations of the samples from the expected are "smoothed" by a consideration of the distribution of the number of letters occurring *x or more times* as is given in the diagram below. Samples A and B are the cumulative data of the two samples, while the last column is calculated from Table II by multiplying the entries under  $a=1.5$  by 26.

c	Sample A	Sample B	Expected Cumulative Data
0	26	26	26
1	21	17	20
2	13	9	11.5
3	6	7	4.97
4		2	1.71
5		2	.48
6		2	.12
7		1	.02

2. In another sample of cipher text consisting of 116 digraphs the observed and calculated data for individual and cumulative distributions are as follows:

x	Table I		c	Table II	
	Observed	Calculated		Observed	Calculated
0	606	570	0	676	676
1	34	97	1	70	106
2	27	8.2	2	36	8.7
3	8	.47	3	9	.49
4	1	.02	4	1	.02

Since  $n=676$  and  $N=116$ , then  $a=\frac{116}{676}=.17$ ; and the values under .17 in the tables are multiplied by 676 to derive the calculated expectancies. A few moments' study of the foregoing data shows that the manifestations in this sample must be due to causal factors, since the respective numbers of 2-fold, 3-fold and 4-fold repetitions in the sample far exceed those which could reasonably be attributed to chance. The system used in this cryptogram was actually a Playfair cipher.

3. A cipher message of 209 dinomes has the following distribution of x-fold repetitions. Given also is the calculated number of x-fold random repetitions to be expected in cases where all dinomes have an equal probability of occurrence. The calculated numbers were obtained by multiplying by 100 the entries in Table I and Table II for the value of  $a=\frac{209}{100}$ =approximately 2.1.

x	Table I		c	Table II	
	Observed	Calculated		Observed	Calculated
0	30	12	0	100	100
1	24	26	1	70	88
2	12	27	2	46	62
3	11	19	3	34	35
4	9	10	4	23	16
5	2	4	5	14	6
6	7	1	6	12	2
7	3	0.4	7	5	0.6
8	-	.1	8	2	.1
9	1	.03	9	2	.03
10	1	.006	10	1	.007



A comparison of the observed data with the expected data for non-causal repetitions leaves little doubt that the repetitions are a causal by-product of the nature of the cryptographic system involved. The cryptogram was actually produced by a variant system in which each plaintext letter has four dinome cipher equivalents.

4. The following tabulation gives the distributions of x-fold repetitions found in three samples, A, B, and C, of four-letter code text, each containing 275,000 groups. The calculated expectancies shown in the second column were derived from Table I, using the value  $a = \frac{275,000}{26^4} = .6$

x	Expected	Sample A	Sample B	Sample C
0	250,793	249,992	249,481	250,122
1	150,476	151,348	152,344	152,343
2	45,143	44,987	44,685	44,312
3	9,028	9,121	8,825	8,131
4	1,354	1,342	1,427	1,305
5	163	171	188	395
6	16.5	13	21	201
7	1.4	2	3	123
8			2	26
9				12
10				4
11				2

The deviation of the entries in sample A from the expected could be due to chance, and therefore there is nothing in the number of repetitions to confirm a hypothesis that the sample is other than a sample of random 4-letter groups. It is also quite clear from an inspection of the foregoing data that sample C could not have occurred by chance, hence sample C may easily be vulnerable to cryptanalytic attack. However, in the case of sample B, although there are small deviations from the expected, it should be noted that these deviations, some plus and some minus, reflect the characteristics of deviations usual for samples of non-random text (cf. sample C). Furthermore, these deviations are less than our estimated norm of  $2\frac{1}{2}\sigma$ , except for the first two entries.

x	Deviations from the Expected in Sample B	$2\frac{1}{2}\sigma$
0	-1,312	1,252
1	1,868	970
2	-458	531
3	-203	237
4	73	92
5	25	32
6	4.4	10.2
7	1.6	2.9

However, when examined critically, by other mathematical tests³ it may be shown that the set of such deviations could have come from a random sample in less than 1 chance in 10,000; therefore sample B should undergo further scrutiny to reveal possible weaknesses in other than repetitive phenomena. Actually, sample A is an extremely complex form of enciphered code and sample B is code text subjected to a fairly complex encipherment; whereas sample C is typical of a simple encipherment superimposed upon a code of rather large proportions and condensing power.

³ The chi-square test.

TABLE I

X	A=.001	A=.002	A=.003	A=.004	A=.005	A=.006	A=.007	A=.008	X
0	.99900005	.99800020	.99700045	.99600080	.9950125	.9940180	.9930244	.9920319	0
1	.00099990	.0019960	.0029910	.0039840	.0049751	.0059641	.0069512	.0079363	1
2	.00000005	.00000020	.00000045	.00000080	.0000124	.0000179	.0000243	.0000317	2
3							.00000001	.00000001	3
X	A=.009	A=.010	A=.02	A=.03	A=.04	A=.05	A=.06	A=.07	X
0	.9910404	.9900498	.9801987	.9704455	.9607894	.9512294	.9417645	.9323938	0
1	.0089194	.0099005	.0196040	.0291134	.0384316	.0475615	.0565059	.0652676	1
2	.0000401	.0000495	.0001960	.0004367	.0007686	.0011890	.0016952	.0022844	2
3	.0000001	.0000002	.0000013	.0000044	.0000102	.0000198	.0000339	.0000533	3
4					.0000001	.0000002	.0000005	.0000009	4
X	A=.08	A=.09	A=.10	A=.11	A=.12	A=.13	A=.14	A=.15	X
0	.9231163	.9139312	.9048374	.8958341	.8869204	.8780954	.8693582	.8607080	0
1	.0738493	.0822538	.0904837	.0985410	.1064304	.1141524	.1217102	.1291062	1
2	.0029540	.0037014	.0045242	.0054198	.0063858	.0074199	.0085197	.0096830	2
3	.0000788	.0001110	.0001508	.0001987	.0002554	.0003215	.0003976	.0004841	3
4	.0000016	.0000025	.0000038	.0000055	.0000077	.0000104	.0000139	.0000182	4
5			.0000001	.0000001	.0000002	.0000003	.0000004	.0000005	5
X	A=.16	A=.17	A=.18	A=.19	A=.20	A=.21	A=.22	A=.23	X
0	.8521438	.8436648	.8352702	.8269591	.8187308	.8105842	.8025188	.7945336	0
1	.1363430	.1434230	.1503486	.1571222	.1637462	.1702227	.1765541	.1827427	1
2	.0109074	.0121910	.0135314	.0149266	.0163746	.0178734	.0194210	.0210154	2
3	.0005817	.0006908	.0008119	.0009454	.0010916	.0012511	.0014242	.0016112	3
4	.0000233	.0000294	.0000365	.0000449	.0000546	.0000657	.0000783	.0000926	4
5	.0000007	.0000010	.0000013	.0000017	.0000022	.0000028	.0000034	.0000043	5
6				.0000001	.0000001	.0000001	.0000001	.0000002	6
X	A=.24	A=.25	A=.26	A=.27	A=.28	A=.29	A=.30	A=.40	X
0	.7866279	.7788008	.7710516	.7633795	.7557837	.7482636	.7408182	.6703200	0
1	.1887907	.1947002	.2004734	.2061125	.2116194	.2169964	.2222455	.2681280	1
2	.0226549	.0243375	.0260615	.0278252	.0296267	.0314645	.0333368	.0352596	2
3	.0018124	.0022281	.002587	.0029043	.00327652	.00360416	.00389337	.0041501	3
4	.0001087	.0001268	.0001468	.0001690	.0001936	.0002205	.0002500	.00027150	4
5	.0000052	.0000063	.0000076	.0000091	.0000108	.0000128	.0000150	.0000172	5
6	.0000002	.0000003	.0000003	.0000004	.0000005	.0000006	.0000008	.0000008	6
7								.0000002	7
X	A=.5	A=.6	A=.7	A=.8	A=.9	A=1.0	A=1.1	A=1.2	X
0	.606531	.548812	.496585	.449329	.406570	.367879	.332871	.301194	0
1	.303265	.329287	.347610	.359463	.365913	.367879	.366158	.361433	1
2	.075816	.098786	.121663	.143785	.164661	.183940	.201387	.216860	2
3	.012636	.019757	.028388	.038343	.049398	.061313	.073842	.086744	3
4	.001580	.002964	.004968	.007669	.011115	.015328	.020307	.026023	4
5	.000158	.000356	.000696	.001227	.002001	.003066	.004467	.006246	5
6	.000013	.000036	.000081	.000164	.000300	.000511	.000819	.001249	6
7	.000001	.000003	.000008	.000019	.000039	.000073	.000129	.000214	7
8			.000001	.000002	.000004	.000009	.000018	.000032	8
9						.000001	.000002	.000004	9
10								.000001	10
X	A=1.3	A=1.4	A=1.5	A=1.6	A=1.7	A=1.8	A=1.9	A=2.0	X
0	.272532	.246597	.223130	.201897	.182684	.165299	.149569	.135335	0
1	.354291	.345236	.334695	.323034	.310562	.297538	.284180	.270671	1
2	.230289	.241665	.251021	.258428	.263978	.267784	.269971	.270671	2
3	.099792	.112777	.125511	.137828	.149587	.160671	.170982	.180447	3
4	.032432	.039472	.047067	.055131	.063575	.072302	.081216	.090224	4
5	.008432	.011052	.014120	.017642	.021615	.026029	.030862	.036089	5
6	.001827	.002579	.003530	.004705	.006124	.007809	.009773	.012030	6
7	.000339	.000516	.000756	.001075	.001487	.002008	.002653	.003437	7
8	.000055	.000090	.000142	.000215	.000316	.000452	.000630	.000859	8
9	.000008	.000014	.000024	.000038	.000060	.000090	.000133	.000191	9

TABLE 1

X	A=1.3	A=1.4	A=1.5	A=1.6	A=1.7	A=1.8	A=1.9	A=2.0	X
10	.000001	.000002	.000004	.000006	.000010	.000016	.000025	.000038	10
11				.000001	.000002	.000003	.000004	.000007	11
12							.000001	.000001	12
X	A=2.1	A=2.2	A=2.3	A=2.4	A=2.5	A=2.6	A=2.7	A=2.8	X
0	.122456	.110803	.100259	.090718	.082085	.074274	.067206	.060810	0
1	.257159	.243767	.230595	.217723	.205212	.193111	.181455	.170268	1
2	.270016	.268144	.265185	.261268	.256516	.251045	.244964	.238375	2
3	.189012	.196639	.203308	.209014	.213763	.217572	.220468	.222484	3
4	.099231	.108151	.116902	.125409	.133602	.141422	.148816	.155739	4
5	.041677	.047587	.053775	.060196	.066801	.073539	.080360	.087214	5
6	.014587	.017448	.020614	.024078	.027834	.031867	.036162	.040700	6
7	.004376	.005484	.006773	.008255	.009941	.011836	.013948	.016280	7
8	.001149	.001508	.001947	.002477	.003106	.003847	.004708	.005698	8
9	.000268	.000369	.000498	.000660	.000863	.001111	.001412	.001773	9
10	.000056	.000081	.000114	.000159	.000216	.000289	.000381	.000496	10
11	.000011	.000016	.000024	.000035	.000049	.000068	.000094	.000126	11
12	.000002	.000003	.000005	.000007	.000010	.000015	.000021	.000029	12
13		.000001	.000001	.000001	.000002	.000003	.000004	.000006	13
14						.000001	.000001	.000001	14
X	A=2.9	A=3.0	A=3.1	A=3.2	A=3.3	A=3.4	A=3.5	A=3.6	X
0	.055023	.049787	.045049	.040762	.036883	.033373	.030197	.027324	0
1	.159567	.149361	.139653	.130439	.121714	.113469	.105691	.098365	1
2	.231373	.224042	.216461	.208702	.200829	.192898	.184959	.177058	2
3	.223660	.224042	.223677	.222616	.220912	.218617	.215785	.212469	3
4	.162154	.168031	.173350	.178093	.182252	.185825	.188812	.191222	4
5	.094049	.100819	.107477	.113979	.120286	.126361	.132169	.137680	5
6	.045457	.050409	.055530	.060789	.066158	.071604	.077098	.082608	6
7	.018832	.021604	.024592	.027789	.031189	.034779	.038549	.042484	7
8	.006827	.008102	.009529	.011116	.012865	.014781	.016865	.019118	8
9	.002200	.002701	.003282	.003952	.004717	.005584	.006559	.007647	9
10	.000638	.000810	.001018	.001265	.001557	.001899	.002296	.002753	10
11	.000168	.000221	.000287	.000368	.000467	.000587	.000730	.000901	11
12	.000041	.000055	.000074	.000098	.000128	.000166	.000213	.000270	12
13	.000009	.000013	.000018	.000024	.000033	.000043	.000057	.000075	13
14	.000002	.000003	.000004	.000006	.000008	.000011	.000014	.000019	14
15		.000001	.000001	.000001	.000002	.000002	.000003	.000005	15
16						.000001	.000001	.000001	16
X	A=3.7	A=3.8	A=3.9	A=4.0	A=4.1	A=4.2	A=4.3	A=4.4	X
0	.024724	.022371	.020242	.018316	.016573	.014996	.013569	.012277	0
1	.091477	.085009	.078943	.073263	.067948	.062981	.058345	.054020	1
2	.169233	.161517	.153940	.146525	.139293	.132261	.125441	.118845	2
3	.208720	.204588	.200122	.195367	.190368	.185165	.179799	.174305	3
4	.193066	.194359	.195119	.195367	.195127	.194424	.193284	.191736	4
5	.142869	.147713	.152193	.156293	.160004	.163316	.166224	.168728	5
6	.088103	.093551	.098925	.104196	.109336	.114321	.119127	.123734	6
7	.046568	.050785	.055115	.059540	.064040	.068593	.073178	.077775	7
8	.021538	.024123	.026869	.029770	.032820	.036011	.039333	.042776	8
9	.008854	.010185	.011643	.013231	.014951	.016805	.018793	.020913	9
10	.003276	.003870	.004541	.005292	.006130	.007058	.008081	.009202	10
11	.001102	.001337	.001610	.001925	.002285	.002695	.003159	.003681	11
12	.000340	.000423	.000523	.000642	.000781	.000943	.001132	.001350	12
13	.000097	.000124	.000157	.000197	.000246	.000305	.000374	.000457	13
14	.000026	.000034	.000044	.000056	.000072	.000091	.000115	.000144	14
15	.000006	.000009	.000011	.000015	.000020	.000026	.000033	.000042	15
16	.000001	.000002	.000003	.000004	.000005	.000007	.000009	.000012	16
17			.000001	.000001	.000001	.000002	.000002	.000003	17
18							.000001	.000001	18
X	A=4.5	A=4.6	A=4.7	A=4.8	A=4.9	A=5.0	A=5.1	A=5.2	X
0	.011109	.010052	.009095	.008230	.007447	.006738	.006097	.005517	0
1	.049990	.046238	.042748	.039503	.036488	.033690	.031093	.028686	1
2	.112479	.106348	.100457	.094807	.089396	.084224	.079288	.074584	2

TABLE I

X	A=4.5	A=4.6	A=4.7	A=4.8	A=4.9	A=5.0	A=5.1	A=5.2	X
3	.168718	.163068	.157383	.151691	.146014	.140374	.134790	.129279	3
4	.189808	.187528	.184925	.182029	.178867	.175467	.171857	.168063	4
5	.170827	.172526	.173803	.174748	.175290	.175467	.175294	.174785	5
6	.128120	.132270	.136167	.139798	.143153	.146223	.149000	.151480	6
7	.082363	.086920	.091426	.095862	.100207	.104445	.108557	.112528	7
8	.046329	.049979	.053713	.057517	.061377	.065278	.069205	.073143	8
9	.023165	.025545	.028050	.030676	.033416	.036266	.039216	.042261	9
10	.010424	.011751	.013184	.014724	.016374	.018133	.020000	.021976	10
11	.004264	.004914	.005633	.006425	.007294	.008242	.009273	.010388	11
12	.001599	.001884	.002206	.002570	.002978	.003434	.003941	.004502	12
13	.000554	.000667	.000798	.000949	.001123	.001321	.001546	.001801	13
14	.000178	.000219	.000268	.000325	.000393	.000472	.000563	.000669	14
15	.000053	.000067	.000084	.000104	.000128	.000157	.000191	.000232	15
16	.000015	.000019	.000025	.000031	.000039	.000049	.000061	.000075	16
17	.000004	.000005	.000007	.000009	.000011	.000014	.000018	.000023	17
18	.000001	.000001	.000002	.000002	.000003	.000004	.000005	.000007	18
19				.000001	.000001	.000001	.000001	.000002	19

X	A=5.3	A=5.4	A=5.5	A=5.6	A=5.7	A=5.8	A=5.9	A=6.0	X
0	.004992	.004517	.004087	.003698	.003346	.003028	.002739	.002479	0
1	.026455	.024390	.022477	.020708	.019072	.017560	.016163	.014873	1
2	.070107	.065852	.061812	.057983	.054355	.050923	.047680	.044618	2
3	.123856	.118533	.113323	.108234	.103275	.098452	.093771	.089235	3
4	.164109	.160020	.155819	.151528	.147167	.142755	.138312	.133853	4
5	.173955	.172821	.171401	.169711	.167770	.165596	.163208	.160623	5
6	.153660	.155539	.157117	.158397	.159382	.160076	.160488	.160623	6
7	.116343	.119987	.123449	.126717	.129782	.132635	.135268	.137677	7
8	.077077	.080991	.084871	.088702	.092470	.096160	.099768	.103288	8
9	.045390	.048595	.051866	.055193	.058564	.061970	.065398	.068838	9
10	.024057	.026241	.028526	.030908	.033382	.035943	.038585	.041303	10
11	.011591	.012882	.014263	.015735	.017298	.018952	.020696	.022529	11
12	.005119	.005797	.006537	.007343	.008216	.009160	.010175	.011264	12
13	.002087	.002408	.002766	.003163	.003603	.004087	.004618	.005199	13
14	.000790	.000929	.001087	.001265	.001467	.001693	.001946	.002228	14
15	.000279	.000334	.000398	.000472	.000557	.000655	.000765	.000891	15
16	.000092	.000113	.000137	.000165	.000199	.000237	.000282	.000334	16
17	.000029	.000036	.000044	.000054	.000067	.000081	.000098	.000118	17
18	.000008	.000011	.000014	.000017	.000021	.000026	.000032	.000039	18
19	.000002	.000003	.000004	.000005	.000006	.000008	.000010	.000012	19
20	.000001	.000001	.000001	.000001	.000002	.000002	.000003	.000004	20
21				.000001	.000001	.000001	.000001	.000001	21

X	A=6.1	A=6.2	A=6.3	A=6.4	A=6.5	A=6.6	A=6.7	A=6.8	X
0	.002243	.002029	.001836	.001662	.001503	.001360	.001231	.001114	0
1	.013681	.012582	.011569	.010634	.009772	.008978	.008247	.007574	1
2	.041729	.039006	.036441	.034029	.031760	.029629	.027628	.025750	2
3	.084848	.080612	.076527	.072595	.068814	.065183	.061702	.058368	3
4	.129393	.124948	.120530	.116151	.111822	.107553	.103351	.099225	4
5	.157860	.154936	.151868	.148674	.145369	.141969	.138490	.134946	5
6	.160491	.160100	.159461	.158585	.157483	.156166	.154648	.152939	6
7	.139856	.141803	.143515	.144992	.146234	.147243	.148020	.148569	7
8	.106640	.109897	.113018	.115994	.118815	.121475	.123967	.126284	8
9	.072279	.075707	.079113	.082484	.085811	.089082	.092286	.095415	9
10	.044090	.046938	.049841	.052790	.055777	.058794	.061832	.064882	10
11	.024450	.026456	.028545	.030714	.032959	.035276	.037661	.040109	11
12	.012429	.013669	.014986	.016381	.017853	.019402	.021028	.022728	12
13	.005832	.006519	.007263	.008064	.008926	.009850	.010837	.011889	13
14	.002541	.002887	.003268	.003687	.004144	.004644	.005186	.005774	14
15	.001033	.001193	.001373	.001573	.001796	.002043	.002317	.002618	15
16	.000394	.000462	.000540	.000629	.000730	.000843	.000970	.001113	16
17	.000141	.000169	.000200	.000237	.000279	.000327	.000382	.000445	17
18	.000048	.000058	.000070	.000084	.000101	.000120	.000142	.000168	18
19	.000015	.000019	.000023	.000028	.000034	.000042	.000050	.000060	19
20	.000005	.000006	.000007	.000009	.000011	.000014	.000017	.000020	20
21	.000001	.000002	.000002	.000003	.000003	.000004	.000005	.000007	21
22			.000001	.000001	.000001	.000001	.000002	.000002	22

TABLE I

X	A=6.1	A=6.2	A=6.3	A=6.4	A=6.5	A=6.6	A=6.7	A=6.8	X
23								000001	23
X	A=6.9	A=7.0	A=7.1	A=7.2	A=7.3	A=7.4	A=7.5	A=7.6	X
0	001008	000912	000825	000747	000676	000611	000553	000500	0
1	006954	006383	005858	005375	004931	004523	004148	003803	1
2	023990	022341	020797	019352	018000	016736	015555	014453	2
3	055178	052129	049219	046444	043799	041282	038889	036614	3
4	095182	091226	087364	083598	079934	076372	072916	069567	4
5	131351	127717	124057	120382	116703	113031	109375	105742	5
6	151053	149003	146800	144458	141989	139405	136718	133940	6
7	148895	149003	148897	148586	148074	147371	146484	145421	7
8	128422	130377	132146	133727	135118	136318	137329	138150	8
9	098457	101405	104249	106982	109596	112084	114440	116660	9
10	067935	070983	074017	077027	080005	082942	085830	088661	10
11	042614	045171	047774	050418	053094	055797	058521	061257	11
12	024503	026350	028267	030251	032299	034408	036575	038796	12
13	013005	014188	015438	016754	018137	019586	021101	022681	13
14	006410	007094	007829	008616	009457	010353	011304	012312	14
15	002949	003311	003706	004136	004602	005107	005652	006238	15
16	001272	001448	001644	001861	002100	002362	002649	002963	16
17	000516	000596	000687	000788	000902	001028	001169	001325	17
18	000198	000232	000271	000315	000366	000423	000487	000559	18
19	000072	000085	000101	000119	000141	000165	000192	000224	19
20	000025	000030	000036	000043	000051	000061	000072	000085	20
21	000008	000010	000012	000015	000018	000021	000026	000031	21
22	000003	000003	000004	000005	000006	000007	000009	000011	22
23	000001	000001	000001	000002	000002	000002	000003	000004	23
24					000001	000001	000001	000001	24
X	A=7.7	A=7.8	A=7.9	A=8.0	A=8.1	A=8.2	A=8.3	A=8.4	X
0	000453	000410	000371	000335	000304	000275	000249	000225	0
1	003487	003196	002929	002684	002459	002252	002063	001889	1
2	013424	012464	011569	010735	009958	009234	008560	007933	2
3	034455	032407	030465	028626	026886	025239	023683	022213	3
4	066326	063193	060169	057252	054443	051740	049142	046648	4
5	102142	098581	095067	091604	088198	084854	081576	078369	5
6	131082	128156	125171	122138	119067	115967	112847	109716	6
7	144191	142802	141264	139587	137778	135848	133805	131659	7
8	138783	139232	139499	139587	139500	139244	138823	138242	8
9	118737	120668	122449	124077	125550	126866	128025	129026	9
10	091427	094121	096735	099262	101696	104031	106261	108382	10
11	063999	066740	069473	072190	074885	077550	080179	082764	11
12	041066	043381	045736	048127	050547	052993	055457	058035	12
13	024324	026029	027794	029616	031495	033426	035407	037435	13
14	013378	014502	015684	016924	018222	019578	020991	022461	14
15	006867	007541	008260	009026	009840	010703	011615	012578	15
16	003305	003676	004078	004513	004981	005485	006025	006604	16
17	001497	001687	001895	002124	002374	002646	002942	003263	17
18	000640	000731	000832	000944	001068	001205	001357	001523	18
19	000260	000300	000346	000397	000455	000520	000593	000673	19
20	000100	000117	000137	000159	000184	000213	000246	000283	20
21	000037	000043	000051	000061	000071	000083	000097	000113	21
22	000013	000015	000018	000022	000026	000031	000037	000043	22
23	000004	000005	000006	000008	000009	000011	000013	000016	23
24	000001	000002	000002	000003	000003	000004	000005	000006	24
25		000001	000001	000001	000001	000001	000002	000002	25
26								000001	26
X	A=8.5	A=8.6	A=8.7	A=8.8	A=8.9	A=9.0	A=9.1	A=9.2	X
0	000203	000184	000167	000151	000136	000123	000112	000101	0
1	001729	001583	001449	001326	001214	001111	001016	000930	1
2	007350	006808	006304	005836	005402	004998	004624	004276	2
3	020826	019517	018283	017120	016025	014994	014025	013113	3
4	044255	041961	039765	037664	035656	033737	031906	030160	4
5	075233	072174	069192	066289	063467	060727	058069	055494	5

TABLE I

X	A=8.5	A=8.6	A=8.7	A=8.8	A=8.9	A=9.0	A=9.1	A=9.2	X
6	.106581	.103449	.100328	.097224	.094143	.091090	.088072	.085091	6
7	.129419	.127094	.124693	.122224	.119696	.117116	.114493	.111834	7
8	.137508	.136626	.135604	.134446	.133161	.131756	.130236	.128609	8
9	.129869	.130554	.131084	.131459	.131682	.131756	.131683	.131467	9
10	.110388	.112277	.114043	.115684	.117197	.118580	.119832	.120950	10
11	.085300	.087780	.090197	.092547	.094823	.097020	.099133	.101158	11
12	.060421	.062909	.065393	.067868	.070327	.072765	.075176	.077555	12
13	.039506	.041617	.043763	.045941	.048147	.050376	.052623	.054885	13
14	.023986	.025565	.027196	.028877	.030608	.032384	.034205	.036067	14
15	.013592	.014657	.015773	.016941	.018161	.019431	.020751	.022121	15
16	.007221	.007878	.008577	.009318	.010102	.010930	.011802	.012720	16
17	.003610	.003985	.004389	.004823	.005289	.005786	.006318	.006894	17
18	.001705	.001904	.002122	.002358	.002615	.002893	.003194	.003518	18
19	.000763	.000862	.000971	.001092	.001225	.001370	.001530	.001704	19
20	.000324	.000371	.000423	.000481	.000545	.000617	.000696	.000784	20
21	.000131	.000152	.000175	.000201	.000231	.000264	.000302	.000343	21
22	.000051	.000059	.000069	.000081	.000093	.000108	.000125	.000144	22
23	.000019	.000022	.000026	.000031	.000036	.000042	.000049	.000057	23
24	.000007	.000008	.000009	.000011	.000013	.000016	.000019	.000022	24
25	.000002	.000003	.000003	.000004	.000005	.000006	.000007	.000008	25
26	.000001	.000001	.000001	.000001	.000002	.000002	.000002	.000003	26
27					.000001	.000001	.000001	.000001	27
X	A=9.3	A=9.4	A=9.5	A=9.6	A=9.7	A=9.8	A=9.9	A=10.0	X
0	.000091	.000083	.000075	.000068	.000061	.000055	.000050	.000045	0
1	.000850	.000778	.000711	.000650	.000594	.000543	.000497	.000454	1
2	.003954	.003655	.003378	.003121	.002883	.002663	.002459	.002270	2
3	.012256	.011452	.010696	.009987	.009322	.008698	.008114	.007567	3
4	.028496	.026911	.025403	.023969	.022606	.021311	.020082	.018917	4
5	.053002	.050593	.048266	.046020	.043855	.041770	.039763	.037833	5
6	.082154	.079262	.076421	.073632	.070899	.068224	.065609	.063055	6
7	.109147	.106438	.103714	.100981	.098246	.095514	.092790	.090079	7
8	.126883	.125065	.123160	.121178	.119123	.117004	.114827	.112599	8
9	.131113	.130623	.130003	.129256	.128388	.127405	.126310	.125110	9
10	.121935	.122786	.123502	.124086	.124537	.124857	.125047	.125110	10
11	.103090	.104926	.106661	.108293	.109819	.111236	.112542	.113736	11
12	.079895	.082192	.084440	.086634	.088770	.090843	.092847	.094780	12
13	.057156	.059431	.061706	.063976	.066236	.068481	.070707	.072908	13
14	.037968	.039904	.041872	.043869	.045892	.047937	.050000	.052077	14
15	.023540	.025006	.026519	.028076	.029677	.031319	.033000	.034718	15
16	.013683	.014691	.015746	.016846	.017992	.019183	.020410	.021699	16
17	.007485	.008123	.008799	.009513	.010266	.011058	.011891	.012764	17
18	.003867	.004242	.004644	.005074	.005532	.006021	.006540	.007091	18
19	.001893	.002099	.002322	.002563	.002824	.003105	.003408	.003732	19
20	.000880	.000986	.001103	.001230	.001370	.001522	.001687	.001866	20
21	.000390	.000442	.000499	.000563	.000633	.000710	.000795	.000889	21
22	.000165	.000189	.000215	.000245	.000279	.000316	.000358	.000404	22
23	.000067	.000077	.000089	.000102	.000118	.000135	.000154	.000176	23
24	.000026	.000030	.000035	.000041	.000048	.000055	.000064	.000073	24
25	.000010	.000011	.000013	.000016	.000018	.000022	.000025	.000029	25
26	.000003	.000004	.000005	.000006	.000007	.000008	.000010	.000011	26
27	.000001	.000001	.000002	.000002	.000002	.000003	.000004	.000004	27
28			.000001	.000001	.000001	.000001	.000001	.000001	28
29								.000001	29
X	A=10.1	A=10.2	A=10.3	A=10.4	A=10.5	A=10.6	A=10.7	A=10.8	X
0	.000041	.000037	.000034	.000030	.000028	.000025	.000023	.000020	0
1	.000415	.000379	.000346	.000317	.000289	.000264	.000241	.000220	1
2	.002095	.001934	.001784	.001646	.001518	.001400	.001291	.001190	2
3	.007054	.006574	.006125	.005705	.005313	.004946	.004603	.004283	3
4	.017811	.016764	.015773	.014834	.013946	.013107	.012313	.011564	4
5	.035979	.034199	.032492	.030855	.029287	.027786	.026350	.024978	5
6	.060565	.058139	.055777	.053482	.051252	.049089	.046991	.044960	6
7	.087387	.084716	.082072	.079458	.076878	.074334	.071830	.069367	7
8	.110326	.108013	.105668	.103296	.100902	.098493	.096072	.093646	8
9	.123810	.122415	.120931	.119364	.117720	.116003	.114219	.112375	9
10	.125048	.124863	.124559	.124139	.123606	.122963	.122215	.121365	10

TABLE I

X	A=10.1	A=10.2	A=10.3	A=10.4	A=10.5	A=10.6	A=10.7	A=10.8	X
11	.114817	.115782	.116633	.117368	.117987	.118492	.118882	.119159	11
12	.096637	.098415	.100110	.101719	.103239	.104668	.106003	.107243	12
13	.075080	.077218	.079318	.081375	.083385	.085344	.087248	.089094	13
14	.054165	.056259	.058355	.060450	.062539	.064618	.066683	.068730	14
15	.036471	.038256	.040071	.041912	.043777	.045663	.047567	.049485	15
16	.023022	.024388	.025795	.027243	.028729	.030252	.031810	.033403	16
17	.013678	.014633	.015629	.016666	.017744	.018863	.020022	.021220	17
18	.007675	.008292	.008943	.009629	.010351	.011108	.011902	.012732	18
19	.004080	.004451	.004848	.005271	.005720	.006197	.006703	.007237	19
20	.002060	.002270	.002497	.002741	.003003	.003285	.003586	.003908	20
21	.000991	.001103	.001225	.001357	.001502	.001658	.001827	.002010	21
22	.000455	.000511	.000573	.000642	.000717	.000799	.000889	.000987	22
23	.000200	.000227	.000257	.000290	.000327	.000368	.000413	.000463	23
24	.000084	.000096	.000110	.000126	.000143	.000163	.000184	.000208	24
25	.000034	.000039	.000045	.000052	.000060	.000069	.000079	.000090	25
26	.000013	.000015	.000018	.000021	.000024	.000028	.000032	.000037	26
27	.000005	.000006	.000007	.000008	.000009	.000011	.000013	.000015	27
28	.000002	.000002	.000003	.000003	.000004	.000004	.000005	.000006	28
29	.000001	.000001	.000001	.000001	.000001	.000002	.000002	.000002	29
30						.000001	.000001	.000001	30
X	A=10.9	A=11.0	A=11.1	A=11.2	A=11.3	A=11.4	A=11.5	A=11.6	X
0	.000018	.000017	.000015	.000014	.000012	.000011	.000010	.000009	0
1	.000201	.000184	.000168	.000153	.000140	.000128	.000117	.000106	1
2	.001097	.001010	.000931	.000858	.000790	.000727	.000670	.000617	2
3	.003984	.003705	.003445	.003202	.002975	.002764	.002568	.002385	3
4	.010856	.010189	.009559	.008965	.008406	.007879	.007382	.006915	4
5	.023667	.022415	.021221	.020082	.018997	.017963	.016979	.016043	5
6	.042995	.041095	.039259	.037487	.035778	.034130	.032544	.031017	6
7	.066949	.064577	.062253	.059979	.057755	.055584	.053465	.051400	7
8	.091218	.088794	.086376	.083970	.081579	.079207	.076856	.074529	8
9	.110475	.108526	.106531	.104496	.102427	.100328	.098204	.096060	9
10	.120418	.119378	.118249	.117036	.115743	.114374	.112935	.111430	10
11	.119323	.119378	.119324	.119164	.118899	.118533	.118068	.117508	11
12	.108385	.109430	.110375	.111220	.111964	.112607	.113149	.113591	12
13	.090877	.092595	.094243	.095820	.097322	.098747	.100093	.101358	13
14	.070754	.072753	.074721	.076656	.078553	.080409	.082220	.083982	14
15	.051415	.053352	.055294	.057236	.059177	.061111	.063035	.064946	15
16	.033026	.036680	.038360	.040065	.041793	.043541	.045306	.047086	16
17	.022458	.023734	.025047	.026396	.027780	.029198	.030640	.032129	17
18	.013600	.014504	.015446	.016424	.017440	.018492	.019581	.020706	18
19	.007802	.008397	.009023	.009682	.010372	.011095	.011852	.012641	19
20	.004252	.004618	.005008	.005422	.005860	.006324	.006815	.007332	20
21	.002207	.002419	.002647	.002892	.003153	.003433	.003732	.004050	21
22	.001093	.001210	.001336	.001472	.001620	.001779	.001951	.002135	22
23	.000518	.000578	.000645	.000717	.000796	.000882	.000975	.001077	23
24	.000235	.000265	.000298	.000335	.000375	.000419	.000467	.000521	24
25	.000103	.000117	.000132	.000150	.000169	.000191	.000215	.000242	25
26	.000043	.000049	.000057	.000065	.000074	.000084	.000095	.000108	26
27	.000017	.000020	.000023	.000027	.000031	.000035	.000041	.000046	27
28	.000007	.000008	.000009	.000011	.000012	.000014	.000017	.000019	28
29	.000003	.000003	.000004	.000004	.000005	.000006	.000007	.000008	29
30	.000001	.000001	.000001	.000002	.000002	.000002	.000003	.000003	30
31				.000001	.000001	.000001	.000001	.000001	31
X	A=11.7	A=11.8	A=11.9	A=12.0	A=12.1	A=12.2	A=12.3	A=12.4	X
0	.000008	.000008	.000007	.000006	.000006	.000005	.000005	.000004	0
1	.000097	.000089	.000081	.000074	.000067	.000061	.000056	.000051	1
2	.000568	.000522	.000481	.000442	.000407	.000374	.000344	.000317	2
3	.002214	.002055	.001907	.001770	.001642	.001522	.001412	.001309	3
4	.006476	.006062	.005674	.005309	.004966	.004643	.004341	.004057	4
5	.015153	.014307	.013504	.012741	.012017	.011330	.010679	.010062	5
6	.029549	.028137	.026782	.025481	.024234	.023037	.021892	.020794	6
7	.049388	.047432	.045530	.043682	.041889	.040151	.038467	.036836	7
8	.072231	.069962	.067725	.065523	.063358	.061230	.059142	.057095	8
9	.093900	.091776	.089548	.087364	.085181	.083001	.080828	.078665	9

TABLE I

X	A=11.7	A=11.8	A=11.9	A=12.0	A=12.1	A=12.2	A=12.3	A=12.4	X
10	.109863	.108239	.106562	.104837	.103069	.101261	.099418	.097544	10
11	.116854	.116110	.115281	.114368	.113376	.112308	.111168	.109959	11
12	.113933	.114175	.114320	.114368	.114321	.114180	.113947	.113624	12
13	.102539	.103636	.104647	.105570	.106406	.107153	.107811	.108380	13
14	.085694	.087350	.088950	.090489	.091965	.093376	.094720	.095994	14
15	.066841	.068716	.070567	.072391	.074185	.075946	.077670	.079355	15
16	.048877	.050678	.052484	.054293	.056103	.057909	.059709	.061500	16
17	.033639	.035176	.036739	.038325	.039932	.041558	.043201	.044859	17
18	.021865	.023060	.024288	.025550	.026843	.028167	.029521	.030903	18
19	.013465	.014322	.015213	.016137	.017095	.018086	.019111	.020168	19
20	.007877	.008450	.009051	.009682	.010342	.011033	.011753	.012504	20
21	.004388	.004748	.005129	.005533	.005959	.006409	.006884	.007383	21
22	.002334	.002547	.002774	.003018	.003278	.003554	.003849	.004162	22
23	.001187	.001307	.001435	.001574	.001724	.001885	.002058	.002244	23
24	.000579	.000642	.000712	.000787	.000869	.000958	.001055	.001159	24
25	.000271	.000303	.000339	.000378	.000421	.000468	.000519	.000575	25
26	.000122	.000138	.000155	.000174	.000196	.000219	.000246	.000274	26
27	.000053	.000060	.000068	.000078	.000088	.000099	.000112	.000126	27
28	.000022	.000025	.000029	.000033	.000038	.000043	.000049	.000056	28
29	.000009	.000010	.000012	.000014	.000016	.000018	.000021	.000024	29
30	.000003	.000004	.000005	.000005	.000006	.000007	.000009	.000010	30
31	.000001	.000002	.000002	.000002	.000002	.000003	.000003	.000004	31
32		.000001	.000001	.000001	.000001	.000001	.000001	.000002	32
33								.000001	33
X	A=12.5	A=12.6	A=12.7	A=12.8	A=12.9	A=13.0	A=13.1	A=13.2	X
0	.000004	.000003	.000003	.000003	.000002	.000002	.000002	.000002	0
1	.000047	.000042	.000039	.000035	.000032	.000029	.000027	.000024	1
2	.000291	.000268	.000246	.000226	.000208	.000191	.000175	.000161	2
3	.001213	.001124	.001042	.000965	.000894	.000828	.000766	.000709	3
4	.003791	.003541	.003307	.003088	.002882	.002690	.002510	.002341	4
5	.009477	.008924	.008400	.007905	.007436	.006994	.006575	.006180	5
6	.019745	.018740	.017781	.016864	.015988	.015153	.014356	.013596	6
7	.035258	.033733	.032259	.030837	.029464	.028141	.026866	.025639	7
8	.055091	.053129	.051212	.049339	.047511	.045730	.043994	.042304	8
9	.076515	.074381	.072265	.070171	.068100	.066054	.064036	.062046	9
10	.095644	.093720	.091777	.089819	.087849	.085870	.083887	.081901	10
11	.108686	.107352	.105961	.104516	.103023	.101483	.099901	.098281	11
12	.113215	.112720	.112142	.111484	.110749	.109940	.109059	.108109	12
13	.108860	.109251	.109554	.109769	.109897	.109940	.109898	.109773	13
14	.097197	.098326	.099381	.100360	.101263	.102087	.102833	.103500	14
15	.080997	.082594	.084143	.085641	.087086	.088475	.089807	.091080	15
16	.063279	.065043	.066788	.068513	.070213	.071886	.073530	.075141	16
17	.046529	.048208	.049895	.051586	.053279	.054972	.056661	.058345	17
18	.032312	.033746	.035204	.036683	.038183	.039702	.041237	.042786	18
19	.021258	.022379	.023531	.024713	.025925	.027164	.028432	.029723	19
20	.013286	.014099	.014942	.015816	.016721	.017657	.018623	.019619	20
21	.007908	.008459	.009036	.009640	.010272	.010930	.011617	.012332	21
22	.004493	.004845	.005216	.005609	.006023	.006459	.006917	.007399	22
23	.002442	.002654	.002880	.003122	.003378	.003651	.003940	.004246	23
24	.001272	.001393	.001524	.001665	.001816	.001977	.002151	.002336	24
25	.000636	.000702	.000774	.000852	.000937	.001028	.001127	.001233	25
26	.000306	.000340	.000378	.000420	.000465	.000514	.000568	.000626	26
27	.000142	.000159	.000178	.000199	.000222	.000248	.000275	.000306	27
28	.000063	.000071	.000081	.000091	.000102	.000115	.000129	.000144	28
29	.000027	.000031	.000035	.000040	.000046	.000052	.000058	.000066	29
30	.000011	.000013	.000015	.000017	.000020	.000022	.000025	.000029	30
31	.000005	.000005	.000006	.000007	.000008	.000009	.000011	.000012	31
32	.000002	.000002	.000002	.000003	.000003	.000004	.000004	.000005	32
33	.000001	.000001	.000001	.000001	.000001	.000001	.000002	.000002	33
34						.000001	.000001	.000001	34
X	A=13.3	A=13.4	A=13.5	A=13.6	A=13.7	A=13.8	A=13.9	A=14.0	X
0	.000002	.000002	.000001	.000001	.000001	.000001	.000001	.000001	0
1	.000022	.000020	.000019	.000017	.000015	.000014	.000013	.000011	1
2	.000148	.000136	.000125	.000115	.000105	.000097	.000089	.000081	2
3	.000657	.000608	.000562	.000520	.000481	.000445	.000411	.000381	3



TABLE I

X	A=13.3	A=13.4	A=13.5	A=13.6	A=13.7	A=13.8	A=13.9	A=14.0	X
4	.002183	.002039	.001897	.001768	.001648	.001535	.001429	.000380	4
5	.005807	.005455	.005123	.004810	.004514	.004236	.003974	.001331	5
6	.012872	.012183	.011526	.010902	.010308	.009743	.009206	.003727	6
7	.024458	.023322	.022230	.021181	.020173	.019207	.018280	.008696	7
8	.040661	.039064	.037512	.036007	.034547	.033132	.031762	.017392	8
9	.060088	.058161	.056269	.054410	.052588	.050802	.049054	.030436	9
10	.079917	.077936	.075962	.073998	.072046	.070107	.068185	.047344	10
11	.096626	.094490	.093227	.091489	.089730	.087953	.086162	.066282	11
12	.107094	.106017	.104880	.103687	.102441	.101146	.099804	.084359	12
13	.109566	.109279	.108914	.108473	.107957	.107370	.106713	.098418	13
14	.104087	.104595	.105024	.105374	.105644	.105836	.105951	.105989	14
15	.092291	.093439	.094522	.095539	.096488	.097369	.098181	.105989	15
16	.076717	.078255	.079753	.081208	.082618	.083981	.085295	.088923	16
17	.060020	.061683	.063333	.064966	.066580	.068173	.069741	.086558	17
18	.044348	.045920	.047500	.049086	.050675	.052266	.053856	.071283	18
19	.031043	.032385	.033750	.035135	.036539	.037962	.039400	.055442	19
20	.020644	.021698	.022781	.023892	.025030	.026193	.027383	.040852	20
21	.013074	.013846	.014645	.015473	.016329	.017213	.018125	.028597	21
22	.007904	.008433	.008987	.009565	.010168	.010797	.011452	.019064	22
23	.004571	.004913	.005275	.005656	.006057	.006478	.006921	.012132	23
24	.002533	.002743	.002967	.003205	.003457	.003725	.004008	.007385	24
25	.001347	.001470	.001602	.001744	.001895	.002056	.002229	.004308	25
26	.000689	.000758	.000832	.000912	.000998	.001091	.001191	.002412	26
27	.000340	.000376	.000416	.000459	.000507	.000558	.000613	.001299	27
28	.000161	.000180	.000201	.000223	.000248	.000275	.000304	.000674	28
29	.000074	.000083	.000093	.000105	.000117	.000131	.000146	.000337	29
30	.000033	.000037	.000042	.000047	.000053	.000060	.000068	.000163	30
31	.000014	.000016	.000018	.000021	.000024	.000027	.000033	.000076	31
32	.000006	.000007	.000008	.000009	.000010	.000012	.000013	.000034	32
33	.000002	.000003	.000003	.000004	.000004	.000005	.000006	.000015	33
34	.000001	.000001	.000001	.000001	.000002	.000002	.000002	.000006	34
35				.000001	.000001	.000001	.000001	.000003	35
36								.000001	36
X	A=14.1	A=14.2	A=14.3	A=14.4	A=14.5	A=14.6	A=14.7	A=14.8	X
0	.000001	.000001	.000001	.000001	.000001				0
1	.000011	.000010	.000009	.000008	.000007	.000007	.000006	.000006	1
2	.000075	.000069	.000063	.000058	.000053	.000049	.000045	.000041	2
3	.000352	.000325	.000300	.000277	.000256	.000237	.000219	.000202	3
4	.001239	.001153	.001073	.000999	.000929	.000864	.000803	.000747	4
5	.003494	.003276	.003070	.002876	.002694	.002523	.002362	.002211	5
6	.008212	.007752	.007316	.006902	.006510	.006139	.005787	.005454	6
7	.016541	.015726	.014946	.014199	.013486	.012804	.012152	.011530	7
8	.029153	.027913	.026715	.025559	.024443	.023367	.022330	.021331	8
9	.045673	.044040	.042447	.040894	.039380	.037906	.036472	.035078	9
10	.064399	.062537	.060700	.058887	.057101	.055343	.053614	.051915	10
11	.082547	.080730	.078910	.077089	.075270	.073456	.071648	.069850	11
12	.096993	.095530	.094034	.092507	.090951	.089371	.087769	.086148	12
13	.105200	.104349	.103437	.102469	.101446	.100371	.099247	.098076	13
14	.105951	.105839	.105654	.105396	.105069	.104672	.104209	.103681	14
15	.099594	.100195	.100723	.101181	.101566	.101881	.102125	.102298	15
16	.087768	.088923	.090021	.091063	.092045	.092967	.093827	.094626	16
17	.072795	.074277	.075724	.077135	.078509	.079842	.081133	.082380	17
18	.057023	.058596	.060158	.061708	.063243	.064761	.066259	.067735	18
19	.042317	.043793	.045277	.046768	.048264	.049763	.051263	.052762	19
20	.029834	.031093	.032373	.033673	.034992	.036327	.037678	.039044	20
21	.020031	.021025	.022045	.023090	.024161	.025256	.026375	.027511	21
22	.012838	.013570	.014329	.015114	.015924	.016761	.017623	.018511	22
23	.007870	.008378	.008909	.009462	.010039	.010640	.011264	.011912	23
24	.004624	.004957	.005308	.005677	.006065	.006472	.006899	.007345	24
25	.002608	.002816	.003036	.003270	.003518	.003780	.004057	.004348	25
26	.001414	.001538	.001670	.001811	.001962	.002123	.002294	.002475	26
27	.000739	.000809	.000884	.000966	.001054	.001148	.001249	.001357	27
28	.000372	.000410	.000452	.000497	.000546	.000598	.000656	.000717	28

TABLE I

X	A=14.1	A=14.2	A=14.3	A=14.4	A=14.5	A=14.6	A=14.7	A=14.8	X
29	•000181	•000201	•000223	•000247	•000273	•000301	•000332	•000366	29
30	•000085	•000095	•000106	•000118	•000132	•000147	•000163	•000181	30
31	•000039	•000044	•000049	•000055	•000062	•000069	•000077	•000086	31
32	•000017	•000019	•000022	•000025	•000028	•000032	•000035	•000040	32
33	•000007	•000008	•000009	•000011	•000012	•000014	•000016	•000018	33
34	•000003	•000003	•000004	•000005	•000005	•000006	•000007	•000008	34
35	•000001	•000001	•000002	•000002	•000002	•000002	•000003	•000003	35
36		•000001	•000001	•000001	•000001	•000001	•000001	•000001	36
37								•000001	37

X	A=14.9	A=15.0	A=16	A=17	A=18	A=19	A=20	A=21	X
1	•000005	•000005	•000002	•000001					1
2	•000038	•000034	•000014	•000006	•000002	•000001			2
3	•000186	•000172	•000077	•000034	•000015	•000006	•000003	•000001	3
4	•000694	•000645	•000307	•000144	•000067	•000030	•000014	•000006	4
5	•002069	•001936	•000983	•000490	•000240	•000116	•000055	•000026	5
6	•005138	•004839	•002622	•001388	•000719	•000366	•000183	•000090	6
7	•010937	•010370	•005994	•003371	•001850	•000994	•000523	•000271	7
8	•020370	•019444	•011987	•007163	•004163	•002360	•001309	•000711	8
9	•033723	•032407	•021311	•013529	•008325	•004982	•002908	•001660	9
10	•050247	•048611	•034098	•023000	•014985	•009466	•005816	•003485	10
11	•068062	•066287	•049597	•035545	•024521	•016351	•010575	•006654	11
12	•084510	•082859	•066129	•050355	•036782	•025889	•017625	•011644	12
13	•096862	•095607	•081389	•065849	•050929	•037837	•027116	•018810	13
14	•103089	•102436	•093016	•079960	•065480	•051351	•038737	•028215	14
15	•102402	•102436	•099218	•090621	•078576	•065044	•051649	•039501	15
16	•095361	•096034	•099218	•096285	•088397	•077240	•064561	•051845	16
17	•083582	•084736	•093381	•096285	•093597	•086327	•075954	•064044	17
18	•069187	•070613	•083006	•090935	•093597	•091123	•084394	•074717	18
19	•054257	•055747	•069899	•081363	•088671	•091123	•088835	•082582	19
20	•040422	•041810	•055920	•069159	•079804	•086567	•088835	•086712	20
21	•028680	•029865	•042605	•055986	•068403	•078328	•084605	•086712	21
22	•019424	•020362	•030986	•043262	•055966	•067642	•076914	•082770	22
23	•012584	•013280	•021555	•031976	•043800	•055878	•066881	•075573	23
24	•007812	•008300	•014370	•022650	•032850	•044237	•055735	•066126	24
25	•004656	•004980	•009197	•015402	•023652	•033620	•044588	•055546	25
26	•002668	•002873	•005660	•010070	•016374	•024569	•034298	•044864	26
27	•001473	•001596	•003354	•006341	•010916	•017289	•025406	•034894	27
28	•000784	•000855	•001916	•003850	•007018	•011732	•018147	•026171	28
29	•000403	•000442	•001057	•002257	•004356	•007686	•012515	•018951	29
30	•000200	•000221	•000564	•001279	•002613	•004868	•008344	•013266	30
31	•000096	•000107	•002291	•000701	•001517	•002984	•005383	•008987	31
32	•000045	•000050	•000146	•000373	•000854	•001772	•003364	•005897	32
33	•000020	•000023	•000071	•000192	•000466	•001020	•002039	•003753	33
34	•000009	•000010	•000033	•000096	•000246	•000570	•001199	•002318	34
35	•000004	•000004	•000015	•000047	•000127	•000309	•000685	•001391	35
36	•000002	•000002	•000007	•000022	•000063	•000163	•000381	•000811	36
37	•000001	•000001	•000003	•000010	•000031	•000084	•000206	•000460	37
38			•000001	•000005	•000015	•000042	•000108	•000254	38
39			•000001	•000002	•000007	•000020	•000056	•000137	39
40				•000001	•000003	•000010	•000028	•000072	40
41					•000001	•000004	•000014	•000037	41
42					•000001	•000002	•000006	•000018	42
43						•000001	•000003	•000009	43
44							•000001	•000004	44
45							•000001	•000002	45
46								•000001	46

X	A=22	A=23	A=24	A=25	A=26	A=27	A=28	A=29	X
4	•000003	•000001	•000001						4
5	•000012	•000006	•000003	•000001					5
6	•000044	•000021	•000010	•000005	•000002	•000001			6
7	•000138	•000069	•000034	•000017	•000008	•000004	•000002	•000001	7
8	•000380	•000199	•000103	•000053	•000026	•000013	•000006	•000003	8
9	•000928	•000509	•000275	•000146	•000076	•000039	•000020	•000010	9

TABLE I

X	A=22	A=23	A=24	A=25	A=26	A=27	A=28	A=29	X
10	•002042	•001171	•0000660	•000365	•000199	•000107	•000056	•000029	10
11	•004083	•002449	•001439	•000830	•000470	•000262	•000144	•000078	11
12	•007486	•004695	•002878	•001728	•001018	•000589	•000335	•000188	12
13	•012669	•008306	•005314	•003323	•002036	•001223	•000722	•000419	13
14	•019908	•013646	•009109	•005935	•003781	•002359	•001444	•000868	14
15	•029199	•020924	•014575	•009891	•006553	•004246	•002695	•001679	15
16	•040148	•030078	•021862	•015455	•010649	•007166	•004717	•003042	16
17	•051956	•040694	•030864	•022727	•016286	•011381	•007769	•005190	17
18	•063502	•051998	•041152	•031566	•023525	•017071	•012085	•008361	18
19	•073529	•062945	•051982	•041534	•032192	•024259	•017810	•012762	19
20	•080882	•072387	•062378	•051917	•041849	•032749	•024934	•018505	20
21	•084733	•079281	•071289	•061807	•051813	•042106	•033245	•025555	21
22	•084733	•082884	•077770	•070235	•061234	•051676	•042312	•033686	22
23	•081049	•082884	•081152	•076342	•069221	•060663	•051510	•042474	23
24	•074295	•079431	•081152	•079523	•074989	•068245	•060095	•051322	24
25	•065380	•073076	•077905	•079523	•077989	•073705	•067307	•059534	25
26	•055321	•064645	•071913	•076464	•077989	•076540	•072484	•066403	26
27	•045077	•055068	•063922	•070800	•075100	•076540	•075169	•071322	27
28	•035417	•045234	•054791	•063215	•069736	•073806	•075169	•073869	28
29	•026868	•035875	•045344	•054495	•062522	•068716	•072577	•073869	29
30	•019703	•027504	•036275	•045413	•054186	•061845	•067738	•071407	30
31	•013983	•020406	•028084	•036623	•045446	•053865	•061183	•066800	31
32	•009613	•014667	•021063	•028612	•036925	•045448	•053535	•060537	32
33	•006409	•010223	•015319	•021676	•029092	•037185	•045424	•053200	33
34	•004147	•006915	•010813	•015938	•022247	•029529	•037408	•045376	34
35	•002607	•004544	•007415	•011384	•016526	•022780	•029926	•037597	35
36	•001593	•002903	•004943	•007906	•011936	•017085	•023276	•030287	36
37	•000947	•001805	•003206	•005342	•008387	•012467	•017614	•023738	37
38	•000548	•001092	•002025	•003514	•005739	•008858	•012979	•018116	38
39	•000309	•000644	•001246	•002253	•003826	•006133	•009318	•013471	39
40	•000170	•000370	•000748	•001408	•002487	•004140	•006523	•009766	40
41	•000091	•000208	•000438	•000859	•001577	•002726	•004455	•006908	41
42	•000048	•000114	•000250	•000511	•000976	•001752	•002970	•004770	42
43	•000024	•000061	•000140	•000297	•000590	•001100	•001934	•003217	43
44	•000012	•000032	•000076	•000169	•000349	•000675	•001231	•002120	44
45	•000006	•000016	•000041	•000094	•000202	•000405	•000766	•001366	45
46	•000003	•000008	•000021	•000051	•000114	•000238	•000466	•000861	46
47	•000001	•000004	•000011	•000027	•000063	•000137	•000278	•000531	47
48	•000001	•000002	•000005	•000014	•000034	•000077	•000162	•000321	48
49	•000001	•000001	•000003	•000007	•000018	•000042	•000093	•000190	49
50			•000001	•000004	•000009	•000023	•000052	•000110	50
51			•000001	•000002	•000005	•000012	•000028	•000063	51
52				•000001	•000002	•000006	•000015	•000035	52
53					•000001	•000003	•000008	•000019	53
54					•000001	•000002	•000004	•000010	54
55						•000001	•000002	•000005	55
56							•000001	•000003	56
57							•000001	•000001	57
58								•000001	58
X	A=30	A=31	A=32	A=33	A=34	A=35	A=36	A=37	X
8	•000002	•000001							8
9	•000005	•000003	•000001	•000001					9
10	•000015	•000008	•000004	•000002	•000001				10
11	•000042	•000022	•000011	•000006	•000003	•000002	•000001		11
12	•000104	•000057	•000030	•000016	•000009	•000004	•000002	•000001	12
13	•000240	•000135	•000075	•000041	•000022	•000012	•000006	•000003	13
14	•000513	•000299	•000172	•000097	•000054	•000030	•000016	•000009	14
15	•001027	•000618	•000366	•000214	•000123	•000070	•000039	•000022	15
16	•001925	•001197	•000732	•000440	•000261	•000153	•000088	•000050	16
17	•003397	•002182	•001377	•000855	•000522	•000315	•000187	•000110	17
18	•005662	•003759	•002449	•001567	•000987	•000612	•000374	•000225	18
19	•008941	•006133	•004124	•002722	•001766	•001127	•000708	•000438	19
20	•013411	•009506	•006599	•004492	•003002	•001972	•001274	•000811	20
21	•019159	•014032	•010055	•007059	•004861	•003287	•002185	•001429	21

TABLE I

X	A=30	A=31	A=32	A=33	A=34	A=35	A=36	A=37	X
22	026126	019773	014625	010588	007512	005229	003575	002403	22
23	034077	026650	020348	015192	011105	007957	005596	003866	23
24	042596	034423	027131	020889	015732	011604	008394	005960	24
25	051115	042684	034728	027573	021395	016246	012087	008821	25
26	058979	050893	042742	034997	027978	021870	016736	012552	26
27	065532	058432	050657	042774	035232	028350	022314	017202	27
28	070213	064693	057894	050412	042782	035437	028690	022731	28
29	072635	069155	063883	057365	050158	042769	035615	029001	29
30	072635	071460	068142	063102	056845	049897	042738	035768	30
31	070291	071460	070340	067173	062347	056335	049631	042691	31
32	065898	069227	070340	069272	066243	061617	055835	049361	32
33	059908	065031	068209	069272	068251	065351	060911	055345	33
34	052860	059293	064196	067234	068251	067273	064494	060228	34
35	045308	052517	058694	063392	066301	067273	066337	063670	35
36	037757	045223	052172	058110	062617	065404	066337	065438	36
37	030614	037889	045122	051828	057540	061869	064544	065438	37
38	024169	030910	037998	045008	051483	056985	061147	063716	38
39	018591	024569	031177	038084	044883	051140	056443	060449	39
40	013943	019041	024942	031419	038150	044748	050799	055915	40
41	010203	014397	019467	025289	031637	038199	044604	050460	41
42	007286	010626	014832	019870	025611	031833	038232	044453	42
43	005084	007661	011038	015249	020250	025910	032008	038250	43
44	003467	005397	008027	011437	015648	020610	026188	032165	44
45	002311	003718	005708	008387	011823	016030	020951	026447	45
46	001507	002506	003971	006017	008739	012197	016396	021272	46
47	000962	001653	002704	004224	006322	009083	012559	016746	47
48	000601	001067	001802	002904	004478	006623	009419	012909	48
49	000368	000675	001177	001956	003107	004731	006920	009747	49
50	000221	000419	000753	001291	002113	003311	004983	007213	50
51	000130	000254	000473	000835	001409	002273	003517	005233	51
52	000075	000152	000291	000530	000921	001530	002435	003723	52
53	000042	000089	000176	000330	000591	001010	001654	002599	53
54	000024	000051	000104	000202	000372	000655	001103	001781	54
55	000013	000029	000061	000121	000230	000417	000722	001198	55
56	000007	000016	000035	000071	000140	000260	000464	000792	56
57	000004	000009	000019	000041	000083	000160	000293	000514	57
58	000002	000005	000011	000023	000049	000096	000182	000328	58
59	000001	000002	000006	000013	000028	000057	000111	000206	59
60		000001	000003	000007	000016	000033	000067	000127	60
61		000001	000002	000004	000009	000019	000039	000077	61
62			000001	000002	000005	000011	000023	000046	62
63				000001	000003	000006	000013	000027	63
64				000001	000001	000003	000007	000016	64
65					000001	000002	000004	000009	65
66						000001	000002	000005	66
67							000001	000003	67
68							000001	000001	68
69								000001	69

X	A=38	A=39	A=40	A=41	A=42	A=43	A=44	A=45	X
12	000001								12
13	000002	000001							13
14	000005	000002	000001	000001					14
15	000012	000006	000003	000002	000001	000001			15
16	000028	000016	000009	000005	000003	000001	000001		16
17	000063	000036	000021	000011	000006	000003	000002	000001	17
18	000134	000079	000046	000026	000015	000008	000005	000003	18
19	000268	000161	000096	000056	000033	000019	000011	000006	19
20	000509	000315	000192	000116	000069	000041	000024	000014	20
21	000920	000584	000366	000226	000138	000083	000050	000029	21
22	001590	001036	000605	000421	000263	000163	000099	000060	22
23	002262	001756	001156	000751	000481	000304	000190	000117	23
24	004158	002853	001927	001282	000841	000544	000348	000219	24
25	006321	004451	003084	002103	001413	000936	000612	000395	25
26	009238	006677	004744	003317	002283	001548	001036	000683	26
27	013001	009644	007028	005036	003551	002466	001688	001139	27
28	017645	013430	010041	007375	005327	003787	002652	001830	28

TABLE I

X	A=38	A=39	A=40	A=41	A=42	A=43	A=44	A=45	X
29	•023120	•018065	•013849	•010426	•007715	•005615	•004024	•002840	29
30	•029286	•023485	•018465	•014249	•010801	•008049	•005902	•004261	30
31	•035899	•029546	•023826	•018845	•014633	•011164	•008376	•006185	31
32	•042630	•036009	•029783	•024146	•019206	•015002	•011517	•008697	32
33	•049089	•042556	•036101	•029999	•024444	•019548	•015357	•011860	33
34	•054864	•048814	•042471	•036175	•030196	•024723	•019873	•015697	34
35	•059567	•054393	•048539	•042377	•036235	•030374	•024984	•020182	35
36	•062876	•058926	•053932	•048263	•042274	•036280	•030535	•025227	36
37	•064575	•062111	•058305	•053480	•047986	•042163	•036312	•030681	37
38	•064575	•063746	•061373	•057702	•053038	•047711	•042046	•036333	38
39	•062919	•063746	•062947	•060661	•057117	•052604	•047436	•041923	39
40	•059773	•062152	•062947	•062178	•059973	•056550	•052180	•047163	40
41	•055400	•059120	•061412	•062178	•061436	•059308	•055998	•051763	41
42	•050124	•054897	•058487	•060697	•061436	•060720	•058665	•055462	42
43	•044295	•049791	•054407	•057874	•060007	•060720	•060029	•058042	43
44	•038255	•044133	•049461	•053928	•057280	•059340	•060029	•059361	44
45	•032304	•038248	•043965	•049135	•053461	•056703	•058695	•059361	45
46	•026686	•032428	•038231	•043794	•048812	•053005	•056143	•058070	46
47	•021576	•026908	•032537	•038203	•043620	•048494	•052559	•055599	47
48	•017081	•021863	•027114	•032632	•038167	•043442	•048180	•052124	48
49	•013246	•017401	•022134	•027304	•032715	•038123	•043263	•047869	49
50	•010067	•013573	•017707	•022389	•027480	•032786	•038072	•043082	50
51	•007501	•010379	•013888	•017999	•022631	•027643	•032846	•038014	51
52	•005482	•007784	•010683	•014192	•018279	•022859	•027793	•032897	52
53	•003930	•005728	•008063	•010979	•014485	•018546	•023073	•027931	53
54	•002766	•004137	•005972	•008336	•011266	•014768	•018800	•023276	54
55	•001911	•002934	•004343	•006214	•008603	•011546	•015040	•019044	55
56	•001297	•002043	•003102	•004549	•006452	•008865	•011817	•015303	56
57	•000864	•001398	•002177	•003272	•004754	•006688	•009122	•012081	57
58	•000566	•000940	•001502	•002313	•003443	•004958	•006920	•009374	58
59	•000365	•000621	•001018	•001607	•002451	•003614	•005161	•007149	59
60	•000231	•000404	•000679	•001098	•001716	•002590	•003785	•005362	60
61	•000144	•000258	•000445	•000738	•001181	•001826	•002730	•003956	61
62	•000088	•000162	•000287	•000488	•000800	•001266	•001937	•002871	62
63	•000053	•000101	•000182	•000318	•000533	•000864	•001353	•002051	63
64	•000032	•000061	•000114	•000204	•000350	•000581	•000930	•001442	64
65	•000018	•000037	•000070	•000128	•000226	•000384	•000630	•000998	65
66	•000011	•000022	•000042	•000080	•000144	•000250	•000420	•000681	66
67	•000006	•000013	•000025	•000049	•000090	•000161	•000276	•000457	67
68	•000003	•000007	•000015	•000029	•000056	•000102	•000178	•000303	68
69	•000002	•000004	•000009	•000017	•000034	•000063	•000114	•000197	69
70	•000001	•000002	•000005	•000010	•000020	•000039	•000072	•000127	70
71	•000001	•000001	•000003	•000006	•000012	•000024	•000044	•000080	71
72		•000001	•000002	•000003	•000007	•000014	•000027	•000050	72
73			•000001	•000002	•000004	•000008	•000016	•000031	73
74				•000001	•000002	•000005	•000010	•000019	74
75				•000001	•000001	•000003	•000006	•000011	75
76					•000001	•000002	•000003	•000007	76
77						•000001	•000002	•000004	77
78							•000001	•000002	78
79							•000001	•000001	79
80								•000001	80
X	A=46	A=47	A=48	A=49	A=50	A=51	A=52	A=53	X
17	•000001								17
18	•000001	•000001							18
19	•000003	•000002	•000001	•000001					19
20	•000008	•000004	•000002	•000001	•000001				20
21	•000017	•000010	•000006	•000003	•000002	•000001	•000001		21
22	•000036	•000021	•000012	•000007	•000004	•000002	•000001	•000001	22
23	•000071	•000043	•000026	•000015	•000009	•000005	•000003	•000002	23
24	•000137	•000084	•000051	•000031	•000019	•000011	•000006	•000004	24
25	•000252	•000158	•000099	•000061	•000037	•000022	•000013	•000008	25
26	•000445	•000286	•000182	•000115	•000071	•000044	•000027	•000016	26
27	•000758	•000499	•000324	•000208	•000132	•000083	•000051	•000032	27
28	•001246	•000837	•000555	•000364	•000236	•000151	•000096	•000060	28

TABLE 1

X	A=46	A=47	A=48	A=49	A=50	A=51	A=52	A=53	X
29	•001976	•001357	•000919	•000615	•000406	•000265	•000171	•000110	29
30	•003031	•002125	•001470	•001004	•000677	•000451	•000297	•000194	30
31	•004497	•003222	•002277	•001587	•001092	•000742	•000499	•000331	31
32	•006464	•004733	•003415	•002430	•001707	•001183	•000810	•000548	32
33	•009011	•006741	•004968	•003609	•002586	•001829	•001277	•000881	33
34	•012191	•009318	•007013	•005201	•003803	•002743	•001953	•001373	34
35	•016023	•012513	•009618	•007281	•005432	•003997	•002901	•002079	35
36	•020474	•016336	•012824	•009910	•007545	•005662	•004191	•003060	36
37	•025454	•020751	•016636	•013125	•010196	•007804	•005889	•004384	37
38	•030813	•025666	•021014	•016924	•013416	•010474	•008059	•006114	38
39	•036343	•030931	•025864	•021263	•017200	•013697	•010746	•008309	39
40	•041795	•036344	•031036	•026048	•021500	•017464	•013969	•011010	40
41	•046892	•041662	•036335	•031130	•026219	•021723	•017717	•014232	41
42	•051358	•046622	•041526	•036318	•031213	•026379	•021936	•017960	42
43	•054941	•050959	•046354	•041386	•036294	•031286	•026527	•022136	43
44	•057438	•054433	•050568	•046089	•041244	•036264	•031350	•026664	44
45	•058714	•056853	•053940	•050186	•045826	•041099	•036226	•031405	45
46	•058714	•058089	•056285	•053459	•049811	•045566	•040952	•036184	46
47	•057465	•058089	•057482	•055734	•052991	•049444	•045308	•040803	47
48	•055071	•056878	•057482	•056895	•055199	•052534	•049084	•045053	48
49	•051699	•054557	•056309	•056895	•056325	•054678	•052089	•048731	49
50	•047563	•051283	•054057	•055757	•056325	•055772	•054173	•051655	50
51	•042900	•047261	•050877	•053570	•055221	•055772	•055235	•053661	51
52	•037950	•042717	•046964	•050480	•053097	•054699	•055235	•054713	52
53	•032938	•037881	•042533	•046670	•050091	•052635	•054193	•054713	53
54	•028058	•032971	•037807	•042349	•046381	•049711	•052185	•053700	54
55	•023467	•028175	•032995	•037729	•042164	•046096	•049339	•051747	55
56	•019276	•023647	•028282	•033013	•037647	•041980	•045815	•048975	56
57	•015556	•019498	•023816	•028379	•033023	•037561	•041796	•045538	57
58	•012338	•015800	•019710	•023976	•028468	•033028	•037472	•041612	58
59	•009619	•012587	•016035	•019912	•024126	•028549	•033026	•037381	59
60	•007375	•009860	•012828	•016261	•020105	•024267	•028623	•033019	60
61	•005561	•007597	•010094	•013063	•016479	•020289	•024400	•028689	61
62	•004126	•005759	•007815	•010324	•013290	•016689	•020464	•024524	62
63	•003013	•004296	•005954	•008029	•010547	•013510	•016891	•020632	63
64	•002165	•003155	•004466	•006148	•008240	•010766	•013724	•017086	64
65	•001532	•002281	•003298	•004634	•006339	•008447	•010979	•013931	65
66	•001068	•001625	•002398	•003441	•004802	•006527	•008650	•011187	66
67	•000733	•001140	•001718	•002516	•003584	•004969	•006714	•008850	67
68	•000496	•000788	•001213	•001813	•002635	•003726	•005134	•006898	68
69	•000331	•000537	•000844	•001288	•001909	•002754	•003869	•005298	69
70	•000217	•000360	•000579	•000901	•001364	•002007	•002874	•004011	70
71	•000141	•000238	•000391	•000622	•000960	•001441	•002105	•002994	71
72	•000090	•000156	•000261	•000423	•000667	•001021	•001520	•002204	72
73	•000057	•000100	•000171	•000284	•000457	•000713	•001083	•001600	73
74	•000035	•000064	•000111	•000188	•000309	•000492	•000761	•001146	74
75	•000022	•000040	•000071	•000123	•000206	•000334	•000528	•000810	75
76	•000013	•000025	•000045	•000079	•000135	•000224	•000361	•000565	76
77	•000008	•000015	•000028	•000050	•000088	•000149	•000244	•000389	77
78	•000005	•000009	•000017	•000032	•000056	•000097	•000163	•000264	78
79	•000003	•000005	•000010	•000020	•000036	•000063	•000107	•000177	79
80	•000002	•000003	•000006	•000012	•000022	•000040	•000070	•000117	80
81	•000001	•000002	•000004	•000007	•000014	•000025	•000045	•000077	81
82		•000001	•000002	•000004	•000008	•000016	•000028	•000050	82
83		•000001	•000001	•000003	•000005	•000010	•000018	•000032	83
84		•000001	•000001	•000003	•000003	•000006	•000011	•000020	84
85			•000001	•000002	•000004	•000007	•000012	•000022	85
86				•000001	•000002	•000004	•000008	•000016	86
87				•000001	•000001	•000002	•000005	•000011	87
88					•000001	•000001	•000003	•000006	88
89						•000001	•000002	•000004	89
90							•000001	•000001	90
91							•000001	•000001	91
X	A=54	A=55	A=56	A=57	A=58	A=59	A=60	A=61	X
23	•000001	•000001							23

TABLE I

X	A=54	A=55	A=56	A=57	A=58	A=59	A=60	A=61	X
24	000002	000001	000001						24
25	000005	000003	000002	000001	000001				25
26	000010	000006	000003	000002	000001	000001			26
27	000019	000012	000007	000004	000002	000001	000001		27
28	000037	000023	000014	000008	000005	000003	000002	000001	28
29	000069	000043	000027	000017	000010	000006	000004	000002	29
30	000125	000080	000030	000031	000020	000012	000007	000004	30
31	000217	000141	000091	000058	000036	000023	000014	000009	31
32	000367	000243	000159	000103	000066	000042	000026	000017	32
33	000600	000403	000270	000178	000116	000075	000048	000031	33
34	000954	000655	000444	000298	000198	000130	000085	000055	34
35	001471	001029	000711	000486	000329	000220	000146	000096	35
36	002207	001572	001106	000769	000529	000360	000243	000162	36
37	003221	002336	001674	001185	000830	000575	000394	000267	37
38	004577	003381	002467	001778	001267	000892	000622	000429	38
39	006337	004768	003542	002599	001884	001350	000956	000670	39
40	008555	006556	004959	003703	002731	001991	001435	001022	40
41	011267	008795	006773	005148	003864	002865	002099	001521	41
42	014486	011518	009031	006987	005336	004025	002999	002209	42
43	018192	014732	011761	009262	007197	005522	004185	003134	43
44	022327	018415	014969	011998	009488	007405	005707	004345	44
45	026792	022507	018628	015197	012228	009709	007609	005889	45
46	031451	026910	022677	018832	015418	012452	009925	007810	46
47	036136	031491	027020	022838	019027	015632	012670	010136	47
48	040653	036083	031523	027121	022991	019214	015837	012881	48
49	044801	040501	036026	031548	027214	023135	019393	016036	49
50	048385	044552	040349	035965	031568	027299	023271	019564	50
51	051231	048046	044305	040196	035901	031582	027378	023400	51
52	053202	050818	047713	044061	040043	035833	031590	027490	52
53	054205	052735	050414	047307	045821	039889	035762	031593	53
54	054205	053712	052281	050019	047067	043583	039736	035689	54
55	053220	053712	053232	051838	049634	046753	043348	039582	55
56	051319	052753	053232	052764	051407	049257	046444	043115	56
57	048618	050902	052298	052764	052308	050985	048889	046142	57
58	045265	048269	050494	051854	052308	051865	050575	048528	58
59	041429	044996	047927	050097	051422	051865	051432	0500173	59
60	037286	041247	044732	047592	049708	051000	051432	051010	60
61	033008	037190	041065	044471	047263	049328	050589	051010	61
62	028748	032991	037091	040885	044214	046941	048957	050187	62
63	024642	028802	032970	036991	040705	043961	046625	048594	63
64	020791	024751	028849	032945	036889	040526	043711	046316	64
65	017273	020943	024854	028890	032916	036785	040349	043466	65
66	014132	017453	021088	024951	028926	032884	036681	040173	66
67	011390	014327	017626	021227	025041	028958	032849	036575	67
68	009045	011588	014516	017793	021358	025125	028984	032810	68
69	007079	009237	011781	014698	017953	021484	025203	029006	69
70	005461	007257	009425	011969	014876	018108	021603	025277	70
71	004153	005622	007434	009609	012152	015047	018256	021717	71
72	003115	004295	005782	007607	009789	012330	015213	018399	72
73	002304	003236	004435	005940	007778	009966	012504	015374	73
74	001681	002405	003356	004575	006096	007946	010138	012673	74
75	001211	001764	002506	003477	004714	006250	008111	010308	75
76	000860	001276	001847	002608	003598	004852	006403	008273	76
77	000603	000912	001343	001930	002710	003718	004990	006554	77
78	000418	000643	000964	001411	002015	002812	003838	005126	78
79	000285	000448	000683	001018	001479	002100	002915	003958	79
80	000193	000308	000478	000725	001073	001549	002186	003018	80
81	000120	000209	000331	000510	000768	001128	001619	002273	81
82	000085	000140	000226	000355	000543	000812	001185	001691	82
83	000055	000093	000152	000244	000380	000577	000857	001243	83
84	000035	000061	000102	000165	000262	000405	000612	000902	84
85	000022	000039	000067	000111	000179	000281	000432	000648	85
86	000014	000025	000044	000073	000121	000193	000301	000459	86
87	000009	000016	000028	000048	000080	000131	000208	000322	87
88	000005	000010	000018	000031	000053	000088	000142	000223	88
89	000003	000006	000011	000020	000035	000058	000096	000153	89
90	000002	000004	000007	000013	000022	000038	000064	000104	90

TABLE I

X	A=54	A=55	A=56	A=57	A=58	A=59	A=60	A=61	X
91	•000001	•000002	•000004	•000008	•000014	•000025	•000042	•000070	91
92	•000001	•000001	•000003	•000005	•000009	•000016	•000027	•000046	92
93		•000001	•000002	•000003	•000006	•000010	•000018	•000030	93
94			•000001	•000002	•000003	•000006	•000011	•000020	94
95			•000001	•000001	•000002	•000004	•000007	•000013	95
96				•000001	•000001	•000002	•000004	•000008	96
97					•000001	•000001	•000003	•000005	97
98					•000001	•000001	•000002	•000003	98
99						•000001	•000001	•000002	99
100							•000001	•000001	100
101								•000001	101

X	A=62	A=63	A=64	A=65	A=66	A=67	A=68	A=69	X
28	•000001								28
29	•000001	•000001							29
30	•000003	•000002	•000001	•000001					30
31	•000005	•000003	•000002	•000001	•000001				31
32	•000010	•000006	•000004	•000002	•000001	•000001			32
33	•000019	•000012	•000007	•000005	•000003	•000002	•000001	•000001	33
34	•000035	•000022	•000014	•000009	•000005	•000003	•000002	•000001	34
35	•000062	•000040	•000026	•000016	•000010	•000006	•000004	•000002	35
36	•000107	•000070	•000045	•000029	•000019	•000012	•000007	•000005	36
37	•000179	•000119	•000079	•000051	•000033	•000021	•000014	•000009	37
38	•000292	•000198	•000132	•000088	•000058	•000038	•000024	•000016	38
39	•000465	•000319	•000217	•000146	•000098	•000065	•000042	•000027	39
40	•000721	•000503	•000347	•000238	•000161	•000108	•000072	•000047	40
41	•001090	•000773	•000542	•000377	•000259	•000177	•000119	•000080	41
42	•001609	•001159	•000826	•000583	•000407	•000282	•000193	•000131	42
43	•002320	•001698	•001230	•000881	•000625	•000439	•000305	•000210	43
44	•003269	•002431	•001788	•001302	•000937	•000668	•000472	•000330	44
45	•004504	•003404	•002544	•001880	•001375	•000995	•000713	•000506	45
46	•006070	•004662	•003539	•002656	•001972	•001449	•001054	•000759	46
47	•008007	•006249	•004819	•003674	•002770	•002066	•001525	•001114	47
48	•010343	•008201	•006425	•004975	•003809	•002884	•002160	•001602	48
49	•013087	•010545	•008392	•006599	•005130	•003943	•002998	•002255	49
50	•016228	•013286	•010742	•008579	•006772	•005284	•004077	•003112	50
51	•019728	•016412	•013480	•010934	•008763	•006941	•005436	•004211	51
52	•023521	•019884	•016591	•013668	•011122	•008944	•007109	•005587	52
53	•027516	•023636	•020034	•016763	•013851	•011306	•009121	•007274	53
54	•031592	•027575	•023744	•020177	•016929	•014028	•011485	•009294	54
55	•035613	•031586	•027629	•023846	•020314	•017088	•014200	•011660	55
56	•039428	•035534	•031576	•027678	•023942	•020445	•017243	•014367	56
57	•042887	•039275	•035454	•031563	•027722	•024032	•020570	•017391	57
58	•045845	•042661	•039122	•035372	•031546	•027761	•024117	•020690	58
59	•048176	•045553	•042437	•038969	•035288	•031525	•027796	•024197	59
60	•049782	•047831	•045266	•042217	•038817	•035203	•031502	•027826	60
61	•050598	•049399	•047493	•044985	•041999	•038666	•035117	•031475	61
62	•050598	•050196	•049025	•047162	•044709	•041784	•038515	•035029	62
63	•049795	•050196	•049803	•048659	•046838	•044437	•041572	•038365	63
64	•048238	•049411	•049803	•049419	•048301	•046520	•044170	•041362	64
65	•046012	•047891	•049037	•049419	•049044	•047951	•046209	•043908	65
66	•043223	•045714	•047551	•048671	•049044	•048678	•047609	•045904	66
67	•039998	•042985	•045422	•047218	•048312	•048678	•048320	•047274	67
68	•036469	•039824	•042750	•045135	•046891	•047962	•048320	•047969	68
69	•032769	•036361	•039652	•042518	•044853	•046572	•047619	•047969	69
70	•029024	•032725	•036253	•039481	•042290	•044576	•046259	•047284	70
71	•025345	•029038	•032679	•036145	•039312	•042065	•044304	•045952	71
72	•021825	•025408	•029048	•032631	•036036	•039144	•041843	•044037	72
73	•018536	•021927	•025467	•029055	•032580	•035926	•038977	•041624	73
74	•015530	•018668	•022025	•025521	•029058	•032528	•035817	•038812	74
75	•012838	•015681	•018795	•022118	•025571	•029058	•032474	•035707	75
76	•010473	•012999	•015827	•018917	•022206	•025617	•029055	•032418	76
77	•008433	•010635	•013155	•015969	•019034	•022290	•025659	•029050	77
78	•006703	•008590	•010794	•013307	•016106	•019147	•022370	•025698	78
79	•005261	•006850	•008744	•010949	•013455	•016238	•019255	•022445	79
80	•004077	•005395	•006996	•008896	•011101	•013600	•016367	•019359	80



TABLE I

X	A=62	A=63	A=64	A=65	A=66	A=67	A=68	A=69	X
81	•003121	•004196	•005527	•007139	•009045	•011249	•013740	•016491	81
82	•002360	•003224	•004314	•005659	•007200	•009191	•011394	•013876	82
83	•001763	•002447	•003326	•004432	•005789	•007419	•009335	•011536	83
84	•001301	•002185	•002534	•003429	•004549	•005918	•007557	•009476	84
85	•000949	•001360	•001908	•002622	•003532	•004665	•006045	•007692	85
86	•000684	•000996	•001420	•001982	•002710	•003634	•004780	•006172	86
87	•000488	•000722	•001045	•001481	•002056	•002799	•003736	•004895	87
88	•000343	•000517	•000760	•001094	•001542	•002131	•002887	•003838	88
89	•000239	•000366	•000546	•000799	•001144	•001604	•002206	•002975	89
90	•000165	•000256	•000389	•000577	•000839	•001194	•001667	•002281	90
91	•000112	•000177	•000273	•000412	•000608	•000879	•001245	•001730	91
92	•000076	•000121	•000190	•000291	•000436	•000640	•000921	•001297	92
93	•000050	•000082	•000131	•000203	•000310	•000461	•000673	•000962	93
94	•000033	•000055	•000089	•000141	•000217	•000329	•000487	•000707	94
95	•000022	•000037	•000060	•000096	•000151	•000232	•000349	•000513	95
96	•000014	•000024	•000040	•000065	•000104	•000162	•000247	•000369	96
97	•000009	•000016	•000026	•000044	•000071	•000112	•000173	•000262	97
98	•000006	•000010	•000017	•000029	•000048	•000076	•000120	•000185	98
99	•000004	•000006	•000011	•000019	•000032	•000052	•000082	•000129	99
100	•000002	•000004	•000007	•000012	•000021	•000035	•000056	•000089	100
101	•000001	•000003	•000005	•000008	•000014	•000023	•000038	•000061	101
102	•000001	•000002	•000003	•000005	•000009	•000015	•000025	•000041	102
103		•000001	•000002	•000003	•000006	•000010	•000017	•000028	103
104		•000001	•000001	•000002	•000004	•000006	•000011	•000018	104
105			•000001	•000001	•000002	•000004	•000007	•000012	105
106				•000001	•000001	•000003	•000005	•000008	106
107					•000001	•000002	•000003	•000005	107
108					•000001	•000001	•000002	•000003	108
109						•000001	•000001	•000002	109
110							•000001	•000001	110
111								•000001	111

X	A=70	A=71	A=72	A=73	A=74	A=75	A=76	A=77	X
34	•000001								34
35	•000001	•000001	•000001						35
36	•000003	•000002	•000001	•000001					36
37	•000005	•000003	•000002	•000001	•000001				37
38	•000010	•000006	•000004	•000002	•000001	•000001	•000001		38
39	•000018	•000011	•000007	•000005	•000003	•000002	•000001	•000001	39
40	•000031	•000020	•000013	•000008	•000005	•000003	•000002	•000001	40
41	•000053	•000035	•000023	•000015	•000009	•000006	•000004	•000002	41
42	•000088	•000059	•000039	•000026	•000017	•000011	•000007	•000004	42
43	•000144	•000097	•000065	•000043	•000029	•000019	•000012	•000008	43
44	•000229	•000157	•000107	•000072	•000048	•000032	•000021	•000014	44
45	•000356	•000248	•000171	•000117	•000079	•000053	•000036	•000024	45
46	•000541	•000382	•000268	•000186	•000128	•000087	•000059	•000040	46
47	•000806	•000578	•000410	•000288	•000201	•000139	•000095	•000065	47
48	•001175	•000854	•000615	•000439	•000310	•000217	•000151	•000104	48
49	•001679	•001238	•000904	•000653	•000468	•000333	•000234	•000163	49
50	•002351	•001758	•001301	•000954	•000693	•000499	•000356	•000252	50
51	•003227	•002447	•001837	•001366	•001005	•000733	•000530	•000380	51
52	•004343	•003341	•002544	•001917	•001431	•001058	•000775	•000563	52
53	•005737	•004476	•003455	•002641	•001998	•001497	•001111	•000817	53
54	•007436	•005885	•004607	•003570	•002738	•002079	•001564	•001165	54
55	•009465	•007597	•006031	•004738	•003684	•002835	•002161	•001632	55
56	•011831	•009631	•007754	•006176	•004868	•003797	•002933	•002244	56
57	•014529	•011997	•009795	•007910	•006319	•004996	•003911	•003031	57
58	•017535	•014686	•012159	•009955	•008063	•006461	•005124	•004024	58
59	•020804	•017673	•014839	•012318	•010112	•008213	•006601	•005251	59
60	•024271	•020913	•017806	•014986	•012472	•010266	•008361	•006739	60
61	•027852	•024341	•021017	•017935	•015130	•012623	•010417	•008507	61
62	•031446	•027875	•024407	•021117	•018058	•015269	•012769	•010565	62
63	•034940	•031415	•027894	•024468	•021211	•018178	•015404	•012912	63
64	•038216	•034851	•031381	•027909	•024526	•021302	•018292	•015535	64
65	•041156	•038067	•034760	•031344	•027922	•024579	•021388	•018403	65
66	•043650	•040951	•037920	•034669	•031306	•027931	•024629	•021470	66

TABLE I

X	A=70	A=71	A=72	A=73	A=74	A=75	A=76	A=77	X
67	045604	043396	040750	037773	034577	031266	027937	024675	67
68	046946	045311	043147	040551	037628	034484	031224	027941	68
69	047626	046624	045023	042902	040354	037483	034391	031180	69
70	047626	047290	046309	044740	042660	040160	037339	034298	70
71	046955	047290	046961	046000	044463	042423	039969	037197	71
72	045651	046633	046961	046639	045698	044191	042189	039780	72
73	043775	045356	046318	046639	046324	045401	043923	041959	73
74	041409	043517	045066	046009	046324	046015	045110	043660	74
75	038648	041196	043264	044782	045706	046015	045712	044825	75
76	035597	038486	040987	043014	044503	045409	045712	045415	76
77	032361	035487	038325	040780	042770	044230	045118	045415	77
78	029042	032302	035377	038166	040576	042529	043961	044832	78
79	025733	029031	032242	035267	038008	040375	042292	043697	79
80	022517	025765	029018	032181	035158	037852	040177	042059	80
81	019459	022584	025794	029003	032119	035048	037697	039982	81
82	016611	019555	022648	025802	028986	032056	034939	037544	82
83	014009	016727	019647	022709	025843	028966	031992	034830	83
84	011674	014139	016840	019735	022766	025863	028945	031927	84
85	009614	011810	014265	016949	019820	022820	025880	028922	85
86	007826	009750	011942	014387	017054	019901	022871	025896	86
87	006296	007957	009883	012072	014506	017156	019979	022919	87
88	005009	006420	008086	010014	012198	014622	017255	020054	88
89	003939	005121	006542	008214	010142	012322	014735	017350	89
90	003064	004040	005233	006662	008339	010268	012442	014844	90
91	002357	003152	004141	005344	006781	008463	010392	012560	91
92	001793	002433	003241	004241	005455	006899	008584	010513	92
93	001350	001857	002509	003329	004340	005564	007015	008704	93
94	001005	001403	001922	002585	003417	004439	005672	007130	94
95	000741	001048	001456	001986	002661	003505	004537	005779	95
96	000540	000775	001092	001511	002052	002738	003592	004635	96
97	000390	000568	000811	001137	001565	002117	002814	003679	97
98	000278	000411	000596	000847	001182	001620	002183	002891	98
99	000197	000295	000433	000624	000883	001227	001676	002249	99
100	000138	000209	000312	000456	000654	000921	001273	001731	100
101	000095	000147	000222	000329	000479	000684	000958	001320	101
102	000066	000102	000157	000236	000347	000503	000714	000996	102
103	000045	000071	000110	000167	000250	000366	000527	000745	103
104	000030	000048	000076	000117	000178	000264	000385	000552	104
105	000020	000033	000052	000082	000125	000189	000279	000404	105
106	000013	000022	000035	000056	000087	000133	000200	000294	106
107	000009	000014	000024	000038	000060	000093	000142	000211	107
108	000006	000010	000016	000026	000041	000065	000100	000151	108
109	000004	000006	000010	000017	000028	000045	000070	000106	109
110	000002	000004	000007	000012	000019	000030	000048	000075	110
111	000001	000003	000004	000008	000013	000021	000033	000052	111
112	000001	000002	000003	000005	000008	000014	000022	000036	112
113	000001	000001	000002	000003	000005	000009	000015	000024	113
114		000001	000001	000002	000004	000006	000010	000016	114
115			000001	000001	000002	000004	000007	000011	115
116				000001	000001	000003	000004	000007	116
117				000001	000001	000002	000003	000005	117
118					000001	000001	000002	000003	118
119						000001	000001	000002	119
120							000001	000001	120
121								000001	121
122								000001	122

X	A=78	A=79	A=80	A=81	A=82	A=83	A=84	A=85	X
40	000001								40
41	000002	000001	000001						41
42	000003	000002	000001	000001					42
43	000005	000003	000002	000001	000001				43
44	000009	000006	000004	000002	000001	000001	000001		44
45	000016	000010	000007	000004	000003	000002	000001	000001	45
46	000026	000017	000011	000007	000005	000003	000002	000001	46
47	000044	000029	000019	000013	000008	000005	000004	000002	47
48	000071	000048	000032	000022	000014	000009	000006	000004	48

TABLE I

X	A=78	A=79	A=80	A=81	A=82	A=83	A=84	A=85	X
49	0000113	0000078	0000053	0000036	0000024	0000016	0000011	0000007	49
50	0000176	0000123	0000085	0000058	0000039	0000027	0000018	0000012	50
51	0000270	0000190	0000133	0000092	0000063	0000043	0000029	0000020	51
52	0000405	0000289	0000204	0000143	0000100	0000069	0000047	0000032	52
53	0000596	0000431	0000309	0000219	0000155	0000108	0000075	0000052	53
54	0000861	0000630	0000457	0000329	0000235	0000166	0000117	0000081	54
55	0001221	0000905	0000665	0000484	0000350	0000251	0000178	0000126	55
56	0001700	0001276	0000950	0000701	0000512	0000372	0000267	0000191	56
57	0002326	0001769	0001333	0000996	0000737	0000541	0000394	0000285	57
58	0003129	0002410	0001833	0001390	0001042	0000774	0000571	0000417	58
59	0004136	0003226	000249	0001909	0001448	0001089	0000812	0000601	59
60	0005377	0004248	0003324	0002577	0001979	0001507	0001137	0000851	60
61	0006875	0005502	0004359	0003422	0002661	0002050	0001566	0001186	61
62	0008650	0007010	0005625	0004470	0003519	0002745	0002122	0001626	62
63	0010709	0008790	0007143	0005747	0004580	0003616	0002829	0002193	63
64	0013052	0010851	0008929	0007274	0005868	0004690	0003713	0002913	64
65	0015662	0013188	0010989	0009064	0007403	0005988	0004798	0003810	65
66	0018510	0015785	0013320	0011125	0009198	0007531	0006107	0004906	66
67	0021549	0018612	0015905	0013449	0011257	0009329	0007656	0006224	67
68	0024718	0021623	0018711	0016020	0013575	0011387	0009458	0007780	68
69	0027942	0024757	0021694	0018806	0016132	0013697	0011514	0009584	69
70	0031135	0027940	0024793	0021762	0018898	0016241	0013817	0011638	70
71	0034205	0031088	0027936	0024827	0021826	0018986	0016347	0013933	71
72	0037055	0034111	0031040	0027930	0024857	0021887	0019071	0016449	72
73	0039593	0036914	0034017	0030991	0027922	0024885	0021945	0019153	73
74	0041733	0039409	0036075	0033923	0030940	0027912	0024910	0022000	74
75	0043402	0041510	0039226	0036636	0033828	0030889	0027900	0024933	75
76	0044545	0043149	0041291	0039047	0036499	0033734	0030836	0027886	76
77	0045123	0044270	0042900	0041075	0038869	0036363	0033640	0030783	77
78	0045123	0044837	0044000	0042655	0040862	0038694	0036227	0033546	78
79	0044552	0044837	0044557	0043735	0042414	0040653	0038520	0036093	79
80	0043438	0044277	0044557	0044281	0043474	0042177	0040446	0038349	80
81	0041829	0043183	0044007	0044281	0044011	0043219	0041944	0040243	81
82	0039789	0041604	0042937	0043741	0044011	0043746	0042967	0041715	82
83	0037392	0039599	0041381	0042687	0043481	0043746	0043485	0042720	83
84	0034721	0037242	0039411	0041163	0042446	0043225	0043485	0043229	84
85	0031862	0034613	0037093	0039226	0040947	0042208	0042973	0043229	85
86	0028898	0031795	0034505	0036945	0039043	0040735	0041974	0042726	86
87	0025908	0028872	0031729	0034397	0036799	0038863	0040527	0041744	87
88	0022964	0025919	0028844	0031661	0034290	0036654	0038685	0040321	88
89	0020126	0023007	0025927	0028815	0031593	0034183	0036511	0038509	89
90	0017443	0020195	0023046	0025934	0028785	0031525	0034077	0036369	90
91	0014951	0017532	0020261	0023084	0025938	0028753	0031456	0033971	91
92	0012676	0015054	0017618	0020324	0023119	0025940	0028721	0031387	92
93	0010631	0012788	0015155	0017701	0020384	0023151	0025941	0028687	93
94	0008822	0010747	0012898	0015253	0017782	0020442	0023181	0025940	94
95	0007243	0008937	0010862	0013005	0015349	0017860	0020497	0023210	95
96	0005885	0007355	0009051	0010973	0013110	0015441	0017935	0020550	96
97	0004732	0005990	0007465	0009163	0011083	0013213	0015531	0018008	97
98	0003766	0004829	0006094	0007574	0009273	0011190	0013313	0015619	98
99	0002968	0003853	0004924	0006197	0007681	0009382	0011296	0013410	99
100	0002315	0003044	0003939	0005019	0006298	0007787	0009488	0011399	100
101	0001788	0002381	0003120	0004025	0005114	0006399	0007891	0009593	101
102	0001367	0001844	0002447	0003197	0004111	0005207	0006499	0007994	102
103	0001035	0001414	0001901	0002514	0003273	0004196	0005300	0006597	103
104	0000776	0001074	0001462	0001958	0002580	0003349	0004281	0005392	104
105	0000577	0000808	0001114	0001510	0002015	0002647	0003425	0004365	105
106	0000424	0000602	0000841	0001154	0001559	0002073	0002714	0003500	106
107	0000309	0000445	0000629	0000874	0001195	0001608	0002130	0002780	107
108	0000223	0000325	0000466	0000655	0000907	0001236	0001657	0002188	108
109	0000160	0000236	0000342	0000487	0000682	0000941	0001277	0001707	109
110	0000113	0000169	0000249	0000359	0000509	0000710	0000975	0001319	110
111	0000080	0000121	0000179	0000262	0000376	0000531	0000738	0001010	111
112	0000055	0000085	0000128	0000189	0000275	0000393	0000553	0000766	112
113	0000038	0000059	0000091	0000136	0000200	0000289	0000411	0000576	113
114	0000026	0000041	0000064	0000096	0000144	0000210	0000303	0000430	114
115	0000018	0000028	0000044	0000068	0000102	0000152	0000221	0000318	115

TABLE I

X	A=78	A=79	A=80	A=81	A=82	A=83	A=84	A=85	X
116	•000012	•000019	•000030	•000047	•000072	•000109	•000160	•000233	116
117	•000008	•000013	•000021	•000033	•000051	•000077	•000115	•000169	117
118	•000005	•000009	•000014	•000023	•000035	•000054	•000082	•000122	118
119	•000003	•000006	•000010	•000015	•000024	•000038	•000058	•000087	119
120	•000002	•000004	•000006	•000010	•000017	•000026	•000040	•000062	120
121	•000001	•000002	•000004	•000007	•000011	•000018	•000028	•000043	121
122	•000001	•000002	•000003	•000005	•000008	•000012	•000019	•000030	122
123	•000001	•000001	•000002	•000003	•000005	•000008	•000013	•000021	123
124		•000001	•000001	•000002	•000003	•000006	•000009	•000014	124
125			•000001	•000001	•000002	•000004	•000006	•000010	125
126				•000001	•000001	•000002	•000004	•000007	126
127				•000001	•000001	•000002	•000003	•000004	127
128					•000001	•000001	•000002	•000003	128
129						•000001	•000001	•000002	129
130							•000001	•000001	130
131								•000001	131
132								•000001	132

X	A=86	A=87	A=88	A=89	A=90	A=91	A=92	A=93	X
46	•000001								46
47	•000001	•000001	•000001						47
48	•000003	•000002	•000001	•000001					48
49	•000005	•000003	•000002	•000001	•000001				49
50	•000008	•000005	•000003	•000002	•000001	•000001	•000001		50
51	•000013	•000009	•000006	•000004	•000002	•000002	•000001	•000001	51
52	•000022	•000015	•000010	•000006	•000004	•000003	•000002	•000001	52
53	•000035	•000024	•000016	•000011	•000007	•000005	•000003	•000002	53
54	•000056	•000039	•000026	•000018	•000012	•000008	•000005	•000004	54
55	•000088	•000061	•000042	•000029	•000020	•000013	•000009	•000006	55
56	•000135	•000095	•000066	•000046	•000032	•000022	•000015	•000010	56
57	•000204	•000145	•000102	•000072	•000050	•000034	•000024	•000016	57
58	•000302	•000217	•000155	•000110	•000077	•000054	•000037	•000026	58
59	•000441	•000321	•000231	•000166	•000118	•000083	•000058	•000041	59
60	•000632	•000465	•000340	•000246	•000177	•000126	•000090	•000063	60
61	•000890	•000663	•000490	•000359	•000261	•000188	•000135	•000096	61
62	•001235	•000930	•000695	•000515	•000379	•000277	•000200	•000144	62
63	•001686	•001285	•000971	•000728	•000541	•000400	•000293	•000213	63
64	•002265	•001747	•001335	•001012	•000761	•000568	•000421	•000309	64
65	•002997	•002338	•001808	•001386	•001054	•000795	•000595	•000442	65
66	•003906	•003082	•002410	•001869	•001438	•001097	•000830	•000623	66
67	•005013	•004001	•003166	•002483	•001931	•001489	•001140	•000865	67
68	•006340	•005120	•004097	•003250	•002556	•001993	•001542	•001183	68
69	•007902	•006455	•005225	•004192	•003334	•002629	•002056	•001595	69
70	•009709	•008023	•006569	•005330	•004286	•003417	•002002	•002118	70
71	•011760	•009831	•008141	•006681	•005433	•004380	•003501	•002775	71
72	•014046	•011879	•009950	•008258	•006791	•005536	•004473	•003584	72
73	•016548	•014157	•011995	•010068	•008373	•006901	•005638	•004566	73
74	•019231	•016644	•014264	•012109	•010183	•008486	•007009	•005739	74
75	•022052	•019307	•016737	•014369	•012220	•010297	•008598	•007116	75
76	•024954	•022101	•019380	•016827	•014471	•012329	•010408	•008707	76
77	•027870	•024972	•022148	•019449	•016914	•014570	•012435	•010517	77
78	•030729	•027853	•024987	•022192	•019516	•016999	•014667	•012539	78
79	•033451	•030673	•027834	•025001	•022234	•019581	•017081	•014761	79
80	•035960	•033357	•030618	•027814	•025013	•022273	•019643	•017160	80
81	•038180	•035828	•033264	•030561	•027792	•025023	•022310	•019702	81
82	•040042	•038013	•035698	•033170	•030504	•027770	•025031	•022345	82
83	•041490	•039845	•037848	•035568	•033077	•030446	•027746	•025038	83
84	•042478	•041268	•039650	•037685	•035439	•032983	•030388	•027720	84
85	•042977	•042239	•041050	•039458	•037524	•035312	•032890	•030329	85
86	•042977	•042730	•042004	•040835	•039269	•037365	•035185	•032798	86
87	•042483	•042730	•042487	•041774	•040623	•039083	•037207	•035060	87
88	•041518	•042245	•042487	•042248	•041546	•040415	•038899	•037052	88
89	•040118	•041295	•042010	•042248	•042013	•041323	•040210	•038717	89
90	•038335	•039919	•041076	•041779	•042013	•041782	•041103	•040008	90
91	•036229	•038164	•039722	•040861	•041552	•041782	•041555	•040887	91
92	•033866	•036090	•037995	•039528	•040648	•041328	•041555	•041331	92
93	•031317	•033762	•035952	•037828	•039337	•040439	•041108	•041331	93

TABLE I

X	A=86	A=87	A=88	A=89	A=90	A=91	A=92	A=93	X
94	•028652	•031247	•033657	•035816	•037663	•039149	•040233	•040892	94
95	•025937	•028616	•031177	•033554	•035681	•037500	•038963	•040031	95
96	•023236	•025933	•028579	•031107	•033345	•035547	•037339	•038780	96
97	•020601	•023260	•025928	•028542	•031037	•033348	•035415	•037181	97
98	•018078	•020649	•023282	•025920	•028503	•030966	•033247	•035284	98
99	•015704	•018146	•020695	•023302	•025912	•028464	•030896	•033145	99
100	•013506	•015787	•018212	•020739	•023321	•025902	•028424	•030825	100
101	•011500	•013599	•015868	•018275	•020781	•023338	•025891	•028384	101
102	•009696	•011599	•013690	•015946	•018336	•020821	•023353	•025879	102
103	•008096	•009797	•011696	•013778	•016022	•018395	•020859	•023367	103
104	•006694	•008196	•009897	•011791	•013865	•016096	•018452	•020895	104
105	•005483	•006791	•008294	•009994	•011884	•013950	•016168	•018507	105
106	•004449	•005574	•006886	•008392	•010090	•011976	•014032	•016237	106
107	•003575	•004532	•005663	•006980	•008487	•010185	•012065	•014113	107
108	•002847	•003651	•004614	•005752	•007073	•008582	•010278	•012153	108
109	•002246	•002914	•003725	•004697	•005840	•007165	•008675	•010369	109
110	•001756	•002305	•002980	•003800	•004778	•005927	•007255	•008766	110
111	•001361	•001806	•002363	•003047	•003874	•004859	•006013	•007345	111
112	•001045	•001403	•001856	•002421	•003113	•003948	•004940	•006099	112
113	•000795	•001080	•001446	•001907	•002479	•003179	•004022	•005019	113
114	•000600	•000824	•001116	•001489	•001957	•002538	•003245	•004095	114
115	•000449	•000624	•000854	•001152	•001532	•002008	•002596	•003311	115
116	•000333	•000468	•000648	•000884	•001189	•001575	•002059	•002655	116
117	•000244	•000348	•000487	•000672	•000914	•001225	•001619	•002110	117
118	•000178	•000256	•000363	•000507	•000697	•000945	•001262	•001663	118
119	•000129	•000187	•000269	•000379	•000527	•000723	•000976	•001300	119
120	•000092	•000136	•000197	•000281	•000396	•000548	•000748	•001007	120
121	•000066	•000098	•000143	•000207	•000294	•000412	•000569	•000774	121
122	•000046	•000070	•000103	•000151	•000217	•000307	•000429	•000590	122
123	•000032	•000049	•000074	•000109	•000159	•000227	•000321	•000446	123
124	•000022	•000035	•000052	•000078	•000115	•000167	•000238	•000335	124
125	•000015	•000024	•000037	•000056	•000083	•000122	•000175	•000249	125
126	•000011	•000017	•000026	•000039	•000059	•000088	•000128	•000184	126
127	•000007	•000011	•000018	•000028	•000042	•000063	•000093	•000135	127
128	•000005	•000008	•000012	•000019	•000030	•000045	•000067	•000098	128
129	•000003	•000005	•000008	•000013	•000021	•000032	•000048	•000070	129
130	•000002	•000003	•000006	•000009	•000014	•000022	•000034	•000050	130
131	•000001	•000002	•000004	•000006	•000010	•000015	•000024	•000036	131
132	•000001	•000002	•000003	•000004	•000007	•000011	•000016	•000025	132
133	•000001	•000001	•000002	•000003	•000005	•000007	•000011	•000018	133
134		•000001	•000001	•000002	•000003	•000005	•000008	•000012	134
135			•000001	•000001	•000002	•000003	•000005	•000008	135
136			•000001	•000001	•000001	•000002	•000004	•000006	136
137			•000001	•000001	•000001	•000001	•000002	•000004	137
138				•000001	•000001	•000001	•000002	•000003	138
139					•000001	•000001	•000001	•000002	139
140							•000001	•000001	140
141							•000001	•000001	141
142							•000001	•000001	142

X	A=94	A=95	A=96	A=97	A=98	A=99	A=100	A=101	X
52	•000001								52
53	•000001	•000001	•000001						53
54	•000002	•000001	•000001	•000001					54
55	•000004	•000003	•000002	•000001	•000001				55
56	•000007	•000004	•000003	•000002	•000001	•000001	•000001		56
57	•000011	•000007	•000005	•000003	•000002	•000001	•000001	•000001	57
58	•000018	•000012	•000008	•000005	•000004	•000002	•000002	•000001	58
59	•000028	•000019	•000013	•000009	•000006	•000004	•000003	•000002	59
60	•000044	•000031	•000021	•000014	•000010	•000007	•000004	•000003	60
61	•000068	•000048	•000033	•000023	•000016	•000011	•000007	•000005	61
62	•000103	•000073	•000051	•000036	•000025	•000017	•000012	•000008	62
63	•000154	•000110	•000078	•000055	•000039	•000027	•000019	•000013	63
64	•000225	•000163	•000117	•000084	•000059	•000042	•000029	•000020	64
65	•000326	•000239	•000173	•000125	•000090	•000064	•000045	•000032	65
66	•000464	•000343	•000252	•000184	•000133	•000096	•000068	•000048	66

TABLE I

X	A=94	A=95	A=96	A=97	A=98	A=99	A=100	A=101	X
67	000652	000487	000361	000266	000195	000141	000102	000073	67
68	000901	000680	000510	000380	000281	000206	000150	000109	68
69	001227	000937	000710	000534	000399	000295	000217	000159	69
70	001648	001271	000973	000740	000558	000418	000311	000229	70
71	002181	001701	001316	001011	000770	000582	000437	000326	71
72	002848	002245	001755	001351	001048	000801	000608	000458	72
73	003667	002921	002308	001809	001407	001086	000832	000633	73
74	004658	003750	002994	002371	001863	001453	001125	000864	74
75	005838	004750	003832	003067	002435	001918	001499	001163	75
76	007221	005937	004841	003914	003140	002499	001973	001546	76
77	008816	007325	006035	004931	003996	003212	002562	002028	77
78	010624	008922	007428	006132	005021	004077	003285	002626	78
79	012641	010729	009027	007529	006228	005110	004158	003357	79
80	014853	012740	010832	009129	007630	006323	005198	004239	80
81	017237	014943	012838	010933	009231	007728	006417	005285	81
82	019760	017311	015029	012933	011032	009331	007826	006510	82
83	022378	019814	017384	015114	013026	011129	009429	007922	83
84	025042	022409	019867	017453	015197	013117	011225	009525	84
85	027694	025045	022438	019917	017521	015277	013205	011318	85
86	030270	027666	025047	022465	019966	017586	015355	013292	86
87	032706	030210	027638	025047	022490	020012	017649	015431	87
88	034935	032614	030151	027609	025046	022513	020056	017711	88
89	036898	034812	032522	030090	027578	025043	022535	020099	89
90	038538	036746	034690	032431	030030	027547	025039	022555	90
91	039809	038361	036596	034569	032340	029969	027515	025034	91
92	040674	039612	038187	036448	034449	032249	029908	027483	92
93	041111	040464	039419	038015	036301	034330	032189	029847	93
94	041111	040895	040258	039229	037846	036156	034212	032069	94
95	040679	040895	040682	040054	039041	037678	036012	034095	95
96	039831	040469	040682	040472	039854	038856	037513	035871	96
97	038599	039634	040262	040472	040265	039657	038673	037390	97
98	037024	038421	039440	040059	040265	040061	039462	038493	98
99	035154	036869	038245	039249	039858	040061	039861	039271	99
100	033045	035025	036715	038072	039061	039661	039861	039663	100
101	030754	032945	034898	036564	037901	038875	039466	039663	101
102	028342	030684	032845	034772	036415	037732	038692	039275	102
103	025866	028300	030613	032746	034647	036267	037566	038512	103
104	023379	025851	028258	030542	032648	034523	036121	037401	104
105	020929	023389	025836	028215	030471	032550	034401	035976	105
106	018560	020962	023399	025820	028172	030401	032453	034279	106
107	016305	018611	020993	023406	025802	028128	030330	032357	107
108	014192	016371	018661	021022	023413	025784	028084	030260	108
109	012239	014268	016435	018708	021050	023418	025765	028039	109
110	010458	012323	014343	016497	018754	021077	023423	025745	110
111	008857	010546	012405	014416	016557	018798	021101	023426	111
112	007433	008946	010633	012486	014488	016616	018841	021125	112
113	006183	007521	009033	010718	012565	014557	016673	018881	113
114	005099	006267	007607	009120	010801	012642	014625	016728	114
115	004168	005177	006350	007692	009204	010883	012718	014692	115
116	003377	004240	005255	006432	007776	009288	010964	012792	116
117	002713	003443	004312	005333	006513	007859	009371	011043	117
118	002161	002772	003508	004384	005409	006594	007941	009452	118
119	001707	002213	002830	003573	004455	005486	006673	008022	119
120	001337	001752	002264	002888	003638	004526	005561	006752	120
121	001039	001375	001796	002315	002947	003703	004596	005636	121
122	000801	001071	001413	001841	002367	003005	003767	004666	122
123	000612	000827	001103	001452	001886	002418	003063	003831	123
124	000464	000634	000854	001136	001490	001931	002470	003121	124
125	000349	000482	000656	000881	001168	001529	001976	002521	125
126	000260	000363	000500	000678	000909	001202	001568	002021	126
127	000193	000272	000378	000518	000701	000937	001235	001607	127
128	000141	000202	000283	000393	000537	000724	000985	001268	128
129	000103	000148	000211	000295	000408	000556	000748	000993	129
130	000075	000108	000156	000220	000308	000423	000575	000771	130
131	000053	000079	000114	000163	000230	000320	000439	000595	131
132	000038	000057	000083	000120	000171	000240	000333	000455	132
133	000027	000040	000060	000087	000126	000179	000250	000346	133
134	000019	000029	000043	000063	000092	000132	000187	000260	134

TABLE I.

X	A=94	A=95	A=96	A=97	A=98	A=99	A=100	A=101	X
135	•000013	•000020	•000031	•000045	•000067	•000097	•000138	•000195	135
136	•000009	•000014	•000022	•000032	•000048	•000070	•000102	•000145	136
137	•000006	•000010	•000015	•000023	•000034	•000051	•000074	•000107	137
138	•000004	•000007	•000011	•000016	•000024	•000037	•000054	•000078	138
139	•000003	•000005	•000007	•000011	•000017	•000026	•000039	•000057	139
140	•000002	•000003	•000005	•000008	•000012	•000018	•000028	•000041	140
141	•000001	•000002	•000003	•000005	•000008	•000013	•000020	•000029	141
142	•000001	•000001	•000002	•000004	•000006	•000009	•000014	•000021	142
143	•000001	•000001	•000002	•000002	•000004	•000006	•000010	•000015	143
144	•000001	•000001	•000001	•000002	•000003	•000004	•000007	•000010	144
145			•000001	•000001	•000002	•000003	•000005	•000007	145
146				•000001	•000001	•000002	•000003	•000005	146
147					•000001	•000001	•000002	•000003	147
148					•000001	•000001	•000001	•000002	148
149						•000001	•000001	•000002	149
150							•000001	•000001	150
151								•000001	151

X	A=102	A=103	A=104	A=105	A=106	A=107	A=108	A=109	X
58	•000001								58
59	•000001	•000001							59
60	•000002	•000001	•000001	•000001					60
61	•000003	•000002	•000001	•000001	•000001				61
62	•000005	•000004	•000002	•000002	•000001	•000001			62
63	•000009	•000006	•000004	•000003	•000002	•000001	•000001	•000001	63
64	•000014	•000010	•000007	•000004	•000003	•000002	•000001	•000001	64
65	•000022	•000015	•000011	•000007	•000005	•000003	•000002	•000002	65
66	•000034	•000024	•000017	•000012	•000008	•000005	•000004	•000002	66
67	•000052	•000037	•000026	•000018	•000013	•000009	•000006	•000004	67
68	•000078	•000056	•000040	•000028	•000020	•000014	•000009	•000006	68
69	•000115	•000083	•000060	•000042	•000030	•000021	•000015	•000010	69
70	•000168	•000122	•000089	•000064	•000045	•000032	•000023	•000016	70
71	•000241	•000178	•000130	•000094	•000068	•000049	•000035	•000025	71
72	•000342	•000254	•000187	•000137	•000100	•000072	•000052	•000037	72
73	•000478	•000358	•000267	•000197	•000145	•000106	•000077	•000055	73
74	•000659	•000499	•000375	•000280	•000208	•000153	•000112	•000082	74
75	•000896	•000685	•000520	•000392	•000294	•000219	•000162	•000119	75
76	•001203	•000929	•000712	•000542	•000410	•000308	•000230	•000170	76
77	•001593	•001242	•000962	•000739	•000564	•000428	•000322	•000241	77
78	•002083	•001640	•001282	•000995	•000767	•000587	•000446	•000337	78
79	•002690	•002139	•001688	•001322	•001029	•000795	•000610	•000464	79
80	•003430	•002754	•002194	•001736	•001363	•001063	•000823	•000633	80
81	•004319	•003502	•002817	•002250	•001784	•001404	•001097	•000852	81
82	•005372	•004398	•003573	•002881	•002306	•001832	•001445	•001132	82
83	•006602	•005458	•004478	•003645	•002945	•002362	•001880	•001487	83
84	•008017	•006693	•005544	•004556	•003716	•003008	•002418	•001929	84
85	•009620	•008110	•006783	•005628	•004634	•003787	•003072	•002474	85
86	•011410	•009713	•008202	•006872	•005712	•004712	•003858	•003135	86
87	•013377	•011500	•009805	•008293	•006959	•005795	•004789	•003928	87
88	•015505	•013460	•011588	•009895	•008383	•007046	•005877	•004866	88
89	•017770	•015577	•013541	•011674	•009984	•008471	•007132	•005959	89
90	•020139	•017827	•015647	•013620	•011759	•010072	•008559	•007217	90
91	•022574	•020178	•017883	•015715	•013697	•011842	•010157	•008644	91
92	•025027	•022591	•020215	•017936	•015782	•013773	•011924	•010242	92
93	•027449	•025020	•022606	•020251	•017988	•015847	•013847	•012004	93
94	•029785	•027415	•025011	•022620	•020284	•018038	•015909	•013919	94
95	•031980	•029724	•027381	•025001	•022633	•020317	•018086	•015971	95
96	•033979	•031891	•029662	•027345	•024991	•022644	•020347	•018133	96
97	•035730	•033864	•031803	•029600	•027309	•024979	•022655	•020376	97
98	•037189	•035592	•033750	•031715	•029539	•027273	•024966	•022664	98
99	•038316	•037030	•035454	•033637	•031627	•029477	•027236	•024953	99
100	•039082	•038141	•036873	•035319	•033525	•031540	•029415	•027199	100
101	•039469	•038896	•037968	•036718	•035185	•033414	•031454	•029353	101
102	•039469	•039277	•038712	•037797	•036564	•035052	•033304	•031367	102
103	•039086	•039277	•039088	•038531	•037629	•036413	•034920	•033195	103
104	•038334	•038899	•039088	•038902	•038353	•037463	•036264	•034791	104
105	•037239	•038159	•038716	•038902	•038718	•038177	•037300	•036116	105

TABLE I

X	A=102	A=103	A=104	A=105	A=106	A=107	A=108	A=109	X
106	035834	037079	037985	038535	038718	038537	038003	037138	106
107	034159	035692	036920	037815	038356	038537	038359	037832	107
108	032261	034040	035553	036764	037646	038180	038359	038183	108
109	030190	032166	033922	035415	036610	037480	038007	038183	109
110	027994	030119	032072	033805	035279	036458	037316	037835	110
111	025724	027949	030049	031978	033690	035144	036307	037154	111
112	023427	025703	027903	029979	031885	033575	035010	036159	112
113	021147	023428	025681	027857	029910	031792	033461	034879	113
114	018921	021168	023428	025658	027811	029840	031700	033349	114
115	016782	018959	021187	023427	025634	027764	029771	031609	115
116	014757	016834	018995	021205	023424	025610	027717	029701	116
117	012865	014820	016885	019030	021222	023421	025585	027671	117
118	011120	012936	014881	016934	019064	021238	023417	025560	118
119	009532	011197	013006	014941	016981	019096	021253	023412	119
120	008102	009610	011271	013074	015000	017027	019127	021266	120
121	006830	008181	009688	011345	013141	015057	017072	019157	121
122	005710	006907	008259	009764	011417	013206	015113	017116	122
123	004735	005784	006983	008335	009839	011488	013270	015168	123
124	003895	004804	005857	007058	008411	009913	011558	013333	124
125	003178	003959	004873	005929	007132	008486	009986	011626	125
126	002573	003236	004022	004941	006000	007206	008559	010058	126
127	002066	002624	003293	004085	005008	006071	007279	008632	127
128	001647	002112	002676	003351	004147	005075	006142	007351	128
129	001302	001686	002157	002727	003408	004210	005142	006211	129
130	001022	001336	001726	002203	002779	003465	004272	005208	130
131	000795	001050	001370	001766	002248	002830	003522	004333	131
132	000615	000820	001080	001405	001806	002294	002881	003578	132
133	000471	000635	000844	001109	001439	001846	002340	002932	133
134	000359	000488	000655	000869	001138	001474	001886	002385	134
135	000271	000372	000505	000676	000894	001168	001509	001926	135
136	000203	000282	000386	000522	000697	000919	001198	001544	136
137	000151	000212	000293	000400	000539	000718	000944	001228	137
138	000112	000158	000221	000304	000414	000557	000739	000970	138
139	000082	000117	000165	000230	000316	000428	000574	000761	139
140	000060	000086	000123	000172	000239	000327	000443	000592	140
141	000043	000063	000091	000128	000180	000248	000339	000458	141
142	000031	000046	000066	000095	000134	000187	000258	000351	142
143	000022	000033	000048	000070	000099	000140	000195	000268	143
144	000016	000024	000035	000051	000073	000104	000146	000203	144
145	000011	000017	000025	000037	000054	000077	000109	000152	145
146	000008	000012	000018	000026	000039	000056	000081	000114	146
147	000005	000008	000013	000019	000028	000041	000059	000084	147
148	000004	000006	000009	000013	000020	000030	000043	000062	148
149	000003	000004	000006	000009	000014	000021	000031	000045	149
150	000002	000003	000004	000007	000010	000015	000023	000033	150
151	000001	000002	000003	000005	000007	000011	000016	000024	151
152	000001	000001	000002	000003	000005	000008	000011	000017	152
153	000001	000001	000001	000002	000003	000005	000008	000012	153
154		000001	000001	000001	000002	000004	000006	000009	154
155			000001	000001	000002	000003	000004	000006	155
156				000001	000001	000002	000003	000004	156
157					000001	000001	000002	000003	157
158						000001	000001	000002	158
159							000001	000001	159
160								000001	160
161									161
X	A=110	A=111	A=112	A=113	A=114	A=115	A=116	A=117	X
64	000001								64
65	000001	000001							65
66	000002	000001	000001						66
67	000003	000002	000001	000001	000001				67
68	000004	000003	000002	000001	000001	000001			68
69	000007	000005	000003	000002	000002	000001	000001		69
70	000011	000008	000005	000004	000002	000002	000001	000001	70
71	000017	000012	000008	000006	000004	000003	000002	000001	71



TABLE I

X	A=110	A=111	A=112	A=113	A=114	A=115	A=116	A=117	X
72	•000026	•000019	•000013	•000009	•000006	•000004	•000003	•000002	72
73	•000040	•000028	•000020	•000014	•000010	•000007	•000005	•000003	73
74	•000059	•000042	•000030	•000022	•000015	•000011	•000007	•000005	74
75	•000087	•000063	•000045	•000032	•000023	•000016	•000012	•000008	75
76	•000125	•000092	•000067	•000048	•000035	•000025	•000018	•000012	76
77	•000179	•000132	•000097	•000071	•000051	•000037	•000026	•000019	77
78	•000252	•000188	•000139	•000103	•000075	•000055	•000039	•000028	78
79	•000352	•000264	•000198	•000147	•000108	•000079	•000058	•000042	79
80	•000483	•000367	•000277	•000207	•000154	•000114	•000084	•000051	80
81	•000656	•000503	•000382	•000289	•000217	•000162	•000120	•000089	81
82	•000881	•000680	•000522	•000398	•000302	•000227	•000170	•000126	82
83	•001167	•000910	•000705	•000542	•000414	•000315	•000238	•000178	83
84	•001528	•001202	•000940	•000729	•000562	•000431	•000328	•000248	84
85	•001978	•001570	•001238	•000970	•000754	•000583	•000448	•000342	85
86	•002530	•002027	•001612	•001274	•001000	•000780	•000604	•000465	86
87	•003199	•002586	•002076	•001655	•001310	•001030	•000805	•000625	87
88	•003998	•003262	•002642	•002125	•001697	•001347	•001061	•000831	88
89	•004942	•004068	•003325	•002698	•002174	•001740	•001383	•001092	89
90	•006040	•005017	•004137	•003387	•002754	•002223	•001783	•001420	90
91	•007301	•006120	•005092	•004206	•003450	•002810	•002273	•001826	91
92	•008729	•007383	•006199	•005166	•004275	•003512	•002866	•002322	92
93	•010325	•008813	•007465	•006277	•005240	•004343	•003574	•002921	93
94	•012082	•010406	•008895	•007546	•006355	•005313	•004411	•003636	94
95	•013990	•012159	•010486	•008976	•007626	•006432	•005386	•004478	95
96	•016030	•014059	•012234	•010565	•009056	•007705	•006508	•005458	96
97	•018178	•016088	•014126	•012308	•010643	•009134	•007783	•006583	97
98	•020404	•018222	•016144	•014192	•012380	•010719	•009212	•007859	98
99	•022671	•020431	•018264	•016199	•014256	•012451	•010794	•009288	99
100	•024939	•022678	•020456	•018305	•016252	•014319	•012521	•010867	100
101	•027161	•024923	•022684	•020480	•018344	•016304	•014380	•012589	101
102	•029291	•027123	•024908	•022688	•020502	•018382	•016354	•014440	102
103	•031282	•029229	•027084	•024891	•022692	•020523	•018418	•016403	103
104	•033086	•031197	•029167	•027045	•024804	•022694	•020544	•018454	104
105	•034662	•032979	•031112	•029105	•027006	•024856	•022696	•020562	105
106	•035970	•034535	•032873	•031028	•029044	•026966	•024837	•022696	106
107	•036979	•035826	•034409	•032767	•030944	•028982	•026926	•024818	107
108	•037663	•036821	•035683	•034284	•032663	•030860	•028920	•026886	108
109	•038009	•037497	•036665	•035543	•034161	•032559	•030778	•028859	109
110	•038009	•037838	•037332	•036512	•035403	•034039	•032456	•030695	110
111	•037666	•037838	•037668	•037170	•036360	•035266	•033918	•032355	111
112	•036994	•037500	•037668	•037502	•037010	•036210	•035130	•033799	112
113	•036012	•036836	•037335	•037502	•037337	•036851	•036062	•034995	113
114	•034748	•035867	•036680	•037173	•037337	•037175	•036695	•035916	114
115	•033237	•034619	•035723	•036526	•037012	•037175	•037014	•036541	115
116	•031518	•033127	•034491	•035582	•036374	•036854	•037014	•036856	116
117	•029632	•031428	•033017	•034365	•035442	•036224	•036698	•036856	117
118	•027623	•029564	•031339	•032909	•034240	•035303	•036076	•036544	118
119	•025534	•027576	•029495	•031250	•032801	•034117	•035166	•035929	119
120	•023406	•025508	•027529	•029427	•031161	•032695	•033994	•035031	120
121	•021279	•023400	•025481	•027481	•029359	•031074	•032589	•033873	121
122	•019186	•021290	•023393	•025454	•027434	•029291	•030987	•032485	122
123	•017158	•019213	•021301	•023384	•025426	•027386	•029223	•030900	123
124	•015221	•017199	•019239	•021310	•023376	•025398	•027338	•029156	124
125	•013394	•015272	•017238	•019264	•021319	•023366	•025370	•027290	125
126	•011693	•013454	•015323	•017277	•019288	•021326	•023356	•025341	126
127	•010128	•011759	•013513	•015302	•017314	•019311	•021333	•023345	127
128	•008704	•010197	•011824	•013571	•015420	•017350	•019333	•021339	128
129	•007422	•008775	•010266	•011888	•013627	•015467	•017385	•019354	129
130	•006280	•007492	•008844	•010333	•011950	•013682	•015513	•017419	130
131	•005273	•006348	•007562	•008913	•010399	•012011	•013736	•015557	131
132	•004394	•005338	•006416	•007630	•008981	•010464	•012071	•013789	132
133	•003634	•004455	•005403	•006483	•007698	•009048	•010528	•012130	133
134	•002984	•003691	•004516	•005467	•006549	•007765	•009114	•010591	134
135	•002431	•003034	•003746	•004576	•005530	•006615	•007831	•009179	135
136	•001966	•002477	•003085	•003802	•004636	•005593	•006680	•007897	136
137	•001579	•002007	•002522	•003136	•003857	•004695	•005656	•006744	137
138	•001258	•001614	•002047	•002568	•003187	•003913	•004754	•005718	138
139	•000996	•001289	•001649	•002088	•002613	•003237	•003967	•004813	139

TABLE I

X	A=110	A=111	A=112	A=113	A=114	A=115	A=116	A=117	X
140	.000782	.001022	.001320	.001685	.002128	.002659	.003287	.004022	140
141	.000610	.000804	.001048	.001350	.001721	.002169	.002705	.003338	141
142	.000473	.000629	.000827	.001075	.001381	.001756	.002209	.002750	142
143	.000364	.000488	.000647	.000849	.001101	.001412	.001792	.002250	143
144	.000278	.000376	.000504	.000666	.000872	.001128	.001444	.001828	144
145	.000211	.000288	.000389	.000519	.000685	.000895	.001155	.001475	145
146	.000159	.000219	.000298	.000402	.000535	.000705	.000918	.001182	146
147	.000119	.000165	.000227	.000309	.000415	.000551	.000724	.000941	147
148	.000088	.000124	.000172	.000236	.000320	.000428	.000568	.000744	148
149	.000065	.000092	.000129	.000179	.000245	.000331	.000442	.000584	149
150	.000048	.000068	.000097	.000135	.000186	.000253	.000342	.000456	150
151	.000035	.000050	.000072	.000101	.000140	.000193	.000262	.000353	151
152	.000025	.000037	.000053	.000075	.000105	.000146	.000200	.000272	152
153	.000018	.000027	.000039	.000055	.000078	.000110	.000152	.000208	153
154	.000013	.000019	.000028	.000041	.000058	.000082	.000114	.000158	154
155	.000009	.000014	.000020	.000030	.000043	.000061	.000086	.000119	155
156	.000006	.000010	.000015	.000021	.000031	.000045	.000064	.000089	156
157	.000005	.000007	.000010	.000015	.000023	.000033	.000047	.000067	157
158	.000003	.000005	.000007	.000011	.000016	.000024	.000035	.000049	158
159	.000002	.000003	.000005	.000008	.000012	.000017	.000025	.000036	159
160	.000001	.000002	.000004	.000006	.000008	.000012	.000018	.000027	160
161	.000001	.000002	.000003	.000004	.000006	.000009	.000013	.000019	161
162	.000001	.000001	.000002	.000003	.000004	.000006	.000009	.000014	162
163	.000001	.000001	.000001	.000002	.000003	.000004	.000007	.000010	163
164	.000001	.000001	.000001	.000001	.000002	.000003	.000005	.000007	164
165			.000001	.000001	.000001	.000002	.000003	.000005	165
166				.000001	.000001	.000001	.000002	.000004	166
167					.000001	.000001	.000002	.000002	167
168						.000001	.000001	.000002	168
169							.000001	.000001	169
170							.000001		170
171								.000001	171
X	A=118	A=119	A=120	A=121	A=122	A=123	A=124	A=125	X
70	.000001								70
71	.000001	.000001							71
72	.000001	.000001	.000001						72
73	.000002	.000002	.000001	.000001					73
74	.000004	.000002	.000002	.000001	.000001	.000001			74
75	.000006	.000004	.000003	.000002	.000001	.000001	.000001		75
76	.000009	.000006	.000004	.000003	.000002	.000001	.000001	.000001	76
77	.000013	.000009	.000007	.000005	.000003	.000002	.000002	.000001	77
78	.000020	.000014	.000010	.000007	.000005	.000003	.000002	.000002	78
79	.000030	.000022	.000015	.000011	.000008	.000005	.000004	.000003	79
80	.000045	.000032	.000023	.000017	.000012	.000008	.000006	.000004	80
81	.000065	.000047	.000034	.000025	.000018	.000013	.000009	.000006	81
82	.000093	.000069	.000050	.000036	.000026	.000019	.000014	.000010	82
83	.000133	.000098	.000073	.000053	.000039	.000028	.000020	.000014	83
84	.000187	.000139	.000104	.000077	.000056	.000041	.000030	.000022	84
85	.000259	.000195	.000146	.000109	.000081	.000059	.000043	.000032	85
86	.000355	.000270	.000204	.000153	.000114	.000085	.000063	.000046	86
87	.000482	.000370	.000282	.000213	.000161	.000120	.000089	.000065	87
88	.000646	.000500	.000384	.000293	.000223	.000168	.000126	.000094	88
89	.000857	.000668	.000518	.000399	.000305	.000232	.000176	.000132	89
90	.001124	.000884	.000690	.000536	.000414	.000317	.000242	.000183	90
91	.001457	.001155	.000910	.000713	.000554	.000429	.000330	.000252	91
92	.001869	.001495	.001187	.000937	.000735	.000573	.000444	.000342	92
93	.002372	.001912	.001532	.001219	.000964	.000758	.000592	.000460	93
94	.002977	.002421	.001956	.001570	.001252	.000992	.000781	.000611	94
95	.003698	.003033	.002470	.001999	.001608	.001284	.001020	.000805	95
96	.004545	.003759	.003088	.002520	.002043	.001645	.001317	.001048	96
97	.005529	.004612	.003820	.003143	.002569	.002087	.001684	.001350	97
98	.006658	.005600	.004678	.003881	.003199	.002619	.002130	.001722	98
99	.007935	.006731	.005670	.004744	.003942	.003254	.002668	.002174	99
100	.009364	.008010	.006804	.005740	.004809	.004002	.003309	.002718	100
101	.010940	.009438	.008084	.006876	.005809	.004874	.004062	.003363	101
102	.012656	.011011	.009511	.008157	.006948	.005877	.004938	.004122	102

TABLE I

X	A=118	A=119	A=120	A=121	A=122	A=123	A=124	A=125	X
103	•014499	•012721	•011081	•009583	•008229	•007018	•005945	•005002	103
104	•016451	•014556	•012785	•011149	•009654	•008301	•007088	•006012	104
105	•018487	•016497	•014612	•012848	•011217	•009724	•008371	•007157	105
106	•020580	•018520	•016542	•014666	•012910	•011283	•009792	•008440	106
107	•022696	•020597	•018552	•016585	•014720	•012970	•011348	•009860	107
108	•024798	•022695	•020613	•018582	•016628	•014772	•013029	•011412	108
109	•026845	•024777	•022693	•020628	•018611	•016669	•014823	•013087	109
110	•028797	•026804	•024756	•022690	•020641	•018639	•016709	•014872	110
111	•030614	•028736	•026763	•024734	•022687	•020654	•018666	•016748	111
112	•032254	•030532	•028675	•026722	•024712	•022683	•020666	•018692	112
113	•033681	•032153	•030451	•028614	•026681	•024690	•022678	•020677	113
114	•034862	•033564	•032054	•030371	•028553	•026639	•024667	•022672	114
115	•035772	•034731	•033448	•031955	•030291	•028492	•026597	•024643	115
116	•036389	•035629	•034601	•033333	•031858	•030212	•028432	•026555	116
117	•036700	•036238	•035488	•034472	•033219	•031761	•030133	•028371	117
118	•036700	•036545	•036090	•035349	•034345	•033107	•031665	•030054	118
119	•036391	•036545	•036393	•035943	•035211	•034220	•032995	•031570	119
120	•035785	•036241	•036393	•036242	•035798	•035075	•034095	•032885	120
121	•034898	•035642	•036092	•036242	•036094	•035655	•034940	•033972	121
122	•033753	•034765	•035501	•035945	•036094	•035947	•035513	•034807	122
123	•032381	•033635	•034635	•035361	•035800	•035947	•035802	•035373	123
124	•030814	•032279	•033517	•034505	•035223	•035657	•035802	•035659	124
125	•029089	•030729	•032177	•033401	•034378	•035087	•035516	•035659	125
126	•027242	•029022	•030644	•032076	•033286	•034251	•034952	•035376	126
127	•025311	•027194	•028955	•030560	•031976	•033172	•034126	•034819	127
128	•023334	•025282	•027146	•028889	•030477	•031877	•033060	•034003	128
129	•021344	•023322	•025252	•027098	•028823	•030394	•031778	•032948	129
130	•019374	•021349	•023309	•025222	•027049	•028757	•030312	•031681	130
131	•017451	•019393	•021352	•023296	•025191	•027001	•028692	•030230	131
132	•015600	•017483	•019411	•021355	•023283	•025160	•026953	•028627	132
133	•013841	•015643	•017514	•019428	•021357	•023268	•025129	•026905	133
134	•012188	•013892	•015684	•017543	•019444	•021358	•023254	•025098	134
135	•010654	•012245	•013941	•015724	•017572	•019460	•021359	•023239	135
136	•009243	•010715	•012301	•013990	•015763	•017600	•019474	•021359	136
137	•007962	•009307	•010775	•012356	•014037	•015801	•017627	•019488	137
138	•006808	•008025	•009369	•010834	•012410	•014084	•015838	•017652	138
139	•005779	•006871	•008089	•009431	•010892	•012463	•014129	•015874	139
140	•004871	•005840	•006933	•008151	•009492	•010949	•012514	•014174	140
141	•004076	•004929	•005900	•006995	•008213	•009551	•011006	•012565	141
142	•003387	•004131	•004986	•005960	•007056	•008273	•009610	•011061	142
143	•002795	•003437	•004184	•005043	•006020	•007116	•008334	•009669	143
144	•002291	•002841	•003487	•004238	•005100	•006079	•007176	•008393	144
145	•001864	•002331	•002886	•003536	•004291	•005156	•006137	•007235	145
146	•001507	•001900	•002372	•002931	•003586	•004344	•005212	•006195	146
147	•001209	•001538	•001936	•002412	•002976	•003635	•004397	•005268	147
148	•000964	•001237	•001570	•001972	•002453	•003021	•003684	•004449	148
149	•000764	•000988	•001264	•001602	•002009	•002494	•003066	•003732	149
150	•000601	•000784	•001011	•001292	•001634	•002045	•002534	•003110	150
151	•000469	•000618	•000804	•001035	•001320	•001666	•002081	•002575	151
152	•000364	•000483	•000635	•000824	•001059	•001348	•001698	•002117	152
153	•000281	•000376	•000498	•000652	•000845	•001084	•001376	•001730	153
154	•000215	•000291	•000388	•000512	•000669	•000865	•001108	•001404	154
155	•000164	•000223	•000300	•000400	•000527	•000687	•000886	•001132	155
156	•000124	•000170	•000231	•000310	•000412	•000541	•000704	•000907	156
157	•000093	•000129	•000177	•000239	•000320	•000424	•000556	•000722	157
158	•000070	•000097	•000134	•000183	•000247	•000330	•000437	•000572	158
159	•000052	•000073	•000101	•000139	•000190	•000255	•000341	•000449	159
160	•000038	•000054	•000076	•000105	•000145	•000196	•000264	•000351	160
161	•000028	•000040	•000057	•000079	•000110	•000150	•000203	•000273	161
162	•000020	•000029	•000042	•000059	•000083	•000114	•000156	•000210	162
163	•000015	•000021	•000031	•000044	•000062	•000086	•000118	•000161	163
164	•000011	•000016	•000023	•000032	•000046	•000064	•000089	•000123	164
165	•000008	•000011	•000016	•000024	•000034	•000048	•000067	•000093	165
166	•000005	•000008	•000012	•000017	•000025	•000036	•000050	•000070	166
167	•000004	•000006	•000009	•000013	•000018	•000026	•000037	•000052	167
168	•000003	•000004	•000006	•000009	•000013	•000019	•000028	•000039	168
169	•000002	•000003	•000004	•000006	•000010	•000014	•000020	•000029	169
170	•000001	•000002	•000003	•000005	•000007	•000010	•000015	•000021	170

TABLE I

X	A=118	A=119	A=120	A=121	A=122	A=123	A=124	A=125	X
171	•000001	•000001	•000002	•000003	•000005	•000007	•000011	•000016	171
172	•000001	•000001	•000001	•000002	•000003	•000005	•000008	•000011	172
173		•000001	•000001	•000002	•000002	•000004	•000006	•000008	173
174			•000001	•000001	•000002	•000003	•000004	•000006	174
175				•000001	•000001	•000002	•000003	•000004	175
176				•000001	•000001	•000001	•000002	•000003	176
177					•000001	•000001	•000001	•000002	177
178						•000001	•000001	•000001	178
179							•000001	•000001	179
180								•000001	180
X	A=126	A=127	A=128	A=129	A=130	A=131	A=132	A=133	X
77	•000001								77
78	•000001	•000001	•000001						78
79	•000002	•000001	•000001	•000001					79
80	•000003	•000002	•000001	•000001	•000001				80
81	•000004	•000003	•000002	•000001	•000001	•000001			81
82	•000007	•000005	•000003	•000002	•000002	•000001	•000001	•000001	82
83	•000010	•000007	•000005	•000004	•000003	•000002	•000001	•000001	83
84	•000015	•000011	•000008	•000006	•000004	•000003	•000002	•000001	84
85	•000023	•000017	•000012	•000008	•000006	•000004	•000003	•000002	85
86	•000034	•000024	•000018	•000013	•000009	•000006	•000005	•000003	86
87	•000049	•000036	•000026	•000019	•000014	•000010	•000007	•000005	87
88	•000070	•000051	•000038	•000028	•000020	•000014	•000010	•000007	88
89	•000099	•000073	•000054	•000040	•000029	•000021	•000015	•000011	89
90	•000138	•000104	•000077	•000057	•000042	•000031	•000023	•000016	90
91	•000191	•000144	•000108	•000081	•000060	•000044	•000033	•000024	91
92	•000262	•000199	•000151	•000114	•000085	•000063	•000047	•000035	92
93	•000355	•000272	•000208	•000158	•000119	•000089	•000067	•000049	93
94	•000476	•000368	•000283	•000216	•000164	•000124	•000093	•000070	94
95	•000631	•000492	•000381	•000294	•000225	•000171	•000130	•000098	95
96	•000828	•000651	•000508	•000395	•000305	•000234	•000179	•000136	96
97	•001076	•000852	•000671	•000525	•000408	•000316	•000243	•000186	97
98	•001383	•001104	•000876	•000691	•000542	•000422	•000327	•000252	98
99	•001760	•001416	•001133	•000900	•000711	•000559	•000436	•000339	99
100	•002218	•001799	•001450	•001161	•000925	•000732	•000576	•000451	100
101	•002767	•002262	•001837	•001483	•001190	•000950	•000753	•000594	101
102	•003418	•002816	•002306	•001876	•001517	•001219	•000974	•000774	102
103	•004181	•003472	•002865	•002350	•001915	•001551	•001249	•001000	103
104	•005066	•004240	•003527	•002914	•002393	•001954	•001585	•001278	104
105	•006079	•005129	•004299	•003581	•002963	•002437	•001993	•001619	105
106	•007226	•006145	•005191	•004357	•003634	•003012	•002481	•002031	106
107	•008509	•007293	•006210	•005253	•004416	•003688	•003061	•002525	107
108	•009927	•008576	•007360	•006275	•005315	•004473	•003741	•003110	108
109	•011475	•009993	•008643	•007426	•006339	•005376	•004531	•003794	109
110	•013144	•011537	•010057	•008709	•007491	•006402	•005437	•004588	110
111	•014921	•013200	•011598	•010121	•008774	•007556	•006465	•005497	111
112	•016786	•014968	•013255	•011657	•010184	•008838	•007620	•006528	112
113	•018717	•016822	•015014	•013308	•011716	•010246	•008901	•007683	113
114	•020687	•018741	•016858	•015059	•013360	•011774	•010307	•008964	114
115	•022666	•020696	•018763	•016892	•015103	•013412	•011830	•010367	115
116	•024620	•022659	•020705	•018785	•016926	•015146	•013462	•011886	116
117	•026513	•024595	•022651	•020712	•018806	•016958	•015188	•013511	117
118	•028311	•026471	•024571	•022643	•020719	•018827	•016990	•015229	118
119	•029976	•028251	•026429	•024546	•022634	•020725	•018846	•017020	119
120	•031475	•029899	•028191	•026387	•024520	•022625	•020730	•018864	120
121	•032776	•031381	•029822	•028131	•026344	•024495	•022615	•020735	121
122	•033850	•032667	•031288	•029745	•028072	•026302	•024469	•022605	122
123	•034676	•033730	•032560	•031196	•029669	•028012	•026259	•024442	123
124	•035235	•034546	•033611	•032454	•031105	•029594	•027953	•026216	124
125	•035517	•035099	•034417	•033493	•032349	•031014	•029518	•027894	125
126	•035517	•035377	•034964	•034290	•033376	•032245	•030924	•029444	126
127	•035237	•035377	•035239	•034830	•034164	•033260	•032142	•030835	127
128	•034687	•035101	•035102	•034698	•034698	•034040	•033146	•032039	128
129	•033880	•034557	•034966	•035102	•034967	•034568	•033917	•033033	129
130	•0332838	•033759	•034428	•034832	•034967	•034834	•034439	•033795	130

TABLE I

X	A=126	A=127	A=128	A=129	A=130	A=131	A=132	A=133	X
131	031584	032728	033639	034300	034700	034834	034702	034311	131
132	030149	031489	032620	033521	034174	034570	034702	034571	132
133	028562	030068	031394	032513	033404	034050	034441	034571	133
134	026857	028497	029988	031300	032406	033288	033927	034313	134
135	025066	026809	028433	029908	031206	032301	033173	033805	135
136	023223	025035	026761	028369	029829	031114	032197	033059	136
137	021359	023207	025003	026712	028305	029751	031022	032094	137
138	019501	021357	023191	024970	026664	028242	029673	030931	138
139	017677	019514	021356	023174	024938	026616	028179	029596	139
140	015910	017702	019525	021353	0223157	024905	026569	028116	140
141	014217	015944	017725	019536	021350	023139	024873	026521	141
142	012615	014260	015977	017747	019546	021347	023121	024840	142
143	011116	012664	014301	016010	017769	019555	021343	023103	143
144	0099726	011169	012712	014342	016041	017790	019564	021338	144
145	008452	0099783	011222	012760	014382	016072	017810	019572	145
146	007294	008510	009838	011274	012806	014421	016102	017829	146
147	006252	007352	008567	009893	011325	012851	014459	016131	147
148	005323	006309	007409	008623	009948	011375	012896	014496	148
149	004501	005377	006365	007466	008679	010001	011425	012940	149
150	003781	004553	005431	006421	007522	008734	010054	011473	150
151	003155	003829	004604	005485	006476	007577	008789	010106	151
152	002615	003199	003877	004655	005538	006530	007632	008842	152
153	002154	002656	003244	003929	004706	005591	006585	007687	153
154	001762	002190	002696	003288	003973	004756	005644	006638	154
155	001432	001794	002226	002736	003332	004020	004807	005696	155
156	001157	001461	001827	002263	002777	003376	004067	004856	156
157	000928	001182	001489	001859	002299	002817	003419	004114	157
158	000740	000950	001207	001518	001892	002335	002857	003463	158
159	000587	000759	000971	001232	001547	001924	002372	002897	159
160	000462	000602	000777	000993	001257	001575	001957	002408	160
161	000362	000475	000618	000796	001015	001282	001604	001989	161
162	000281	000372	000488	000633	000814	001037	001307	001633	162
163	000217	000290	000383	000501	000649	000833	001058	001332	163
164	000167	000225	000299	000394	000515	000665	000852	001081	164
165	000128	000173	000232	000308	000406	000528	000682	000871	165
166	000097	000132	000179	000240	000318	000417	000542	000698	166
167	000073	000101	000137	000185	000247	000327	000428	000556	167
168	000055	000076	000104	000142	000191	000255	000337	000440	168
169	000041	000057	000079	000108	000147	000198	000263	000346	169
170	000030	000043	000060	000082	000113	000152	000204	000271	170
171	000022	000032	000045	000062	000086	000117	000158	000211	171
172	000016	000023	000033	000047	000065	000089	000121	000163	172
173	000012	000017	000025	000035	000049	000067	000092	000125	173
174	000009	000013	000018	000026	000036	000051	000070	000096	174
175	000006	000009	000013	000019	000027	000038	000053	000073	175
176	000004	000007	000010	000014	000020	000028	000040	000055	176
177	000003	000005	000007	000010	000015	000021	000030	000041	177
178	000002	000003	000005	000007	000011	000015	000022	000031	178
179	000002	000002	000004	000005	000008	000011	000016	000023	179
180	000001	000002	000003	000004	000006	000008	000012	000017	180
181	000001	000001	000002	000003	000004	000006	000009	000012	181
182	000001	000001	000001	000002	000003	000004	000006	000009	182
183		000001	000001	000001	000002	000003	000005	000007	183
184			000001	000001	000001	000002	000003	000005	184
185				000001	000001	000002	000002	000003	185
186					000001	000001	000002	000002	186
187						000001	000001	000002	187
188							000001	000001	188
189								000001	189
190								000001	190
X	A=134	A=135	A=136	A=137	A=138	A=139	A=140	A=141	X
83	000001								83
84	000001	000001							84
85	000001	000001	000001						85
86	000002	000002	000001	000001	000001				86

TABLE I

X	A=134	A=135	A=136	A=137	A=138	A=139	A=140	A=141	X
87	•000003	•000002	•000002	•000001	•000001	•000001			87
88	•000005	•000004	•000003	•000002	•000001	•000001	•000001		88
89	•000008	•000006	•000004	•000003	•000002	•000001	•000001	•000001	89
90	•000012	•000008	•000006	•000004	•000003	•000002	•000002	•000001	90
91	•000017	•000013	•000009	•000006	•000005	•000003	•000002	•000002	91
92	•000025	•000018	•000013	•000010	•000007	•000005	•000004	•000002	92
93	•000036	•000027	•000020	•000014	•000010	•000007	•000005	•000004	93
94	•000052	•000038	•000028	•000021	•000015	•000011	•000008	•000006	94
95	•000073	•000055	•000041	•000030	•000022	•000016	•000012	•000008	95
96	•000102	•000077	•000057	•000043	•000032	•000023	•000017	•000012	96
97	•000141	•000107	•000081	•000060	•000045	•000033	•000025	•000018	97
98	•000193	•000147	•000112	•000084	•000063	•000047	•000035	•000026	98
99	•000262	•000201	•000154	•000117	•000088	•000066	•000050	•000037	99
100	•000351	•000271	•000209	•000160	•000122	•000092	•000069	•000052	100
101	•000465	•000363	•000281	•000217	•000166	•000127	•000096	•000073	101
102	•000611	•000480	•000375	•000291	•000225	•000173	•000132	•000100	102
103	•000795	•000629	•000495	•000387	•000301	•000233	•000180	•000137	103
104	•001025	•000817	•000647	•000510	•000400	•000312	•000242	•000186	104
105	•001308	•001050	•000839	•000666	•000526	•000413	•000322	•000250	105
106	•001653	•001338	•001076	•000860	•000684	•000541	•000426	•000333	106
107	•002070	•001688	•001368	•001102	•000883	•000703	•000557	•000439	107
108	•002569	•002110	•001722	•001398	•001128	•000905	•000722	•000573	108
109	•003158	•002613	•002149	•001757	•001428	•001154	•000927	•000741	109
110	•003847	•003207	•002657	•002188	•001791	•001458	•001180	•000950	110
111	•004644	•003900	•003255	•002700	•002227	•001826	•001488	•001207	111
112	•005557	•004701	•003952	•003303	•002744	•002266	•001861	•001519	112
113	•006589	•005616	•004757	•004004	•003351	•002787	•002305	•001895	113
114	•007745	•006650	•005675	•004812	•004056	•003399	•002831	•002344	114
115	•009025	•007807	•006711	•005733	•004868	•004108	•003446	•002874	115
116	•010426	•009086	•007868	•006771	•005791	•004922	•004159	•003494	116
117	•011940	•010484	•009146	•007928	•006830	•005848	•004977	•004210	117
118	•013559	•011994	•010541	•009205	•007988	•006889	•005905	•005031	118
119	•015269	•013607	•012047	•010597	•009263	•008047	•006947	•005961	119
120	•017050	•015307	•013653	•012098	•010653	•009321	•008105	•007004	120
121	•018882	•017079	•015345	•013698	•012149	•010707	•009377	•008162	121
122	•020739	•018898	•017106	•015382	•013743	•012199	•010761	•009433	122
123	•022594	•020742	•018914	•017133	•015419	•013786	•012248	•010814	123
124	•024416	•022582	•018930	•018930	•017159	•015454	•013829	•012297	124
125	•026174	•024389	•022570	•020747	•018944	•017185	•015488	•013870	125
126	•027835	•026131	•024362	•022558	•020748	•018958	•017209	•015522	126
127	•029370	•027777	•026088	•024334	•022545	•020749	•018971	•017233	127
128	•030746	•029296	•027719	•026045	•024307	•022532	•020749	•018983	128
129	•031938	•030659	•029223	•027660	•026002	•024279	•022518	•020749	129
130	•032921	•031838	•030571	•029150	•027603	•025960	•024251	•022504	130
131	•033675	•032810	•031738	•030485	•029078	•027545	•025917	•024222	131
132	•034185	•033586	•032700	•031640	•030399	•029006	•027487	•025874	132
133	•034442	•034060	•033438	•032591	•031542	•030314	•028934	•027430	133
134	•034442	•034314	•033937	•033321	•032484	•031445	•030230	•028863	134
135	•034187	•034314	•034188	•033815	•033205	•032377	•031349	•030146	135
136	•033684	•034062	•034188	•034063	•033694	•033091	•032271	•031254	136
137	•032946	•033565	•033939	•034063	•033940	•033574	•032978	•032167	137
138	•031991	•032835	•033447	•033816	•033940	•033818	•033456	•032866	138
139	•030841	•031890	•032725	•033330	•033696	•033818	•033697	•033339	139
140	•029519	•030751	•031790	•032616	•033214	•033576	•033697	•033577	140
141	•028053	•029443	•030662	•031690	•032507	•033100	•033458	•033577	141
142	•026473	•027991	•029367	•030574	•031592	•032400	•032986	•033341	142
143	•024807	•026425	•027929	•029292	•030487	•031494	•032294	•032874	143
144	•023084	•024774	•026378	•027868	•029217	•030401	•031397	•032189	144
145	•021333	•023065	•024740	•026330	•027806	•029143	•030315	•031301	145
146	•019580	•021327	•023046	•024707	•026283	•027745	•029069	•030230	146
147	•017848	•019586	•021321	•023026	•024674	•026235	•027685	•028996	147
148	•016160	•017866	•019593	•021315	•023006	•024640	•026188	•027624	148
149	•014533	•016187	•017883	•019598	•021308	•022986	•024606	•026141	149
150	•012983	•014569	•016214	•017900	•019603	•021301	•022966	•024573	150
151	•011521	•013025	•014603	•016240	•017916	•019608	•021293	•022945	151
152	•010157	•011568	•013066	•014638	•016266	•017931	•019612	•021285	152
153	•008895	•010207	•011614	•013107	•014671	•016290	•017946	•019615	153
154	•007740	•008948	•010257	•011660	•013147	•014703	•016314	•017960	154

TABLE I

X	A=134	A=135	A=136	A=137	A=138	A=139	A=140	A=141	X
155	•006692	•007793	•009000	•010306	•011705	•013186	•014735	•016337	155
156	•005748	•006744	•007846	•009051	•010354	•011749	•013224	•014766	156
157	•004906	•005799	•006796	•007898	•009101	•010402	•011792	•013262	157
158	•004161	•004955	•005850	•006848	•007949	•009151	•010449	•011835	158
159	•003506	•004207	•005004	•005901	•006899	•008000	•009200	•010495	159
160	•002937	•003550	•004253	•005052	•005951	•006950	•008050	•009249	160
161	•002444	•002976	•003593	•004299	•005100	•006000	•007000	•008100	161
162	•002022	•002480	•003016	•003636	•004345	•005148	•006049	•007050	162
163	•001662	•002054	•002517	•003056	•003678	•004390	•005196	•006098	163
164	•001358	•001384	•002087	•002553	•003095	•003721	•004435	•005243	164
165	•001103	•001125	•001720	•002120	•002589	•003135	•003763	•004480	165
166	•000890	•000910	•001409	•001749	•002152	•002625	•003174	•003806	166
167	•000714	•000731	•001148	•001435	•001778	•002185	•002661	•003213	167
168	•000570	•000584	•000929	•001170	•001461	•001808	•002217	•002697	168
169	•000452	•000464	•000748	•000949	•001193	•001487	•001837	•002250	169
170	•000356	•000366	•000598	•000764	•000968	•001216	•001513	•001866	170
171	•000279	•000287	•000476	•000612	•000781	•000988	•001238	•001539	171
172	•000217	•000224	•000376	•000488	•000627	•000799	•001008	•001261	172
173	•000168	•000174	•000296	•000386	•000500	•000642	•000816	•001028	173
174	•000130	•000134	•000231	•000304	•000397	•000513	•000656	•000833	174
175	•000099	•000103	•000180	•000238	•000313	•000407	•000525	•000671	175
176	•000076	•000078	•000139	•000185	•000245	•000322	•000418	•000538	176
177	•000057	•000060	•000107	•000143	•000191	•000252	•000330	•000428	177
178	•000043	•000045	•000081	•000110	•000148	•000197	•000260	•000339	178
179	•000032	•000034	•000062	•000085	•000114	•000153	•000203	•000267	179
180	•000024	•000025	•000047	•000064	•000088	•000118	•000158	•000209	180
181	•000018	•000019	•000035	•000049	•000067	•000091	•000122	•000163	181
182	•000013	•000014	•000026	•000037	•000051	•000069	•000094	•000126	182
183	•000010	•000010	•000020	•000027	•000038	•000053	•000072	•000097	183
184	•000007	•000007	•000014	•000020	•000029	•000040	•000055	•000075	184
185	•000005	•000005	•000011	•000015	•000021	•000030	•000041	•000057	185
186	•000004	•000004	•000008	•000011	•000016	•000022	•000031	•000043	186
187	•000003	•000003	•000006	•000008	•000012	•000017	•000023	•000032	187
188	•000002	•000002	•000004	•000006	•000009	•000012	•000017	•000024	188
189	•000001	•000001	•000003	•000004	•000006	•000009	•000013	•000018	189
190	•000001	•000001	•000002	•000003	•000005	•000007	•000009	•000013	190
191	•000001	•000001	•000001	•000002	•000003	•000005	•000007	•000010	191
192			•000001	•000002	•000002	•000003	•000005	•000007	192
193			•000001	•000001	•000002	•000003	•000004	•000005	193
194			•000001	•000001	•000001	•000002	•000003	•000004	194
195				•000001	•000001	•000001	•000002	•000003	195
196					•000001	•000001	•000001	•000002	196
197						•000001	•000001	•000001	197
198							•000001	•000001	198
199							•000001	•000001	199
200								•000001	200
X	A=142	A=143	A=144	A=145	A=146	A=147	A=148	A=149	X
90	•000001								90
91	•000001	•000001	•000001						91
92	•000002	•000001	•000001	•000001					92
93	•000003	•000002	•000001	•000001	•000001				93
94	•000004	•000003	•000002	•000001	•000001	•000001			94
95	•000006	•000004	•000003	•000002	•000002	•000001	•000001	•000001	95
96	•000009	•000006	•000005	•000003	•000002	•000002	•000001	•000001	96
97	•000013	•000010	•000007	•000005	•000004	•000003	•000002	•000001	97
98	•000019	•000014	•000010	•000007	•000005	•000004	•000003	•000002	98
99	•000027	•000020	•000015	•000011	•000008	•000006	•000004	•000003	99
100	•000039	•000029	•000021	•000016	•000011	•000008	•000006	•000004	100
101	•000055	•000041	•000030	•000022	•000017	•000012	•000009	•000006	101
102	•000076	•000057	•000043	•000032	•000024	•000017	•000013	•000009	102
103	•000105	•000079	•000060	•000045	•000034	•000025	•000018	•000014	103
104	•000143	•000109	•000083	•000063	•000047	•000035	•000026	•000019	104
105	•000193	•000149	•000114	•000086	•000065	•000049	•000037	•000028	105
106	•000259	•000201	•000154	•000118	•000090	•000068	•000052	•000039	106
107	•000344	•000268	•000208	•000160	•000123	•000094	•000071	•000054	107
108	•000452	•000355	•000277	•000215	•000166	•000128	•000098	•000074	108

~~SECRET~~

TABLE I

X	A=142	A=143	A=144	A=145	A=146	A=147	A=148	A=149	X
109	000589	000466	000366	000286	000223	000172	000133	000102	109
110	000760	000605	000479	000377	000296	000231	000179	000138	110
111	000973	000780	000622	000493	000389	000305	000238	000185	111
112	001233	000996	000799	000638	000507	000401	000315	000246	112
113	001550	001260	001019	000819	000655	000521	000413	000325	113
114	001930	001580	001287	001042	000839	000672	000536	000425	114
115	002383	001965	001611	001314	001065	000859	000689	000550	115
116	002918	002423	002000	001642	001341	001089	000879	000707	116
117	003541	002961	002462	002035	001673	001368	001112	000900	117
118	004261	003588	003004	002501	002070	001704	001395	001136	118
119	005085	004312	003635	003047	002540	002105	001735	001423	119
120	006017	005138	004362	003682	003090	002579	002140	001766	120
121	007061	006073	005191	004412	003728	003133	002618	002175	121
122	008219	007118	006127	005244	004462	003775	003175	002656	122
123	009489	008275	007174	006182	005296	004511	003821	003218	123
124	010866	009543	008331	007229	006236	005348	004560	003867	124
125	012344	010917	009597	008385	007283	006289	005400	004609	125
126	013911	012390	010968	009650	008440	007338	006342	005451	126
127	015554	013951	012436	011018	009702	008493	007391	006395	127
128	017256	015586	013990	012401	011067	009754	008546	007444	128
129	018995	017278	015617	014029	012525	011115	009805	008598	129
130	020748	019006	017299	015648	014066	012568	011162	009855	130
131	022490	020747	019016	017320	015677	014103	012611	011209	131
132	024194	022475	020745	019026	017340	015706	014139	012652	132
133	025831	024165	022460	020742	019035	017359	015734	014174	133
134	027373	025788	024136	022445	020739	019043	017378	015761	134
135	028793	027317	025746	024107	022429	020736	019051	017396	135
136	030063	028723	027260	025703	024078	022413	020732	019058	136
137	031160	029980	028653	027204	025660	024049	022397	020728	137
138	032063	031067	029899	028584	027148	025617	024020	022380	138
139	032755	031961	030974	029817	028515	027092	025575	023990	139
140	033223	032646	031859	030882	029737	028446	027036	025532	140
141	033459	033109	032537	031758	030791	029657	028378	026981	141
142	033459	033342	032995	032429	031659	030701	029578	028311	142
143	033225	033342	033226	032883	032323	031560	030612	029499	143
144	032763	033110	033226	033111	032772	032217	031462	030523	144
145	032086	032654	032997	033111	032998	032662	032113	031365	145
146	031206	031983	032545	032885	032998	032886	032553	032010	146
147	030145	031112	031881	032437	032773	032886	032774	032445	147
148	028923	030061	031019	031780	032330	032663	032774	032664	148
149	027564	028851	029978	030926	031680	032225	032554	032664	149
150	026094	027504	028779	029896	030835	031580	032120	032447	150
151	024539	026047	027445	028708	029814	030744	031482	032017	151
152	022924	024505	026000	027386	028637	029733	030654	031385	152
153	021276	022903	024471	025954	027327	028567	029652	030564	153
154	019618	021267	022882	024437	025907	027268	028497	029572	154
155	017973	019621	021258	022860	024403	025861	027210	028427	155
156	016360	017986	019623	021248	022839	024369	025814	027152	156
157	014797	016382	017998	019624	021238	022817	024335	025768	157
158	013298	014827	016403	018010	019625	021228	022794	024300	158
159	011877	013335	014856	016424	018021	019626	021217	022772	159
160	010541	011918	013370	014884	016444	018031	019626	021206	160
161	009297	010585	011958	013405	014912	016463	018041	019626	161
162	008149	009344	010630	011998	013439	014939	016482	018051	162
163	007099	008197	009391	010673	012037	013473	014965	016501	163
164	006147	007148	008245	009437	010716	012076	013505	014991	164
165	005290	006195	007196	008293	009482	010759	012114	013538	165
166	004525	005336	006242	007244	008340	009527	010800	012151	166
167	003848	004570	005383	006290	007291	008386	009572	010842	167
168	003252	003890	004614	005428	006336	007338	008432	009615	168
169	002733	003291	003931	004658	005474	006383	007384	008478	169
170	002283	002768	003330	003973	004701	005519	006429	007430	170
171	001895	002315	002804	003369	004014	004745	005564	006474	171
172	001565	001925	002348	002840	003407	004055	004788	005609	172
173	001284	001591	001954	002380	002875	003446	004096	004831	173
174	001048	001308	001617	001983	002413	002911	003484	004136	174
175	000851	001068	001331	001643	002013	002445	002946	003522	175

~~SECRET~~



TABLE I

X	A=142	A=143	A=144	A=145	A=146	A=147	A=148	A=149	X
176	•000686	•000868	•001089	•001354	•001670	•002042	•002478	•002982	176
177	•000551	•000701	•000886	•001109	•001377	•001696	•002072	•002510	177
178	•000439	•000563	•000717	•000904	•001130	•001401	•001722	•002101	178
179	•000348	•000450	•000576	•000732	•000921	•001150	•001424	•001749	179
180	•000275	•000358	•000461	•000590	•000747	•000939	•001171	•001448	180
181	•000216	•000283	•000367	•000472	•000603	•000763	•000957	•001192	181
182	•000168	•000222	•000290	•000376	•000484	•000616	•000779	•000976	182
183	•000131	•000173	•000228	•000298	•000386	•000495	•000630	•000794	183
184	•000101	•000135	•000179	•000235	•000306	•000395	•000506	•000643	184
185	•000077	•000104	•000139	•000184	•000242	•000314	•000405	•000518	185
186	•000059	•000080	•000108	•000144	•000190	•000248	•000322	•000415	186
187	•000045	•000061	•000083	•000111	•000148	•000195	•000255	•000331	187
188	•000034	•000047	•000064	•000086	•000115	•000153	•000201	•000262	188
189	•000025	•000035	•000048	•000066	•000089	•000119	•000157	•000207	189
190	•000019	•000027	•000037	•000050	•000068	•000092	•000123	•000162	190
191	•000014	•000020	•000028	•000038	•000052	•000071	•000095	•000126	191
192	•000010	•000015	•000021	•000029	•000040	•000054	•000073	•000098	192
193	•000008	•000011	•000015	•000022	•000030	•000041	•000056	•000076	193
194	•000006	•000008	•000011	•000016	•000023	•000031	•000043	•000058	194
195	•000004	•000006	•000008	•000012	•000017	•000024	•000032	•000044	195
196	•000003	•000004	•000006	•000009	•000013	•000018	•000025	•000034	196
197	•000002	•000003	•000005	•000007	•000009	•000013	•000018	•000026	197
198	•000002	•000002	•000003	•000005	•000007	•000010	•000014	•000019	198
199	•000001	•000002	•000002	•000003	•000005	•000007	•000010	•000014	199
200	•000001	•000001	•000002	•000003	•000004	•000005	•000008	•000011	200
201	•000001	•000001	•000001	•000002	•000003	•000004	•000006	•000008	201
202		•000001	•000001	•000001	•000002	•000003	•000004	•000006	202
203			•000001	•000001	•000001	•000002	•000003	•000004	203
204				•000001	•000001	•000001	•000002	•000003	204
205					•000001	•000001	•000002	•000002	205
206						•000001	•000001	•000002	206
207						•000001	•000001	•000001	207
208							•000001	•000001	208
209							•000001	•000001	209
X	A=150	A=151	A=152	A=153	A=154	A=155	A=156	A=157	X
96	•000001								96
97	•000001	•000001							97
98	•000001	•000001	•000001						98
99	•000002	•000001	•000001	•000001	•000001				99
100	•000003	•000002	•000002	•000001	•000001	•000001			100
101	•000005	•000003	•000002	•000002	•000001	•000001	•000001		101
102	•000007	•000005	•000004	•000003	•000002	•000001	•000001	•000001	102
103	•000010	•000007	•000005	•000004	•000003	•000002	•000001	•000001	103
104	•000014	•000011	•000008	•000006	•000004	•000003	•000002	•000001	104
105	•000020	•000015	•000011	•000008	•000006	•000004	•000003	•000002	105
106	•000029	•000022	•000016	•000012	•000009	•000006	•000005	•000003	106
107	•000041	•000030	•000023	•000017	•000012	•000009	•000007	•000005	107
108	•000056	•000043	•000032	•000024	•000018	•000013	•000010	•000007	108
109	•000078	•000059	•000045	•000033	•000025	•000019	•000014	•000010	109
110	•000106	•000081	•000062	•000047	•000035	•000026	•000020	•000015	110
111	•000143	•000110	•000084	•000064	•000049	•000037	•000028	•000021	111
112	•000192	•000148	•000114	•000088	•000067	•000051	•000038	•000029	112
113	•000254	•000198	•000154	•000119	•000091	•000070	•000053	•000040	113
114	•000335	•000263	•000205	•000159	•000123	•000095	•000073	•000055	114
115	•000437	•000345	•000271	•000212	•000165	•000128	•000098	•000076	115
116	•000565	•000449	•000355	•000280	•000219	•000171	•000132	•000102	116
117	•000724	•000579	•000461	•000366	•000288	•000226	•000177	•000137	117
118	•000920	•000742	•000594	•000474	•000376	•000297	•000233	•000182	118
119	•001160	•000941	•000759	•000610	•000487	•000387	•000306	•000241	119
120	•001450	•001184	•000962	•000777	•000625	•000500	•000398	•000315	120
121	•001798	•001478	•001208	•000983	•000795	•000640	•000513	•000409	121
122	•002210	•001829	•001505	•001232	•001004	•000813	•000656	•000526	122
123	•002695	•002245	•001860	•001533	•001257	•001025	•000832	•000671	123
124	•003260	•002734	•002280	•001892	•001561	•001281	•001046	•000850	124
125	•003913	•003303	•002773	•002315	•001923	•001589	•001306	•001068	125
126	•004658	•003958	•003345	•002811	•002350	•001954	•001617	•001330	126

TABLE I

X	A=150	A=151	A=152	A=153	A=154	A=155	A=156	A=157	X
127	•005501	•004706	•004003	•003387	•002850	•002385	•001986	•001645	127
128	•005447	•005552	•004754	•004048	•003429	•002888	•002420	•002017	128
129	•007496	•006498	•005602	•004802	•004093	•003471	•002927	•002455	129
130	•008650	•007548	•006550	•005651	•004849	•004138	•003512	•002965	130
131	•009904	•008701	•007599	•006600	•005700	•004896	•004182	•003553	131
132	•011255	•009953	•008751	•007650	•006650	•005749	•004943	•004227	132
133	•012693	•011300	•010001	•008801	•007700	•006700	•005798	•004989	133
134	•014209	•012734	•011344	•010048	•008850	•007750	•006749	•005846	134
135	•015788	•014243	•012773	•011388	•010095	•008898	•007799	•006798	135
136	•017413	•015814	•014276	•012812	•011431	•010141	•008946	•007848	136
137	•019065	•017430	•015839	•014308	•012850	•011474	•010187	•008994	137
138	•020723	•019071	•017446	•015863	•014340	•012887	•011516	•010232	138
139	•022363	•020718	•019077	•017461	•015887	•014371	•012924	•011557	139
140	•023960	•022346	•020712	•019082	•017476	•015910	•014401	•012960	140
141	•025490	•023931	•022328	•020707	•019087	•017490	•015933	•014431	141
142	•026926	•025447	•023901	•022311	•020700	•019091	•017504	•015955	142
143	•028244	•026871	•025405	•023871	•022293	•020694	•019095	•017517	143
144	•029421	•028177	•026816	•025363	•023841	•022274	•020686	•019099	144
145	•030435	•029343	•028111	•026762	•025320	•023810	•022256	•020679	145
146	•031269	•030348	•029266	•028045	•026708	•025278	•023780	•022237	146
147	•031907	•031174	•030262	•029190	•027980	•026654	•025236	•023750	147
148	•032338	•031806	•031079	•030176	•029114	•027915	•026600	•025194	148
149	•032555	•032233	•031705	•030986	•030091	•029039	•027850	•026547	149
150	•032555	•032448	•032128	•031606	•030893	•030007	•028964	•027786	150
151	•032340	•032448	•032341	•032024	•031507	•030801	•029923	•028890	151
152	•031914	•032234	•032341	•032235	•031922	•031409	•030710	•029840	152
153	•031289	•031813	•032129	•032235	•032130	•031820	•031313	•030620	153
154	•030476	•031193	•031712	•032026	•032130	•032027	•031719	•031217	154
155	•029493	•030388	•031098	•031612	•031923	•032027	•031924	•031619	155
156	•028358	•029414	•030301	•031005	•031514	•031821	•031924	•031822	156
157	•027094	•028290	•029336	•030215	•030912	•031416	•031721	•031822	157
158	•025722	•027037	•028222	•029258	•030129	•030819	•031319	•031621	158
159	•024266	•025676	•026979	•028154	•029182	•030044	•030728	•031223	159
160	•022750	•024232	•025630	•026923	•028087	•029105	•029960	•030638	160
161	•021195	•022727	•024198	•025585	•026866	•028021	•029029	•029876	161
162	•019625	•021184	•022704	•024163	•025539	•026810	•027954	•028954	162
163	•018060	•019624	•021172	•022681	•024129	•025494	•026754	•027888	163
164	•016518	•018069	•019623	•021160	•022658	•024095	•025449	•026698	164
165	•015017	•016535	•018077	•019621	•021147	•022635	•024061	•025404	165
166	•013569	•015041	•016552	•018084	•019619	•021135	•022611	•024026	166
167	•012188	•013600	•015065	•016568	•018091	•019616	•021122	•022588	167
168	•010882	•012224	•013631	•015089	•016584	•018098	•019613	•021109	168
169	•009659	•010922	•012259	•013660	•015112	•016599	•018104	•019610	169
170	•008522	•009701	•010961	•012294	•013690	•015134	•016613	•018110	170
171	•007476	•008567	•009743	•011000	•012329	•013718	•015156	•016628	171
172	•006520	•007521	•008611	•009785	•011038	•012362	•013746	•015177	172
173	•005653	•006564	•007565	•008654	•009826	•011076	•012395	•013774	173
174	•004873	•005697	•006609	•007609	•008697	•009867	•011113	•012428	174
175	•004177	•004915	•005740	•006653	•007653	•008739	•009907	•011150	175
176	•003560	•004217	•004957	•005783	•006696	•007696	•008781	•009946	176
177	•003017	•003598	•004257	•004999	•005826	•006740	•007739	•008822	177
178	•002542	•003052	•003635	•004297	•005041	•005869	•006783	•007781	178
179	•002130	•002575	•003087	•003673	•004337	•005082	•005911	•006825	179
180	•001775	•002160	•002607	•003122	•003710	•004376	•005123	•005953	180
181	•001471	•001802	•002189	•002639	•003157	•003747	•004415	•005164	181
182	•001213	•001495	•001828	•002219	•002671	•003192	•003785	•004454	182
183	•000994	•001233	•001519	•001855	•002248	•002703	•003226	•003821	183
184	•000810	•001012	•001254	•001542	•001881	•002277	•002735	•003261	184
185	•000657	•000826	•001031	•001276	•001566	•001908	•002306	•002767	185
186	•000530	•000671	•000842	•001049	•001297	•001590	•001934	•002336	186
187	•000425	•000542	•000685	•000858	•001068	•001318	•001614	•001961	187
188	•000339	•000435	•000554	•000699	•000875	•001087	•001339	•001638	188
189	•000269	•000348	•000445	•000566	•000713	•000891	•001105	•001360	189
190	•000212	•000276	•000356	•000455	•000578	•000727	•000907	•001124	190
191	•000167	•000218	•000283	•000365	•000466	•000590	•000741	•000924	191
192	•000130	•000172	•000224	•000291	•000374	•000476	•000602	•000756	192
193	•000101	•000134	•000177	•000230	•000298	•000382	•000487	•000615	193
194	•000078	•000105	•000138	•000182	•000237	•000306	•000391	•000497	194

TABLE I

X	A=150	A=151	A=152	A=153	A=154	A=155	A=156	A=157	X
195	•000060	•000081	•000108	•000143	•000187	•000243	•000313	•000400	195
196	•000046	•000062	•000084	•000111	•000147	•000192	•000249	•000321	196
197	•000035	•000048	•000065	•000086	•000115	•000151	•000197	•000256	197
198	•000027	•000036	•000050	•000067	•000089	•000118	•000155	•000203	198
199	•000020	•000028	•000038	•000051	•000069	•000092	•000122	•000160	199
200	•000015	•000021	•000029	•000039	•000053	•000071	•000095	•000126	200
201	•000011	•000016	•000022	•000030	•000041	•000055	•000074	•000098	201
202	•000008	•000012	•000016	•000023	•000031	•000042	•000057	•000076	202
203	•000006	•000009	•000012	•000017	•000024	•000032	•000044	•000059	203
204	•000005	•000006	•000009	•000013	•000018	•000025	•000033	•000045	204
205	•000003	•000005	•000007	•000010	•000013	•000019	•000025	•000035	205
206	•000002	•000003	•000005	•000007	•000010	•000014	•000019	•000026	206
207	•000002	•000003	•000004	•000005	•000007	•000010	•000015	•000020	207
208	•000001	•000002	•000003	•000004	•000005	•000008	•000011	•000015	208
209	•000001	•000001	•000002	•000003	•000004	•000006	•000008	•000011	209
210	•000001	•000001	•000001	•000002	•000003	•000004	•000006	•000008	210
211		•000001	•000001	•000001	•000002	•000003	•000004	•000006	211
212			•000001	•000001	•000002	•000002	•000003	•000005	212
213			•000001	•000001	•000001	•000002	•000002	•000003	213
214				•000001	•000001	•000001	•000002	•000003	214
215					•000001	•000001	•000001	•000002	215
216						•000001	•000001	•000001	216
217							•000001	•000001	217
218								•000001	218
X	A=158	A=159	A=160	A=161	A=162	A=163	A=164	A=165	X
103	•000001								103
104	•000001	•000001	•000001						104
105	•000002	•000001	•000001	•000001					105
106	•000002	•000002	•000001	•000001	•000001				106
107	•000004	•000003	•000002	•000001	•000001	•000001			107
108	•000005	•000004	•000003	•000002	•000001	•000001	•000001	•000001	108
109	•000007	•000005	•000004	•000003	•000002	•000002	•000001	•000001	109
110	•000011	•000008	•000006	•000004	•000003	•000002	•000002	•000001	110
111	•000015	•000011	•000008	•000006	•000005	•000003	•000002	•000002	111
112	•000022	•000016	•000012	•000009	•000007	•000005	•000003	•000003	112
113	•000030	•000023	•000017	•000013	•000009	•000007	•000005	•000004	113
114	•000042	•000032	•000024	•000018	•000013	•000010	•000007	•000005	114
115	•000058	•000044	•000033	•000025	•000019	•000014	•000010	•000008	115
116	•000079	•000060	•000046	•000035	•000026	•000020	•000015	•000011	116
117	•000106	•000082	•000063	•000048	•000036	•000027	•000021	•000015	117
118	•000142	•000110	•000085	•000065	•000050	•000038	•000029	•000022	118
119	•000189	•000147	•000114	•000088	•000068	•000052	•000039	•000030	119
120	•000248	•000195	•000152	•000118	•000091	•000070	•000054	•000041	120
121	•000324	•000256	•000201	•000157	•000122	•000095	•000073	•000056	121
122	•000420	•000333	•000264	•000207	•000162	•000127	•000098	•000076	122
123	•000539	•000431	•000343	•000271	•000214	•000168	•000131	•000102	123
124	•000687	•000553	•000442	•000352	•000279	•000220	•000173	•000135	124
125	•000869	•000703	•000566	•000454	•000362	•000288	•000227	•000179	125
126	•001089	•000887	•000719	•000580	•000466	•000372	•000296	•000234	126
127	•001355	•001111	•000906	•000735	•000594	•000477	•000382	•000304	127
128	•001673	•001380	•001133	•000925	•000752	•000608	•000489	•000392	128
129	•002049	•001701	•001405	•001154	•000944	•000768	•000622	•000501	129
130	•002490	•002080	•001729	•001430	•001176	•000963	•000785	•000636	130
131	•003003	•002525	•002112	•001757	•001455	•001198	•000982	•000801	131
132	•003595	•003041	•002560	•002143	•001785	•001480	•001221	•001002	132
133	•004270	•003636	•003079	•002594	•002175	•001814	•001505	•001243	133
134	•005035	•004314	•003677	•003117	•002629	•002206	•001842	•001530	134
135	•005893	•005081	•004358	•003718	•003155	•002664	•002238	•001870	135
136	•006846	•005940	•005127	•004401	•003758	•003193	•002698	•002269	136
137	•007896	•006894	•005987	•005172	•004444	•003798	•003230	•002733	137
138	•009040	•007944	•006942	•006034	•005217	•004487	•003839	•003268	138
139	•010276	•009086	•007991	•006989	•006080	•005261	•004529	•003879	139
140	•011597	•010320	•009132	•008037	•007035	•006126	•005306	•004571	140
141	•012995	•011637	•010363	•009177	•008083	•007081	•006171	•005350	141
142	•014460	•013030	•011676	•010405	•009222	•008129	•007127	•006216	142
143	•015977	•014488	•013064	•011715	•010447	•009266	•008174	•007172	143

TABLE I

X	A=158	A=159	A=160	A=161	A=162	A=163	A=164	A=165	X
144	•017530	•015997	•014516	•013098	•011753	•010488	•009309	•008218	144
145	•019101	•017542	•016018	•014543	•013131	•011790	•010529	•009352	145
146	•020671	•019104	•017553	•016037	•014570	•013163	•011827	•010569	146
147	•022218	•020663	•019106	•017565	•016056	•014596	•013195	•011863	147
148	•023719	•022199	•020655	•019107	•017575	•016075	•014621	•013226	148
149	•025152	•023689	•022180	•020646	•019109	•017585	•016097	•014646	149
150	•026494	•025110	•023658	•022160	•020637	•019109	•017595	•016110	150
151	•027722	•026441	•025069	•023628	•022141	•020628	•019110	•017604	151
152	•028816	•027658	•026388	•025027	•023597	•022121	•020618	•019110	152
153	•029758	•028743	•027595	•026336	•024985	•023567	•022101	•020609	153
154	•030551	•029676	•028670	•027533	•026283	•024944	•023536	•022081	154
155	•031122	•030442	•029595	•028598	•027470	•026231	•024903	•023505	155
156	•031521	•031027	•030354	•029515	•028527	•027408	•026180	•024861	156
157	•031721	•031423	•030934	•030267	•029435	•028456	•027347	•026128	157
158	•031721	•031622	•031326	•030842	•030181	•029356	•028385	•027286	158
159	•031522	•031622	•031523	•031230	•030750	•030095	•029278	•028315	159
160	•031128	•031424	•031523	•031425	•031134	•030659	•030010	•029200	160
161	•030548	•031034	•031327	•031425	•031328	•031040	•030569	•029926	161
162	•029794	•030459	•030940	•031231	•031328	•031232	•030946	•030480	162
163	•028880	•029711	•030371	•030848	•031136	•031232	•031136	•030854	163
164	•027823	•028806	•029630	•030283	•030756	•031041	•031136	•031042	164
165	•026643	•027758	•028732	•029549	•030197	•030665	•030948	•031042	165
166	•025359	•026588	•027694	•028659	•029469	•030111	•030575	•030855	166
167	•023992	•025314	•026533	•027629	•028587	•029390	•030026	•030485	167
168	•022564	•023958	•025269	•026478	•027566	•028515	•029311	•029941	168
169	•021095	•022540	•023924	•025225	•026424	•027502	•028443	•029232	169
170	•019606	•021082	•022516	•023889	•025180	•026370	•027440	•028373	170
171	•018116	•019602	•021068	•022492	•023855	•025136	•026316	•027377	171
172	•016641	•018121	•019598	•021054	•022468	•023821	•025092	•026263	172
173	•015198	•016654	•018125	•019594	•021040	•022444	•023787	•025048	173
174	•013801	•015219	•016667	•018130	•019589	•021025	•022420	•023753	174
175	•012460	•013827	•015238	•016679	•018133	•019583	•021011	•022395	175
176	•011186	•012492	•013853	•015258	•016691	•018137	•019578	•020996	176
177	•009985	•011221	•012523	•013879	•015277	•016702	•018140	•019572	177
178	•008863	•010023	•011256	•012553	•013903	•015295	•016713	•018143	178
179	•007823	•008904	•010061	•011291	•012583	•013928	•015313	•016724	179
180	•006867	•007865	•008944	•010099	•011325	•012612	•013952	•015330	180
181	•005995	•006909	•008093	•009983	•010136	•011358	•012641	•013975	181
182	•005204	•006036	•006950	•007947	•009022	•010172	•011391	•012670	182
183	•004493	•005244	•006077	•006991	•007987	•009061	•010208	•011424	183
184	•003858	•004532	•005284	•006117	•007032	•008027	•009099	•010244	184
185	•003295	•003895	•004570	•005324	•006158	•007072	•008066	•009136	185
186	•002799	•003329	•003931	•004608	•005363	•006198	•007112	•008105	186
187	•002365	•002831	•003364	•003967	•004646	•005402	•006237	•007151	187
188	•001988	•002394	•002863	•003398	•004004	•004684	•005441	•006277	188
189	•001662	•002014	•002423	•002894	•003432	•004039	•004721	•005479	189
190	•001382	•001686	•002041	•002453	•002926	•003465	•004075	•004758	190
191	•001143	•001403	•001710	•002067	•002482	•002957	•003499	•004111	191
192	•000941	•001162	•001425	•001734	•002094	•002511	•002989	•003533	192
193	•000770	•000957	•001181	•001446	•001758	•002120	•002540	•003020	193
194	•000627	•000785	•000974	•001200	•001468	•001782	•002147	•002569	194
195	•000508	•000404	•000799	•000991	•001219	•001489	•001806	•002173	195
196	•000410	•000519	•000652	•000814	•001008	•001238	•001511	•001830	196
197	•000329	•000419	•000530	•000665	•000829	•001025	•001258	•001533	197
198	•000262	•000336	•000428	•000541	•000678	•000844	•001042	•001277	198
199	•000208	•000269	•000344	•000438	•000552	•000691	•000859	•001059	199
200	•000164	•000214	•000275	•000352	•000447	•000563	•000704	•000874	200
201	•000129	•000169	•000219	•000282	•000360	•000457	•000574	•000717	201
202	•000101	•000133	•000174	•000225	•000289	•000369	•000466	•000586	202
203	•000079	•000104	•000137	•000178	•000231	•000296	•000377	•000476	203
204	•000061	•000081	•000107	•000141	•000183	•000236	•000303	•000385	204
205	•000047	•000063	•000084	•000111	•000145	•000188	•000242	•000310	205
206	•000036	•000049	•000065	•000086	•000114	•000149	•000193	•000248	206
207	•000027	•000037	•000050	•000067	•000089	•000117	•000153	•000198	207
208	•000021	•000029	•000039	•000052	•000069	•000092	•000120	•000157	208
209	•000016	•000022	•000030	•000040	•000054	•000072	•000095	•000124	209
210	•000012	•000016	•000023	•000031	•000041	•000056	•000074	•000097	210

TABLE I

X	A=158	A=159	A=160	A=161	A=162	A=163	A=164	A=165	X
211	•000009	•000012	•000017	•000023	•000032	•000043	•000057	•000076	211
212	•000007	•000009	•000013	•000018	•000024	•000033	•000044	•000059	212
213	•000005	•000007	•000010	•000013	•000019	•000025	•000034	•000046	213
214	•000004	•000005	•000007	•000010	•000014	•000019	•000026	•000035	214
215	•000003	•000004	•000005	•000008	•000011	•000015	•000020	•000027	215
216	•000002	•000003	•000004	•000006	•000008	•000011	•000015	•000021	216
217	•000001	•000002	•000003	•000004	•000006	•000008	•000011	•000016	217
218	•000001	•000001	•000002	•000003	•000004	•000006	•000009	•000012	218
219	•000001	•000001	•000002	•000002	•000003	•000005	•000006	•000009	219
220	•000001	•000001	•000001	•000002	•000002	•000003	•000005	•000007	220
221	•000001	•000001	•000001	•000001	•000002	•000003	•000004	•000005	221
222			•000001	•000001	•000001	•000002	•000003	•000004	222
223				•000001	•000001	•000001	•000002	•000003	223
224					•000001	•000001	•000001	•000002	224
225						•000001	•000001	•000001	225
226						•000001	•000001	•000001	226
227							•000001	•000001	227
228								•000001	228
X	A=166	A=167	A=168	A=169	A=170	A=171	A=172	A=173	X
109	•000001								109
110	•000001	•000001							110
111	•000001	•000001	•000001						111
112	•000002	•000001	•000001	•000001					112
113	•000003	•000002	•000001	•000001	•000001	•000001			113
114	•000004	•000003	•000002	•000002	•000001	•000001	•000001		114
115	•000006	•000004	•000003	•000002	•000002	•000001	•000001	•000001	115
116	•000008	•000006	•000004	•000003	•000002	•000002	•000001	•000001	116
117	•000012	•000009	•000006	•000005	•000003	•000002	•000002	•000001	117
118	•000016	•000012	•000009	•000007	•000005	•000004	•000003	•000002	118
119	•000023	•000017	•000013	•000009	•000007	•000005	•000004	•000003	119
120	•000031	•000024	•000018	•000013	•000010	•000007	•000005	•000004	120
121	•000043	•000033	•000025	•000019	•000014	•000010	•000008	•000006	121
122	•000058	•000045	•000034	•000026	•000020	•000015	•000011	•000008	122
123	•000079	•000061	•000046	•000035	•000027	•000020	•000015	•000012	123
124	•000105	•000082	•000063	•000048	•000037	•000028	•000021	•000016	124
125	•000140	•000109	•000085	•000065	•000050	•000038	•000029	•000022	125
126	•000184	•000145	•000113	•000088	•000068	•000052	•000040	•000031	126
127	•000241	•000190	•000149	•000117	•000091	•000070	•000054	•000042	127
128	•000312	•000248	•000196	•000154	•000121	•000094	•000073	•000056	128
129	•000402	•000321	•000255	•000202	•000159	•000125	•000097	•000076	129
130	•000513	•000412	•000330	•000262	•000208	•000164	•000129	•000101	130
131	•000651	•000526	•000423	•000338	•000270	•000214	•000169	•000133	131
132	•000818	•000665	•000538	•000433	•000347	•000277	•000220	•000174	132
133	•001021	•000835	•000680	•000551	•000444	•000356	•000285	•000226	133
134	•001265	•001041	•000852	•000694	•000563	•000455	•000365	•000292	134
135	•001556	•001287	•001060	•000869	•000709	•000576	•000465	•000374	135
136	•001899	•001581	•001310	•001080	•000886	•000724	•000589	•000476	136
137	•002301	•001927	•001606	•001332	•001100	•000904	•000739	•000602	137
138	•002767	•002332	•001955	•001632	•001355	•001120	•000921	•000754	138
139	•003305	•002802	•002363	•001984	•001657	•001378	•001140	•000939	139
140	•003919	•003342	•002836	•002395	•002012	•001683	•001400	•001160	140
141	•004613	•003958	•003379	•002870	•002426	•002041	•001708	•001423	141
142	•005393	•004655	•003998	•003416	•002904	•002457	•002069	•001734	142
143	•006261	•005437	•004697	•004037	•003453	•002939	•002489	•002097	143
144	•007217	•006305	•005480	•004738	•004076	•003490	•002973	•002520	144
145	•008262	•007261	•006349	•005522	•004779	•004115	•003526	•003006	145
146	•009394	•008306	•007305	•006392	•005565	•004820	•004154	•003562	146
147	•010608	•009436	•008349	•007349	•006435	•005607	•004860	•004193	147
148	•011899	•010647	•009477	•008392	•007392	•006478	•005649	•004901	148
149	•013256	•011934	•010686	•009518	•008434	•007435	•006521	•005690	149
150	•014670	•013286	•011968	•010724	•009558	•008476	•007477	•006563	150
151	•016127	•014694	•013316	•012002	•010761	•009598	•008517	•007519	151
152	•017613	•016144	•014717	•013344	•012035	•010798	•009637	•008558	152
153	•019109	•017621	•016160	•014740	•013373	•012068	•010834	•009676	153
154	•020598	•019109	•017629	•016176	•014762	•013400	•012101	•010870	154
155	•022060	•020588	•019108	•017637	•016191	•014784	•013428	•012132	155

TABLE I

X	A=166	A=167	A=168	A=169	A=170	A=171	A=172	A=173	X
156	•023474	•022040	•020577	•019106	•017644	•016205	•014805	•013454	156
157	•024820	•023444	•022019	•020567	•019105	•017650	•016219	•014826	157
158	•026077	•024779	•023413	•021998	•020556	•019102	•017656	•016233	158
159	•027225	•026026	•024738	•023382	•021978	•020544	•019100	•017662	159
160	•028246	•027164	•025975	•024697	•023351	•021957	•020533	•019097	160
161	•029123	•028177	•027104	•025924	•024657	•023320	•021935	•020521	161
162	•029842	•029046	•028108	•027045	•025874	•024616	•023290	•021914	162
163	•030391	•029759	•028970	•028040	•026985	•025824	•024575	•023259	163
164	•030762	•030304	•029677	•028895	•027973	•026926	•025774	•024535	164
165	•030948	•030671	•030217	•029596	•028820	•027905	•026868	•025725	165
166	•030948	•030856	•030581	•030130	•029515	•028746	•027839	•026809	166
167	•030763	•030856	•030764	•030491	•030045	•029435	•028672	•027773	167
168	•030397	•030672	•030764	•030673	•030403	•029960	•029355	•028599	168
169	•029857	•030309	•030582	•030673	•030582	•030315	•029876	•029276	169
170	•029155	•029774	•030222	•030492	•030582	•030493	•030228	•029793	170
171	•028302	•029078	•029692	•030136	•030404	•030493	•030404	•030141	171
172	•027315	•028232	•029001	•029610	•030005	•030316	•030404	•030316	172
173	•026210	•027253	•028163	•028925	•029529	•029965	•030229	•030316	173
174	•025005	•026157	•027192	•028094	•028850	•029449	•029881	•030142	174
175	•023719	•024961	•026104	•027131	•028026	•028775	•029369	•029798	175
176	•022371	•023685	•024918	•026052	•027070	•027958	•028701	•029290	176
177	•020981	•022365	•022347	•023651	•024874	•026000	•027891	•028628	177
178	•019566	•020966	•022322	•023617	•024831	•025948	•026950	•027824	178
179	•018145	•019560	•020950	•022297	•023583	•024788	•025897	•026891	179
180	•016734	•018147	•019554	•020935	•022273	•023549	•024746	•025845	180
181	•015347	•016744	•018149	•019547	•020919	•022248	•023515	•024703	181
182	•013998	•015364	•016753	•018151	•019540	•020903	•022223	•023481	182
183	•012698	•014020	•015380	•016762	•018152	•019533	•020887	•022198	183
184	•011455	•012725	•014042	•015396	•016771	•018153	•019525	•020871	184
185	•010279	•011487	•012752	•014064	•015411	•016779	•018153	•019517	185
186	•009174	•010314	•011518	•012779	•014085	•015426	•016787	•018153	186
187	•008144	•009211	•010348	•011549	•012805	•014106	•015440	•016794	187
188	•007191	•008182	•009247	•010381	•011579	•012830	•014126	•015454	188
189	•006316	•007229	•008219	•009283	•010415	•011608	•012855	•014146	189
190	•005518	•006354	•007268	•008257	•009318	•010448	•011638	•012880	190
191	•004796	•005556	•006393	•007306	•008294	•009354	•010480	•011666	191
192	•004146	•004832	•005594	•006431	•007344	•008331	•009388	•010512	192
193	•003566	•004181	•004869	•005631	•006468	•007381	•008367	•009423	193
194	•003051	•003599	•004216	•004905	•005668	•006506	•007418	•008403	194
195	•002598	•003083	•003633	•004251	•004941	•005705	•006543	•007455	195
196	•002200	•002626	•003114	•003666	•004286	•004977	•005742	•006580	196
197	•001854	•002227	•002655	•003145	•003699	•004321	•005013	•005778	197
198	•001554	•001878	•002253	•002684	•003176	•003731	•004355	•005049	198
199	•001296	•001902	•002279	•002713	•003206	•003764	•004376	•004389	199
200	•001076	•001316	•001598	•001926	•002306	•002741	•003237	•003797	200
201	•000889	•001093	•001335	•001619	•001950	•002332	•002770	•003268	201
202	•000730	•000904	•001111	•001355	•001641	•001974	•002359	•002799	202
203	•000597	•000744	•000919	•001128	•001374	•001663	•001998	•002385	203
204	•000486	•000609	•000757	•000934	•001145	•001394	•001685	•002023	204
205	•000394	•000496	•000620	•000770	•000950	•001163	•001414	•001707	205
206	•000317	•000402	•000506	•000632	•000784	•000965	•001180	•001433	206
207	•000254	•000324	•000411	•000516	•000644	•000797	•000981	•001198	207
208	•000203	•000260	•000332	•000419	•000526	•000656	•000811	•000996	208
209	•000161	•000208	•000267	•000339	•000428	•000536	•000667	•000825	209
210	•000127	•000165	•000213	•000273	•000346	•000437	•000547	•000679	210
211	•000100	•000131	•000170	•000218	•000279	•000354	•000446	•000557	211
212	•000078	•000103	•000135	•000174	•000224	•000286	•000362	•000455	212
213	•000061	•000081	•000106	•000138	•000179	•000229	•000292	•000369	213
214	•000047	•000063	•000083	•000109	•000142	•000183	•000235	•000298	214
215	•000037	•000049	•000065	•000086	•000112	•000146	•000188	•000240	215
216	•000028	•000038	•000051	•000067	•000088	•000115	•000149	•000192	216
217	•000022	•000029	•000039	•000052	•000069	•000091	•000118	•000153	217
218	•000016	•000022	•000030	•000041	•000054	•000071	•000093	•000122	218
219	•000012	•000017	•000023	•000031	•000042	•000056	•000073	•000096	219
220	•000009	•000013	•000018	•000024	•000032	•000043	•000057	•000076	220
221	•000007	•000010	•000013	•000018	•000025	•000033	•000045	•000059	221
222	•000005	•000007	•000010	•000014	•000019	•000026	•000035	•000046	222
223	•000004	•000005	•000008	•000011	•000015	•000020	•000027	•000036	223

TABLE I

X	A=166	A=167	A=168	A=169	A=170	A=171	A=172	A=173	X
224	•000003	•000004	•000006	•000008	•000011	•000015	•000020	•000028	224
225	•000002	•000003	•000004	•000006	•000008	•000011	•000016	•000021	225
226	•000002	•000002	•000003	•000004	•000006	•000009	•000012	•000016	226
227	•000001	•000002	•000002	•000003	•000005	•000007	•000009	•000012	227
228	•000001	•000001	•000002	•000002	•000003	•000005	•000007	•000009	228
229	•000001	•000001	•000001	•000002	•000003	•000004	•000005	•000007	229
230		•000001	•000001	•000001	•000002	•000003	•000004	•000005	230
231			•000001	•000001	•000001	•000002	•000003	•000004	231
232				•000001	•000001	•000001	•000002	•000003	232
233				•000001	•000001	•000001	•000002	•000002	233
234					•000001	•000001	•000001	•000002	234
235						•000001	•000001	•000001	235
236							•000001	•000001	236
237								•000001	237

X	A=174	A=175	A=176	A=177	A=178	A=179	A=180	A=181	X
116	•000001								116
117	•000001	•000001							117
118	•000001	•000001	•000001	•000001					118
119	•000002	•000001	•000001	•000001	•000001				119
120	•000003	•000002	•000002	•000001	•000001	•000001			120
121	•000004	•000003	•000002	•000002	•000001	•000001	•000001		121
122	•000006	•000005	•000003	•000002	•000002	•000001	•000001	•000001	122
123	•000009	•000006	•000005	•000004	•000003	•000002	•000001	•000001	123
124	•000012	•000009	•000007	•000005	•000004	•000003	•000002	•000001	124
125	•000017	•000013	•000010	•000007	•000005	•000004	•000003	•000002	125
126	•000023	•000018	•000013	•000010	•000007	•000006	•000004	•000003	126
127	•000032	•000024	•000018	•000014	•000010	•000008	•000006	•000004	127
128	•000043	•000033	•000025	•000019	•000015	•000011	•000008	•000006	128
129	•000058	•000045	•000035	•000026	•000020	•000015	•000011	•000009	129
130	•000078	•000061	•000047	•000036	•000028	•000021	•000016	•000012	130
131	•000104	•000081	•000063	•000049	•000037	•000029	•000022	•000017	131
132	•000137	•000107	•000084	•000065	•000050	•000039	•000030	•000023	132
133	•000179	•000141	•000111	•000087	•000067	•000052	•000040	•000031	133
134	•000233	•000185	•000146	•000114	•000090	•000070	•000054	•000042	134
135	•000300	•000239	•000190	•000150	•000118	•000093	•000072	•000056	135
136	•000384	•000308	•000246	•000195	•000155	•000122	•000096	•000075	136
137	•000487	•000393	•000316	•000252	•000201	•000159	•000126	•000099	137
138	•000615	•000499	•000403	•000324	•000259	•000207	•000164	•000130	138
139	•000769	•000628	•000510	•000412	•000332	•000266	•000212	•000169	139
140	•000956	•000785	•000641	•000521	•000422	•000340	•000273	•000218	140
141	•001180	•000974	•000800	•000654	•000533	•000432	•000348	•000280	141
142	•001446	•001200	•000992	•000816	•000668	•000544	•000442	•000357	142
143	•001759	•001469	•001220	•001009	•000831	•000681	•000556	•000452	143
144	•002126	•001785	•001492	•001241	•001027	•000847	•000695	•000568	144
145	•002551	•002154	•001811	•001515	•001261	•001045	•000863	•000709	145
146	•003040	•002582	•002183	•001836	•001538	•001282	•001064	•000878	146
147	•003599	•003074	•002613	•002211	•001862	•001561	•001302	•001082	147
148	•004231	•003635	•003108	•002644	•002239	•001888	•001584	•001323	148
149	•004941	•004269	•003671	•003141	•002675	•002268	•001913	•001607	149
150	•005731	•004981	•004307	•003707	•003175	•002706	•002296	•001939	150
151	•006604	•005772	•005020	•004345	•003742	•003208	•002737	•002324	151
152	•007500	•006646	•005813	•005059	•004382	•003778	•003241	•002768	152
153	•008598	•007601	•006687	•005853	•005098	•004420	•003813	•003274	153
154	•009714	•008638	•007642	•006727	•005893	•005137	•004457	•003848	154
155	•010905	•009752	•008677	•007682	•006767	•005933	•005176	•004494	155
156	•012164	•010940	•009790	•008716	•007722	•006807	•005972	•005214	156
157	•013481	•012194	•010974	•009826	•008755	•007761	•006847	•006011	157
158	•014846	•013506	•012225	•011008	•009863	•008793	•007800	•006886	158
159	•016246	•014865	•013532	•012254	•011041	•009899	•008830	•007839	159
160	•017668	•016259	•014885	•013556	•012284	•011074	•009934	•008868	160
161	•019094	•017673	•016272	•014904	•013581	•012312	•011107	•009969	161
162	•020509	•019091	•017678	•016284	•014922	•013604	•012341	•011139	162
163	•021893	•020497	•019088	•017682	•016295	•014940	•013628	•012369	163
164	•023228	•021871	•020484	•019084	•017686	•016308	•014957	•013651	164
165	•024495	•023197	•021850	•020472	•019080	•017690	•016317	•014974	165

TABLE I

X	A=174	A=175	A=176	A=177	A=178	A=179	A=180	A=181	X
166	•025675	•024455	•023166	•021828	•020459	•019005	•017693	•016528	166
167	•026751	•025626	•024415	•023135	•021806	•020446	•019071	•017696	167
168	•027707	•026694	•025577	•024375	•023104	•021785	•020433	•019066	168
169	•028527	•027642	•026637	•025529	•024335	•023074	•021763	•020419	169
170	•029198	•028455	•027577	•026580	•025480	•024295	•023043	•021741	170
171	•029710	•029120	•028383	•027512	•026523	•025432	•024256	•023012	171
172	•030056	•029628	•029043	•028312	•027448	•026467	•025384	•024216	172
173	•030229	•029971	•029547	•028967	•028242	•027385	•026411	•025336	173
174	•030229	•030143	•029886	•029466	•028891	•028172	•027322	•026355	174
175	•030057	•030143	•030057	•029803	•029386	•028816	•028102	•027259	175
176	•029715	•029972	•030057	•029972	•029720	•029307	•028741	•028033	176
177	•029211	•029633	•029887	•029972	•029888	•029638	•029228	•028667	177
178	•028555	•029133	•029552	•029804	•029888	•029804	•029557	•029150	178
179	•027757	•028482	•029056	•029471	•029721	•029804	•029722	•029476	179
180	•026832	•027691	•028411	•028980	•029391	•029639	•029722	•029639	180
181	•025794	•026773	•027626	•028339	•028904	•029311	•029557	•029639	181
182	•024661	•025744	•026715	•027561	•028268	•028828	•029233	•029477	182
183	•023448	•024618	•025693	•026657	•027496	•028198	•028753	•029154	183
184	•022173	•023414	•024576	•025643	•026599	•027432	•028128	•028679	184
185	•020855	•022148	•023380	•024534	•025593	•026542	•027368	•028059	185
186	•019509	•020839	•022123	•023347	•024492	•025543	•026485	•027305	186
187	•018153	•019501	•020822	•022098	•023313	•024451	•025494	•026429	187
188	•016801	•018153	•019493	•020805	•022073	•023280	•024409	•025445	188
189	•015468	•016808	•018152	•019484	•020789	•022048	•023247	•024368	189
190	•014165	•015481	•016815	•018151	•019476	•020772	•022023	•023213	190
191	•012905	•014184	•015494	•016821	•018150	•019467	•020755	•021998	191
192	•011695	•012928	•014203	•015507	•016827	•018149	•019458	•020738	192
193	•010543	•011723	•012952	•014221	•015519	•016832	•018147	•019448	193
194	•009457	•010575	•011750	•012905	•014239	•015531	•016837	•018145	194
195	•008438	•009490	•010605	•011777	•012998	•014256	•015542	•016842	195
196	•007491	•008473	•009523	•010636	•011804	•013020	•014273	•015553	196
197	•006616	•007527	•008508	•009556	•010666	•011830	•013042	•014290	197
198	•005814	•006653	•007563	•008542	•009588	•010695	•011856	•013063	198
199	•005084	•005850	•006689	•007598	•008576	•009620	•010724	•011882	199
200	•004423	•005119	•005886	•006724	•007633	•008610	•009652	•010753	200
201	•003829	•004457	•005154	•005921	•006760	•007668	•008643	•009683	201
202	•003298	•003861	•004490	•005188	•005956	•006795	•007702	•008676	202
203	•002827	•003329	•004052	•004893	•005223	•005991	•006829	•007736	203
204	•002411	•002855	•003359	•003925	•004557	•005257	•006026	•006864	204
205	•002047	•002438	•002884	•003389	•003957	•004590	•005291	•006060	205
206	•001729	•002071	•002464	•002912	•003419	•003989	•004623	•005325	206
207	•001453	•001751	•002095	•002490	•002940	•003449	•004020	•004656	207
208	•001216	•001473	•001772	•002119	•002516	•002968	•003479	•004052	208
209	•001012	•001233	•001493	•001794	•002143	•002542	•002996	•003509	209
210	•000839	•001028	•001251	•001512	•001816	•002167	•002568	•003024	210
211	•000691	•000852	•001043	•001269	•001532	•001838	•002191	•002594	211
212	•000568	•000704	•000866	•001059	•001287	•001552	•001860	•002215	212
213	•000464	•000578	•000716	•000880	•001075	•001304	•001572	•001882	213
214	•000377	•000473	•000589	•000728	•000894	•001091	•001322	•001592	214
215	•000305	•000385	•000482	•000599	•000740	•000908	•001107	•001340	215
216	•000246	•000312	•000393	•000491	•000610	•000753	•000923	•001123	216
217	•000197	•000251	•000318	•000401	•000500	•000621	•000765	•000937	217
218	•000157	•000202	•000257	•000325	•000409	•000510	•000632	•000778	218
219	•000125	•000161	•000207	•000263	•000332	•000417	•000519	•000643	219
220	•000099	•000128	•000165	•000211	•000269	•000339	•000425	•000529	220
221	•000078	•000102	•000132	•000169	•000216	•000275	•000346	•000433	221
222	•000061	•000080	•000104	•000135	•000174	•000221	•000281	•000353	222
223	•000048	•000063	•000082	•000107	•000139	•000178	•000226	•000287	223
224	•000037	•000049	•000065	•000085	•000110	•000142	•000182	•000232	224
225	•000029	•000038	•000051	•000067	•000087	•000113	•000146	•000186	225
226	•000022	•000030	•000039	•000052	•000069	•000089	•000116	•000149	226
227	•000017	•000023	•000031	•000041	•000054	•000071	•000092	•000119	227
228	•000013	•000017	•000024	•000032	•000042	•000055	•000073	•000094	228
229	•000010	•000013	•000018	•000024	•000033	•000043	•000057	•000075	229
230	•000007	•000010	•000014	•000019	•000025	•000034	•000045	•000059	230
231	•000006	•000008	•000011	•000014	•000019	•000026	•000035	•000046	231
232	•000004	•000006	•000008	•000011	•000015	•000020	•000027	•000036	232
233	•000003	•000004	•000006	•000008	•000011	•000015	•000021	•000028	233



TABLE I

X	A=174	A=175	A=176	A=177	A=178	A=179	A=180	A=181	X
234	•000002	•000003	•000005	•000006	•000009	•000012	•000016	•000022	234
235	•000002	•000002	•000003	•000005	•000007	•000009	•000012	•000017	235
236	•000001	•000002	•000003	•000004	•000005	•000007	•000009	•000013	236
237	•000001	•000001	•000002	•000003	•000004	•000005	•000007	•000010	237
238	•000001	•000001	•000001	•000002	•000003	•000004	•000005	•000007	238
239		•000001	•000001	•000001	•000002	•000003	•000004	•000006	239
240		•000001	•000001	•000001	•000002	•000002	•000003	•000004	240
241			•000001	•000001	•000001	•000002	•000002	•000003	241
242				•000001	•000001	•000001	•000002	•000002	242
243					•000001	•000001	•000001	•000002	243
244						•000001	•000001	•000001	244
245							•000001	•000001	245
246								•000001	246
247								•000001	247
X	A=182	A=183	A=184	A=185	A=186	A=187	A=188	A=189	X
123	•000001	•000001							123
124	•000001	•000001	•000001						124
125	•000002	•000001	•000001	•000001					125
126	•000002	•000002	•000001	•000001	•000001				126
127	•000003	•000002	•000002	•000001	•000001	•000001			127
128	•000005	•000003	•000003	•000002	•000001	•000001	•000001	•000001	128
129	•000006	•000005	•000004	•000003	•000002	•000001	•000001	•000001	129
130	•000009	•000007	•000005	•000004	•000003	•000002	•000002	•000001	130
131	•000013	•000009	•000007	•000005	•000004	•000003	•000002	•000002	131
132	•000017	•000013	•000010	•000007	•000006	•000004	•000003	•000002	132
133	•000024	•000018	•000014	•000010	•000008	•000006	•000004	•000003	133
134	•000032	•000025	•000019	•000014	•000011	•000008	•000006	•000005	134
135	•000043	•000033	•000026	•000020	•000015	•000011	•000009	•000006	135
136	•000058	•000045	•000035	•000027	•000020	•000016	•000012	•000009	136
137	•000077	•000060	•000047	•000036	•000028	•000021	•000016	•000012	137
138	•000102	•000080	•000062	•000048	•000037	•000029	•000022	•000017	138
139	•000133	•000105	•000083	•000064	•000050	•000039	•000030	•000023	139
140	•000173	•000137	•000108	•000085	•000067	•000052	•000040	•000031	140
141	•000224	•000178	•000142	•000112	•000088	•000069	•000054	•000042	141
142	•000287	•000230	•000183	•000146	•000115	•000091	•000071	•000056	142
143	•000365	•000294	•000236	•000188	•000150	•000119	•000094	•000074	143
144	•000462	•000374	•000301	•000242	•000194	•000154	•000122	•000096	144
145	•000580	•000472	•000383	•000309	•000248	•000199	•000158	•000126	145
146	•000722	•000591	•000482	•000391	•000316	•000255	•000204	•000163	146
147	•000894	•000736	•000603	•000493	•000400	•000324	•000261	•000209	147
148	•001100	•000910	•000750	•000616	•000503	•000409	•000331	•000267	148
149	•001343	•001118	•000927	•000764	•000628	•000513	•000418	•000339	149
150	•001630	•001364	•001137	•000943	•000779	•000640	•000524	•000427	150
151	•001965	•001653	•001385	•001155	•000959	•000793	•000653	•000535	151
152	•002353	•001990	•001677	•001406	•001173	•000975	•000807	•000665	152
153	•002798	•002381	•002016	•001700	•001427	•001192	•000992	•000821	153
154	•003307	•002829	•002409	•002042	•001723	•001447	•001211	•001008	154
155	•003883	•003340	•002860	•002437	•002068	•001746	•001468	•001229	155
156	•004531	•003918	•003373	•002890	•002465	•002093	•001770	•001489	156
157	•005252	•004567	•003953	•003406	•002921	•002493	•002119	•001793	157
158	•006050	•005290	•004604	•003988	•003438	•002951	•002521	•002145	158
159	•006925	•006088	•005327	•004640	•004022	•003471	•002981	•002549	159
160	•007877	•006964	•006126	•005365	•004676	•004056	•003503	•003011	160
161	•008905	•007915	•007002	•006164	•005402	•004711	•004090	•003535	161
162	•010004	•008941	•007953	•007040	•006202	•005438	•004747	•004124	162
163	•011170	•010038	•008977	•007990	•007077	•006239	•005475	•004782	163
164	•012396	•011201	•010072	•009013	•008026	•007114	•006276	•005511	164
165	•013673	•012423	•011232	•010105	•009048	•008063	•007151	•006313	165
166	•014991	•013695	•012450	•011262	•010138	•009083	•008099	•007188	166
167	•016338	•015007	•013717	•012476	•011291	•010171	•009117	•008134	167
168	•017699	•016347	•015023	•013738	•012501	•011321	•010203	•009151	168
169	•019061	•017702	•016357	•015039	•013759	•012527	•011350	•010234	169
170	•020406	•019055	•017704	•016366	•015054	•013779	•012551	•011378	170
171	•021719	•020392	•019050	•017706	•016374	•015068	•013799	•012576	171
172	•022981	•021697	•020379	•019044	•017707	•016383	•015083	•013819	172

TABLE I

X	A=182	A=183	A=184	A=185	A=186	A=187	A=188	A=189	X
173	•024177	•022951	•021674	•020365	•019038	•017708	•016391	•015097	173
174	•025289	•024138	•022920	•021652	•020351	•019031	•017709	•016398	174
175	•026300	•025241	•024099	•022889	•021630	•020336	•019025	•017710	175
176	•027197	•026245	•025194	•024060	•022859	•021607	•020322	•019018	176
177	•027965	•027135	•026191	•025147	•024021	•022828	•021585	•020307	177
178	•028593	•027897	•027073	•026136	•025101	•023982	•022798	•021562	178
179	•029073	•028520	•027830	•027012	•026082	•025054	•023944	•022767	179
180	•029396	•028996	•028448	•027763	•026952	•026029	•025008	•023905	180
181	•029558	•029316	•028920	•028376	•027696	•026891	•025975	•024962	181
182	•029558	•029477	•029237	•028844	•028305	•027630	•026831	•025922	182
183	•029397	•029477	•029397	•029159	•028769	•028234	•027565	•026772	183
184	•029077	•029317	•029397	•029318	•029082	•028694	•028164	•027499	184
185	•028605	•029000	•029238	•029318	•029239	•029005	•028621	•028094	185
186	•027990	•028532	•028924	•029160	•029239	•029161	•028928	•028547	186
187	•027242	•027922	•028460	•028848	•029082	•029161	•029083	•028853	187
188	•026372	•027179	•027854	•028388	•028773	•029005	•029083	•029006	188
189	•025396	•026317	•027117	•027787	•028316	•028699	•028929	•029006	189
190	•024326	•025347	•026261	•027056	•027720	•028245	•028625	•028853	190
191	•023180	•024285	•025299	•026206	•026995	•027654	•028175	•028551	191
192	•021973	•023147	•024244	•025250	•026151	•026934	•027588	•028105	192
193	•020721	•021948	•023114	•024204	•025202	•026096	•026873	•027523	193
194	•019439	•020703	•021922	•023081	•024163	•025155	•026042	•026813	194
195	•018143	•019429	•020686	•021897	•023048	•024123	•025107	•025988	195
196	•016847	•018140	•019419	•020668	•021872	•023015	•024083	•025060	196
197	•015564	•016851	•018138	•019409	•020651	•021847	•022982	•024042	197
198	•014306	•015575	•016855	•018135	•019399	•020633	•021822	•022950	198
199	•013084	•014322	•015585	•016859	•018132	•019389	•020615	•021796	199
200	•011907	•013105	•014338	•015595	•016863	•018129	•019378	•020598	200
201	•010781	•011931	•013125	•014353	•015604	•016866	•018125	•019368	201
202	•009714	•010809	•011956	•013145	•014368	•015613	•016869	•018121	202
203	•008709	•009744	•010837	•011980	•013165	•014383	•015622	•016872	203
204	•007770	•008741	•009774	•010864	•012003	•013184	•014397	•015631	204
205	•006898	•007803	•008773	•009804	•010891	•012027	•013203	•014411	205
206	•006094	•006932	•007836	•008805	•009834	•010917	•012050	•013222	206
207	•005358	•006128	•006965	•007869	•008836	•009863	•010944	•012072	207
208	•004689	•005392	•006162	•006999	•007901	•008867	•009891	•010969	208
209	•004083	•004721	•005425	•006195	•007032	•007933	•008897	•009920	209
210	•003538	•004114	•004753	•005458	•006228	•007065	•007965	•008928	210
211	•003052	•003568	•004145	•004785	•005490	•006261	•007097	•007997	211
212	•002620	•003080	•003597	•004176	•004817	•005523	•006294	•007129	212
213	•002239	•002646	•003108	•003627	•004206	•004849	•005555	•006326	213
214	•001904	•002263	•002672	•003135	•003656	•004237	•004880	•005587	214
215	•001612	•001926	•002287	•002698	•003163	•003685	•004267	•004911	215
216	•001358	•001632	•001948	•002311	•002724	•003190	•003714	•004297	216
217	•001139	•001376	•001652	•001970	•002334	•002749	•003218	•003743	217
218	•000951	•001155	•001394	•001672	•001992	•002358	•002775	•003245	218
219	•000790	•000965	•001171	•001412	•001692	•002014	•002382	•002800	219
220	•000654	•000803	•000980	•001187	•001430	•001712	•002036	•002406	220
221	•000538	•000665	•000816	•000994	•001204	•001448	•001732	•002057	221
222	•000441	•000548	•000676	•000828	•001009	•001220	•001466	•001752	222
223	•000360	•000450	•000558	•000687	•000841	•001023	•001236	•001485	223
224	•000293	•000367	•000458	•000568	•000698	•000854	•001038	•001253	224
225	•000237	•000299	•000375	•000467	•000577	•000710	•000867	•001052	225
226	•000191	•000242	•000305	•000382	•000475	•000587	•000721	•000880	226
227	•000153	•000195	•000247	•000311	•000389	•000484	•000597	•000733	227
228	•000122	•000157	•000200	•000253	•000318	•000397	•000492	•000607	228
229	•000097	•000125	•000160	•000204	•000258	•000324	•000404	•000501	229
230	•000077	•000100	•000128	•000164	•000209	•000263	•000330	•000412	230
231	•000060	•000079	•000102	•000131	•000168	•000213	•000269	•000337	231
232	•000047	•000062	•000081	•000105	•000135	•000172	•000218	•000275	232
233	•000037	•000049	•000064	•000083	•000108	•000138	•000176	•000223	233
234	•000029	•000038	•000050	•000066	•000085	•000110	•000141	•000180	234
235	•000022	•000030	•000039	•000052	•000068	•000088	•000113	•000145	235
236	•000017	•000023	•000031	•000041	•000053	•000070	•000090	•000116	236
237	•000013	•000018	•000024	•000032	•000042	•000055	•000071	•000092	237
238	•000010	•000014	•000018	•000025	•000033	•000043	•000056	•000073	238
239	•000008	•000010	•000014	•000019	•000025	•000034	•000044	•000058	239
240	•000006	•000008	•000011	•000015	•000020	•000026	•000035	•000046	240

TABLE I

X	A=182	A=183	A=184	A=185	A=186	A=187	A=188	A=189	X
241	•000004	•000006	•000008	•000011	•000015	•000020	•000027	•000036	241
242	•000003	•000005	•000006	•000009	•000012	•000016	•000021	•000028	242
243	•000002	•000003	•000005	•000007	•000009	•000012	•000016	•000022	243
244	•000002	•000003	•000004	•000005	•000007	•000009	•000013	•000017	244
245	•000001	•000002	•000003	•000004	•000005	•000007	•000010	•000013	245
246	•000001	•000001	•000002	•000003	•000004	•000005	•000007	•000010	246
247	•000001	•000001	•000002	•000002	•000003	•000004	•000006	•000008	247
248	•000001	•000001	•000001	•000002	•000002	•000003	•000004	•000006	248
249		•000001	•000001	•000001	•000002	•000002	•000003	•000004	249
250			•000001	•000001	•000001	•000002	•000002	•000003	250
251				•000001	•000001	•000001	•000002	•000003	251
252					•000001	•000001	•000001	•000002	252
253						•000001	•000001	•000001	253
254						•000001	•000001	•000001	254
255							•000001	•000001	255
256								•000001	256
X	A=190	A=191	A=192	A=193	A=194	A=195	A=196	A=197	X
129	•000001								129
130	•000001	•000001							130
131	•000001	•000001	•000001						131
132	•000002	•000001	•000001	•000001					132
133	•000002	•000002	•000001	•000001	•000001	•000001			133
134	•000003	•000003	•000002	•000001	•000001	•000001	•000001		134
135	•000005	•000004	•000003	•000002	•000001	•000001	•000001	•000001	135
136	•000007	•000005	•000004	•000003	•000002	•000002	•000001	•000001	136
137	•000009	•000007	•000005	•000004	•000003	•000002	•000002	•000001	137
138	•000013	•000010	•000007	•000006	•000004	•000003	•000002	•000002	138
139	•000018	•000013	•000010	•000008	•000006	•000004	•000003	•000002	139
140	•000024	•000018	•000014	•000011	•000008	•000006	•000005	•000003	140
141	•000032	•000025	•000019	•000015	•000011	•000008	•000006	•000005	141
142	•000043	•000034	•000026	•000020	•000015	•000012	•000009	•000007	142
143	•000058	•000045	•000035	•000027	•000021	•000016	•000012	•000009	143
144	•000076	•000059	•000046	•000036	•000028	•000022	•000017	•000013	144
145	•000099	•000078	•000061	•000048	•000037	•000029	•000022	•000017	145
146	•000129	•000102	•000081	•000063	•000050	•000039	•000030	•000023	146
147	•000167	•000133	•000106	•000083	•000066	•000051	•000040	•000031	147
148	•000215	•000172	•000137	•000109	•000086	•000068	•000053	•000041	148
149	•000274	•000220	•000176	•000141	•000112	•000088	•000070	•000055	149
150	•000347	•000280	•000226	•000181	•000145	•000115	•000091	•000072	150
151	•000436	•000355	•000287	•000231	•000186	•000149	•000118	•000094	151
152	•000546	•000446	•000363	•000294	•000237	•000191	•000153	•000122	152
153	•000678	•000556	•000455	•000371	•000301	•000243	•000195	•000157	153
154	•000836	•000690	•000567	•000465	•000379	•000308	•000249	•000200	154
155	•001025	•000850	•000703	•000578	•000474	•000387	•000315	•000255	155
156	•001248	•001041	•000865	•000716	•000590	•000484	•000395	•000322	156
157	•001510	•001267	•001058	•000880	•000729	•000601	•000493	•000404	157
158	•001816	•001531	•001286	•001075	•000895	•000741	•000612	•000503	158
159	•002170	•001840	•001552	•001304	•001091	•000909	•000754	•000623	159
160	•002577	•002196	•001863	•001574	•001323	•001108	•000924	•000768	160
161	•003042	•002605	•002222	•001886	•001595	•001342	•001125	•000939	161
162	•003567	•003072	•002633	•002247	•001910	•001616	•001361	•001142	162
163	•004158	•003599	•003102	•002661	•002273	•001933	•001637	•001380	163
164	•004817	•004192	•003631	•003131	•002689	•002298	•001956	•001658	164
165	•005547	•004852	•004225	•003663	•003161	•002716	•002324	•001980	165
166	•006349	•005583	•004887	•004259	•003694	•003191	•002744	•002349	166
167	•007224	•006385	•005619	•004922	•004292	•003726	•003220	•002771	167
168	•008170	•007260	•006421	•005654	•004956	•004325	•003757	•003250	168
169	•009185	•008205	•007295	•006457	•005689	•004990	•004357	•003788	169
170	•010265	•009218	•008239	•007330	•006492	•005724	•005024	•004390	170
171	•011406	•010296	•009251	•008273	•007365	•006527	•005758	•005057	171
172	•012600	•011434	•010327	•009284	•008307	•007400	•006562	•005793	172
173	•013838	•012623	•011461	•010357	•009316	•008341	•007434	•006596	173
174	•015110	•013857	•012647	•011488	•010387	•009348	•008374	•007468	174
175	•016405	•015124	•013875	•012669	•011514	•010416	•009379	•008407	175
176	•017710	•016412	•015136	•013893	•012692	•011540	•010445	•009410	176

TABLE I

X	A=190	A=191	A=192	A=193	A=194	A=195	A=196	A=197	X
177	•019011	•017711	•016419	•015149	•013911	•012714	•011566	•010473	177
178	•020293	•019004	•017711	•016426	•015161	•013928	•012735	•011591	178
179	•021540	•020278	•018997	•017710	•016432	•015173	•013945	•012757	179
180	•022737	•021517	•020263	•018989	•017710	•016437	•015185	•013962	180
181	•023867	•022706	•021495	•020248	•018982	•017709	•016443	•015196	181
182	•024916	•023829	•022676	•021472	•020233	•018974	•017708	•016448	182
183	•025869	•024871	•023791	•022645	•021449	•020218	•018966	•017707	183
184	•026713	•025817	•024825	•023753	•022615	•021427	•020203	•018958	184
185	•027435	•026654	•025765	•024780	•023715	•022585	•021404	•020187	185
186	•028025	•027371	•026596	•025713	•024735	•023678	•022555	•021381	186
187	•028474	•027956	•027307	•026538	•025661	•024691	•023640	•022524	187
188	•028777	•028402	•027888	•027244	•026480	•025610	•024646	•023603	188
189	•028930	•028703	•028331	•027820	•027181	•026423	•025559	•024602	189
190	•028930	•028854	•028629	•028259	•027753	•027118	•026366	•025508	190
191	•028778	•028854	•028779	•028555	•028189	•027686	•027056	•026310	191
192	•028478	•028704	•028779	•028704	•028482	•028119	•027620	•026995	192
193	•028036	•028406	•028630	•028704	•028630	•028410	•028049	•027554	193
194	•027458	•027967	•028334	•028556	•028630	•028557	•028338	•027980	194
195	•026754	•027393	•027899	•028263	•028483	•028557	•028484	•028267	195
196	•025935	•026694	•027329	•027831	•028193	•028411	•028484	•028411	196
197	•025013	•025881	•026636	•027266	•027763	•028122	•028339	•028411	197
198	•024002	•024966	•025828	•026577	•027202	•027696	•028053	•028268	198
199	•022917	•023963	•024920	•025776	•026519	•027140	•027630	•027984	199
200	•021771	•022884	•023923	•024874	•025723	•026461	•027077	•027564	200
201	•020580	•021746	•022852	•023884	•024828	•025671	•026404	•027016	201
202	•019357	•020562	•021721	•022819	•023844	•024782	•025620	•026347	202
203	•018117	•019346	•020544	•021695	•022787	•023805	•024736	•025568	203
204	•016874	•018113	•019335	•020525	•021670	•022755	•023766	•024691	204
205	•015639	•016876	•018109	•019324	•020507	•021645	•022723	•023727	205
206	•014425	•015647	•016878	•018105	•019313	•020489	•021620	•022691	206
207	•013240	•014438	•015655	•016880	•018100	•019301	•020471	•021594	207
208	•012094	•013258	•014451	•015663	•016882	•018095	•019290	•020452	208
209	•010995	•012116	•013276	•014464	•015670	•016883	•018090	•019278	209
210	•009948	•011020	•012138	•013293	•014476	•015677	•016884	•018085	210
211	•008958	•009975	•011045	•012159	•013310	•014488	•015684	•016885	211
212	•008028	•008987	•010003	•011069	•012180	•013326	•014500	•015690	212
213	•007161	•008059	•009017	•010030	•011093	•012200	•013343	•014512	213
214	•006358	•007193	•008090	•009046	•010056	•011117	•012220	•013359	214
215	•005619	•006390	•007224	•008120	•009074	•010083	•011140	•012240	215
216	•004942	•005650	•006422	•007255	•008150	•009103	•010109	•011164	216
217	•004327	•004973	•005682	•006453	•007286	•008180	•009131	•010135	217
218	•003772	•004357	•005004	•005713	•006484	•007317	•008209	•009158	218
219	•003272	•003800	•004387	•005035	•005744	•006515	•007347	•008238	219
220	•002826	•003299	•003829	•004417	•005065	•005775	•006546	•007377	220
221	•002430	•002851	•003326	•003857	•004446	•005095	•005805	•006576	221
222	•002079	•002453	•002877	•003353	•003885	•004476	•005125	•005835	222
223	•001772	•002101	•002477	•002902	•003380	•003914	•004505	•005155	223
224	•001503	•001792	•002123	•002501	•002927	•003407	•003942	•004534	224
225	•001269	•001521	•001812	•002145	•002524	•002953	•003434	•003970	225
226	•001067	•001285	•001539	•001832	•002167	•002548	•002978	•003460	226
227	•000893	•001082	•001302	•001557	•001852	•002189	•002571	•003003	227
228	•000744	•000906	•001096	•001318	•001576	•001872	•002210	•002595	228
229	•000617	•000756	•000919	•001111	•001335	•001594	•001892	•002232	229
230	•000510	•000628	•000767	•000932	•001126	•001351	•001612	•001912	230
231	•000419	•000519	•000638	•000779	•000946	•001141	•001368	•001630	231
232	•000344	•000427	•000528	•000648	•000791	•000959	•001156	•001384	232
233	•000280	•000350	•000435	•000537	•000658	•000802	•000972	•001171	233
234	•000227	•000286	•000357	•000443	•000546	•000669	•000814	•000985	234
235	•000184	•000232	•000292	•000364	•000451	•000555	•000679	•000826	235
236	•000148	•000188	•000237	•000297	•000370	•000458	•000564	•000690	236
237	•000119	•000152	•000192	•000242	•000303	•000377	•000466	•000573	237
238	•000095	•000122	•000155	•000196	•000247	•000309	•000384	•000474	238
239	•000075	•000097	•000125	•000159	•000201	•000252	•000315	•000391	239
240	•000060	•000077	•000100	•000128	•000162	•000205	•000257	•000321	240
241	•000047	•000061	•000079	•000102	•000131	•000166	•000209	•000262	241
242	•000037	•000048	•000063	•000081	•000105	•000134	•000169	•000214	242
243	•000029	•000038	•000050	•000065	•000084	•000107	•000137	•000173	243
244	•000022	•000030	•000039	•000051	•000066	•000086	•000110	•000140	244

TABLE I

X	A=190	A=191	A=192	A=193	A=194	A=195	A=196	A=197	X
245	•000017	•000023	•000031	•000040	•000053	•000068	•000088	•000112	245
246	•000013	•000018	•000024	•000032	•000041	•000054	•000070	•000090	246
247	•000010	•000014	•000019	•000025	•000033	•000043	•000056	•000072	247
248	•000008	•000011	•000014	•000019	•000025	•000034	•000044	•000057	248
249	•000006	•000008	•000011	•000015	•000020	•000026	•000035	•000045	249
250	•000005	•000006	•000009	•000012	•000015	•000020	•000027	•000036	250
251	•000003	•000005	•000007	•000009	•000012	•000016	•000021	•000028	251
252	•000003	•000004	•000005	•000007	•000009	•000012	•000016	•000022	252
253	•000002	•000003	•000004	•000005	•000007	•000009	•000013	•000017	253
254	•000001	•000002	•000003	•000004	•000005	•000007	•000010	•000013	254
255	•000001	•000002	•000002	•000003	•000004	•000006	•000008	•000010	255
256	•000001	•000001	•000002	•000002	•000003	•000004	•000006	•000008	256
257	•000001	•000001	•000001	•000002	•000002	•000003	•000004	•000006	257
258	•000001	•000001	•000001	•000001	•000002	•000002	•000003	•000005	258
259			•000001	•000001	•000001	•000002	•000003	•000003	259
260				•000001	•000001	•000001	•000002	•000003	260
261				•000001	•000001	•000001	•000001	•000002	261
262					•000001	•000001	•000001	•000001	262
263						•000001	•000001	•000001	263
264						•000001	•000001	•000001	264
265							•000001	•000001	265
X	A=198	A=199	A=200						
136	•000001								
137	•000001	•000001							
138	•000001	•000001	•000001						
139	•000002	•000001	•000001						
140	•000003	•000002	•000001						
141	•000004	•000003	•000002						
142	•000005	•000004	•000003						
143	•000007	•000005	•000004						
144	•000010	•000007	•000006						
145	•000013	•000010	•000008						
146	•000018	•000014	•000011						
147	•000024	•000019	•000014						
148	•000032	•000025	•000019						
149	•000043	•000033	•000026						
150	•000057	•000044	•000035						
151	•000074	•000058	•000046						
152	•000097	•000076	•000060						
153	•000125	•000099	•000079						
154	•000161	•000128	•000102						
155	•000205	•000165	•000132						
156	•000261	•000210	•000169						
157	•000329	•000267	•000216						
158	•000412	•000336	•000273						
159	•000513	•000420	•000343						
160	•000635	•000523	•000429						
161	•000781	•000646	•000533						
162	•000954	•000794	•000658						
163	•001159	•000969	•000807						
164	•001399	•001176	•000984						
165	•001679	•001419	•001193						
166	•002003	•001701	•001438						
167	•002375	•002026	•001722						
168	•002799	•002400	•002050						
169	•003279	•002826	•002426						
170	•003819	•003309	•002854						
171	•004422	•003850	•003338						
172	•005091	•004455	•003881						
173	•005827	•005124	•004487						
174	•006630	•005860	•005157						
175	•007502	•006664	•005894						
176	•008439	•007535	•006698						
177	•009441	•008472	•007568						
178	•010501	•009471	•008503						
179	•011616	•010529	•009501						

TABLE I

X	A=198	A=199	A=200
180	•012778	•011641	•010557
181	•013978	•012798	•011665
182	•015207	•013994	•012819
183	•016453	•015217	•014009
184	•017705	•016458	•015228
185	•018949	•017703	•016462
186	•020172	•018941	•017701
187	•021358	•020156	•018932
188	•022494	•021335	•020140
189	•023566	•022464	•021313
190	•024558	•023528	•022434
191	•025458	•024514	•023491
192	•026253	•025408	•024470
193	•026933	•026198	•025358
194	•027489	•026873	•026142
195	•027912	•027424	•026812
196	•028197	•027844	•027360
197	•028340	•028126	•027776
198	•028340	•028268	•028057
199	•028197	•028268	•028198
200	•027915	•028127	•028198
201	•027499	•027847	•028057
202	•026954	•027434	•027780
203	•026290	•026893	•027369
204	•025517	•026234	•026832
205	•024646	•025466	•026178
206	•023689	•024601	•025416
207	•022659	•023650	•024556
208	•021569	•022627	•023612
209	•020434	•021544	•022595
210	•020397	•020416	•021519
211	•018079	•019254	•019266
212	•016885	•018074	•019243
213	•015696	•016886	•018068
214	•014523	•015702	•016886
215	•013374	•014534	•015708
216	•012260	•013390	•014544
217	•011186	•012279	•013405
218	•010160	•011209	•012298
219	•009186	•010185	•011231
220	•008267	•009213	•010210
221	•007407	•008296	•009240
222	•006606	•007436	•008324
223	•005866	•006636	•007466
224	•005185	•005895	•006666
225	•004563	•005214	•005925
226	•003997	•004591	•005244
227	•003487	•004025	•004620
228	•003028	•003513	•004052
229	•002618	•003053	•003539
230	•002254	•002641	•003078
231	•001932	•002275	•002665
232	•001649	•001952	•002297
233	•001401	•001667	•001972
234	•001185	•001418	•001685
235	•000999	•001200	•001434
236	•000838	•001012	•001215
237	•000700	•000850	•001026
238	•000582	•000711	•000862
239	•000483	•000592	•000721
240	•000398	•000491	•000601
241	•000327	•000405	•000499
242	•000268	•000333	•000412
243	•000218	•000273	•000339
244	•000177	•000223	•000278
245	•000143	•000181	•000227
246	•000115	•000146	•000185
247	•000092	•000118	•000149

TABLE I

X	A=198	A=199	A=200
248	•000074	•000095	•000121
249	•000059	•000076	•000097
250	•000046	•000060	•000007
251	•000037	•000048	•000062
252	•000029	•000038	•000049
253	•000022	•000030	•000039
254	•000018	•000023	•000030
255	•000014	•000018	•000024
256	•000011	•000014	•000019
257	•000008	•000011	•000015
258	•000006	•000008	•000001
259	•000005	•000006	•000009
260	•000004	•000005	•000007
261	•000003	•000004	•000005
262	•000002	•000003	•000004
263	•000002	•000002	•000003
264	•000001	•000002	•000002
265	•000001	•000001	•000002
266	•000001	•000001	•000001
267		•000001	•000001
268		•000001	•000001

TABLE II

X	A=.001	A=.002	A=.003	A=.004	A=.005	A=.006	A=.007	A=.008	X
0	1.00000000	1.00000000	1.00000000	1.00000000	1.00000000	1.00000000	1.00000000	1.00000000	0
1	.0009995	.0019980	.0029955	.0039920	.0049875	.0059820	.0069756	.0079681	1
2	.0000005	.0000020	.0000045	.0000080	.0000125	.0000179	.0000244	.0000318	2
3							.0000001	.0000001	3
X	A=.009	A=.010	A=.02	A=.03	A=.04	A=.05	A=.06	A=.07	X
0	1.00000000	1.00000000	1.00000000	1.00000000	1.00000000	1.00000000	1.00000000	1.00000000	0
1	.0089596	.0099502	.0198013	.0295545	.0392106	.0487706	.0582355	.0676062	1
2	.0000403	.0000497	.0001973	.0004411	.0007790	.0012091	.0017296	.0023386	2
3	.0000001	.0000002	.0000013	.0000044	.0000104	.0000201	.0000344	.0000542	3
4					.0000001	.0000003	.0000005	.0000009	4
X	A=.08	A=.09	A=.10	A=.11	A=.12	A=.13	A=.14	A=.15	X
0	1.00000000	1.00000000	1.00000000	1.00000000	1.00000000	1.00000000	1.00000000	1.00000000	0
1	.0768837	.0860688	.0951626	.1041659	.1130796	.1219046	.1306418	.1302920	1
2	.0030343	.0038150	.0046788	.0056241	.0066491	.0077522	.0089316	.0101858	2
3	.0000804	.0001136	.0001547	.0002043	.0002633	.0003323	.0004119	.0005029	3
4	.0000016	.0000025	.0000038	.0000056	.0000079	.0000107	.0000143	.0000187	4
5				.0000001	.0000002	.0000003	.0000004	.0000006	5
X	A=.16	A=.17	A=.18	A=.19	A=.20	A=.21	A=.22	A=.23	X
0	1.00000000	1.00000000	1.00000000	1.00000000	1.00000000	1.00000000	1.00000000	1.00000000	0
1	.1478562	.1563352	.1647298	.1730409	.1812692	.1894158	.1974812	.2054664	1
2	.0115132	.0129122	.0143812	.0159187	.0175231	.0191931	.0209271	.0227237	2
3	.0006058	.0007212	.0008498	.0009920	.0011485	.0013197	.0015060	.0017083	3
4	.0000240	.0000304	.0000379	.0000467	.0000568	.0000685	.0000819	.0000971	4
5	.0000008	.0000010	.0000014	.0000018	.0000023	.0000029	.0000036	.0000044	5
6				.0000001	.0000001	.0000001	.0000001	.0000002	6
X	A=.24	A=.25	A=.26	A=.27	A=.28	A=.29	A=.30	A=.40	X
0	1.00000000	1.00000000	1.00000000	1.00000000	1.00000000	1.00000000	1.00000000	1.00000000	0
1	.2133721	.2211992	.2289484	.2366205	.2442163	.2517364	.2591818	.3296800	1
2	.0245815	.0264990	.0284750	.0305080	.0325968	.0347400	.0369363	.0615519	2
3	.0019266	.0021615	.0024135	.0026829	.0029701	.0032755	.0035995	.0079263	3
4	.0001142	.0001334	.0001548	.0001786	.0002049	.0002339	.0002658	.0007763	4
5	.0000054	.0000066	.0000080	.0000096	.0000113	.0000134	.0000158	.0000612	5
6	.0000002	.0000003	.0000003	.0000004	.0000005	.0000006	.0000008	.0000040	6
7								.0000002	7
X	A=.5	A=.6	A=.7	A=.8	A=.9	A=1.0	A=1.1	A=1.2	X
0	1.00000000	1.00000000	1.00000000	1.00000000	1.00000000	1.00000000	1.00000000	1.00000000	0
1	.393469	.451188	.503415	.550671	.593430	.632121	.667129	.698806	1
2	.090204	.121901	.155805	.191208	.227518	.264241	.300971	.337373	2
3	.014388	.023115	.034142	.047423	.062857	.080301	.099584	.120513	3
4	.001752	.003358	.005753	.009080	.013459	.018988	.025742	.033769	4
5	.000172	.000394	.000786	.001411	.002344	.003660	.005435	.007746	5
6	.000014	.000039	.000090	.000184	.000343	.000594	.000968	.001500	6
7	.000001	.000003	.000009	.000021	.000043	.000083	.000149	.000251	7
8			.000001	.000002	.000005	.000010	.000020	.000037	8
9						.000001	.000002	.000005	9
10								.000001	10
X	A=1.3	A=1.4	A=1.5	A=1.6	A=1.7	A=1.8	A=1.9	A=2.0	X
0	1.00000000	1.00000000	1.00000000	1.00000000	1.00000000	1.00000000	1.00000000	1.00000000	0
1	.727468	.753403	.776870	.798103	.817316	.834701	.850431	.864665	1
2	.373177	.408167	.442175	.475069	.506754	.537163	.566251	.593994	2
3	.142888	.166502	.191153	.216642	.242777	.269379	.296280	.323324	3
4	.043095	.053725	.065642	.078813	.093189	.108708	.125298	.142877	4
5	.010663	.014253	.018576	.023682	.029615	.036407	.044081	.052653	5
6	.002231	.003201	.004456	.006040	.007999	.010378	.013219	.016564	6
7	.000404	.000622	.000926	.001336	.001875	.002569	.003446	.004534	7
8	.000064	.000107	.000170	.000260	.000388	.000562	.000793	.001097	8
9	.000009	.000016	.000028	.000045	.000072	.000110	.000163	.000237	9



TABLE II

X	A=1.3	A=1.4	A=1.5	A=1.6	A=1.7	A=1.8	A=1.9	A=2.0	X
10	.000001	.000002	.000004	.000007	.000012	.000019	.000030	.000046	10
11			.000001	.000001	.000002	.000003	.000005	.000008	11
12							.000001	.000001	12
X	A=2.1	A=2.2	A=2.3	A=2.4	A=2.5	A=2.6	A=2.7	A=2.8	X
0	1.000000	1.000000	1.000000	1.000000	1.000000	1.000000	1.000000	1.000000	0
1	.877544	.889197	.899741	.909282	.917915	.925726	.932794	.939190	1
2	.620385	.643430	.669146	.691559	.712703	.732615	.751340	.768922	2
3	.350369	.377286	.403961	.430291	.456187	.481570	.506375	.530546	3
4	.161357	.180648	.200653	.221277	.242424	.263998	.285908	.308063	4
5	.062126	.072496	.083751	.095869	.108822	.122577	.137092	.152324	5
6	.020449	.024910	.029976	.035673	.042021	.049037	.056732	.065110	6
7	.005862	.007461	.009362	.011594	.014187	.017170	.020569	.024411	7
8	.001486	.001978	.002589	.003339	.004247	.005334	.006621	.008131	8
9	.000337	.000470	.000642	.000862	.001140	.001487	.001914	.002433	9
10	.000069	.000101	.000144	.000202	.000277	.000376	.000501	.000660	10
11	.000013	.000020	.000029	.000043	.000062	.000087	.000120	.000164	11
12	.000002	.000004	.000006	.000008	.000013	.000018	.000026	.000037	12
13		.000001	.000001	.000002	.000002	.000004	.000005	.000008	13
14					.000001	.000001	.000001	.000002	14
X	A=2.9	A=3.0	A=3.1	A=3.2	A=3.3	A=3.4	A=3.5	A=3.6	X
0	1.000000	1.000000	1.000000	1.000000	1.000000	1.000000	1.000000	1.000000	0
1	.944977	.950213	.954951	.959238	.963117	.966627	.969803	.972676	1
2	.785409	.800852	.815298	.828799	.841402	.853158	.864112	.874311	2
3	.554037	.576810	.598837	.620096	.640574	.660260	.679153	.697253	3
4	.330377	.352768	.375160	.397480	.419662	.441643	.463367	.484784	4
5	.168223	.184737	.201811	.219387	.237410	.255818	.274555	.293562	5
6	.074174	.083918	.094334	.105408	.117123	.129458	.142386	.155881	6
7	.028717	.033509	.038804	.044619	.050966	.057853	.065288	.073273	7
8	.009885	.011905	.014213	.016830	.019777	.023074	.026739	.030789	8
9	.003058	.003803	.004683	.005714	.006912	.008293	.009874	.011671	9
10	.000858	.001102	.001401	.001762	.002195	.002709	.003315	.004024	10
11	.000220	.000292	.000383	.000497	.000638	.000810	.001019	.001271	11
12	.000052	.000071	.000097	.000129	.000171	.000223	.000289	.000370	12
13	.000011	.000016	.000023	.000031	.000042	.000057	.000076	.000100	13
14	.000002	.000003	.000005	.000007	.000010	.000014	.000019	.000025	14
15		.000001	.000001	.000001	.000002	.000003	.000004	.000006	15
16					.000001	.000001	.000001	.000001	16
X	A=3.7	A=3.8	A=3.9	A=4.0	A=4.1	A=4.2	A=4.3	A=4.4	X
0	1.000000	1.000000	1.000000	1.000000	1.000000	1.000000	1.000000	1.000000	0
1	.975276	.977629	.979758	.981684	.983427	.985004	.986431	.987723	1
2	.883799	.892620	.900815	.908422	.915479	.922023	.928087	.933702	2
3	.714567	.731103	.746875	.761897	.776186	.789762	.802645	.814858	3
4	.505847	.526515	.546753	.566590	.585818	.604597	.622846	.640552	4
5	.312781	.332156	.351635	.371163	.390692	.410173	.429562	.448816	5
6	.169912	.184444	.199442	.214870	.230688	.246857	.263338	.280088	6
7	.081809	.090892	.100517	.110674	.121352	.132536	.144210	.156355	7
8	.035241	.040107	.045402	.051134	.057312	.063943	.071032	.078579	8
9	.013703	.015984	.018533	.021363	.024492	.027932	.031698	.035803	9
10	.004848	.005799	.006890	.008132	.009540	.011127	.012906	.014890	10
11	.001572	.001929	.002349	.002840	.003410	.004069	.004825	.005688	11
12	.000470	.000592	.000739	.000915	.001125	.001374	.001666	.002008	12
13	.000130	.000168	.000216	.000274	.000345	.000431	.000534	.000658	13
14	.000034	.000045	.000059	.000076	.000098	.000126	.000160	.000201	14
15	.000008	.000011	.000015	.000020	.000026	.000034	.000045	.000058	15
16	.000002	.000003	.000004	.000005	.000007	.000009	.000012	.000016	16
17		.000001	.000001	.000001	.000002	.000002	.000003	.000004	17
18					.000001	.000001	.000001	.000001	18
X	A=4.5	A=4.6	A=4.7	A=4.8	A=4.9	A=5.0	A=5.1	A=5.2	X
0	1.000000	1.000000	1.000000	1.000000	1.000000	1.000000	1.000000	1.000000	0
1	.988891	.989948	.990905	.991770	.992533	.993262	.993903	.994443	1
2	.938901	.943710	.948157	.952267	.956065	.959572	.962810	.965797	2

TABLE II

X	A=4.5	A=4.6	A=4.7	A=4.8	A=4.9	A=5.0	A=5.1	A=5.2	X
3	.826422	.837361	.847700	.857461	.866669	.875348	.883522	.891213	3
4	.657704	.674294	.690316	.705770	.720655	.734974	.748732	.761935	4
5	.467896	.486766	.505391	.523741	.541788	.559507	.576875	.593872	5
6	.297070	.314240	.331562	.348994	.366499	.384039	.401580	.419087	6
7	.168949	.181971	.195395	.209195	.223345	.237817	.252580	.267607	7
8	.086586	.095051	.103969	.113334	.123138	.133372	.144023	.155078	8
9	.040257	.045072	.050256	.055817	.061761	.068094	.074818	.081935	9
10	.017093	.019527	.022206	.025141	.028345	.031828	.035601	.039674	10
11	.006669	.007777	.009022	.010417	.011971	.013695	.015601	.017699	11
12	.002404	.002863	.003389	.003992	.004677	.005453	.006328	.007310	12
13	.000805	.000979	.001183	.001422	.001699	.002019	.002387	.002809	13
14	.000252	.000312	.000385	.000473	.000576	.000698	.000841	.001008	14
15	.000074	.000093	.000118	.000147	.000183	.000226	.000278	.000339	15
16	.000020	.000026	.000034	.000043	.000055	.000069	.000086	.000108	16
17	.000005	.000007	.000009	.000012	.000015	.000020	.000025	.000032	17
18	.000001	.000002	.000002	.000003	.000004	.000005	.000007	.000009	18
19			.000001	.000001	.000001	.000001	.000002	.000002	19
20								.000001	20

X	A=5.3	A=5.4	A=5.5	A=5.6	A=5.7	A=5.8	A=5.9	A=6.0	X
0	1.000000	1.000000	1.000000	1.000000	1.000000	1.000000	1.000000	1.000000	0
1	.995008	.995483	.995913	.996302	.996654	.996972	.997261	.997521	1
2	.968553	.971094	.973436	.975594	.977582	.979413	.981098	.982649	2
3	.898446	.905242	.911624	.917612	.923227	.928489	.933418	.938031	3
4	.774590	.786709	.798301	.809378	.819952	.830037	.839647	.848796	4
5	.610482	.626689	.642482	.657850	.672785	.687282	.701335	.714943	5
6	.436527	.453868	.471081	.488139	.505015	.521685	.538127	.554320	6
7	.282866	.298329	.313964	.329742	.345634	.361609	.377639	.393697	7
8	.166523	.178341	.190515	.203025	.215851	.228974	.242371	.256020	8
9	.089446	.097350	.105643	.114322	.123382	.132814	.142611	.152763	9
10	.044056	.048755	.053777	.059130	.064817	.070844	.077212	.083924	10
11	.020000	.022514	.025251	.028222	.031436	.034901	.038627	.042621	11
12	.008049	.009632	.011388	.013247	.015138	.017050	.019031	.022092	12
13	.003289	.003835	.004451	.005144	.005922	.006790	.007756	.008827	13
14	.001202	.001427	.001685	.001981	.002319	.002703	.003138	.003626	14
15	.000412	.000498	.000599	.000716	.000852	.001010	.001192	.001400	15
16	.000133	.000164	.000200	.000244	.000295	.000356	.000426	.000509	16
17	.000041	.000051	.000063	.000078	.000096	.000118	.000144	.000175	17
18	.000012	.000015	.000019	.000024	.000030	.000037	.000046	.000057	18
19	.000003	.000004	.000005	.000007	.000009	.000011	.000014	.000018	19
20	.000001	.000001	.000001	.000002	.000002	.000003	.000004	.000005	20
21					.000001	.000001	.000001	.000001	21

X	A=6.1	A=6.2	A=6.3	A=6.4	A=6.5	A=6.6	A=6.7	A=6.8	X
0	1.000000	1.000000	1.000000	1.000000	1.000000	1.000000	1.000000	1.000000	0
1	.997757	.997971	.998164	.998338	.998497	.998640	.998769	.998886	1
2	.984076	.985388	.986595	.987704	.988724	.989661	.990522	.991313	2
3	.942347	.946382	.950154	.953676	.956964	.960032	.962894	.965562	3
4	.857499	.865771	.873626	.881081	.888150	.894849	.901192	.907194	4
5	.728106	.740823	.753096	.764930	.776328	.787296	.797841	.807969	5
6	.570246	.585887	.601228	.616256	.630959	.645327	.659351	.673023	6
7	.409755	.425787	.441767	.457671	.473476	.489161	.504703	.520084	7
8	.269899	.283984	.298252	.312679	.327242	.341918	.356683	.371514	8
9	.163258	.174086	.185233	.196685	.208427	.220443	.232716	.245230	9
10	.090980	.098379	.106121	.114201	.122616	.131361	.140430	.149816	10
11	.046890	.051441	.056280	.061411	.066839	.072567	.078598	.084934	11
12	.022440	.024985	.027734	.030697	.033880	.037291	.040937	.044825	12
13	.010012	.011316	.012748	.014316	.016027	.017889	.019910	.022097	13
14	.004180	.004797	.005485	.006251	.007100	.008038	.009072	.010208	14
15	.001639	.001910	.002217	.002565	.002956	.003395	.003886	.004434	15
16	.000605	.000716	.000844	.000992	.001160	.001352	.001569	.001816	16
17	.000211	.000254	.000304	.000362	.000430	.000509	.000599	.000703	17
18	.000070	.000085	.000104	.000126	.000151	.000182	.000217	.000258	18
19	.000022	.000027	.000034	.000041	.000051	.000062	.000075	.000090	19
20	.000007	.000008	.000010	.000013	.000016	.000020	.000024	.000030	20

TABLE II

X	A=6.1	A=6.2	A=6.3	A=6.4	A=6.5	A=6.6	A=6.7	A=6.8	X
21	.000002	.000002	.000003	.000004	.000005	.000006	.000008	.000010	21
22	.000001	.000001	.000001	.000001	.000001	.000002	.000002	.000003	22
23						.000001	.000001	.000001	23
X	A=6.9	A=7.0	A=7.1	A=7.2	A=7.3	A=7.4	A=7.5	A=7.6	X
0	1.000000	1.000000	1.000000	1.000000	1.000000	1.000000	1.000000	1.000000	0
1	.998992	.999088	.999175	.999253	.999324	.999389	.999447	.999500	1
2	.992038	.992005	.993317	.993878	.994393	.994865	.995299	.995696	2
3	.968048	.970364	.972520	.974526	.976393	.978129	.979743	.981243	3
4	.912870	.918235	.923301	.928083	.932594	.936847	.940855	.944629	4
5	.817689	.827008	.835937	.844484	.852660	.860475	.867938	.875061	5
6	.686338	.699292	.711881	.724103	.735957	.747443	.758564	.769319	6
7	.535285	.550289	.565080	.579644	.593968	.608038	.621845	.635379	7
8	.386389	.401286	.416183	.431059	.445893	.460667	.475361	.489958	8
9	.257967	.270909	.284036	.297332	.310776	.324349	.338033	.351808	9
10	.150510	.169504	.179788	.190330	.201180	.212265	.223592	.235149	10
11	.091575	.098521	.105771	.113323	.121175	.129323	.137762	.146487	11
12	.048961	.053350	.057997	.062906	.068081	.073526	.079241	.085230	12
13	.024458	.027000	.029730	.032655	.035782	.039117	.042666	.046434	13
14	.011452	.012811	.014292	.015901	.017645	.019531	.021565	.023753	14
15	.005042	.005717	.006463	.007285	.008188	.009178	.010260	.011441	15
16	.002094	.002407	.002757	.003149	.003586	.004071	.004608	.005202	16
17	.000822	.000958	.001113	.001288	.001486	.001709	.001959	.002239	17
18	.000306	.000362	.000426	.000500	.000584	.000680	.000790	.000915	18
19	.000108	.000130	.000155	.000184	.000218	.000258	.000303	.000355	19
20	.000037	.000044	.000054	.000065	.000078	.000093	.000111	.000132	20
21	.000012	.000014	.000018	.000022	.000026	.000032	.000039	.000046	21
22	.000004	.000005	.000006	.000007	.000009	.000011	.000013	.000016	22
23	.000001	.000001	.000002	.000002	.000003	.000003	.000004	.000005	23
24				.000001	.000001	.000001	.000001	.000002	24
X	A=7.7	A=7.8	A=7.9	A=8.0	A=8.1	A=8.2	A=8.3	A=8.4	X
0	1.000000	1.000000	1.000000	1.000000	1.000000	1.000000	1.000000	1.000000	0
1	.999547	.999590	.999629	.999665	.999696	.999725	.999751	.999775	1
2	.996060	.996394	.996700	.996981	.997238	.997473	.997689	.997886	2
3	.982636	.983930	.985131	.986246	.987280	.988239	.989129	.989953	3
4	.948181	.951523	.954666	.957620	.960395	.963000	.965446	.967740	4
5	.881855	.888330	.894497	.900368	.905951	.911260	.916303	.921092	5
6	.779713	.789749	.799431	.808764	.817753	.826406	.834727	.842723	6
7	.648631	.661593	.674260	.686626	.698686	.710438	.721879	.733007	7
8	.504440	.518791	.532996	.547039	.560908	.574591	.588074	.601348	8
9	.365657	.379559	.393497	.407453	.421408	.435347	.449252	.463106	9
10	.246920	.258891	.271048	.283376	.295858	.308481	.321226	.334080	10
11	.155492	.164770	.174314	.184114	.194163	.204450	.214965	.225699	11
12	.091493	.098800	.104841	.111924	.119278	.126900	.134787	.142934	12
13	.050427	.054649	.059104	.063797	.068731	.073907	.079330	.084999	13
14	.026103	.028620	.031311	.034181	.037236	.040481	.043923	.047564	14
15	.012725	.014118	.015627	.017257	.019014	.020903	.022931	.025103	15
16	.005857	.006577	.007367	.008231	.009174	.010201	.011316	.012525	16
17	.002552	.002901	.003289	.003718	.004192	.004715	.005291	.005922	17
18	.001055	.001215	.001393	.001594	.001819	.002070	.002349	.002659	18
19	.000415	.000484	.000562	.000650	.000751	.000864	.000992	.001136	19
20	.000156	.000184	.000216	.000253	.000296	.000344	.000400	.000463	20
21	.000056	.000067	.000079	.000094	.000111	.000131	.000154	.000180	21
22	.000019	.000023	.000028	.000033	.000040	.000048	.000057	.000067	22
23	.000006	.000008	.000009	.000011	.000014	.000017	.000020	.000024	23
24	.000002	.000002	.000003	.000004	.000005	.000006	.000007	.000008	24
25	.000001	.000001	.000001	.000001	.000001	.000002	.000002	.000003	25
26						.000001	.000001	.000001	26
X	A=8.5	A=8.6	A=8.7	A=8.8	A=8.9	A=9.0	A=9.1	A=9.2	X
0	1.000000	1.000000	1.000000	1.000000	1.000000	1.000000	1.000000	1.000000	0
1	.999797	.999816	.999833	.999849	.999864	.999877	.999888	.999899	1
2	.998067	.998233	.998384	.998523	.998650	.998766	.998872	.998969	2
3	.990717	.991424	.992080	.992686	.993248	.993768	.994249	.994693	3
4	.969891	.971907	.973797	.975566	.977223	.978774	.980224	.981580	4

TABLE II

X	A=8.5	A=8.6	A=8.7	A=8.8	A=8.9	A=9.0	A=9.1	A=9.2	X
5	.925636	.929946	.934032	.937902	.941567	.945036	.948318	.951420	5
6	.850403	.857772	.864840	.871613	.878100	.884309	.890249	.895926	6
7	.743822	.754324	.764512	.774390	.783958	.793319	.802177	.810835	7
8	.614403	.627229	.639819	.652166	.664262	.676103	.687684	.699000	8
9	.476895	.490603	.504216	.517719	.531101	.544347	.557448	.570391	9
10	.347026	.360049	.373132	.386260	.399419	.412592	.425765	.438924	10
11	.236638	.247772	.259089	.270577	.282222	.294012	.305933	.317974	11
12	.151338	.159922	.168892	.178030	.187399	.196992	.206800	.216815	12
13	.090917	.097084	.103499	.110162	.117072	.124227	.131624	.139261	13
14	.051411	.055467	.059736	.064221	.068925	.073851	.079001	.084376	14
15	.027425	.029902	.032540	.035343	.038317	.041466	.044795	.048309	15
16	.013833	.015245	.016767	.018402	.020157	.022036	.024044	.026188	16
17	.006613	.007367	.008190	.009084	.010055	.011106	.012242	.013468	17
18	.003002	.003382	.003800	.004261	.004766	.005320	.005924	.006584	18
19	.001297	.001478	.001679	.001903	.002151	.002426	.002731	.003066	19
20	.000535	.000616	.000707	.000811	.000926	.001056	.001201	.001362	20
21	.000211	.000245	.000285	.000330	.000381	.000439	.000505	.000579	21
22	.000079	.000094	.000110	.000129	.000150	.000175	.000203	.000235	22
23	.000029	.000034	.000041	.000048	.000057	.000067	.000078	.000092	23
24	.000010	.000012	.000014	.000017	.000021	.000025	.000029	.000034	24
25	.000003	.000004	.000005	.000006	.000007	.000009	.000010	.000012	25
26	.000001	.000001	.000002	.000002	.000002	.000003	.000004	.000004	26
27			.000001	.000001	.000001	.000001	.000001	.000001	27
X	A=9.3	A=9.4	A=9.5	A=9.6	A=9.7	A=9.8	A=9.9	A=10.0	X
0	1.000000	1.000000	1.000000	1.000000	1.000000	1.000000	1.000000	1.000000	0
1	.999909	.999917	.999925	.999932	.999939	.999945	.999950	.999955	1
2	.999058	.999140	.999214	.999282	.999344	.999401	.999453	.999501	2
3	.995105	.995485	.995836	.996161	.996461	.996738	.996994	.997231	3
4	.982848	.984033	.985140	.986174	.987139	.988040	.988880	.989664	4
5	.954353	.957122	.959737	.962205	.964533	.966729	.968798	.970747	5
6	.901350	.906529	.911472	.916185	.920678	.924959	.929035	.932914	6
7	.819197	.827267	.835051	.842553	.849779	.856735	.863426	.869859	7
8	.710050	.720829	.731337	.741572	.751533	.761221	.770636	.779779	8
9	.583166	.595765	.608177	.620394	.632410	.644217	.655809	.667180	9
10	.452054	.465142	.478174	.491138	.504021	.516812	.529498	.542070	10
11	.330119	.342356	.354672	.367052	.379484	.391955	.404451	.416960	11
12	.227029	.237430	.248010	.258759	.269665	.280719	.291909	.303224	12
13	.147133	.155238	.163570	.172124	.180895	.189876	.199062	.208444	13
14	.089978	.095807	.101864	.108148	.114659	.121395	.128355	.135536	14
15	.052010	.055903	.059992	.064279	.068767	.073458	.078355	.083458	15
16	.028470	.030897	.033473	.036202	.039090	.042139	.045355	.048740	16
17	.014788	.016206	.017727	.019357	.021098	.022956	.024936	.027042	17
18	.007302	.008083	.008928	.009844	.010832	.011898	.013045	.014278	18
19	.003435	.003840	.004284	.004770	.005300	.005877	.006505	.007187	19
20	.001542	.001742	.001962	.002207	.002476	.002772	.003098	.003454	20
21	.000662	.000755	.000859	.000976	.001106	.001250	.001411	.001588	21
22	.000272	.000314	.000361	.000414	.000473	.000540	.000616	.000700	22
23	.000107	.000125	.000145	.000168	.000194	.000224	.000258	.000296	23
24	.000041	.000048	.000056	.000066	.000077	.000089	.000104	.000120	24
25	.000015	.000018	.000021	.000025	.000029	.000034	.000040	.000047	25
26	.000005	.000006	.000007	.000009	.000011	.000013	.000015	.000018	26
27	.000002	.000002	.000003	.000003	.000004	.000004	.000005	.000006	27
28	.000001	.000001	.000001	.000001	.000001	.000002	.000002	.000002	28
29						.000001	.000001	.000001	29
X	A=10.1	A=10.2	A=10.3	A=10.4	A=10.5	A=10.6	A=10.7	A=10.8	X
0	1.000000	1.000000	1.000000	1.000000	1.000000	1.000000	1.000000	1.000000	0
1	.999959	.999963	.999966	.999970	.999972	.999975	.999977	.999980	1
2	.999544	.999584	.999620	.999653	.999683	.999711	.999736	.999759	2
3	.997449	.997650	.997836	.998007	.998165	.998311	.998446	.998570	3
4	.990395	.991076	.991711	.992302	.992853	.993365	.993843	.994287	4
5	.972583	.974312	.975938	.977468	.978906	.980259	.981529	.982723	5
6	.936604	.940112	.943446	.946613	.949620	.952473	.955179	.957745	6
7	.876039	.881974	.887669	.893131	.898367	.903384	.908187	.912784	7
8	.788652	.797257	.805597	.813673	.821489	.829050	.836358	.843417	8
9	.678327	.689244	.699928	.710377	.720587	.730557	.740285	.749771	9

TABLE II

X	A=10.1	A=10.2	A=10.3	A=10.4	A=10.5	A=10.6	A=10.7	A=10.8	X
10	.554517	.566829	.578997	.591013	.602867	.614554	.626066	.637396	10
11	.429469	.441966	.454438	.466874	.479262	.491591	.503851	.516031	11
12	.314652	.326183	.337805	.349506	.361275	.373100	.384969	.396872	12
13	.218015	.227768	.237695	.247787	.258036	.268432	.278966	.289630	13
14	.142935	.150550	.158378	.166413	.174651	.183088	.191718	.200536	14
15	.088770	.094292	.100022	.105963	.112112	.118470	.125035	.131806	15
16	.052300	.056036	.059952	.064051	.068335	.072807	.077468	.082321	16
17	.029277	.031647	.034156	.036808	.039606	.042555	.045658	.048918	17
18	.015599	.017015	.018527	.020142	.021862	.023692	.025636	.027698	18
19	.007925	.008723	.009584	.010512	.011511	.012584	.013734	.014965	19
20	.003845	.004271	.004736	.005242	.005791	.006387	.007031	.007728	20
21	.001784	.002001	.002239	.002501	.002788	.003102	.003445	.003820	21
22	.000794	.000898	.001014	.001143	.001286	.001444	.001618	.001810	22
23	.000339	.000387	.000441	.000502	.000570	.000645	.000730	.000823	23
24	.000139	.000160	.000184	.000212	.000242	.000277	.000316	.000360	24
25	.000055	.000064	.000074	.000086	.000099	.000115	.000132	.000152	25
26	.000021	.000024	.000029	.000034	.000039	.000046	.000053	.000061	26
27	.000008	.000009	.000011	.000013	.000015	.000018	.000021	.000024	27
28	.000003	.000003	.000004	.000005	.000005	.000007	.000008	.000009	28
29	.000001	.000001	.000001	.000002	.000002	.000002	.000003	.000003	29
30				.000001	.000001	.000001	.000001	.000001	30
X	A=10.9	A=11.0	A=11.1	A=11.2	A=11.3	A=11.4	A=11.5	A=11.6	X
0	1.000000	1.000000	1.000000	1.000000	1.000000	1.000000	1.000000	1.000000	0
1	.999982	.999983	.999985	.999986	.999988	.999989	.999990	.999991	1
2	.999780	.999800	.999817	.999833	.999848	.999861	.999873	.999885	2
3	.998684	.998789	.998886	.998976	.999058	.999134	.999203	.999268	3
4	.994700	.995084	.995441	.995774	.996082	.996369	.996636	.996883	4
5	.983843	.984895	.985882	.986808	.987677	.988491	.989253	.989968	5
6	.960177	.962480	.964661	.966726	.968680	.970527	.972274	.973925	6
7	.917182	.921386	.925403	.929239	.932902	.936397	.939730	.942908	7
8	.850233	.856808	.863150	.869261	.875147	.880814	.886265	.891508	8
9	.759014	.768015	.776773	.785290	.793568	.801607	.809410	.816979	9
10	.648539	.659489	.670243	.680794	.691141	.701279	.711205	.720919	10
11	.528121	.540111	.551993	.563758	.575398	.586904	.598270	.609489	11
12	.408797	.420733	.432669	.444595	.456499	.468371	.480202	.491982	12
13	.300412	.311303	.322294	.333375	.344535	.355764	.367053	.378391	13
14	.209535	.218709	.228051	.237555	.247213	.257017	.266960	.277033	14
15	.138780	.145956	.153330	.160899	.168660	.176608	.184740	.193051	15
16	.087366	.092604	.098036	.103663	.109483	.115498	.121705	.128104	16
17	.052339	.055924	.059676	.063597	.067690	.071957	.076399	.081018	17
18	.029881	.032191	.034629	.037201	.039910	.042758	.045750	.048889	18
19	.016282	.017687	.019184	.020777	.022470	.024266	.026169	.028183	19
20	.008480	.009289	.010160	.011095	.012098	.013171	.014318	.015542	20
21	.004228	.004671	.005152	.005673	.006237	.006846	.007503	.008210	21
22	.002021	.002252	.002505	.002782	.003084	.003413	.003771	.004160	22
23	.000927	.001042	.001170	.001310	.001464	.001634	.001821	.002025	23
24	.000409	.000464	.000525	.000593	.000669	.000752	.000845	.000948	24
25	.000174	.000199	.000227	.000258	.000294	.000334	.000378	.000427	25
26	.000071	.000082	.000094	.000109	.000125	.000143	.000163	.000186	26
27	.000028	.000033	.000038	.000044	.000051	.000059	.000068	.000078	27
28	.000011	.000013	.000015	.000017	.000020	.000023	.000027	.000032	28
29	.000004	.000005	.000006	.000007	.000008	.000009	.000011	.000012	29
30	.000001	.000002	.000002	.000002	.000003	.000003	.000004	.000005	30
31		.000001	.000001	.000001	.000001	.000001	.000001	.000002	31
32						.000001	.000001	.000001	32
X	A=11.7	A=11.8	A=11.9	A=12.0	A=12.1	A=12.2	A=12.3	A=12.4	X
0	1.000000	1.000000	1.000000	1.000000	1.000000	1.000000	1.000000	1.000000	0
1	.999992	.999992	.999993	.999994	.999994	.999995	.999995	.999996	1
2	.999895	.999904	.999912	.999920	.999927	.999934	.999939	.999945	2
3	.999327	.999381	.999432	.999478	.999520	.999559	.999595	.999628	3
4	.997113	.997326	.997524	.997708	.997879	.998037	.998183	.998319	4
5	.990637	.991264	.991851	.992400	.992913	.993393	.993842	.994262	5
6	.975484	.976957	.978347	.979659	.980897	.982064	.983164	.984200	6
7	.945936	.948819	.951565	.954178	.956663	.959026	.961272	.963406	7

TABLE II

X	A=11.7	A=11.8	A=11.9	A=12.0	A=12.1	A=12.2	A=12.3	A=12.4	X
8	.896547	.901388	.906035	.910496	.914774	.918875	.922806	.926570	8
9	.824317	.831426	.838310	.844972	.851416	.857645	.863663	.869475	9
10	.730417	.739698	.748762	.757608	.766235	.774644	.780835	.790810	10
11	.620554	.631460	.642200	.652771	.663166	.673383	.683417	.693266	11
12	.503700	.515349	.526920	.538403	.549790	.561075	.572250	.583307	12
13	.389768	.401174	.412600	.424035	.435470	.446896	.458303	.469682	13
14	.287228	.296538	.307953	.318464	.329064	.339743	.350492	.361302	14
15	.201535	.210188	.219003	.227975	.237099	.246366	.255772	.265308	15
16	.134694	.141472	.148436	.155584	.162913	.170420	.178101	.185953	16
17	.085816	.090794	.095952	.101291	.106811	.112511	.118392	.124453	17
18	.052177	.055618	.059213	.062966	.066879	.070953	.075191	.079594	18
19	.030312	.032558	.034925	.037417	.040036	.042786	.045670	.048691	19
20	.016847	.018236	.019713	.021280	.022941	.024700	.026559	.028523	20
21	.008970	.009786	.010661	.011598	.012599	.013667	.014806	.016019	21
22	.004582	.005039	.005532	.006065	.006640	.007258	.007922	.008635	22
23	.002248	.002492	.002758	.003047	.003362	.003703	.004073	.004474	23
24	.001061	.001185	.001322	.001473	.001638	.001818	.002015	.002230	24
25	.000482	.000543	.000611	.000686	.000768	.000860	.000960	.001071	25
26	.000211	.000240	.000272	.000308	.000348	.000392	.000441	.000496	26
27	.000089	.000102	.000117	.000133	.000152	.000173	.000196	.000222	27
28	.000036	.000042	.000049	.000056	.000064	.000073	.000084	.000096	28
29	.000014	.000017	.000020	.000023	.000026	.000030	.000035	.000040	29
30	.000006	.000006	.000008	.000009	.000010	.000012	.000014	.000016	30
31	.000002	.000002	.000003	.000003	.000004	.000005	.000005	.000006	31
32	.000001	.000001	.000001	.000001	.000001	.000002	.000002	.000002	32
33					.000001	.000001	.000001	.000001	33
X	A=12.5	A=12.6	A=12.7	A=12.8	A=12.9	A=13.0	A=13.1	A=13.2	X
0	1.000000	1.000000	1.000000	1.000000	1.000000	1.000000	1.000000	1.000000	0
1	.999996	.999997	.999997	.999997	.999997	.999998	.999998	.999998	1
2	.999950	.999954	.999958	.999962	.999965	.999968	.999971	.999974	2
3	.999659	.999686	.999712	.999736	.999757	.999777	.999796	.999812	3
4	.998445	.998562	.998670	.998771	.998864	.998950	.999029	.999103	4
5	.994655	.995021	.995363	.995683	.995981	.996260	.996520	.996762	5
6	.985177	.986097	.986963	.987778	.988545	.989266	.989944	.990582	6
7	.965433	.967356	.969182	.970914	.972556	.974113	.975588	.976986	7
8	.930175	.933624	.936923	.940077	.943092	.945972	.948722	.951347	8
9	.875084	.880494	.885711	.890738	.895580	.900242	.904728	.909042	9
10	.798569	.806114	.813446	.820567	.827481	.834188	.840692	.846996	10
11	.702925	.712394	.721669	.730749	.739632	.748318	.756806	.765095	11
12	.594239	.605042	.615708	.626232	.636609	.646835	.656905	.666814	12
13	.481025	.492322	.503566	.514748	.525860	.536895	.547846	.558705	13
14	.372165	.383071	.394012	.404979	.415963	.426955	.437948	.448932	14
15	.274968	.284745	.294631	.304619	.314700	.324868	.335115	.345432	15
16	.193971	.202151	.210488	.218978	.227615	.236393	.245308	.254353	16
17	.130692	.137108	.143700	.150465	.157402	.164507	.171778	.179212	17
18	.084163	.088900	.093805	.098879	.104122	.109535	.115117	.120867	18
19	.051852	.055154	.058602	.062196	.065939	.069833	.073880	.078081	19
20	.030594	.032776	.035071	.037483	.040014	.042669	.045448	.048356	20
21	.017308	.018677	.020129	.021667	.023293	.025012	.026826	.028737	21
22	.009400	.010218	.011093	.012026	.013021	.014081	.015208	.016406	22
23	.004906	.005373	.005876	.006417	.006999	.007622	.008291	.009007	23
24	.002464	.002719	.002996	.003290	.003620	.003992	.004351	.004760	24
25	.001192	.001326	.001471	.001631	.001805	.001994	.002201	.002425	25
26	.000557	.000623	.000697	.000778	.000868	.000966	.001074	.001192	26
27	.000251	.000283	.000319	.000359	.000403	.000452	.000506	.000566	27
28	.000109	.000124	.000141	.000160	.000181	.000204	.000230	.000260	28
29	.000046	.000053	.000060	.000069	.000079	.000089	.000102	.000115	29
30	.000019	.000022	.000025	.000029	.000033	.000038	.000043	.000050	30
31	.000007	.000009	.000010	.000012	.000013	.000016	.000018	.000021	31
32	.000003	.000003	.000004	.000005	.000005	.000006	.000007	.000008	32
33	.000001	.000001	.000001	.000002	.000002	.000002	.000003	.000003	33
34			.000001	.000001	.000001	.000001	.000001	.000001	34
X	A=13.3	A=13.4	A=13.5	A=13.6	A=13.7	A=13.8	A=13.9	A=14.0	X
0	1.000000	1.000000	1.000000	1.000000	1.000000	1.000000	1.000000	1.000000	0

TABLE 11

X	A=13.3	A=13.4	A=13.5	A=13.6	A=13.7	A=13.8	A=13.9	A=14.0	X
1	.999998	.999999	.999999	.999999	.999999	.999999	.999999	.999999	1
2	.999976	.999978	.999980	.999982	.999983	.999985	.999986	.999988	2
3	.999828	.999842	.999855	.999867	.999878	.999888	.999898	.999906	3
4	.999171	.999235	.999293	.999347	.999397	.999443	.999486	.999526	4
5	.996988	.997199	.997396	.997579	.997750	.997909	.998057	.998195	5
6	.991181	.991744	.992273	.992769	.993235	.993673	.994083	.994468	6
7	.978309	.979561	.980746	.981868	.982928	.983930	.984877	.985772	7
8	.953851	.956240	.958517	.960687	.962754	.964723	.966597	.968380	8
9	.913190	.917176	.921005	.924680	.928207	.931591	.934835	.937945	9
10	.853103	.859015	.864736	.870270	.875619	.880788	.885781	.890601	10
11	.773186	.781079	.788774	.796271	.803574	.810681	.817596	.824319	11
12	.676560	.686138	.695547	.704783	.713844	.722728	.731434	.739960	12
13	.569465	.580122	.590667	.601096	.611402	.621582	.631630	.641542	13
14	.459900	.470843	.481753	.492623	.503445	.514212	.524917	.535552	14
15	.355812	.366247	.376729	.387249	.397801	.408376	.418966	.429563	15
16	.263522	.272809	.282207	.291711	.301313	.311006	.320784	.330640	16
17	.186805	.194554	.202455	.210503	.218695	.227025	.235489	.244082	17
18	.126785	.132871	.139122	.145537	.152114	.158852	.165748	.172799	18
19	.082438	.086951	.091622	.096451	.101439	.106586	.111892	.117357	19
20	.051394	.054565	.057872	.061316	.064900	.068624	.072492	.076505	20
21	.030750	.032867	.035091	.037424	.039870	.042431	.045110	.047908	21
22	.017676	.019022	.020446	.021951	.023541	.025218	.026985	.028844	22
23	.009772	.011588	.013459	.015386	.017373	.019421	.021533	.023712	23
24	.005201	.005675	.006184	.006731	.007316	.007943	.008613	.009328	24
25	.002668	.002932	.003217	.003526	.003859	.004218	.004604	.005020	25
26	.001321	.001461	.001615	.001782	.001964	.002161	.002376	.002608	26
27	.000631	.000704	.000783	.000870	.000966	.001070	.001184	.001309	27
28	.000292	.000328	.000367	.000411	.000459	.000512	.000571	.000635	28
29	.000131	.000148	.000167	.000188	.000211	.000237	.000266	.000298	29
30	.000057	.000064	.000073	.000083	.000094	.000107	.000120	.000136	30
31	.000024	.000027	.000031	.000036	.000041	.000046	.000053	.000060	31
32	.000010	.000011	.000013	.000015	.000017	.000020	.000022	.000026	32
33	.000004	.000004	.000005	.000006	.000007	.000008	.000009	.000011	33
34	.000001	.000002	.000002	.000002	.000003	.000003	.000004	.000004	34
35	.000001	.000001	.000001	.000001	.000001	.000001	.000001	.000002	35
36							.000001	.000001	36
X	A=14.1	A=14.2	A=14.3	A=14.4	A=14.5	A=14.6	A=14.7	A=14.8	X
0	1.000000	1.000000	1.000000	1.000000	1.000000				0
1	.999999	.999999	.999999	.999999	.999999	1.000000	1.000000	1.000000	1
2	.999989	.999990	.999991	.999991	.999992	.999993	.999993	.999994	2
3	.999914	.999921	.999928	.999934	.999939	.999944	.999949	.999953	3
4	.999562	.999596	.999627	.999656	.999683	.999708	.999730	.999751	4
5	.998323	.998443	.998554	.998658	.998754	.998844	.998927	.999004	5
6	.994829	.995167	.995484	.995782	.996060	.996321	.996565	.996793	6
7	.986617	.987415	.988168	.988879	.989550	.990182	.990778	.991340	7
8	.970777	.971690	.972623	.973468	.974264	.975011	.975726	.976410	8
9	.940924	.943777	.946508	.949121	.951621	.954011	.956296	.958418	9
10	.895251	.899736	.904061	.908227	.912241	.916105	.919823	.923400	10
11	.830853	.837199	.843361	.849340	.855139	.860761	.866209	.871485	11
12	.748305	.756469	.764451	.772251	.779869	.787305	.794563	.801635	12
13	.651312	.660939	.670417	.679745	.688918	.697934	.706791	.715487	13
14	.546112	.556590	.566980	.577276	.587472	.597563	.607545	.617411	14
15	.440161	.450751	.461326	.471879	.482403	.492891	.503336	.513731	15
16	.340567	.350557	.360603	.370699	.380837	.391010	.401211	.411432	16
17	.252799	.261634	.270582	.279636	.288792	.298043	.307383	.316807	17
18	.180004	.187357	.194858	.202501	.210284	.218201	.226250	.234426	18
19	.122980	.128761	.134699	.140793	.147040	.153441	.159992	.166692	19
20	.080663	.084969	.089422	.094024	.098776	.103677	.108729	.113930	20
21	.050830	.053876	.057049	.060351	.063784	.067350	.071050	.074886	21
22	.030799	.032851	.035004	.037261	.039623	.042094	.044675	.047370	22
23	.017960	.019281	.020675	.022147	.023699	.025333	.027052	.028859	23
24	.010090	.010902	.011767	.012685	.013660	.014694	.015788	.016947	24
25	.005466	.005945	.006458	.007007	.007594	.008221	.008890	.009602	25
26	.002859	.003130	.003422	.003737	.004077	.004441	.004833	.005253	26
27	.001444	.001592	.001752	.001926	.002115	.002319	.002539	.002778	27
28	.000706	.000783	.000868	.000960	.001061	.001171	.001291	.001421	28

TABLE II

X	A=14.1	A=14.2	A=14.3	A=14.4	A=14.5	A=14.6	A=14.7	A=14.8	X
29	.000334	.000373	.000416	.000463	.000515	.000573	.000635	.000704	29
30	.000153	.000172	.000193	.000217	.000243	.000271	.000303	.000338	30
31	.000068	.000077	.000087	.000098	.000111	.000125	.000140	.000157	31
32	.000029	.000033	.000038	.000043	.000049	.000056	.000063	.000071	32
33	.000012	.000014	.000016	.000018	.000021	.000024	.000027	.000031	33
34	.000005	.000006	.000007	.000008	.000009	.000010	.000012	.000013	34
35	.000002	.000002	.000003	.000003	.000004	.000004	.000005	.000006	35
36	.000001	.000001	.000001	.000001	.000001	.000002	.000002	.000002	36
37					.000001	.000001	.000001	.000001	37
X	A=14.9	A=15.0	A=16	A=17	A=18	A=19	A=20	A=21	X
1	1.000000	1.000000	1.000000	1.000000					1
2	.999995	.999995	.999998	.999999	1.000000	1.000000			2
3	.999957	.999961	.999984	.999993	.999997	.999999	1.000000	1.000000	3
4	.999771	.999789	.999907	.999959	.999982	.999992	.999997	.999999	4
5	.999076	.999143	.999600	.999815	.999916	.999962	.999983	.999993	5
6	.997007	.997208	.998616	.999325	.999676	.999846	.999928	.999967	6
7	.991869	.992368	.995994	.997938	.998957	.999480	.999745	.999876	7
8	.980933	.981998	.990000	.994567	.997107	.998487	.999221	.999605	8
9	.960563	.962554	.978013	.987404	.992944	.996127	.997913	.998894	9
10	.926840	.930146	.956702	.973875	.984619	.991144	.995005	.997234	10
11	.876593	.881536	.922604	.950876	.969634	.981678	.989188	.993749	11
12	.808531	.815248	.873007	.915331	.945113	.965327	.978613	.987095	12
13	.724020	.732389	.806878	.864976	.908331	.939439	.960988	.975451	13
14	.627158	.636782	.725489	.799127	.857402	.901601	.933872	.956641	14
15	.524070	.534346	.632473	.719167	.791923	.850250	.895136	.928426	15
16	.421668	.431910	.533255	.628546	.713347	.785206	.843487	.888925	16
17	.326306	.335877	.434038	.532262	.624950	.707966	.778926	.837081	17
18	.242725	.251141	.340656	.435977	.531352	.621639	.702972	.773037	18
19	.173538	.180528	.257651	.345042	.437755	.530516	.618578	.698320	19
20	.119281	.124781	.187751	.263678	.349084	.439393	.529743	.615737	20
21	.078859	.082971	.131832	.194519	.269280	.352826	.440907	.529026	21
22	.050179	.053106	.089227	.138534	.200876	.274503	.356302	.442314	22
23	.030755	.032744	.058241	.095272	.144910	.206861	.279389	.359544	23
24	.018172	.019465	.036686	.063296	.101110	.150983	.212507	.283971	24
25	.010359	.011165	.022315	.040646	.068260	.106746	.156773	.217845	25
26	.005703	.006185	.013119	.025245	.044608	.073126	.112185	.162299	26
27	.003035	.003312	.007459	.015174	.028234	.048857	.077887	.117435	27
28	.001562	.001716	.004105	.008834	.017318	.031268	.052481	.082541	28
29	.000779	.000861	.002189	.004984	.010300	.019536	.034334	.056370	29
30	.000376	.000418	.001131	.002727	.005944	.011850	.021818	.037419	30
31	.000176	.000197	.000567	.001448	.003331	.006982	.013475	.024153	31
32	.000080	.000090	.000276	.000747	.001813	.003998	.008092	.015166	32
33	.000035	.000040	.000131	.000375	.000960	.002227	.004727	.009269	33
34	.000015	.000017	.000060	.000185	.000494	.001207	.002688	.005516	34
35	.000006	.000007	.000027	.000087	.000248	.000637	.001489	.003198	35
36	.000003	.000003	.000012	.000040	.000121	.000327	.000804	.001807	36
37	.000001	.000001	.000005	.000018	.000058	.000164	.000423	.000996	37
38			.000002	.000008	.000027	.000080	.000217	.000536	38
39			.000001	.000003	.000012	.000038	.000109	.000281	39
40				.000001	.000005	.000018	.000053	.000144	40
41				.000001	.000002	.000008	.000025	.000072	41
42					.000001	.000004	.000012	.000035	42
43						.000002	.000005	.000017	43
44						.000001	.000002	.000008	44
45							.000001	.000004	45
46								.000002	46
47								.000001	47
X	A=22	A=23	A=24	A=25	A=26	A=27	A=28	A=29	X
3	1.000000								3
4	.999999	1.000000	1.000000						4
5	.999997	.999999	.999999	1.000000	1.000000				5
6	.999985	.999993	.999997	.999999	.999999	1.000000	1.000000		6
7	.999941	.999972	.999987	.999994	.999997	.999999	.999999	1.000000	7



TABLE II

X	A=22	A=23	A=24	A=25	A=26	A=27	A=28	A=29	X
8	•999803	•999903	•999953	•999977	•999989	•999995	•999998	•999999	8
9	•999423	•999703	•999849	•999925	•999963	•999982	•999991	•999996	9
10	•998495	•999194	•999575	•999779	•999886	•999942	•999971	•999986	10
11	•996453	•998023	•988513	•999414	•999687	•999836	•999914	•999956	11
12	•992370	•995573	•997476	•998584	•999218	•999574	•999771	•999878	12
13	•984884	•990878	•994598	•998856	•998200	•998985	•999436	•999690	13
14	•972215	•982572	•989284	•993533	•996164	•997762	•998714	•999271	14
15	•952307	•968926	•980175	•987598	•992383	•995403	•997270	•998403	15
16	•923108	•948002	•965600	•977707	•985830	•991156	•994574	•996725	16
17	•882960	•917923	•943728	•962252	•975182	•983991	•989857	•993682	17
18	•831004	•877229	•912874	•939525	•958895	•972610	•982088	•988492	18
19	•767502	•825231	•871721	•907959	•935371	•955539	•970003	•980131	19
20	•693973	•762286	•819739	•866425	•903179	•931281	•952193	•967369	20
21	•613091	•689900	•757361	•814508	•861330	•898532	•927259	•948863	21
22	•528358	•610619	•686072	•752701	•809517	•856426	•894014	•923308	22
23	•443625	•527734	•608302	•682467	•748283	•804750	•851702	•889622	23
24	•362576	•444850	•527150	•606124	•679063	•744087	•800191	•847149	24
25	•288281	•365419	•445999	•526602	•604073	•675842	•740096	•795826	25
26	•222901	•292343	•368093	•447079	•526085	•602137	•672789	•736293	26
27	•167580	•227698	•296181	•370614	•448096	•525597	•600305	•669889	27
28	•122503	•172631	•232258	•299814	•372996	•449057	•525136	•598567	28
29	•087086	•127397	•177468	•236599	•303260	•375251	•449967	•524698	29
30	•060217	•091521	•132124	•182104	•240738	•306535	•377390	•450829	30
31	•040514	•064017	•095848	•136691	•186553	•244690	•309651	•379422	31
32	•026531	•043611	•067764	•100068	•141107	•190825	•248468	•312622	32
33	•016918	•028943	•046701	•071456	•104182	•145377	•194933	•252085	33
34	•010509	•018721	•031383	•049780	•075089	•108192	•149509	•198885	34
35	•006362	•011806	•020570	•033842	•052842	•078663	•112101	•153509	35
36	•003755	•007261	•013155	•022458	•036316	•055883	•082175	•115912	36
37	•002162	•004358	•008212	•014552	•024380	•038798	•058899	•085625	37
38	•001215	•002553	•005006	•009211	•015993	•026331	•041285	•061887	38
39	•000667	•001461	•002980	•005696	•010254	•017473	•028306	•043771	39
40	•000357	•000817	•001734	•003444	•006429	•011340	•018987	•030300	40
41	•000187	•000446	•000987	•002036	•003942	•007200	•012465	•020533	41
42	•000096	•000238	•000549	•001177	•002365	•004474	•008010	•013625	42
43	•000048	•000125	•000299	•000666	•001309	•002722	•005040	•008856	43
44	•000024	•000064	•000159	•000369	•000798	•001622	•003107	•005639	44
45	•000011	•000032	•000083	•000200	•000450	•000946	•001876	•003519	45
46	•000005	•000016	•000042	•000106	•000248	•000541	•001110	•002152	46
47	•000002	•000008	•000021	•000055	•000134	•000303	•000644	•001291	47
48	•000001	•000004	•000010	•000028	•000071	•000167	•000367	•000759	48
49		•000002	•000005	•000014	•000037	•000090	•000205	•000438	49
50		•000001	•000002	•000007	•000019	•000048	•000112	•000248	50
51			•000001	•000003	•000009	•000025	•000061	•000138	51
52				•000002	•000005	•000013	•000032	•000075	52
53				•000001	•000002	•000006	•000016	•000040	53
54					•000001	•000003	•000008	•000021	54
55						•000001	•000004	•000011	55
56						•000001	•000002	•000006	56
57							•000001	•000003	57
58								•000001	58
59								•000001	59
X	A=30	A=31	A=32	A=33	A=34	A=35	A=36	A=37	X
7	1•000000								7
8	•999999	1•000000							8
9	•999998	•999999	1•000000	1•000000					9
10	•999993	•999997	•999998	•999999	1•000000	1•000000			10
11	•999978	•999989	•999994	•999997	•999999	•999999			11
12	•999936	•999967	•999983	•999991	•999996	•999998	1•000000	1•000000	12
13	•999832	•999910	•999952	•999975	•999987	•999993	•999997	•999998	13
14	•999593	•999775	•999877	•999934	•999965	•999981	•999990	•999995	14
15	•999079	•999476	•999706	•999837	•999911	•999951	•999974	•999986	15
16	•998053	•998859	•999340	•999623	•999788	•999882	•999935	•999964	16
17	•996127	•997662	•998608	•999183	•999526	•999729	•999846	•999914	17
18	•992730	•995479	•997231	•998328	•999004	•999414	•999660	•999805	18
19	•987067	•991721	•994782	•996760	•998017	•998802	•999286	•999579	19

TABLE 11

X	A=30	A=31	A=32	A=33	A=34	A=35	A=36	A=37	X
20	.978127	.985588	.990658	.994038	.996251	.997675	.998578	.999141	20
21	.964715	.976082	.984059	.989546	.993249	.995703	.997303	.998330	21
22	.945557	.962050	.974004	.982487	.988388	.992417	.995119	.996901	22
23	.919431	.942278	.959379	.971899	.980876	.987187	.991544	.994498	23
24	.885354	.915628	.939031	.956707	.969771	.979230	.985948	.990632	24
25	.842758	.881205	.911899	.935819	.954040	.967626	.977554	.984672	25
26	.791643	.838521	.877171	.908246	.932644	.951380	.965467	.975852	26
27	.732663	.787628	.834429	.873249	.904666	.929510	.948731	.963299	27
28	.667131	.729196	.783772	.830475	.869434	.901160	.926417	.946098	28
29	.596918	.664502	.725877	.780064	.826653	.865723	.897727	.923367	29
30	.524283	.595348	.661994	.722699	.776495	.822953	.862112	.894366	30
31	.451648	.523888	.593852	.659597	.719650	.773058	.819374	.858598	31
32	.381337	.452428	.523512	.592424	.657303	.716722	.769743	.815907	32
33	.315459	.383202	.453171	.523153	.591060	.655105	.713908	.766545	33
34	.255551	.318170	.384963	.453881	.522810	.589754	.652997	.711201	34
35	.202692	.258877	.320766	.386646	.454559	.522481	.588503	.650973	35
36	.157383	.206361	.262072	.323254	.388258	.455208	.522167	.587303	36
37	.119627	.161138	.209900	.265144	.325641	.389804	.455830	.521865	37
38	.089013	.123249	.164778	.213317	.268101	.327934	.391286	.456427	38
39	.064844	.092339	.126780	.168309	.216618	.270950	.330140	.392711	39
40	.046253	.067770	.095603	.130225	.171735	.219810	.273696	.332262	40
41	.032310	.048728	.070661	.098806	.133585	.175062	.222898	.276347	41
42	.022107	.034331	.051194	.073517	.101948	.136863	.178294	.225887	42
43	.014820	.023705	.036362	.053647	.076337	.105030	.140062	.181435	43
44	.009735	.016044	.025324	.038399	.056086	.079120	.108054	.143185	44
45	.006269	.010647	.017297	.026962	.040438	.058509	.081865	.111020	45
46	.003958	.006929	.011588	.018575	.028615	.042479	.060915	.084573	46
47	.002450	.004423	.007617	.012559	.019877	.030282	.044518	.063301	47
48	.001488	.002770	.004914	.008334	.013555	.021199	.031960	.046555	48
49	.000887	.001703	.003111	.005430	.009077	.014576	.022540	.033646	49
50	.000519	.001027	.001934	.003474	.005970	.009846	.015620	.023899	50
51	.000298	.000609	.001181	.002183	.003857	.006534	.010638	.016686	51
52	.000168	.000354	.000708	.001348	.002449	.004261	.007121	.011453	52
53	.000093	.000202	.000417	.000817	.001528	.002732	.004686	.007729	53
54	.000051	.000114	.000242	.000487	.000937	.001722	.003032	.005130	54
55	.000027	.000063	.000138	.000286	.000565	.001067	.001929	.003349	55
56	.000014	.000034	.000077	.000155	.000335	.000650	.001208	.002151	56
57	.000007	.000018	.000042	.000093	.000195	.000390	.000744	.001359	57
58	.000004	.000010	.000023	.000052	.000112	.000230	.000451	.000845	58
59	.000002	.000005	.000012	.000029	.000063	.000134	.000269	.000517	59
60		.000003	.000006	.000015	.000035	.000076	.000158	.000312	60
61		.000001	.000003	.000008	.000019	.000043	.000091	.000185	61
62		.000001	.000002	.000004	.000010	.000024	.000052	.000108	62
63			.000001	.000002	.000006	.000013	.000029	.000062	63
64				.000001	.000003	.000007	.000016	.000035	64
65				.000001	.000001	.000004	.000009	.000020	65
66					.000001	.000002	.000005	.000011	66
67						.000001	.000002	.000006	67
68						.000001	.000001	.000003	68
69							.000001	.000002	69
70								.000001	70
X	A=38	A=39	A=40	A=41	A=42	A=43	A=44	A=45	X
12	1.000000								12
13	.999999	1.000000	1.000000						13
14	.999997	.999999	.999999	1.000000	1.000000				14
15	.999993	.999996	.999998	.999999	.999999	1.000000			15
16	.999981	.999990	.999995	.999997	.999999	.999999	1.000000	1.000000	16
17	.999952	.999974	.999986	.999992	.999996	.999998	.999999	.999999	17
18	.999889	.999938	.999965	.999981	.999990	.999994	.999997	.999998	18
19	.999755	.999859	.999920	.999955	.999975	.999986	.999992	.999996	19
20	.999487	.999698	.999824	.999889	.999942	.999967	.999982	.999990	20
21	.998979	.999383	.999632	.999783	.999873	.999927	.999958	.999976	21
22	.998059	.998799	.999266	.999557	.999735	.999843	.999908	.999947	22
23	.996469	.997763	.998601	.999135	.999472	.999681	.999809	.999887	23
24	.993843	.996008	.997445	.998385	.998991	.999377	.999620	.999770	24
25	.989685	.993154	.995517	.997102	.998150	.998833	.999272	.999551	25

TABLE II

X	A=38	A=39	A=40	A=41	A=42	A=43	A=44	A=45	X
26	•983364	•988703	•992434	•994999	•996737	•997896	•998660	•999156	26
27	•974126	•982026	•987689	•991683	•994454	•996348	•997624	•998473	27
28	•961125	•972382	•980661	•986646	•990902	•993882	•995937	•997334	28
29	•943481	•958948	•970620	•979272	•985576	•990095	•993285	•995503	29
30	•920360	•940883	•956771	•968846	•977861	•984479	•989261	•992663	30
31	•891074	•917398	•938306	•954597	•967060	•976431	•983359	•988402	31
32	•855176	•887852	•914479	•935751	•952427	•965266	•974983	•982218	32
33	•812546	•851843	•884696	•911606	•933221	•950264	•963466	•973520	33
34	•763457	•809287	•848596	•881607	•908777	•930715	•948109	•961661	34
35	•708593	•760472	•806124	•845431	•878581	•905993	•928236	•945964	35
36	•649026	•706079	•757586	•803055	•842347	•875619	•903252	•925782	36
37	•586151	•647153	•703654	•754792	•800073	•839339	•872717	•900556	37
38	•521575	•585042	•645349	•701312	•752087	•797176	•836404	•869874	38
39	•457000	•521297	•583976	•643610	•699049	•749465	•794358	•833541	39
40	•394081	•457551	•521029	•582949	•641931	•696860	•746922	•791618	40
41	•334307	•395399	•458082	•520771	•581958	•640310	•694742	•744455	41
42	•278907	•336279	•396670	•458593	•520522	•581002	•638744	•692690	42
43	•228784	•281382	•338183	•397896	•459086	•520282	•580079	•637228	43
44	•184488	•231592	•283776	•340021	•399078	•459562	•520050	•579187	44
45	•146233	•187459	•234315	•286093	•341799	•400221	•460021	•519826	45
46	•113929	•149211	•190350	•236958	•288338	•343518	•401326	•460465	46
47	•087243	•116783	•152119	•193164	•239525	•290513	•345183	•402395	47
48	•065667	•089875	•119583	•154961	•195906	•242019	•292623	•346796	48
49	•048586	•068012	•092469	•122329	•157739	•198577	•244444	•294671	49
50	•035339	•050611	•070335	•095025	•125024	•160454	•201181	•246802	50
51	•025272	•037038	•052628	•072636	•097544	•127668	•163109	•203720	51
52	•017771	•026659	•038740	•054636	•074913	•100025	•130263	•165706	52
53	•012289	•018874	•028057	•040444	•056634	•077167	•102470	•132809	53
54	•008359	•013146	•029466	•042149	•058621	•079397	•104878	•132809	54
55	•005593	•009009	•014022	•021130	•030883	•043853	•060596	•081602	55
56	•003683	•006076	•009679	•014916	•022280	•033208	•045556	•062558	56
57	•002386	•004033	•006576	•010367	•015827	•023442	•033738	•047255	57
58	•001522	•002635	•004399	•007095	•011073	•016754	•024616	•035174	58
59	•000955	•001695	•002898	•004781	•007630	•011796	•017696	•025800	59
60	•000590	•001074	•001880	•003174	•005179	•008182	•012535	•018651	60
61	•000359	•000670	•001201	•002075	•003464	•005592	•008750	•013289	61
62	•000215	•000412	•000756	•001337	•002282	•003767	•005020	•009334	62
63	•000127	•000249	•000469	•000849	•001482	•002500	•004083	•006463	63
64	•000074	•000149	•000287	•000531	•000949	•001636	•002730	•004412	64
65	•000042	•000087	•000173	•000328	•000599	•001056	•001799	•002970	65
66	•000024	•000051	•000103	•000199	•000372	•000672	•001170	•001972	66
67	•000013	•000029	•000060	•000119	•000228	•000421	•000750	•001291	67
68	•000007	•000016	•000035	•000071	•000138	•000261	•000474	•000834	68
69	•000004	•000009	•000020	•000041	•000083	•000159	•000296	•000532	69
70	•000002	•000005	•000011	•000024	•000049	•000096	•000182	•000334	70
71	•000001	•000003	•000006	•000013	•000028	•000057	•000111	•000207	71
72	•000001	•000001	•000003	•000008	•000016	•000033	•000066	•000127	72
73		•000001	•000002	•000004	•000009	•000019	•000039	•000077	73
74			•000001	•000002	•000005	•000011	•000023	•000046	74
75			•000001	•000001	•000003	•000006	•000013	•000027	75
76				•000001	•000002	•000003	•000008	•000016	76
77					•000001	•000002	•000004	•000009	77
78						•000001	•000002	•000005	78
79						•000001	•000001	•000003	79
80							•000001	•000002	80
81								•000001	81
X	A=46	A=47	A=48	A=49	A=50	A=51	A=52	A=53	X
17	1•000000								17
18	•999999	1•000000	1•000000						18
19	•999998	•999999	•999999	1•000000	1•000000				19
20	•999994	•999997	•999998	•999999	•999999	1•000000			20
21	•999987	•999993	•999996	•999998	•999999	•999999	1•000000	1•000000	21
22	•999970	•999983	•999990	•999995	•999997	•999998	•999999	•999999	22
23	•999934	•999962	•999978	•999987	•999993	•999996	•999998	•999999	23
24	•999862	•999919	•999952	•999972	•999984	•999991	•999995	•999997	24
25	•999726	•999834	•999901	•999941	•999965	•999980	•999988	•999993	25

TABLE 11

X	A=46	A=47	A=48	A=49	A=50	A=51	A=52	A=53	X
26	.999474	.999676	.999802	.999880	.999928	.999958	.999975	.999985	26
27	.999029	.999389	.999620	.999766	.999857	.999914	.999948	.999969	27
28	.998270	.998891	.999296	.999558	.999725	.999831	.999897	.999938	28
29	.997024	.998054	.998741	.999194	.999489	.999680	.999801	.999878	29
30	.995048	.996697	.997822	.998579	.999083	.999414	.999630	.999768	30
31	.992017	.994572	.996351	.997575	.998406	.998963	.999332	.999574	31
32	.987520	.991349	.994075	.995988	.997314	.998221	.998834	.999243	32
33	.981056	.986616	.990659	.993558	.995607	.997038	.998024	.998695	33
34	.972045	.979876	.985692	.989949	.993021	.995209	.996747	.997814	34
35	.959853	.970558	.978679	.984748	.989219	.992466	.994794	.996441	35
36	.943830	.958045	.969061	.977467	.983786	.988469	.991893	.994363	36
37	.923356	.941709	.956237	.967556	.976241	.982807	.987702	.991302	37
38	.897902	.920958	.939601	.954432	.966045	.975003	.981813	.986918	38
39	.867090	.895292	.918587	.937508	.952629	.964529	.973754	.980804	39
40	.830746	.864361	.892724	.916244	.935430	.950831	.963008	.972495	40
41	.788951	.828017	.861687	.890197	.913930	.933367	.949039	.961485	41
42	.742060	.786355	.825352	.859067	.887711	.911644	.931321	.947252	42
43	.690702	.739733	.783826	.822748	.856498	.885265	.909386	.929293	43
44	.635762	.688774	.737472	.781362	.820203	.853979	.882859	.907156	44
45	.578324	.634341	.686903	.735273	.778960	.817716	.851509	.880492	45
46	.519609	.577488	.632964	.685087	.733134	.776617	.815283	.849087	46
47	.460895	.519399	.576679	.631628	.683322	.731051	.774331	.812903	47
48	.403430	.461311	.519196	.575894	.630332	.681607	.729023	.772100	48
49	.348359	.404432	.461714	.518999	.575133	.629073	.679939	.727047	49
50	.296660	.349875	.405404	.462104	.518808	.574395	.627850	.678316	50
51	.249097	.298592	.351347	.406347	.462483	.518623	.573678	.626661	51
52	.206197	.251331	.300470	.352777	.407263	.462851	.518443	.572981	52
53	.168247	.208614	.253507	.302297	.354166	.408152	.463208	.518268	53
54	.135309	.170733	.210974	.255627	.304075	.355516	.409016	.463555	54
55	.107251	.137762	.173167	.213278	.257694	.305805	.356830	.409856	55
56	.083784	.109588	.140171	.175549	.215530	.259710	.307491	.358109	56
57	.064508	.085941	.111890	.142537	.177883	.217730	.261676	.309134	57
58	.048951	.066443	.088873	.114157	.144859	.180169	.219881	.263596	58
59	.036613	.050642	.068363	.090181	.116391	.147141	.182408	.221984	59
60	.026994	.038056	.052328	.070269	.092265	.118591	.149382	.184603	60
61	.019619	.028196	.039500	.054008	.072160	.094324	.120759	.151584	61
62	.014058	.020600	.029406	.040945	.055681	.074035	.096359	.122895	62
63	.009932	.014841	.021591	.030622	.042391	.057346	.075895	.098370	63
64	.006919	.010545	.015637	.022592	.031843	.043836	.059004	.077739	64
65	.004754	.007390	.011171	.016445	.023603	.033070	.045280	.060653	65
66	.003221	.005108	.007873	.011810	.017265	.024623	.034300	.046722	66
67	.002153	.003484	.005475	.008370	.012463	.018095	.025650	.035534	67
68	.001420	.002344	.003757	.005854	.008879	.013127	.018936	.026685	68
69	.000924	.001556	.002544	.004040	.006244	.009400	.013802	.019787	69
70	.000593	.001020	.001700	.002753	.004335	.006646	.009933	.014489	70
71	.000376	.000660	.001122	.001851	.002971	.004639	.007059	.010478	71
72	.000235	.000421	.000730	.001229	.002010	.003198	.004954	.007483	72
73	.000145	.000265	.000470	.000806	.001343	.002177	.003434	.005279	73
74	.000089	.000165	.000298	.000522	.000886	.001463	.002351	.003679	74
75	.000053	.000101	.000187	.000334	.000578	.000972	.001590	.002532	75
76	.000032	.000062	.000116	.000211	.000372	.000637	.001062	.001722	76
77	.000019	.000037	.000071	.000131	.000237	.000413	.000701	.001158	77
78	.000011	.000022	.000043	.000081	.000149	.000265	.000457	.000769	78
79	.000006	.000013	.000026	.000049	.000092	.000167	.000295	.000505	79
80	.000004	.000007	.000015	.000030	.000057	.000105	.000188	.000327	80
81	.000002	.000004	.000009	.000018	.000034	.000065	.000118	.000210	81
82	.000001	.000002	.000005	.000010	.000021	.000040	.000074	.000133	82
83	.000001	.000001	.000003	.000006	.000012	.000024	.000045	.000083	83
84		.000001	.000002	.000003	.000007	.000014	.000028	.000052	84
85			.000001	.000002	.000004	.000008	.000017	.000032	85
86				.000001	.000002	.000005	.000010	.000019	86
87				.000001	.000001	.000003	.000006	.000012	87
88					.000001	.000002	.000003	.000007	88
89						.000001	.000002	.000004	89
90						.000001	.000001	.000002	90
91							.000001	.000001	91
92								.000001	92

TABLE II

X	A=54	A=55	A=56	A=57	A=58	A=59	A=60	A=61	X
22	1.000000								22
23	.999999	1.000000	1.000000						23
24	.999998	.999999	.999999	1.000000					24
25	.999996	.999998	.999999	.999999	1.000000	1.000000			25
26	.999992	.999995	.999997	.999998	.999999	.999999	1.000000		26
27	.999982	.999989	.999994	.999996	.999998	.999999	.999999	1.000000	27
28	.999963	.999978	.999987	.999992	.999996	.999997	.999998	.999999	28
29	.999925	.999955	.999973	.999984	.999991	.999994	.999997	.999998	29
30	.999856	.999911	.999946	.999967	.999980	.999988	.999993	.999996	30
31	.999731	.999832	.999896	.999936	.999961	.999976	.999986	.999992	31
32	.999514	.999691	.999805	.999878	.999924	.999954	.999972	.999983	32
33	.999147	.999448	.999646	.999775	.999858	.999912	.999945	.999966	33
34	.998547	.999043	.999376	.999597	.999742	.999836	.999897	.999936	34
35	.997593	.998389	.998932	.999299	.999544	.999706	.999812	.999881	35
36	.996122	.997360	.998221	.998813	.999215	.999486	.999666	.999785	36
37	.993915	.995788	.997115	.998043	.998686	.999126	.999424	.999623	37
38	.990695	.993452	.995441	.996858	.997856	.998551	.999030	.999356	38
39	.986118	.990071	.992974	.995080	.996589	.997659	.998408	.998928	39
40	.979781	.985303	.989432	.992481	.994705	.996309	.997452	.998257	40
41	.971227	.978746	.984473	.988778	.991974	.994318	.996017	.997235	41
42	.959960	.969951	.977700	.983630	.988110	.991453	.993918	.995714	42
43	.945473	.958434	.968669	.976643	.982774	.987428	.990919	.993505	43
44	.927281	.943702	.956908	.967381	.975577	.981906	.986734	.990371	44
45	.904954	.925287	.941939	.955383	.966089	.974501	.981027	.986027	45
46	.878162	.902781	.923312	.940186	.953861	.964793	.973418	.980137	46
47	.846711	.875870	.900635	.921354	.938442	.952340	.963493	.972328	47
48	.810575	.844380	.873615	.898516	.919415	.936709	.950823	.962191	48
49	.769922	.808297	.842092	.871395	.896425	.917495	.934986	.949310	49
50	.725122	.767795	.806066	.839847	.869211	.894360	.915593	.933274	50
51	.676736	.723244	.765717	.803882	.837643	.867061	.892322	.913710	51
52	.625505	.675198	.721412	.763685	.801742	.835479	.864944	.890311	52
53	.572304	.624380	.673699	.719624	.761699	.799646	.833354	.862861	53
54	.518098	.571645	.623285	.672237	.717879	.759757	.797592	.831267	54
55	.463893	.517933	.571004	.622218	.670812	.716174	.757857	.795579	55
56	.410673	.464221	.517772	.570379	.621178	.669421	.714509	.755997	56
57	.359354	.411468	.464540	.517615	.569771	.620164	.668064	.712881	57
58	.310735	.360566	.412243	.464851	.517463	.569179	.619176	.666739	58
59	.265470	.312297	.361748	.412997	.465154	.517314	.568601	.618211	59
60	.224041	.267301	.313821	.362901	.413732	.465450	.517169	.568038	60
61	.186755	.226054	.269090	.315309	.364025	.414449	.465738	.517028	61
62	.153747	.188864	.228024	.270838	.316761	.365121	.415149	.466018	62
63	.124999	.155874	.190933	.229953	.272548	.318180	.366192	.415831	63
64	.100357	.127072	.157963	.192963	.231843	.274220	.319567	.367238	64
65	.079566	.102321	.129115	.160018	.194954	.233693	.275855	.320922	65
66	.062293	.081377	.104260	.131128	.162038	.196908	.235006	.277456	66
67	.048161	.063924	.083172	.106177	.133111	.164024	.198826	.237284	67
68	.036771	.049597	.065546	.084950	.108071	.135066	.165977	.200709	68
69	.027726	.038009	.051030	.067157	.086712	.109941	.136993	.167898	69
70	.020647	.028773	.039249	.052459	.068759	.088458	.111790	.138892	70
71	.015186	.021515	.029825	.040490	.053883	.070350	.090187	.113616	71
72	.011033	.015893	.022291	.030882	.041731	.055303	.071931	.091899	72
73	.007918	.011198	.016610	.023275	.031942	.042973	.056717	.073500	73
74	.005614	.008363	.012174	.017335	.024165	.033007	.044213	.058126	74
75	.003932	.005958	.008818	.012760	.018069	.025061	.034075	.045453	75
76	.002721	.004194	.006312	.009283	.013355	.018811	.025964	.035145	76
77	.001861	.002918	.004465	.006675	.009757	.013959	.019561	.026872	77
78	.001258	.002006	.003122	.004744	.007047	.010241	.014571	.020317	78
79	.000840	.001364	.002158	.003334	.005032	.007428	.010733	.015192	79
80	.000555	.000916	.001475	.002316	.003553	.005328	.007818	.011234	80
81	.000362	.000608	.000996	.001591	.002480	.003779	.005632	.008216	81
82	.000234	.000400	.000665	.001080	.001712	.002650	.004012	.005943	82
83	.000149	.000259	.000439	.000726	.001169	.001839	.002827	.004253	83
84	.000094	.000167	.000287	.000482	.000789	.001262	.001971	.003010	84
85	.000059	.000106	.000185	.000317	.000527	.000856	.001359	.002108	85
86	.000036	.000066	.000118	.000206	.000348	.000575	.000927	.001460	86
87	.000022	.000041	.000075	.000132	.000228	.000382	.000626	.001001	87
88	.000013	.000025	.000047	.000084	.000147	.000251	.000418	.000679	88

TABLE II

X	A=54	A=55	A=56	A=57	A=58	A=59	A=60	A=61	X
89	•000008	•000015	•000029	•000053	•000094	•000163	•000276	•000456	89
90	•000005	•000009	•000018	•000033	•000060	•000105	•000181	•000303	90
91	•000003	•000006	•000011	•000020	•000037	•000067	•000117	•000199	91
92	•000002	•000003	•000006	•000012	•000023	•000042	•000075	•000130	92
93	•000001	•000002	•000004	•000007	•000014	•000026	•000047	•000083	93
94	•000001	•000001	•000002	•000004	•000009	•000016	•000030	•000053	94
95		•000001	•000001	•000003	•000005	•000010	•000019	•000034	95
96			•000001	•000002	•000003	•000006	•000011	•000021	96
97				•000001	•000002	•000004	•000007	•000013	97
98				•000001	•000001	•000002	•000004	•000008	98
99					•000001	•000001	•000003	•000005	99
100						•000001	•000001	•000003	100
101							•000001	•000002	101
102							•000001	•000001	102
103								•000001	103
X	A=62	A=63	A=64	A=65	A=66	A=67	A=68	A=69	X
28	1.000000	1.000000							28
29	•999999	•999999	1.000000						29
30	•999998	•999999	•999999	1.000000	1.000000				30
31	•999995	•999997	•999998	•999999	•999999	1.000000			31
32	•999990	•999994	•999996	•999998	•999999	•999999	1.000000	1.000000	32
33	•999979	•999988	•999993	•999996	•999997	•999998	•999999	•999999	33
34	•999960	•999976	•999985	•999991	•999995	•999997	•999998	•999999	34
35	•999925	•999953	•999971	•999982	•999989	•999993	•999996	•999998	35
36	•999863	•999913	•999946	•999966	•999979	•999987	•999992	•999995	36
37	•999756	•999843	•999900	•999937	•999960	•999975	•999985	•999991	37
38	•999577	•999724	•999822	•999886	•999927	•999954	•999971	•999982	38
39	•999284	•999527	•999689	•999798	•999870	•999917	•999947	•999967	39
40	•998819	•999207	•999472	•999652	•999772	•999852	•999905	•999939	40
41	•998099	•998704	•999125	•999414	•999611	•999744	•999833	•999892	41
42	•997009	•997932	•998583	•999038	•999352	•999567	•999714	•999812	42
43	•995400	•996773	•997757	•998455	•998945	•999286	•999521	•999681	43
44	•993080	•995075	•996527	•997574	•998320	•998847	•999215	•999470	44
45	•989811	•992644	•994739	•996272	•997383	•998179	•998743	•999140	45
46	•985308	•899240	•992195	•994392	•996008	•997184	•998030	•998634	46
47	•979238	•984578	•988656	•991736	•994035	•995734	•996977	•997876	47
48	•971231	•978329	•983838	•988062	•991266	•993668	•995452	•996762	48
49	•960888	•970128	•977412	•983087	•987457	•990785	•993291	•995160	49
50	•947801	•959583	•969020	•976488	•982327	•986842	•990294	•992905	50
51	•931574	•946297	•958279	•967908	•975556	•981558	•986217	•989793	51
52	•911846	•929885	•944799	•956974	•966792	•974617	•980781	•985582	52
53	•888325	•910001	•928208	•943306	•955670	•965673	•973672	•979995	53
54	•860809	•886365	•908174	•926543	•941819	•954367	•964551	•972721	54
55	•829217	•858790	•884430	•906366	•924891	•940339	•953066	•963427	55
56	•793605	•827203	•856801	•882520	•904577	•923251	•938866	•951767	56
57	•754177	•791669	•825224	•854842	•880635	•902806	•921623	•937400	57
58	•711290	•752394	•789770	•823279	•852913	•878774	•901053	•920009	58
59	•665445	•709733	•750648	•787907	•821367	•851013	•876936	•899319	59
60	•617269	•664100	•708211	•748938	•786079	•819487	•849141	•875122	60
61	•567488	•616350	•662944	•706721	•747261	•784284	•817639	•847296	61
62	•516890	•566951	•615452	•661736	•705262	•745618	•782522	•815821	62
63	•466292	•516755	•566427	•614574	•660554	•703834	•744007	•780792	63
64	•416498	•466560	•516624	•565915	•613716	•659397	•702435	•742427	64
65	•368259	•417149	•466821	•516496	•565415	•612877	•658265	•701064	65
66	•322247	•369258	•417784	•467076	•516370	•564925	•612056	•657157	66
67	•279024	•323544	•370234	•418406	•467326	•516247	•564447	•611253	67
68	•239026	•280559	•324812	•371188	•419013	•467570	•516128	•563979	68
69	•202557	•240735	•282062	•326054	•372122	•419607	•467808	•516010	69
70	•169789	•204373	•242410	•283536	•327269	•373035	•420189	•468041	70
71	•140765	•171648	•206157	•244054	•284979	•328459	•373930	•420757	71
72	•115420	•142610	•173478	•207910	•245668	•286395	•329626	•374806	72
73	•093595	•117202	•144430	•175279	•209632	•247251	•287783	•330768	73
74	•075059	•095275	•118964	•146225	•177052	•211325	•248806	•289144	74
75	•059529	•076607	•096938	•120704	•147994	•178797	•212089	•250333	75
76	•046691	•060926	•078143	•098586	•122423	•149739	•180516	•214626	76

TABLE II

X	A=62	A=63	A=64	A=65	A=66	A=67	A=68	A=69	X
77	•036217	•047927	•062316	•079669	•100217	•124122	•151460	•182208	77
78	•027784	•037292	•049161	•063700	•081183	•101832	•125801	•153158	78
79	•021081	•028701	•038367	•050593	•065077	•082685	•103431	•127460	79
80	•015820	•021851	•029623	•039444	•051622	•066447	•084176	•105015	80
81	•011743	•016456	•022627	•030548	•040521	•052847	•067810	•085656	81
82	•008623	•012261	•017100	•023409	•031476	•041938	•054070	•069165	82
83	•006263	•009037	•012786	•017750	•024196	•032407	•042676	•055288	83
84	•004500	•006590	•009459	•013318	•018407	•024987	•033341	•043753	84
85	•003199	•004755	•006925	•009889	•013858	•019070	•025784	•034277	85
86	•002250	•003395	•005016	•007267	•010326	•014405	•019738	•026585	86
87	•001566	•002398	•003596	•005285	•007616	•010771	•014958	•020413	87
88	•001079	•001677	•002552	•003804	•005560	•007972	•011222	•015518	88
89	•000735	•001160	•001792	•002710	•004017	•005841	•008335	•011680	89
90	•000496	•000795	•001245	•001911	•002874	•004237	•006129	•008705	90
91	•000331	•000539	•000857	•001334	•002035	•003043	•004463	•006424	91
92	•000219	•000361	•000584	•000922	•001427	•002164	•003217	•004694	92
93	•000143	•000240	•000394	•000631	•000991	•001523	•002297	•003397	93
94	•000093	•000158	•000263	•000428	•000681	•001062	•001624	•002434	94
95	•000060	•000103	•000174	•000287	•000463	•000733	•001137	•001728	95
96	•000038	•000066	•000114	•000190	•000312	•000501	•000788	•001214	96
97	•000024	•000042	•000074	•000125	•000209	•000340	•000541	•000846	97
98	•000015	•000027	•000047	•000082	•000138	•000228	•000368	•000583	98
99	•000009	•000017	•000030	•000053	•000090	•000151	•000248	•000398	99
100	•000006	•000010	•000019	•000034	•000059	•000100	•000166	•000270	100
101	•000003	•000006	•000012	•000021	•000038	•000065	•000110	•000181	101
102	•000002	•000004	•000007	•000013	•000024	•000042	•000072	•000120	102
103	•000001	•000002	•000004	•000008	•000015	•000027	•000047	•000079	103
104	•000001	•000001	•000003	•000005	•000009	•000017	•000030	•000052	104
105		•000001	•000002	•000003	•000006	•000011	•000019	•000033	105
106		•000001	•000001	•000002	•000004	•000007	•000012	•000021	106
107			•000001	•000001	•000002	•000004	•000008	•000014	107
108				•000001	•000001	•000003	•000005	•000009	108
109					•000001	•000002	•000003	•000005	109
110						•000001	•000002	•000003	110
111						•000001	•000001	•000002	111
112							•000001	•000001	112
113								•000001	113
X	A=70	A=71	A=72	A=73	A=74	A=75	A=76	A=77	X
33	1.000000								33
34	•999999	1.000000	1.000000						34
35	•999999	•999999	•999999	1.000000					35
36	•999997	•999998	•999999	•999999	1.000000				36
37	•999994	•999997	•999998	•999999	•999999	1.000000	1.000000		37
38	•999989	•999993	•999996	•999998	•999999	•999999	•999999	1.000000	38
39	•999979	•999987	•999992	•999995	•999997	•999998	•999999	•999999	39
40	•999961	•999976	•999985	•999991	•999994	•999996	•999998	•999999	40
41	•999930	•999956	•999972	•999982	•999989	•999993	•999996	•999997	41
42	•999877	•999921	•999968	•999979	•999987	•999997	•999999	•999995	42
43	•999789	•999862	•999910	•999942	•999963	•999976	•999985	•999991	43
44	•999645	•999764	•999845	•999898	•999934	•999957	•999973	•999983	44
45	•999417	•999607	•999738	•999826	•999886	•999925	•999952	•999969	45
46	•999061	•999360	•999567	•999709	•999806	•999872	•999916	•999945	46
47	•998520	•998978	•999299	•999524	•999679	•999785	•999857	•999906	47
48	•997714	•998400	•998889	•999235	•999478	•999646	•999762	•999841	48
49	•996539	•997546	•998274	•998797	•999167	•999429	•999611	•999737	49
50	•994859	•996308	•997371	•998143	•998699	•999096	•999377	•999574	50
51	•992509	•994550	•996070	•997189	•998006	•998597	•999021	•999322	51
52	•989282	•992103	•994233	•995823	•997001	•997864	•998491	•998942	52
53	•984939	•988762	•991689	•993906	•995570	•006806	•997716	•998379	53
54	•979202	•984287	•988234	•991266	•993572	•995309	•996604	•997562	54
55	•971766	•978402	•983626	•987696	•990834	•993230	•995040	•996397	55
56	•962301	•970805	•977595	•982958	•987151	•990394	•992879	•994765	56
57	•950471	•961174	•969841	•976782	•982283	•986597	•989946	•992521	57
58	•935942	•949177	•960046	•968873	•975964	•981601	•986036	•989491	58
59	•918407	•934491	•947886	•958917	•967901	•975140	•980911	•985467	59
60	•897603	•915818	•933048	•946600	•957789	•966927	•974310	•980216	60

TABLE II

X	A=70	A=71	A=72	A=73	A=74	A=75	A=76	A=77	X
61	.873332	.895905	.915242	.931613	.945317	.956660	.965949	.973477	61
62	.845479	.871563	.894224	.913678	.930187	.944038	.955532	.964970	62
63	.814033	.843688	.869817	.892562	.912128	.928769	.942763	.954406	63
64	.779093	.812274	.841924	.868093	.890917	.910591	.927359	.941493	64
65	.740877	.777423	.810543	.840184	.866391	.889289	.909066	.925958	65
66	.699721	.739356	.775783	.808840	.838470	.864710	.887678	.907555	66
67	.656071	.698404	.737863	.774171	.807163	.836779	.863050	.886085	67
68	.610467	.655008	.697113	.736398	.772587	.805513	.835113	.861410	68
69	.563521	.609697	.653966	.695847	.734959	.771029	.803889	.833469	69
70	.515895	.563073	.608944	.652945	.694605	.733546	.769497	.802289	70
71	.468269	.515783	.562635	.608205	.651944	.693386	.732158	.767991	71
72	.421314	.468493	.515673	.562205	.607482	.650963	.692189	.730794	72
73	.375663	.421800	.468712	.515565	.561784	.606772	.651015	.691015	73
74	.331889	.376504	.422394	.468926	.515460	.561371	.606077	.649055	74
75	.290480	.332987	.377327	.422917	.469136	.515356	.560967	.605395	75
76	.251832	.291791	.334064	.378135	.423430	.469342	.515255	.560570	76
77	.216235	.253305	.293077	.335120	.378926	.423932	.469543	.515156	77
78	.183874	.217818	.254752	.294340	.336157	.379703	.424425	.469741	78
79	.154832	.185516	.219375	.256174	.295580	.337174	.380464	.424909	79
80	.129099	.156485	.187133	.220907	.257572	.296799	.338172	.381212	80
81	.106583	.130719	.158114	.188726	.222415	.258947	.297995	.339153	81
82	.087124	.108135	.132321	.159723	.190296	.223899	.260298	.299171	82
83	.070513	.088581	.109672	.133903	.161310	.191843	.225360	.261628	83
84	.056503	.071853	.090026	.111194	.135467	.162876	.193367	.226798	84
85	.044829	.057714	.073186	.091459	.112701	.137013	.164422	.194871	85
86	.035215	.045904	.058921	.074510	.092881	.114193	.138542	.165948	86
87	.027389	.036154	.046979	.060123	.075827	.094292	.115671	.140053	87
88	.021093	.028197	.037095	.048052	.061321	.077136	.095691	.117133	88
89	.016084	.021778	.029009	.038037	.049123	.062514	.078436	.097079	89
90	.012145	.016656	.022467	.029824	.038980	.050192	.063702	.079729	90
91	.009081	.012616	.017234	.023161	.030641	.039924	.051259	.064885	91
92	.006724	.009464	.013093	.017817	.023860	.031461	.040868	.052324	92
93	.004931	.007031	.009852	.013576	.018405	.024562	.032284	.041812	93
94	.003581	.005174	.007344	.010247	.014065	.018999	.025268	.033108	94
95	.002576	.003771	.005422	.007662	.010648	.014559	.019597	.025978	95
96	.001835	.002722	.003966	.005676	.007987	.011055	.015059	.020199	96
97	.001295	.001947	.002873	.004165	.005935	.008317	.011467	.015564	97
98	.000906	.001379	.002062	.003029	.004370	.006220	.008653	.011885	98
99	.000627	.000968	.001467	.002182	.003188	.004580	.006470	.008994	99
100	.000430	.000673	.001034	.001557	.002305	.003352	.004794	.006745	100
101	.000293	.000464	.000722	.001102	.001651	.002432	.003521	.005014	101
102	.000197	.000317	.000499	.000772	.001172	.001748	.002563	.003694	102
103	.000132	.000214	.000342	.000536	.000825	.001246	.001849	.002697	103
104	.000087	.000144	.000233	.000369	.000575	.000880	.001322	.001952	104
105	.000057	.000095	.000157	.000252	.000398	.000616	.000937	.001401	105
106	.000037	.000063	.000105	.000170	.000272	.000427	.000658	.000997	106
107	.000024	.000041	.000069	.000114	.000185	.000294	.000459	.000703	107
108	.000015	.000027	.000045	.000076	.000125	.000200	.000317	.000491	108
109	.000010	.000017	.000029	.000050	.000083	.000135	.000217	.000341	109
110	.000006	.000011	.000019	.000033	.000055	.000091	.000147	.000234	110
111	.000004	.000007	.000012	.000021	.000036	.000060	.000099	.000159	111
112	.000002	.000004	.000008	.000014	.000023	.000040	.000066	.000108	112
113	.000001	.000003	.000005	.000009	.000015	.000026	.000044	.000072	113
114	.000001	.000002	.000003	.000005	.000010	.000017	.000029	.000048	114
115	.000001	.000001	.000002	.000003	.000006	.000011	.000019	.000032	115
116		.000001	.000001	.000002	.000004	.000007	.000012	.000021	116
117			.000001	.000001	.000002	.000004	.000008	.000013	117
118				.000001	.000002	.000003	.000005	.000009	118
119					.000001	.000002	.000003	.000006	119
120					.000001	.000001	.000002	.000003	120
121						.000001	.000001	.000002	121
122							.000001	.000001	122
123								.000001	123
124								.000001	124
X	A=78	A=79	A=80	A=81	A=82	A=83	A=84	A=85	X
39	1.000000								39



TABLE II

X	A=78	A=79	A=80	A=81	A=82	A=83	A=84	A=85	X
40	.999999	1.000000	1.000000						40
41	.999998	.999999	.999999	1.000000					41
42	.999997	.999998	.999999	.999999	1.000000	1.000000			42
43	.999994	.999996	.999998	.999999	.999999	.999999	1.000000		43
44	.999989	.999993	.999996	.999997	.999998	.999999	.999999	1.000000	44
45	.999980	.999987	.999992	.999995	.999997	.999998	.999999	.999999	45
46	.999965	.999977	.999985	.999991	.999994	.999996	.999998	.999999	46
47	.999938	.999960	.999974	.999983	.999989	.999993	.999996	.999997	47
48	.999894	.999931	.999955	.999970	.999981	.999988	.999992	.999995	48
49	.999823	.999882	.999922	.999949	.999967	.999978	.999986	.999991	49
50	.999710	.999805	.999869	.999913	.999943	.999962	.999975	.999984	50
51	.999534	.999682	.999785	.999855	.999903	.999936	.999958	.999972	51
52	.999264	.999492	.999652	.999763	.999840	.999893	.999928	.999953	52
53	.998859	.999203	.999447	.999620	.999740	.999824	.999881	.999920	53
54	.998263	.998772	.999139	.999400	.999585	.999715	.999806	.999869	54
55	.997403	.998142	.998682	.999071	.999351	.999549	.999689	.999787	55
56	.996182	.997238	.998017	.998587	.999001	.999299	.999511	.999662	56
57	.994482	.995961	.997067	.997887	.998488	.998927	.999244	.999471	57
58	.992156	.994192	.995734	.996891	.997751	.998386	.998850	.999186	58
59	.989027	.991783	.993896	.995501	.996709	.997612	.998279	.998769	59
60	.984891	.988556	.991402	.993592	.995261	.996522	.997467	.998169	60
61	.979514	.984308	.988078	.991015	.993282	.995015	.996330	.997318	61
62	.972639	.978807	.983719	.987594	.990621	.992965	.994764	.996132	62
63	.963989	.971797	.978094	.983124	.987102	.990220	.992642	.994506	63
64	.953280	.963006	.970951	.977376	.982522	.986604	.989813	.992313	64
65	.940228	.952156	.962023	.970102	.976654	.981915	.986100	.989400	65
66	.924566	.938968	.951033	.961038	.969250	.975926	.981302	.985590	66
67	.906056	.923183	.937713	.949913	.960052	.968396	.975195	.980684	67
68	.884508	.904571	.921809	.936464	.948795	.959066	.967539	.974460	68
69	.859790	.882947	.903098	.920444	.935220	.947679	.958081	.966679	69
70	.831849	.858190	.881403	.901637	.919088	.933982	.946567	.957095	70
71	.800714	.830250	.856610	.879876	.900190	.917741	.932750	.945457	71
72	.766509	.799162	.828674	.855049	.878364	.898755	.916403	.931523	72
73	.729454	.765051	.797634	.827119	.853506	.876868	.897332	.915074	73
74	.689861	.728137	.763617	.796128	.825584	.851982	.875387	.895922	74
75	.648128	.688729	.726842	.762205	.794644	.824071	.850477	.873922	75
76	.604726	.647218	.687616	.725569	.760816	.793182	.822577	.848989	76
77	.560181	.604069	.646325	.686522	.724317	.759448	.791741	.821103	77
78	.515058	.559800	.603425	.645447	.685448	.723085	.758101	.790320	78
79	.469935	.514963	.559425	.602793	.644586	.684392	.721874	.756775	79
80	.425383	.470125	.514869	.559058	.602172	.643739	.683353	.720681	80
81	.381945	.425849	.470312	.514777	.558697	.601562	.642907	.682332	81
82	.340116	.382665	.426305	.470495	.514686	.558343	.600963	.642089	82
83	.300327	.341062	.383372	.426754	.470675	.514597	.557995	.600374	83
84	.262935	.301463	.341991	.384067	.427194	.470852	.514510	.557654	84
85	.228214	.264221	.302580	.342904	.384749	.427627	.471025	.514425	85
86	.196352	.229609	.265487	.303678	.343801	.385419	.428052	.471196	86
87	.167454	.197813	.230982	.266733	.304758	.344684	.386078	.428469	87
88	.141546	.168942	.199254	.232336	.267959	.305821	.345551	.386725	88
89	.118582	.143023	.170410	.200675	.233669	.269167	.306867	.346404	89
90	.098456	.120016	.144483	.171860	.202076	.234983	.270355	.307896	90
91	.081013	.099821	.121436	.145926	.173291	.203459	.236278	.271526	91
92	.066063	.082290	.101175	.122842	.147353	.174705	.204822	.237555	92
93	.053387	.067235	.083558	.102519	.124235	.148765	.176102	.206168	93
94	.042756	.054447	.068402	.084817	.103851	.125614	.150161	.177481	94
95	.033934	.043700	.055504	.069564	.086069	.105172	.126979	.151541	95
96	.026691	.034762	.044643	.056559	.070720	.087312	.106482	.128332	96
97	.020806	.027407	.035591	.045585	.057610	.071871	.088547	.107781	97
98	.016074	.021418	.028126	.036422	.046527	.058658	.073015	.089773	98
99	.012308	.016589	.022033	.028848	.037253	.047468	.059703	.074154	99
100	.009340	.012736	.017108	.022652	.029572	.038086	.048407	.060744	100
101	.007025	.009692	.013169	.017632	.023274	.030299	.038919	.049345	101
102	.005238	.007311	.010048	.013607	.018160	.023900	.031028	.039752	102
103	.003871	.005467	.007601	.010400	.014049	.018693	.024529	.031758	103
104	.002836	.004052	.005700	.007896	.010777	.014497	.019229	.025161	104
105	.002059	.002978	.004238	.005938	.008196	.011148	.014948	.019769	105
106	.001483	.002170	.003124	.004428	.006181	.008501	.011524	.015404	106
107	.001058	.001567	.002283	.003274	.004622	.006428	.008810	.011904	107

TABLE II

X	A=78	A=79	A=80	A=81	A=82	A=83	A=84	A=85	X
108	•000749	•000122	•001655	•002400	•003427	•004820	•006679	•009124	108
109	•000525	•000797	•001189	•001745	•002520	•003585	•005022	•006935	109
110	•000366	•000561	•000847	•001258	•001838	•002644	•003746	•005229	110
111	•000252	•000392	•000599	•000899	•001329	•001934	•002770	•003910	111
112	•000173	•000271	•000420	•000638	•000953	•001403	•002032	•002900	112
113	•000117	•000186	•000292	•000448	•000678	•001009	•001479	•002134	113
114	•000079	•000127	•000201	•000313	•000479	•000720	•001068	•001557	114
115	•000053	•000086	•000137	•000216	•000335	•000510	•000764	•001128	115
116	•000035	•000057	•000093	•000148	•000233	•000358	•000543	•000810	116
117	•000023	•000038	•000063	•000101	•000160	•000250	•000383	•000577	117
118	•000015	•000025	•000042	•000068	•000109	•000173	•000267	•000408	118
119	•000010	•000016	•000028	•000046	•000074	•000118	•000186	•000286	119
120	•000006	•000011	•000018	•000030	•000050	•000080	•000128	•000199	120
121	•000004	•000007	•000012	•000020	•000033	•000054	•000087	•000138	121
122	•000002	•000004	•000008	•000013	•000022	•000036	•000059	•000094	122
123	•000002	•000003	•000005	•000009	•000014	•000024	•000040	•000064	123
124	•000001	•000002	•000003	•000005	•000009	•000016	•000027	•000043	124
125	•000001	•000001	•000002	•000004	•000006	•000010	•000018	•000029	125
126	•000001	•000001	•000002	•000002	•000004	•000007	•000012	•000019	126
127			•000001	•000001	•000002	•000004	•000008	•000013	127
128			•000001	•000001	•000002	•000003	•000005	•000008	128
129			•000001	•000001	•000001	•000002	•000003	•000005	129
130					•000001	•000001	•000002	•000003	130
131						•000001	•000001	•000002	131
132							•000001	•000001	132
133							•000001	•000001	133
134							•000001	•000001	134
X	A=86	A=87	A=88	A=89	A=90	A=91	A=92	A=93	X
44	1•000000								44
45	•999999	1•000000							45
46	•999999	•999999	1•000000						46
47	•999998	•999999	•999999	1•000000	1•000000				47
48	•999997	•999998	•999999	•999999	•999999	1•000000			48
49	•999994	•999996	•999998	•999999	•999999	•999999	1•000000		49
50	•999990	•999993	•999996	•999997	•999998	•999999	•999999	1•000000	50
51	•999982	•999988	•999992	•999995	•999997	•999998	•999999	•999999	51
52	•999969	•999980	•999987	•999991	•999994	•999996	•999998	•999999	52
53	•999947	•999965	•999977	•999985	•999990	•999994	•999996	•999997	53
54	•999912	•999941	•999961	•999974	•999983	•999989	•999993	•999995	54
55	•999855	•999902	•999934	•999956	•999971	•999981	•999988	•999992	55
56	•999767	•999841	•999892	•999927	•999951	•999968	•999979	•999986	56
57	•999632	•999746	•999826	•999882	•999920	•999946	•999964	•999976	57
58	•999428	•999601	•999724	•999810	•999870	•999912	•999940	•999960	58
59	•999126	•999384	•999569	•999700	•999793	•999858	•999903	•999934	59
60	•998686	•999063	•999337	•999534	•999675	•999774	•999845	•999894	60
61	•998054	•998598	•998998	•999288	•999498	•999648	•999755	•999831	61
62	•997164	•997935	•998508	•998929	•999237	•999460	•999620	•999734	62
63	•995929	•997005	•997812	•998414	•998858	•999183	•999420	•999590	63
64	•994243	•995720	•996841	•997686	•998316	•998783	•999127	•999378	64
65	•991977	•993973	•995506	•996673	•997555	•998215	•998706	•999069	65
66	•988980	•991636	•993698	•995287	•996501	•997420	•998111	•998626	66
67	•985074	•988554	•991288	•993418	•995063	•996323	•997281	•998003	67
68	•980061	•984553	•988123	•990935	•993132	•994834	•996141	•997138	68
69	•973720	•979433	•984026	•987685	•990576	•992841	•994600	•995955	69
70	•965818	•972978	•978801	•983493	•987243	•990212	•992544	•994361	70
71	•956109	•964955	•972232	•978164	•982956	•986794	•989842	•992242	71
72	•944349	•955125	•964091	•971483	•977523	•982414	•986341	•989467	72
73	•930303	•943246	•954140	•963225	•970732	•976879	•981868	•985883	73
74	•913755	•929089	•942145	•953157	•962359	•969978	•976230	•981317	74
75	•894524	•912445	•927881	•941049	•952175	•961491	•969221	•975578	75
76	•872472	•893138	•911144	•926679	•939955	•951195	•960624	•968463	76
77	•847518	•871037	•891765	•909852	•925484	•938866	•950216	•959755	77
78	•819648	•846065	•869617	•890403	•908570	•924295	•937781	•949238	78
79	•788920	•818212	•844629	•868211	•889053	•907297	•923113	•936699	79
80	•755468	•787539	•816795	•843209	•866819	•887716	•906033	•921938	80

TABLE II

X	A=86	A=87	A=88	A=89	A=90	A=91	A=92	A=93	X
81	•719508	•754181	•786177	•815395	•841806	•865442	•886390	•904777	81
82	•681328	•718353	•752914	•784884	•814014	•840419	•864079	•885075	82
83	•641285	•680340	•717216	•751664	•783510	•812650	•839048	•862730	83
84	•599796	•640495	•679368	•716097	•750433	•782203	•811302	•837692	84
85	•557318	•599227	•639718	•678412	•714994	•749220	•780914	•809972	85
86	•514341	•556988	•598668	•638953	•677470	•713008	•748024	•779643	86
87	•471363	•514258	•556664	•598119	•638201	•676544	•712839	•746845	87
88	•428880	•471528	•514177	•556345	•597578	•637461	•675632	•711785	88
89	•387362	•429283	•471690	•514097	•556032	•597046	•636733	•674733	89
90	•347244	•387988	•429680	•471849	•514018	•555723	•596523	•636016	90
91	•308908	•348069	•388604	•430070	•472005	•513941	•555420	•596008	91
92	•272679	•309905	•348882	•389209	•430453	•472159	•513865	•555122	92
93	•238813	•273815	•310887	•349681	•389005	•430831	•472310	•513790	93
94	•207496	•240054	•274934	•311853	•350468	•390391	•431702	•472459	94
95	•178844	•208806	•241277	•276037	•312805	•351243	•390968	•431567	95
96	•152906	•180190	•210099	•242483	•277124	•313742	•352006	•391536	96
97	•129671	•154257	•181520	•211376	•243673	•278195	•314666	•352757	97
98	•109070	•130997	•155593	•182834	•212636	•244847	•275251	•315576	98
99	•090992	•110348	•132311	•156914	•184133	•213880	•246005	•280292	99
100	•075288	•092202	•111616	•133612	•158221	•185416	•215109	•247147	100
101	•061782	•076415	•093404	•112873	•134900	•159514	•186685	•216322	101
102	•050282	•062816	•077536	•094598	•114119	•136176	•160794	•187939	102
103	•040586	•051217	•063847	•078652	•095783	•115356	•137441	•162059	103
104	•032490	•041420	•052151	•064873	•079761	•096960	•116582	•138693	104
105	•025796	•033224	•042254	•053088	•065896	•080865	•098130	•117798	105
106	•020313	•026434	•033960	•043088	•054012	•066915	•081962	•099291	106
107	•015864	•020860	•027074	•034696	•043921	•054939	•067930	•083053	107
108	•012289	•016328	•021411	•027716	•035434	•044755	•055865	•068941	108
109	•009442	•012678	•016796	•021964	•028361	•036173	•045587	•056788	109
110	•007195	•009764	•013071	•017268	•022521	•029008	•036912	•046419	110
111	•005439	•007460	•010091	•013468	•017743	•023081	•029657	•037653	111
112	•004078	•005653	•007728	•010421	•013869	•018222	•023644	•030308	112
113	•003033	•004250	•005871	•008000	•010756	•014274	•018704	•024209	113
114	•002238	•003170	•004426	•006093	•008277	•011095	•014683	•019190	114
115	•001638	•002346	•003310	•004605	•006319	•008557	•011437	•015095	115
116	•001190	•001722	•002456	•003452	•004787	•006549	•008841	•011784	116
117	•000857	•001254	•001808	•002568	•003598	•004973	•006782	•009129	117
118	•000613	•000906	•001320	•001896	•002684	•003748	•005163	•007018	118
119	•000435	•000650	•000957	•001389	•001987	•002803	•003900	•005355	119
120	•000306	•000462	•000688	•001010	•001459	•002080	•002924	•004056	120
121	•000214	•000326	•000491	•000728	•001064	•001532	•002176	•003048	121
122	•000148	•000229	•000348	•000521	•000770	•001120	•001607	•002274	122
123	•000102	•000159	•000245	•000370	•000553	•000813	•001178	•001684	123
124	•000069	•000110	•000171	•000261	•000394	•000585	•000857	•001238	124
125	•000047	•000075	•000118	•000183	•000279	•000418	•000619	•000903	125
126	•000032	•000051	•000081	•000127	•000196	•000297	•000444	•000654	126
127	•000021	•000034	•000055	•000088	•000136	•000209	•000316	•000470	127
128	•000014	•000023	•000037	•000060	•000094	•000146	•000223	•000335	128
129	•000009	•000015	•000025	•000041	•000065	•000101	•000156	•000238	129
130	•000006	•000010	•000017	•000027	•000044	•000070	•000109	•000167	130
131	•000004	•000007	•000011	•000018	•000030	•000048	•000075	•000117	131
132	•000002	•000004	•000007	•000012	•000020	•000032	•000052	•000081	132
133	•000002	•000003	•000005	•000008	•000013	•000022	•000035	•000056	133
134	•000001	•000002	•000003	•000005	•000009	•000015	•000024	•000038	134
135	•000001	•000001	•000002	•000003	•000005	•000010	•000016	•000026	135
136	•000001	•000001	•000001	•000002	•000004	•000006	•000011	•000017	136
137			•000001	•000001	•000002	•000004	•000007	•000012	137
138			•000001	•000001	•000002	•000003	•000005	•000008	138
139			•000001	•000001	•000001	•000002	•000003	•000005	139
140					•000001	•000001	•000002	•000003	140
141						•000001	•000001	•000002	141
142							•000001	•000001	142
143							•000001	•000001	143
144							•000001	•000001	144
X	A=94	A=95	A=96	A=97	A=98	A=99	A=100	A=101	X
51	1.000000	1.000000							51

TABLE II

X	A=94	A=95	A=96	A=97	A=98	A=99	A=100	A=101	X
52	.999999	.999999	1.000000						52
53	.999998	.999999	.999999	1.000000					53
54	.999997	.999998	.999999	.999999	1.000000	1.000000			54
55	.999995	.999997	.999998	.999999	.999999	.999999	1.000000		55
56	.999991	.999994	.999996	.999998	.999998	.999999	.999999	1.000000	56
57	.999984	.999990	.999993	.999996	.999997	.999998	.999999	.999999	57
58	.999973	.999982	.999988	.999992	.999995	.999997	.999998	.999999	58
59	.999956	.999970	.999980	.999987	.999991	.999994	.999996	.999998	59
60	.999928	.999951	.999967	.999978	.999985	.999990	.999994	.999996	60
61	.999884	.999920	.999946	.999964	.999976	.999984	.999989	.999993	61
62	.999816	.999873	.999913	.999941	.999960	.999973	.999982	.999988	62
63	.999713	.999800	.999861	.999905	.999935	.999956	.999970	.999980	63
64	.999559	.999690	.999783	.999849	.999896	.999929	.999951	.999967	64
65	.999334	.999527	.999666	.999766	.999837	.999887	.999922	.999947	65
66	.999008	.999288	.999492	.999640	.999747	.999823	.999877	.999915	66
67	.998543	.998945	.999240	.999457	.999614	.999727	.999809	.999866	67
68	.997892	.998458	.998879	.999190	.999419	.999586	.999707	.999793	68
69	.996991	.997777	.998369	.998811	.999139	.999380	.999557	.999685	69
70	.995764	.996840	.997659	.998277	.998740	.999085	.999339	.999526	70
71	.994117	.995569	.996685	.997537	.998182	.998667	.999029	.999297	71
72	.991935	.993868	.995369	.996527	.997412	.998084	.998591	.998971	72
73	.989087	.991623	.993614	.995165	.996364	.997283	.997984	.998513	73
74	.985420	.988702	.991306	.993356	.994957	.996197	.997151	.997880	74
75	.980762	.984952	.988312	.990985	.993093	.994744	.996027	.997016	75
76	.974923	.980202	.984480	.987918	.990658	.992826	.994527	.995853	76
77	.967702	.974265	.979639	.984003	.987519	.990327	.992554	.994307	77
78	.958887	.966940	.973604	.979072	.983523	.987115	.989992	.992278	78
79	.948263	.958018	.966176	.972940	.978502	.983038	.986707	.989652	79
80	.935622	.947289	.957149	.965411	.972274	.977928	.982549	.986295	80
81	.920769	.934549	.946318	.956281	.964644	.971605	.977351	.982056	81
82	.903532	.919606	.933480	.945348	.955413	.963877	.970934	.976771	82
83	.883772	.902295	.918450	.932416	.944381	.954546	.963108	.970261	83
84	.861394	.882480	.901067	.917301	.931356	.943417	.953679	.962339	84
85	.836352	.860071	.881200	.899848	.916159	.930300	.942455	.952814	85
86	.808658	.835026	.858762	.879931	.898638	.915023	.929250	.941496	86
87	.778388	.807360	.833715	.857466	.878673	.897437	.913895	.928204	87
88	.745682	.777149	.806077	.832419	.856183	.877425	.896245	.912773	88
89	.710747	.744536	.775927	.804810	.831137	.854912	.876189	.895062	89
90	.673849	.709723	.743405	.774720	.803559	.829869	.853654	.874963	90
91	.635310	.672977	.708715	.742289	.773529	.802322	.828615	.852408	91
92	.595502	.634616	.672119	.707721	.741189	.772353	.801100	.827374	92
93	.554828	.595003	.633931	.671273	.706740	.740104	.771192	.799892	93
94	.513717	.554539	.594512	.633258	.670439	.705774	.739033	.770045	94
95	.472605	.513644	.554255	.594029	.632594	.669618	.704821	.737976	95
96	.431927	.472750	.513573	.553975	.593553	.631940	.668808	.703881	96
97	.392096	.432281	.472892	.513503	.553699	.593084	.631295	.668010	97
98	.353497	.392647	.432629	.473031	.513434	.553427	.592622	.630661	98
99	.316473	.354225	.393189	.432973	.473169	.513366	.553160	.592167	99
100	.281319	.317357	.354944	.393723	.433311	.473304	.513299	.552897	100
101	.248275	.282332	.318228	.355651	.394249	.433643	.473438	.513233	101
102	.217520	.249387	.283330	.319087	.356349	.394768	.433971	.473570	102
103	.189178	.218703	.250485	.284315	.319934	.357036	.395279	.434295	103
104	.163312	.190403	.219872	.251569	.285287	.320769	.357713	.395783	104
105	.139933	.164552	.191614	.221027	.252639	.286246	.321593	.358382	105
106	.119004	.141162	.165778	.192812	.222168	.253696	.287192	.322405	106
107	.100444	.120200	.142380	.166992	.193996	.223295	.254739	.288126	107
108	.084139	.101589	.121387	.143586	.168194	.195167	.224408	.255769	108
109	.069947	.085218	.102726	.122563	.144781	.169383	.196325	.225509	109
110	.057709	.070950	.086291	.103855	.123730	.145964	.170560	.197470	110
111	.047250	.058627	.071948	.087358	.104976	.124888	.147137	.171725	111
112	.038394	.048081	.059543	.072942	.088419	.106090	.126036	.148300	112
113	.030960	.039135	.048910	.060456	.073931	.089474	.107195	.127175	113
114	.024777	.031614	.039877	.049738	.061366	.074916	.090522	.108294	114
115	.019678	.025347	.032270	.040619	.050565	.062274	.075897	.091565	115
116	.015511	.020170	.025920	.032927	.041361	.051391	.063179	.076874	116
117	.012134	.015930	.020664	.026494	.033585	.042103	.052215	.064082	117
118	.009420	.012487	.016352	.021162	.027071	.034244	.042845	.053039	118
119	.007259	.009716	.012844	.016778	.021662	.027650	.034904	.043587	119

TABLE II

X	A=94	A=95	A=96	A=97	A=98	A=99	A=100	A=101	X
120	•005552	•007503	•010014	•013205	•017207	•022164	•028230	•035565	120
121	•004214	•005751	•007750	•010317	•013569	•017639	•022669	•028813	121
122	•003175	•004376	•005954	•008001	•010622	•013936	•018073	•023177	122
123	•002375	•003305	•004541	•006160	•008255	•010931	•014306	•018511	123
124	•001763	•002478	•003437	•004708	•006369	•008513	•011244	•014680	124
125	•001299	•001844	•002583	•003573	•004879	•006582	•008774	•011559	125
126	•000950	•001362	•001927	•002691	•003711	•005053	•006798	•009038	126
127	•000690	•000999	•001428	•002013	•002802	•003851	•005229	•007017	127
128	•000498	•000728	•001050	•001495	•002100	•002915	•003995	•005409	128
129	•000356	•000526	•000766	•001102	•001563	•002190	•003030	•004141	129
130	•000253	•000378	•000556	•000807	•001156	•001634	•002318	•003148	130
131	•000179	•000269	•000400	•000586	•000848	•001211	•001707	•002377	131
132	•000125	•000190	•000286	•000423	•000618	•000891	•001268	•001782	132
133	•000087	•000134	•000203	•000303	•000447	•000651	•000935	•001327	133
134	•000060	•000093	•000143	•000216	•000321	•000472	•000685	•000981	134
135	•000041	•000065	•000100	•000153	•000229	•000340	•000498	•000721	135
136	•000028	•000044	•000070	•000107	•000163	•000244	•000360	•000526	136
137	•000019	•000030	•000048	•000075	•000114	•000173	•000258	•000381	137
138	•000013	•000021	•000033	•000052	•000080	•000122	•000184	•000274	138
139	•000009	•000014	•000022	•000036	•000056	•000086	•000130	•000196	139
140	•000006	•000009	•000015	•000024	•000038	•000060	•000092	•000139	140
141	•000004	•000006	•000010	•000016	•000026	•000041	•000064	•000098	141
142	•000002	•000004	•000007	•000011	•000018	•000028	•000044	•000069	142
143	•000002	•000003	•000004	•000007	•000012	•000019	•000031	•000048	143
144	•000001	•000002	•000003	•000005	•000008	•000013	•000021	•000033	144
145	•000001	•000001	•000002	•000003	•000005	•000009	•000014	•000023	145
146		•000001	•000001	•000002	•000004	•000006	•000010	•000016	146
147			•000001	•000001	•000002	•000004	•000006	•000011	147
148			•000001	•000001	•000002	•000003	•000004	•000008	148
149				•000001	•000001	•000002	•000003	•000005	149
150					•000001	•000001	•000002	•000004	150
151						•000001	•000001	•000003	151
152							•000001	•000002	152
153							•000001	•000001	153
154							•000001	•000001	154

## APPENDIX 4

**TABLE OF THE BINOMIAL DISTRIBUTION FOR  $p = 1/10$** 

This table gives the probability that *r* or more hits will be obtained in *N* trials if the probability of a hit on any one trial is  $1/10$ . In using the table, we first find the column corresponding to *N*, and then we locate the row corresponding to *r* (the observed number of hits); at the intersection is the desired probability.

*Interpreting the entry.* Probabilities are given to three significant figures. The number from 0 to 10 which directly follows the three significant figures gives the number of zeros to be placed between the decimal point and the first significant figure.

*Example of use of the table.* The entry corresponding to  $N = 480$ ,  $r = 65$  is  $.781-2$ . This means that the probability of getting 65 or more hits in 480 trials with a probability of a hit on one trial equal to  $1/10$  is  $.00781$ . (If desired one can also interpret the entry as  $.781 \times 10^{-2}$ .)

R	N=	*	N=0010	N=0020	N=0030	N=0040	N=0050	N=0060	N=0070	N=0080	N=0090	R	P=1/10
1			.651-0	.878-0	.958-0	.985-0	.995-0	.998-0	.999-0			1	
2			.264-0	.608-0	.816-0	.920-0	.966-0	.986-0	.994-0	.998-0	.999-0	2	
3			.702-1	.323-0	.589-0	.777-0	.888-0	.947-0	.976-0	.989-0	.995-0	3	
4			.128-1	.133-0	.353-0	.577-0	.750-0	.863-0	.929-0	.965-0	.983-0	4	
5			.163-2	.432-1	.175-0	.371-0	.569-0	.729-0	.841-0	.912-0	.954-0	5	
6			.147-3	.113-1	.732-1	.206-0	.384-0	.563-0	.713-0	.823-0	.897-0	6	
7			.912-5	.239-2	.258-1	.995-1	.230-0	.394-0	.558-0	.700-0	.808-0	7	
8			.374-6	.416-3	.778-2	.419-1	.122-0	.248-0	.401-0	.554-0	.689-0	8	
9			.901-8	.599-4	.202-2	.155-1	.579-1	.142-0	.264-0	.407-0	.551-0	9	
10			.100-10	.715-5	.454-3	.506-2	.245-1	.731-1	.159-0	.277-0	.412-0	10	
11				.709-6	.891-4	.147-2	.935-2	.342-1	.873-1	.173-0	.287-0	11	
12				.582-7	.153-4	.381-3	.322-2	.146-1	.441-1	.100-0	.186-0	12	
13				.392-8	.230-5	.884-4	.100-2	.568-2	.205-1	.538-1	.113-0	13	
14				.215-9	.305-6	.185-4	.285-3	.203-2	.876-2	.267-1	.634-1	14	
15					.356-7	.348-5	.738-4	.666-3	.347-2	.123-1	.333-1	15	
16					.366-8	.593-6	.175-4	.201-3	.127-2	.530-2	.163-1	16	
17					.331-9	.914-7	.380-5	.563-4	.434-3	.213-2	.750-2	17	
18						.128-7	.760-6	.146-4	.138-3	.796-3	.323-2	18	
19						.263-10						19	
20							.162-8	.140-6	.350-5	.407-4	.279-3	20	
21							.187-9	.237-7	.782-6	.113-4	.920-4	21	
22							.196-10	.371-8	.163-6	.291-5	.285-4	22	
23								.536-9	.315-7	.707-6	.828-5	23	
24									.571-8	.161-6	.227-5	24	
25									.965-9	.345-7	.588-6	25	
26									.153-9	.696-8	.144-6	26	
27									.226-10	.132-8	.333-7	27	
28										.236-9	.729-8	28	
29										.398-10	.151-8	29	
30											.298-9	30	
31											.556-10	31	
32												32	
33												33	

R	N=0100	N=0110	N=0120	N=0130	N=0140	N=0150	N=0160	N=0170	N=0180	N=0190	R
3	.998-0	.999-0									3
4	.992-0	.996-0	.998-0	.999-0							4
5	.976-0	.988-0	.994-0	.997-0	.999-0	.999-0					5
6	.942-0	.969-0	.984-0	.992-0	.996-0	.998-0	.999-0				6
7	.883-0	.932-0	.962-0	.979-0	.989-0	.994-0	.997-0	.999-0	.999-0		7
8	.794-0	.870-0	.922-0	.954-0	.974-0	.986-0	.993-0	.996-0	.998-0	.999-0	8
9	.679-0	.782-0	.859-0	.912-0	.947-0	.969-0	.983-0	.990-0	.995-0	.997-0	9
10	.549-0	.671-0	.771-0	.848-0	.903-0	.940-0	.964-0	.979-0	.988-0	.993-0	10
11	.417-0	.546-0	.664-0	.762-0	.838-0	.894-0	.933-0	.959-0	.975-0	.986-0	11
12	.297-0	.421-0	.544-0	.658-0	.753-0	.829-0	.886-0	.926-0	.954-0	.972-0	12
13	.198-0	.305-0	.424-0	.543-0	.652-0	.746-0	.821-0	.878-0	.920-0	.949-0	13
14	.124-0	.209-0	.313-0	.427-0	.541-0	.647-0	.738-0	.813-0	.871-0	.913-0	14
15	.726-1	.134-0	.218-0	.319-0	.429-0	.540-0	.642-0	.732-0	.806-0	.864-0	15
16	.399-1	.814-1	.144-0	.227-0	.325-0	.432-0	.539-0	.638-0	.726-0	.799-0	16
17	.206-1	.465-1	.899-1	.153-0	.235-0	.331-0	.434-0	.537-0	.634-0	.720-0	17
18	.100-1	.251-1	.531-1	.979-1	.161-0	.242-0	.336-0	.436-0	.536-0	.631-0	18
19	.458-2	.128-1	.297-1	.596-1	.106-0	.169-0	.249-0	.340-0	.438-0	.535-0	19
20	.198-2	.616-2	.158-1	.344-1	.659-1	.113-0	.176-0	.255-0	.344-0	.439-0	20
21	.808-3	.281-2	.794-2	.189-1	.392-1	.721-1	.120-0	.183-0	.261-0	.348-0	21
22	.312-3	.122-2	.380-2	.991-2	.222-1	.440-1	.781-1	.127-0	.190-0	.266-0	22
23	.114-3	.500-3	.173-2	.494-2	.120-1	.256-1	.487-1	.840-1	.133-0	.196-0	23
24	.396-4	.195-3	.750-3	.235-2	.623-2	.143-1	.291-1	.534-1	.896-1	.139-0	24
25	.131-4	.726-4	.310-3	.107-2	.308-2	.765-2	.167-1	.327-1	.581-1	.951-1	25
26	.410-5	.257-4	.122-3	.464-3	.146-2	.392-2	.919-2	.192-1	.362-1	.627-1	26
27	.122-5	.869-5	.461-4	.193-3	.662-3	.192-2	.485-2	.108-1	.218-1	.398-1	27
28	.348-6	.280-5	.166-4	.767-4	.288-3	.907-3	.246-2	.589-2	.126-1	.244-1	28
29	.944-7	.864-6	.573-5	.292-4	.120-3	.411-3	.120-2	.308-2	.701-2	.144-1	29
30	.244-7	.255-6	.189-5	.107-4	.481-4	.179-3	.565-3	.155-2	.377-2	.822-2	30
31	.605-8	.718-7	.599-6	.375-5	.185-4	.749-4	.256-3	.753-3	.195-2	.453-2	31
32	.143-8	.194-7	.182-6	.126-5	.686-5	.302-4	.111-3	.352-3	.976-3	.241-2	32
33	.323-9	.502-8	.531-7	.410-6	.244-5	.117-4	.468-4	.159-3	.472-3	.124-2	33
34	.700-10	.125-8	.149-7	.128-6	.839-6	.439-5	.190-4	.695-4	.220-3	.615-3	34
35	.145-10	.297-9	.400-8	.383-7	.277-6	.159-5	.743-5	.293-4	.994-4	.296-3	35
36		.680-10	.104-8	.111-7	.884-7	.553-6	.281-5	.119-4	.434-4	.138-3	36
37		.149-10	.258-9	.308-8	.272-7	.186-6	.103-5	.470-5	.183-4	.621-4	37
38			.619-10	.828-9	.808-8	.605-7	.363-6	.179-5	.751-5	.272-4	38
39			.143-10	.214-9	.232-8	.190-7	.124-6	.663-6	.298-5	.115-4	39
40				.536-10	.641-9	.578-8	.410-7	.237-6	.114-5	.473-5	40
41				.129-10	.172-9	.170-8	.132-7	.822-7	.427-6	.189-5	41
42					.445-10	.485-9	.409-8	.276-7	.154-6	.730-6	42
43						.134-9	.123-8	.901-8	.542-7	.274-6	43
44						.111-10	.357-10	.359-9	.285-8	.185-7	44
45								.102-9	.876-9	.612-8	45
46								.279-10	.261-9	.197-8	46
47									.757-10	.616-9	47
48									.213-10	.187-9	48
49										.555-10	49

R	N=0100	N=0110	N=0120	N=0130	N=0140	N=0150	N=0160	N=0170	N=0180	N=0190	R	P=1/10
50									.160-10	.133- 9	50	
51										.401-10	51	
52										.118-10	52	

R	N=0200	N=0210	N=0220	N=0230	N=0240	N=0250	N=0260	N=0270	N=0280	N=0290	R
9	.999- 0	.999- 0									9
10	.996- 0	.998- 0	.999- 0	.999- 0							10
11	.992- 0	.996- 0	.998- 0	.999- 0	.999- 0						11
12	.983- 0	.990- 0	.995- 0	.997- 0	.998- 0	.999- 0					12
13	.968- 0	.981- 0	.989- 0	.993- 0	.996- 0	.998- 0	.999- 0	.999- 0			13
14	.943- 0	.964- 0	.978- 0	.987- 0	.992- 0	.995- 0	.997- 0	.999- 0	.999- 0	.999- 0	14
15	.907- 0	.938- 0	.961- 0	.975- 0	.985- 0	.991- 0	.994- 0	.997- 0	.998- 0	.998- 0	15
16	.857- 0	.901- 0	.934- 0	.956- 0	.972- 0	.982- 0	.989- 0	.994- 0	.996- 0	.998- 0	16
17	.793- 0	.851- 0	.896- 0	.929- 0	.953- 0	.969- 0	.980- 0	.988- 0	.993- 0	.996- 0	17
18	.715- 0	.787- 0	.845- 0	.890- 0	.924- 0	.949- 0	.966- 0	.978- 0	.986- 0	.991- 0	18
19	.628- 0	.710- 0	.781- 0	.839- 0	.885- 0	.919- 0	.945- 0	.963- 0	.976- 0	.985- 0	19
20	.534- 0	.625- 0	.706- 0	.776- 0	.833- 0	.879- 0	.915- 0	.941- 0	.960- 0	.974- 0	20
21	.441- 0	.534- 0	.622- 0	.701- 0	.771- 0	.828- 0	.874- 0	.910- 0	.937- 0	.957- 0	21
22	.352- 0	.442- 0	.533- 0	.619- 0	.697- 0	.766- 0	.823- 0	.870- 0	.906- 0	.934- 0	22
23	.271- 0	.355- 0	.444- 0	.532- 0	.617- 0	.694- 0	.761- 0	.818- 0	.865- 0	.902- 0	23
24	.202- 0	.276- 0	.359- 0	.445- 0	.531- 0	.614- 0	.690- 0	.757- 0	.814- 0	.860- 0	24
25	.145- 0	.207- 0	.281- 0	.361- 0	.446- 0	.531- 0	.612- 0	.687- 0	.753- 0	.809- 0	25
26	.100- 0	.150- 0	.213- 0	.284- 0	.364- 0	.447- 0	.530- 0	.610- 0	.684- 0	.749- 0	26
27	.672- 1	.106- 0	.156- 0	.217- 0	.288- 0	.366- 0	.448- 0	.530- 0	.608- 0	.681- 0	27
28	.434- 1	.717- 1	.111- 0	.161- 0	.222- 0	.292- 0	.369- 0	.449- 0	.529- 0	.606- 0	28
29	.271- 1	.470- 1	.766- 1	.115- 0	.166- 0	.226- 0	.296- 0	.371- 0	.450- 0	.529- 0	29
30	.163- 1	.298- 1	.506- 1	.803- 1	.120- 0	.170- 0	.231- 0	.299- 0	.373- 0	.451- 0	30
31	.951- 2	.183- 1	.326- 1	.541- 1	.845- 1	.125- 0	.175- 0	.235- 0	.302- 0	.376- 0	31
32	.532- 2	.109- 1	.203- 1	.354- 1	.577- 1	.886- 1	.129- 0	.179- 0	.239- 0	.305- 0	32
33	.292- 2	.625- 2	.123- 1	.224- 1	.382- 1	.611- 1	.926- 1	.133- 0	.183- 0	.242- 0	33
34	.154- 2	.348- 2	.720- 2	.138- 1	.245- 1	.410- 1	.646- 1	.965- 1	.137- 0	.187- 0	34
35	.784- 3	.188- 2	.409- 2	.822- 2	.153- 1	.267- 1	.438- 1	.680- 1	.100- 0	.141- 0	35
36	.388- 3	.981- 3	.225- 2	.475- 2	.928- 2	.169- 1	.289- 1	.466- 1	.713- 1	.104- 0	36
37	.186- 3	.497- 3	.120- 2	.267- 2	.547- 2	.104- 1	.185- 1	.311- 1	.494- 1	.746- 1	37
38	.863- 4	.245- 3	.625- 3	.146- 2	.313- 2	.623- 2	.116- 1	.202- 1	.333- 1	.522- 1	38
39	.389- 4	.117- 3	.315- 3	.773- 3	.174- 2	.362- 2	.703- 2	.128- 1	.219- 1	.356- 1	39
40	.170- 4	.541- 4	.154- 3	.398- 3	.942- 3	.205- 2	.416- 2	.788- 2	.140- 1	.236- 1	40
41	.722- 5	.244- 4	.734- 4	.200- 3	.496- 3	.113- 2	.239- 2	.473- 2	.876- 2	.153- 1	41
42	.298- 5	.107- 4	.340- 4	.974- 4	.254- 3	.607- 3	.134- 2	.277- 2	.533- 2	.969- 2	42
43	.119- 5	.454- 5	.153- 4	.462- 4	.127- 3	.317- 3	.734- 3	.158- 2	.317- 2	.597- 2	43
44	.465- 6	.188- 5	.669- 5	.213- 4	.615- 4	.162- 3	.391- 3	.877- 3	.183- 2	.360- 2	44
45	.176- 6	.756- 6	.285- 5	.960- 5	.291- 4	.803- 4	.203- 3	.476- 3	.104- 2	.211- 2	45
46	.650- 7	.296- 6	.118- 5	.420- 5	.134- 4	.388- 4	.103- 3	.252- 3	.572- 3	.121- 2	46
47	.233- 7	.113- 6	.479- 6	.180- 5	.603- 5	.183- 4	.509- 4	.130- 3	.308- 3	.679- 3	47
48	.814- 8	.420- 7	.189- 6	.747- 6	.264- 5	.844- 5	.245- 4	.655- 4	.162- 3	.372- 3	48
49	.277- 8	.152- 7	.724- 7	.303- 6	.113- 5	.379- 5	.116- 4	.323- 4	.831- 4	.199- 3	49
50	.918- 9	.537- 8	.271- 7	.120- 6	.472- 6	.166- 5	.531- 5	.155- 4	.417- 4	.104- 3	50
51	.296- 9	.185- 8	.991- 8	.464- 7	.192- 6	.712- 6	.239- 5	.729- 5	.205- 4	.531- 4	51
52	.933-10	.620- 9	.353- 8	.175- 7	.764- 7	.298- 6	.105- 5	.298- 5	.981- 5	.266- 4	52
53	.286-10	.203- 9	.123- 8	.644- 8	.297- 7	.122- 6	.449- 6	.150- 5	.460- 5	.130- 4	53
54		.649-10	.417- 9	.232- 8	.113- 7	.486- 7	.188- 6	.660- 6	.211- 5	.621- 5	54
55		.202-10	.138- 9	.813- 9	.418- 8	.190- 7	.772- 7	.283- 6	.947- 6	.291- 5	55
56			.447-10	.279- 9	.151- 8	.725- 8	.309- 7	.119- 6	.416- 6	.133- 5	56
57			.141-10	.936-10	.537- 9	.271- 8	.489- 7	.179- 6	.597- 6	.597- 6	57
58				.307-10	.186- 9	.988- 9	.466- 8	.197- 7	.753- 7	.262- 6	58
59					.630-10	.353- 9	.175- 8	.775- 8	.310- 7	.113- 6	59
60					.209-10	.123- 9	.644- 9	.299- 8	.125- 7	.476- 7	60
61						.423-10	.232- 9	.113- 8	.495- 8	.197- 7	61
62						.142-10	.817-10	.418- 9	.192- 8	.797- 8	62
63							.282-10	.152- 9	.730- 9	.316- 8	63
64								.540-10	.272- 9	.123- 8	64
65								.188-10	.992-10	.470- 9	65
66									.355-10	.176- 9	66
67									.125-10	.647-10	67
68										.233-10	68

R	N=0300	N=0310	N=0320	N=0330	N=0340	N=0350	N=0360	N=0370	N=0380	N=0390	R
15	.999- 0										15
16	.999- 0	.999- 0									16
17	.997- 0	.998- 0	.999- 0	.999- 0							17
18	.995- 0	.997- 0	.998- 0	.999- 0	.999- 0						18
19	.990- 0	.994- 0	.996- 0	.998- 0	.999- 0	.999- 0					19
20	.983- 0	.989- 0	.993- 0	.996- 0	.997- 0	.998- 0	.999- 0	.999- 0			20
21	.971- 0	.981- 0	.988- 0	.992- 0	.995- 0	.997- 0	.998- 0	.999- 0	.999- 0		21
22	.954- 0	.969- 0	.979- 0	.987- 0	.991- 0	.995- 0	.997- 0	.998- 0	.999- 0	.999- 0	22
23	.930- 0	.951- 0	.967- 0	.978- 0	.985- 0	.990- 0	.994- 0	.996- 0	.998- 0	.999- 0	23
24	.898- 0	.926- 0	.948- 0	.964- 0	.976- 0	.984- 0	.989- 0	.993- 0	.996- 0	.997- 0	24
25	.856- 0	.894- 0	.923- 0	.945- 0	.962- 0	.974- 0	.982- 0	.988- 0	.992- 0	.995- 0	25
26	.805- 0	.852- 0	.890- 0	.920- 0	.942- 0	.959- 0	.972- 0	.981- 0	.987- 0	.992- 0	26



R	N=0300	N=0310	N=0320	N=0330	N=0340	N=0350	N=0360	N=0370	N=0380	N=0390	R	P=1/10
27	•745-0	•801-0	•848-0	•886-0	•916-0	•939-0	•957-0	•970-0	•980-0	•986-0	27	
28	•678-0	•742-0	•797-0	•844-0	•882-0	•913-0	•937-0	•955-0	•968-0	•978-0	28	
29	•604-0	•675-0	•738-0	•793-0	•840-0	•879-0	•910-0	•934-0	•952-0	•966-0	29	
30	•528-0	•603-0	•672-0	•735-0	•790-0	•836-0	•875-0	•906-0	•931-0	•950-0	30	
31	•452-0	•528-0	•601-0	•670-0	•732-0	•786-0	•833-0	•872-0	•903-0	•928-0	31	
32	•377-0	•452-0	•527-0	•600-0	•667-0	•729-0	•783-0	•829-0	•868-0	•900-0	32	
33	•308-0	•379-0	•453-0	•527-0	•598-0	•665-0	•726-0	•780-0	•826-0	•865-0	33	
34	•246-0	•311-0	•381-0	•454-0	•526-0	•597-0	•663-0	•723-0	•776-0	•823-0	34	
35	•191-0	•249-0	•314-0	•383-0	•455-0	•526-0	•595-0	•661-0	•720-0	•773-0	35	
36	•145-0	•195-0	•253-0	•316-0	•385-0	•455-0	•526-0	•594-0	•659-0	•718-0	36	
37	•108-0	•149-0	•199-0	•256-0	•319-0	•386-0	•456-0	•525-0	•593-0	•657-0	37	
38	•779-1	•111-0	•153-0	•202-0	•259-0	•321-0	•388-0	•456-0	•525-0	•592-0	38	
39	•549-1	•811-1	•115-0	•156-0	•206-0	•262-0	•323-0	•389-0	•457-0	•525-0	39	
40	•378-1	•577-1	•842-1	•118-0	•160-0	•209-0	•265-0	•326-0	•391-0	•457-0	40	
41	•254-1	•401-1	•604-1	•873-1	•122-0	•163-0	•212-0	•267-0	•328-0	•392-0	41	
42	•166-1	•272-1	•423-1	•631-1	•904-1	•125-0	•166-0	•215-0	•270-0	•330-0	42	
43	•106-1	•180-1	•290-1	•446-1	•658-1	•934-1	•128-0	•170-0	•218-0	•272-0	43	
44	•665-2	•116-1	•194-1	•308-1	•468-1	•684-1	•963-1	•131-0	•173-0	•221-0	44	
45	•405-2	•735-2	•127-1	•208-1	•326-1	•491-1	•710-1	•992-1	•134-0	•176-0	45	
46	•242-2	•454-2	•809-2	•137-1	•222-1	•344-1	•513-1	•736-1	•102-0	•137-0	46	
47	•141-2	•274-2	•506-2	•886-2	•148-1	•236-1	•363-1	•535-1	•762-1	•105-0	47	
48	•800-3	•162-2	•309-2	•560-2	•965-2	•159-1	•251-1	•381-1	•557-1	•787-1	48	
49	•444-3	•933-3	•185-2	•346-2	•616-2	•105-1	•170-1	•266-1	•399-1	•579-1	49	
50	•242-3	•526-3	•108-2	•209-2	•385-2	•675-2	•113-1	•182-1	•281-1	•418-1	50	
51	•128-3	•290-3	•617-3	•124-2	•236-2	•426-2	•736-2	•122-1	•193-1	•296-1	51	
52	•668-4	•157-3	•345-3	•717-3	•141-2	•264-2	•470-2	•800-2	•131-1	•205-1	52	
53	•340-4	•828-4	•189-3	•407-3	•828-3	•160-2	•294-2	•515-2	•866-2	•140-1	53	
54	•169-4	•428-4	•102-3	•226-3	•476-3	•949-3	•180-2	•325-2	•563-2	•934-2	54	
55	•824-5	•217-4	•534-4	•123-3	•268-3	•552-3	•108-2	•201-2	•359-2	•612-2	55	
56	•393-5	•108-4	•275-4	•657-4	•148-3	•315-3	•636-3	•122-2	•224-2	•394-2	56	
57	•184-5	•523-5	•139-4	•344-4	•801-4	•176-3	•367-3	•728-3	•138-2	•249-2	57	
58	•841-6	•249-5	•685-5	•176-4	•425-4	•967-4	•208-3	•425-3	•828-3	•154-2	58	
59	•377-6	•116-5	•332-5	•885-5	•221-4	•520-4	•116-3	•244-3	•489-3	•936-3	59	
60	•166-6	•531-6	•158-5	•436-5	•113-4	•274-4	•630-4	•137-3	•284-3	•559-3	60	
61	•713-7	•238-6	•734-6	•211-5	•565-5	•142-4	•337-4	•757-4	•161-3	•328-3	61	
62	•301-7	•105-6	•335-6	•998-6	•277-5	•723-5	•177-4	•411-4	•902-4	•189-3	62	
63	•125-7	•451-7	•150-6	•464-6	•134-5	•360-5	•914-5	•219-4	•495-4	•107-3	63	
64	•507-8	•191-7	•661-7	•212-6	•633-6	•177-5	•463-5	•114-4	•267-4	•593-4	64	
65	•202-8	•792-8	•285-7	•950-7	•294-6	•849-6	•230-5	•587-5	•142-4	•324-4	65	
66	•790-9	•323-8	•121-7	•418-7	•134-6	•401-6	•112-5	•296-5	•737-5	•174-4	66	
67	•303-9	•129-8	•502-8	•180-7	•600-7	•186-6	•539-6	•147-5	•377-5	•916-5	67	
68	•114-9	•506-9	•205-8	•765-8	•264-7	•848-7	•254-6	•715-6	•190-5	•475-5	68	
69	•422-10	•195-9	•823-9	•319-8	•114-7	•380-7	•118-6	•343-6	•937-6	•242-5	69	
70	•153-10	•738-10	•324-9	•131-8	•485-8	•167-7	•537-7	•161-6	•455-6	•121-5	70	
71		•274-10	•125-9	•202-8	•202-8	•723-8	•240-7	•746-7	•218-6	•598-6	71	
72		•100-10	•477-10	•208-9	•831-9	•307-8	•106-7	•340-7	•102-6	•290-6	72	
73			•806-10	•335-9	•129-8	•458-8	•152-7	•473-7	•138-6	•138-6	73	
74			•178-10	•308-10	•133-9	•529-9	•195-8	•670-8	•215-7	•649-7	74	
75				•116-10	•518-10	•214-9	•816-9	•290-8	•963-8	•300-7	75	
76					•199-10	•850-10	•336-9	•124-8	•424-8	•136-7	76	
77						•333-10	•136-9	•519-9	•184-8	•610-8	77	
78						•128-10	•544-10	•214-9	•784-9	•269-8	78	
79							•214-10	•870-10	•329-9	•117-8	79	
80								•348-10	•136-9	•498-9	80	
81								•137-10	•555-10	•209-9	81	
82									•223-10	•867-10	82	
83										•354-10	83	
84										•142-10	84	

R	N=0400	N=0410	N=0420	N=0430	N=0440	N=0450	N=0460	N=0470	N=0480	N=0490	R
23	•999-0	•999-0									23
24	•998-0	•999-0	•999-0								24
25	•997-0	•998-0	•999-0	•999-0							25
26	•995-0	•997-0	•998-0	•999-0	•999-0	•999-0					26
27	•991-0	•994-0	•996-0	•998-0	•998-0	•999-0	•999-0				27
28	•985-0	•990-0	•993-0	•996-0	•997-0	•998-0	•999-0	•999-0			28
29	•977-0	•984-0	•989-0	•993-0	•995-0	•997-0	•998-0	•999-0	•999-0		29
30	•964-0	•975-0	•983-0	•988-0	•992-0	•995-0	•997-0	•998-0	•999-0	•999-0	30
31	•948-0	•962-0	•973-0	•982-0	•987-0	•991-0	•994-0	•996-0	•998-0	•998-0	31
32	•925-0	•945-0	•960-0	•972-0	•980-0	•986-0	•991-0	•994-0	•996-0	•997-0	32
33	•897-0	•923-0	•943-0	•959-0	•970-0	•979-0	•985-0	•990-0	•993-0	•995-0	33
34	•862-0	•894-0	•920-0	•941-0	•957-0	•969-0	•978-0	•984-0	•989-0	•993-0	34
35	•820-0	•859-0	•891-0	•917-0	•938-0	•955-0	•967-0	•976-0	•983-0	•988-0	35
36	•770-0	•816-0	•856-0	•888-0	•915-0	•936-0	•953-0	•965-0	•975-0	•982-0	36
37	•715-0	•768-0	•813-0	•853-0	•885-0	•912-0	•934-0	•951-0	•964-0	•974-0	37
38	•655-0	•713-0	•765-0	•810-0	•850-0	•883-0	•910-0	•932-0	•949-0	•962-0	38
39	•591-0	•653-0	•710-0	•762-0	•808-0	•847-0	•880-0	•907-0	•929-0	•947-0	39
40	•524-0	•589-0	•651-0	•708-0	•759-0	•805-0	•844-0	•877-0	•905-0	•927-0	40
41	•458-0	•524-0	•588-0	•649-0	•706-0	•757-0	•802-0	•841-0	•875-0	•902-0	41
42	•393-0	•459-0	•524-0	•587-0	•648-0	•704-0	•754-0	•800-0	•839-0	•872-0	42
43	•332-0	•395-0	•459-0	•524-0	•586-0	•646-0	•702-0	•752-0	•797-0	•836-0	43
44	•275-0	•334-0	•396-0	•460-0	•523-0	•585-0	•645-0	•700-0	•750-0	•794-0	44

R	N=0400	N=0410	N=0420	N=0430	N=0440	N=0450	N=0460	N=0470	N=0480	N=0490	R	P=1/10
45	.224-0	.277-0	.336-0	.397-0	.460-0	.523-0	.584-0	.643-0	.698-0	.748-0	45	
46	.179-0	.226-0	.280-0	.337-0	.398-0	.460-0	.523-0	.584-0	.642-0	.696-0	46	
47	.140-0	.181-0	.229-0	.282-0	.339-0	.399-0	.461-0	.522-0	.583-0	.640-0	47	
48	.108-0	.143-0	.184-0	.232-0	.284-0	.341-0	.400-0	.461-0	.522-0	.582-0	48	
49	.812-1	.110-0	.146-0	.187-0	.234-0	.286-0	.342-0	.401-0	.462-0	.522-0	49	
50	.601-1	.837-1	.113-0	.148-0	.190-0	.236-0	.288-0	.344-0	.402-0	.462-0	50	
51	.436-1	.623-1	.861-1	.116-0	.151-0	.192-0	.239-0	.290-0	.345-0	.403-0	51	
52	.311-1	.455-1	.644-1	.885-1	.118-0	.154-0	.195-0	.241-0	.292-0	.347-0	52	
53	.217-1	.326-1	.473-1	.666-1	.909-1	.121-0	.156-0	.197-0	.243-0	.294-0	53	
54	.149-1	.230-1	.341-1	.492-1	.687-1	.932-1	.123-0	.159-0	.200-0	.246-0	54	
55	.100-1	.159-1	.242-1	.357-1	.510-1	.708-1	.955-1	.126-0	.161-0	.202-0	55	
56	.664-2	.108-1	.168-1	.254-1	.372-1	.528-1	.728-1	.978-1	.128-0	.164-0	56	
57	.431-2	.717-2	.115-1	.178-1	.267-1	.388-1	.546-1	.749-1	.100-0	.130-0	57	
58	.274-2	.469-2	.772-2	.123-1	.188-1	.280-1	.403-1	.565-1	.770-1	.102-0	58	
59	.171-2	.301-2	.509-2	.829-2	.130-1	.198-1	.292-1	.418-1	.583-1	.790-1	59	
60	.105-2	.190-2	.330-2	.551-2	.887-2	.138-1	.208-1	.305-1	.434-1	.601-1	60	
61	.635-3	.118-2	.210-2	.360-2	.594-2	.947-2	.146-1	.219-1	.318-1	.449-1	61	
62	.376-3	.718-3	.131-2	.231-2	.391-2	.638-2	.101-1	.154-1	.229-1	.331-1	62	
63	.219-3	.429-3	.807-3	.146-2	.253-2	.423-2	.685-2	.107-1	.163-1	.240-1	63	
64	.125-3	.252-3	.487-3	.903-3	.161-2	.276-2	.457-2	.732-2	.114-1	.171-1	64	
65	.704-4	.146-3	.289-3	.550-3	.101-2	.177-2	.300-2	.492-2	.781-2	.120-1	65	
66	.389-4	.829-4	.169-3	.330-3	.619-3	.112-2	.194-2	.325-2	.528-2	.831-2	66	
67	.211-4	.463-4	.971-4	.195-3	.374-3	.692-3	.123-2	.212-2	.352-2	.566-2	67	
68	.113-4	.255-4	.548-4	.113-3	.223-3	.423-3	.771-3	.136-2	.231-2	.379-2	68	
69	.592-5	.138-4	.305-4	.645-4	.131-3	.254-3	.475-3	.856-3	.149-2	.250-2	69	
70	.306-5	.731-5	.167-4	.362-4	.753-4	.150-3	.288-3	.531-3	.946-3	.163-2	70	
71	.155-5	.382-5	.896-5	.200-4	.427-4	.874-4	.172-3	.325-3	.592-3	.104-2	71	
72	.776-6	.197-5	.474-5	.109-4	.239-4	.501-4	.101-3	.195-3	.365-3	.657-3	72	
73	.381-6	.996-6	.247-5	.582-5	.131-4	.283-4	.584-4	.116-3	.221-3	.408-3	73	
74	.185-6	.496-6	.127-5	.307-5	.710-5	.157-4	.333-4	.677-4	.132-3	.250-3	74	
75	.879-7	.243-6	.638-6	.159-5	.378-5	.859-5	.187-4	.389-4	.780-4	.151-3	75	
76	.412-7	.117-6	.317-6	.813-6	.199-5	.463-5	.103-4	.220-4	.453-4	.895-4	76	
77	.190-7	.558-7	.155-6	.409-6	.103-5	.246-5	.562-5	.123-4	.259-4	.524-4	77	
78	.863-8	.261-7	.748-7	.203-6	.523-6	.128-5	.301-5	.677-5	.146-4	.302-4	78	
79	.386-8	.121-7	.355-7	.990-7	.262-6	.662-6	.159-5	.367-5	.810-5	.172-4	79	
80	.170-8	.547-8	.166-7	.476-7	.130-6	.336-6	.830-6	.196-5	.444-5	.964-5	80	
81	.739-9	.245-8	.764-8	.226-7	.632-7	.168-6	.426-6	.103-5	.240-5	.533-5	81	
82	.316-9	.108-8	.347-8	.105-7	.303-7	.829-7	.216-6	.536-6	.127-5	.291-5	82	
83	.133-9	.468-9	.155-8	.485-8	.144-7	.403-7	.108-6	.274-6	.669-6	.156-5	83	
84	.552-10	.200-9	.684-9	.220-8	.669-8	.193-7	.530-7	.139-6	.346-6	.828-6	84	
85	.226-10	.845-10	.297-9	.984-9	.308-8	.913-8	.257-7	.690-7	.177-6	.433-6	85	
86		.351-10	.127-9	.434-9	.140-8	.425-8	.123-7	.339-7	.890-7	.223-6	86	
87		.144-10	.537-10	.189-9	.624-9	.195-8	.580-8	.164-7	.442-7	.114-6	87	
88			.224-10	.800-10	.275-9	.886-9	.270-8	.783-8	.216-7	.571-7	88	
89				.342-10	.120-9	.396-9	.124-8	.369-8	.105-7	.283-7	89	
90				.142-10	.513-10	.175-9	.562-9	.172-8	.499-8	.138-7	90	
91					.217-10	.760-10	.251-9	.788-9	.235-8	.667-8	91	
92						.326-10	.111-9	.357-9	.109-8	.318-8	92	
93						.138-10	.482-10	.159-9	.500-9	.149-8	93	
94							.207-10	.703-10	.227-9	.694-9	94	
95								.306-10	.101-9	.318-9	95	
96								.132-10	.447-10	.144-9	96	
97									.195-10	.643-10	97	
98										.284-10	98	
99										.124-10	99	

R	N=0500	N=0510	N=0520	N=0530	N=0540	N=0550	N=0560	N=0570	N=0580	N=0590	R
30	.999-0										30
31	.999-0	.999-0									31
32	.998-0	.999-0	.999-0								32
33	.997-0	.998-0	.999-0	.999-0	.999-0						33
34	.995-0	.997-0	.998-0	.999-0	.999-0	.999-0					34
35	.992-0	.995-0	.996-0	.998-0	.998-0	.999-0	.999-0				35
36	.988-0	.991-0	.994-0	.996-0	.997-0	.998-0	.999-0	.999-0			36
37	.981-0	.987-0	.991-0	.994-0	.996-0	.997-0	.998-0	.999-0	.999-0		37
38	.973-0	.980-0	.986-0	.990-0	.993-0	.995-0	.997-0	.998-0	.999-0	.999-0	38
39	.961-0	.971-0	.979-0	.985-0	.990-0	.993-0	.995-0	.997-0	.998-0	.998-0	39
40	.945-0	.959-0	.970-0	.978-0	.984-0	.989-0	.992-0	.995-0	.996-0	.998-0	40
41	.925-0	.943-0	.957-0	.969-0	.977-0	.984-0	.988-0	.992-0	.994-0	.996-0	41
42	.900-0	.923-0	.941-0	.956-0	.967-0	.976-0	.983-0	.988-0	.991-0	.994-0	42
43	.869-0	.898-0	.921-0	.939-0	.954-0	.966-0	.975-0	.982-0	.987-0	.991-0	43
44	.834-0	.867-0	.895-0	.918-0	.937-0	.953-0	.965-0	.974-0	.981-0	.986-0	44
45	.792-0	.831-0	.865-0	.893-0	.916-0	.936-0	.951-0	.963-0	.973-0	.980-0	45
46	.745-0	.790-0	.829-0	.862-0	.891-0	.914-0	.934-0	.949-0	.962-0	.971-0	46
47	.694-0	.743-0	.787-0	.826-0	.860-0	.888-0	.912-0	.932-0	.948-0	.960-0	47
48	.639-0	.692-0	.741-0	.785-0	.824-0	.858-0	.886-0	.910-0	.930-0	.946-0	48
49	.581-0	.638-0	.690-0	.739-0	.783-0	.822-0	.855-0	.884-0	.908-0	.928-0	49
50	.522-0	.580-0	.636-0	.689-0	.737-0	.781-0	.819-0	.853-0	.882-0	.906-0	50
51	.462-0	.522-0	.579-0	.635-0	.687-0	.735-0	.779-0	.817-0	.851-0	.880-0	51
52	.404-0	.463-0	.521-0	.579-0	.634-0	.685-0	.733-0	.776-0	.815-0	.849-0	52
53	.348-0	.405-0	.463-0	.521-0	.578-0	.633-0	.684-0	.731-0	.774-0	.813-0	53
54	.296-0	.350-0	.406-0	.464-0	.521-0	.577-0	.631-0	.682-0	.730-0	.772-0	54

R	N=0500	N=0510	N=0520	N=0530	N=0540	N=0550	N=0560	N=0570	N=0580	N=0590	R	P=1/10
55	.248-0	.298-0	.351-0	.407-0	.464-0	.521-0	.577-0	.630-0	.681-0	.728-0	55	
56	.204-0	.250-0	.299-0	.352-0	.408-0	.464-0	.521-0	.576-0	.629-0	.679-0	56	
57	.166-0	.206-0	.252-0	.301-0	.354-0	.409-0	.465-0	.520-0	.575-0	.628-0	57	
58	.133-0	.168-0	.209-0	.254-0	.303-0	.355-0	.409-0	.465-0	.520-0	.575-0	58	
59	.104-0	.135-0	.170-0	.211-0	.256-0	.304-0	.356-0	.410-0	.465-0	.520-0	59	
60	.810-1	.107-0	.137-0	.173-0	.213-0	.258-0	.306-0	.357-0	.411-0	.465-0	60	
61	.618-1	.830-1	.109-0	.139-0	.175-0	.215-0	.259-0	.308-0	.359-0	.412-0	61	
62	.465-1	.636-1	.849-1	.111-0	.142-0	.177-0	.217-0	.261-0	.309-0	.360-0	62	
63	.344-1	.480-1	.654-1	.869-1	.113-0	.144-0	.179-0	.219-0	.263-0	.311-0	63	
64	.251-1	.357-1	.495-1	.671-1	.888-1	.115-0	.146-0	.181-0	.221-0	.265-0	64	
65	.180-1	.261-1	.370-1	.511-1	.688-1	.907-1	.117-0	.148-0	.183-0	.223-0	65	
66	.127-1	.188-1	.272-1	.383-1	.526-1	.706-1	.926-1	.119-0	.150-0	.185-0	66	
67	.883-2	.134-1	.197-1	.283-1	.396-1	.541-1	.723-1	.945-1	.121-0	.152-0	67	
68	.605-2	.936-2	.141-1	.206-1	.294-1	.409-1	.556-1	.740-1	.963-1	.123-0	68	
69	.408-2	.645-2	.990-2	.148-1	.215-1	.305-1	.422-1	.571-1	.756-1	.981-1	69	
70	.271-2	.438-2	.686-2	.104-1	.155-1	.224-1	.316-1	.435-1	.586-1	.773-1	70	
71	.177-2	.293-2	.468-2	.728-2	.110-1	.162-1	.233-1	.327-1	.448-1	.601-1	71	
72	.114-2	.193-2	.315-2	.500-2	.771-2	.116-1	.170-1	.242-1	.338-1	.461-1	72	
73	.727-3	.125-2	.209-2	.338-2	.533-2	.816-2	.122-1	.177-1	.252-1	.349-1	73	
74	.455-3	.801-3	.137-2	.226-2	.363-2	.566-2	.861-2	.128-1	.185-1	.261-1	74	
75	.280-3	.505-3	.879-3	.148-2	.243-2	.388-2	.601-2	.908-2	.134-1	.192-1	75	
76	.170-3	.314-3	.558-3	.963-3	.161-2	.262-2	.414-2	.637-2	.955-2	.140-1	76	
77	.102-3	.192-3	.350-3	.616-3	.105-2	.174-2	.281-2	.441-2	.673-2	.100-1	77	
78	.603-4	.116-3	.216-3	.388-3	.677-3	.114-2	.188-2	.301-2	.468-2	.711-2	78	
79	.351-4	.691-4	.131-3	.241-3	.429-3	.741-3	.124-2	.203-2	.321-2	.497-2	79	
80	.201-4	.406-4	.788-4	.148-3	.269-3	.474-3	.810-3	.135-2	.218-2	.343-2	80	
81	.114-4	.235-4	.466-4	.895-4	.166-3	.299-3	.521-3	.883-3	.145-2	.233-2	81	
82	.636-5	.134-4	.272-4	.534-4	.101-3	.186-3	.331-3	.571-3	.959-3	.157-2	82	
83	.350-5	.755-5	.157-4	.314-4	.608-4	.114-3	.207-3	.365-3	.624-3	.104-2	83	
84	.190-5	.419-5	.890-5	.182-4	.361-4	.690-4	.128-3	.230-3	.401-3	.681-3	84	
85	.102-5	.230-5	.499-5	.104-4	.211-4	.412-4	.780-4	.143-3	.254-3	.440-3	85	
86	.538-6	.124-5	.276-5	.590-5	.122-4	.243-4	.469-4	.878-4	.159-3	.281-3	86	
87	.280-6	.662-6	.151-5	.329-5	.695-5	.142-4	.279-4	.532-4	.985-4	.177-3	87	
88	.144-6	.349-6	.811-6	.181-5	.391-5	.814-5	.164-4	.319-4	.601-4	.110-3	88	
89	.731-7	.181-6	.431-6	.986-6	.217-5	.462-5	.948-5	.188-4	.363-4	.677-4	89	
90	.366-7	.929-7	.226-6	.529-6	.119-5	.259-5	.542-5	.110-4	.216-4	.411-4	90	
91	.181-7	.470-7	.117-6	.280-6	.645-6	.143-5	.306-5	.634-5	.127-4	.246-4	91	
92	.884-8	.235-7	.599-7	.146-6	.345-6	.781-6	.171-5	.361-5	.737-5	.146-4	92	
93	.426-8	.116-7	.302-7	.757-7	.182-6	.421-6	.941-6	.203-5	.423-5	.854-5	93	
94	.203-8	.565-8	.151-7	.386-7	.949-7	.224-6	.512-6	.113-5	.240-5	.494-5	94	
95	.951-9	.272-8	.742-8	.194-7	.488-7	.118-6	.275-6	.618-6	.134-5	.282-5	95	
96	.441-9	.129-8	.361-8	.967-8	.248-7	.614-7	.146-6	.335-6	.742-6	.159-5	96	
97	.202-9	.605-9	.173-8	.475-8	.125-7	.315-7	.766-7	.179-6	.406-6	.887-6	97	
98	.914-10	.280-9	.822-9	.231-8	.620-8	.160-7	.397-7	.950-7	.219-6	.489-6	98	
99	.408-10	.128-9	.385-9	.111-8	.304-8	.802-8	.203-7	.497-7	.117-6	.266-6	99	
100	.180-10	.581-10	.178-9	.524-9	.147-8	.397-8	.103-7	.257-7	.617-7	.143-6	100	
101		.259-10	.816-10	.245-9	.705-9	.195-8	.515-8	.131-7	.322-7	.762-7	101	
102		.114-10	.369-10	.113-9	.334-9	.941-9	.255-8	.663-8	.166-7	.401-7	102	
103			.165-10	.519-10	.156-9	.450-9	.124-8	.331-8	.846-8	.209-7	103	
104				.234-10	.722-10	.213-9	.601-9	.163-8	.426-8	.107-7	104	
105				.105-10	.330-10	.994-10	.287-9	.796-9	.212-8	.545-8	105	
106					.149-10	.459-10	.136-9	.384-9	.105-8	.274-8	106	
107						.210-10	.633-10	.183-9	.510-9	.136-8	107	
108							.292-10	.864-10	.245-9	.670-9	108	
109							.133-10	.403-10	.117-9	.326-9	109	
110								.186-10	.551-10	.157-9	110	
111									.257-10	.746-10	111	
112									.118-10	.351-10	112	
113										.164-10	113	

R	N=0600	N=0610	N=0620	N=0630	N=0640	N=0650	N=0660	N=0670	N=0680	N=0690	R
38	.999-0										38
39	.999-0	.999-0									39
40	.998-0	.999-0	.999-0								40
41	.997-0	.998-0	.999-0	.999-0							41
42	.996-0	.997-0	.998-0	.999-0	.999-0	.999-0					42
43	.993-0	.995-0	.997-0	.998-0	.999-0	.999-0	.999-0				43
44	.990-0	.993-0	.995-0	.997-0	.998-0	.998-0	.999-0	.999-0			44
45	.985-0	.990-0	.993-0	.995-0	.996-0	.998-0	.998-0	.999-0	.999-0	.999-0	45
46	.979-0	.985-0	.989-0	.992-0	.994-0	.996-0	.997-0	.998-0	.999-0	.999-0	46
47	.970-0	.978-0	.984-0	.988-0	.992-0	.994-0	.996-0	.997-0	.998-0	.999-0	47
48	.959-0	.969-0	.977-0	.983-0	.988-0	.991-0	.994-0	.996-0	.997-0	.998-0	48
49	.945-0	.958-0	.968-0	.976-0	.982-0	.987-0	.991-0	.993-0	.995-0	.997-0	49
50	.926-0	.943-0	.956-0	.967-0	.975-0	.982-0	.987-0	.990-0	.993-0	.995-0	50
51	.904-0	.925-0	.941-0	.955-0	.966-0	.974-0	.981-0	.986-0	.990-0	.993-0	51
52	.878-0	.902-0	.923-0	.940-0	.954-0	.965-0	.973-0	.980-0	.985-0	.989-0	52
53	.847-0	.876-0	.900-0	.921-0	.938-0	.952-0	.963-0	.972-0	.979-0	.985-0	53
54	.811-0	.845-0	.874-0	.899-0	.920-0	.937-0	.951-0	.962-0	.971-0	.978-0	54
55	.770-0	.809-0	.842-0	.872-0	.897-0	.918-0	.935-0	.950-0	.961-0	.970-0	55
56	.726-0	.769-0	.807-0	.840-0	.870-0	.895-0	.916-0	.934-0	.948-0	.960-0	56
57	.678-0	.724-0	.767-0	.805-0	.839-0	.868-0	.893-0	.914-0	.932-0	.947-0	57
58	.627-0	.677-0	.723-0	.765-0	.803-0	.837-0	.866-0	.891-0	.913-0	.931-0	58

R	N=0600	N=0610	N=0620	N=0630	N=0640	N=0650	N=0660	N=0670	N=0680	N=0690	R	P=1/10
59	.574-0	.626-0	.675-0	.721-0	.763-0	.801-0	.835-0	.864-0	.889-0	.911-0	59	
60	.520-0	.573-0	.625-0	.674-0	.720-0	.761-0	.799-0	.833-0	.862-0	.888-0	60	
61	.466-0	.520-0	.573-0	.624-0	.673-0	.718-0	.760-0	.797-0	.831-0	.860-0	61	
62	.412-0	.466-0	.520-0	.572-0	.623-0	.671-0	.716-0	.758-0	.796-0	.829-0	62	
63	.361-0	.413-0	.466-0	.519-0	.572-0	.622-0	.670-0	.715-0	.756-0	.794-0	63	
64	.312-0	.362-0	.414-0	.467-0	.519-0	.571-0	.621-0	.669-0	.714-0	.755-0	64	
65	.266-0	.313-0	.363-0	.414-0	.467-0	.519-0	.571-0	.620-0	.668-0	.712-0	65	
66	.225-0	.268-0	.315-0	.364-0	.415-0	.467-0	.519-0	.570-0	.619-0	.667-0	66	
67	.187-0	.226-0	.270-0	.316-0	.365-0	.416-0	.467-0	.519-0	.570-0	.619-0	67	
68	.154-0	.189-0	.228-0	.271-0	.317-0	.366-0	.416-0	.468-0	.519-0	.569-0	68	
69	.125-0	.156-0	.191-0	.230-0	.273-0	.319-0	.367-0	.417-0	.468-0	.519-0	69	
70	.999-1	.127-0	.158-0	.193-0	.232-0	.274-0	.320-0	.368-0	.418-0	.468-0	70	
71	.790-1	.102-0	.129-0	.159-0	.195-0	.233-0	.276-0	.321-0	.369-0	.418-0	71	
72	.616-1	.806-1	.103-0	.130-0	.161-0	.196-0	.235-0	.277-0	.322-0	.370-0	72	
73	.474-1	.631-1	.823-1	.105-0	.132-0	.163-0	.198-0	.237-0	.279-0	.324-0	73	
74	.360-1	.487-1	.646-1	.839-1	.107-0	.134-0	.165-0	.200-0	.238-0	.280-0	74	
75	.270-1	.372-1	.500-1	.660-1	.855-1	.109-0	.136-0	.167-0	.201-0	.240-0	75	
76	.200-1	.280-1	.383-1	.513-1	.675-1	.871-1	.110-0	.137-0	.168-0	.203-0	76	
77	.146-1	.208-1	.289-1	.394-1	.526-1	.689-1	.887-1	.112-0	.139-0	.170-0	77	
78	.105-1	.152-1	.216-1	.299-1	.405-1	.539-1	.704-1	.902-1	.114-0	.141-0	78	
79	.749-2	.110-1	.159-1	.224-1	.308-1	.416-1	.552-1	.718-1	.918-1	.115-0	79	
80	.526-2	.788-2	.115-1	.165-1	.232-1	.318-1	.428-1	.565-1	.732-1	.933-1	80	
81	.365-2	.556-2	.828-2	.121-1	.172-1	.240-1	.327-1	.439-1	.578-1	.746-1	81	
82	.250-2	.387-2	.587-2	.869-2	.126-1	.178-1	.248-1	.337-1	.450-1	.590-1	82	
83	.169-2	.266-2	.411-2	.619-2	.911-2	.131-1	.185-1	.256-1	.347-1	.461-1	83	
84	.112-2	.181-2	.284-2	.435-2	.651-2	.953-2	.137-1	.192-1	.264-1	.356-1	84	
85	.740-3	.121-2	.194-2	.302-2	.460-2	.684-2	.997-2	.142-1	.199-1	.272-1	85	
86	.481-3	.803-3	.131-2	.207-2	.321-2	.485-2	.718-2	.104-1	.148-1	.205-1	86	
87	.309-3	.525-3	.870-3	.140-2	.221-2	.340-2	.512-2	.753-2	.109-1	.153-1	87	
88	.196-3	.339-3	.572-3	.939-3	.150-2	.235-2	.360-2	.530-2	.788-2	.113-1	88	
89	.123-3	.216-3	.371-3	.621-3	.101-2	.161-2	.250-2	.381-2	.566-2	.824-2	89	
90	.760-4	.136-3	.238-3	.406-3	.673-3	.109-2	.172-2	.266-2	.402-2	.594-2	90	
91	.464-4	.849-4	.151-3	.262-3	.442-3	.727-3	.117-2	.184-2	.282-2	.423-2	91	
92	.280-4	.522-4	.947-4	.167-3	.287-3	.480-3	.785-3	.125-2	.195-2	.298-2	92	
93	.167-4	.317-4	.586-4	.105-3	.184-3	.313-3	.521-3	.845-3	.134-2	.208-2	93	
94	.985-5	.191-4	.358-4	.655-4	.117-3	.202-3	.341-3	.563-3	.908-3	.143-2	94	
95	.573-5	.113-4	.217-4	.403-4	.730-4	.129-3	.221-3	.371-3	.608-3	.974-3	95	
96	.330-5	.663-5	.129-4	.245-4	.452-4	.811-4	.142-3	.242-3	.403-3	.655-3	96	
97	.188-5	.384-5	.764-5	.147-4	.277-4	.505-4	.899-4	.156-3	.264-3	.436-3	97	
98	.105-5	.220-5	.446-5	.876-5	.167-4	.311-4	.563-4	.994-4	.171-3	.287-3	98	
99	.585-6	.125-5	.257-5	.515-5	.100-4	.190-4	.349-4	.626-4	.110-3	.187-3	99	
100	.321-6	.697-6	.147-5	.299-5	.593-5	.114-4	.214-4	.390-4	.694-4	.120-3	100	
101	.174-6	.386-6	.827-6	.172-5	.347-5	.679-5	.130-4	.240-4	.435-4	.767-4	101	
102	.936-7	.211-6	.461-6	.976-6	.200-5	.400-5	.776-5	.147-4	.269-4	.483-4	102	
103	.496-7	.114-6	.254-6	.548-6	.115-5	.233-5	.460-5	.883-5	.165-4	.301-4	103	
104	.260-7	.611-7	.139-6	.304-6	.649-6	.134-5	.270-5	.527-5	.999-5	.186-4	104	
105	.135-7	.323-7	.747-7	.167-6	.363-6	.764-6	.156-5	.311-5	.598-5	.113-4	105	
106	.693-8	.169-7	.398-7	.908-7	.201-6	.430-6	.896-6	.181-5	.354-5	.684-5	106	
107	.351-8	.874-8	.210-7	.488-7	.110-6	.240-6	.508-6	.105-5	.206-5	.408-5	107	
108	.176-8	.447-8	.110-7	.259-7	.595-7	.132-6	.285-6	.598-6	.119-5	.241-5	108	
109	.875-9	.226-8	.566-8	.136-7	.319-7	.722-7	.158-6	.338-6	.668-6	.141-5	109	
110	.429-9	.113-8	.289-8	.710-8	.169-7	.390-7	.871-7	.189-6	.367-6	.817-6	110	
111	.208-9	.561-9	.147-8	.365-8	.886-8	.208-7	.474-7	.105-6	.193-6	.468-6	111	
112	.100-9	.275-9	.737-9	.186-8	.460-8	.110-7	.255-7	.573-7	.934-7	.265-6	112	
113	.476-10	.133-9	.360-9	.938-9	.236-8	.576-8	.136-7	.311-7	.689-7	.149-6	113	
114	.224-10	.640-10	.176-9	.468-9	.120-8	.298-8	.716-8	.167-7	.376-7	.826-7	114	
115	.104-10	.304-10	.853-10	.231-9	.604-9	.153-8	.373-8	.805-8	.203-7	.454-7	115	
116		.143-10	.409-10	.113-9	.301-9	.774-9	.193-8	.465-8	.109-7	.247-7	116	
117			.194-10	.546-10	.148-9	.389-9	.986-9	.242-8	.577-8	.133-7	117	
118				.261-10	.723-10	.193-9	.499-9	.125-8	.302-8	.711-8	118	
119				.124-10	.349-10	.950-10	.250-9	.637-9	.157-8	.375-8	119	
120					.167-10	.463-10	.124-9	.322-9	.807-9	.196-8	120	
121						.223-10	.609-10	.161-9	.411-9	.102-8	121	
122						.107-10	.296-10	.797-10	.207-9	.522-9	122	
123								.143-10	.391-10	.103-9	123	
124									.190-10	.512-10	124	
125										.251-10	125	
126										.122-10	126	
127											127	

R	N=0700	N=0710	N=0720	N=0730	N=0740	N=0750	N=0760	N=0770	N=0780	N=0790	R
46	.999-0										46
47	.999-0	.999-0									47
48	.999-0	.999-0	.999-0								48
49	.998-0	.998-0	.999-0	.999-0							49
50	.996-0	.998-0	.998-0	.999-0	.999-0	.999-0					50
51	.995-0	.996-0	.997-0	.998-0	.999-0	.999-0	.999-0				51
52	.992-0	.994-0	.996-0	.997-0	.998-0	.999-0	.999-0	.999-0			52
53	.989-0	.992-0	.994-0	.996-0	.997-0	.998-0	.999-0	.999-0	.999-0		53
54	.984-0	.988-0	.991-0	.994-0	.996-0	.997-0	.998-0	.998-0	.999-0	.999-0	54
55	.978-0	.983-0	.988-0	.991-0	.993-0	.995-0	.997-0	.998-0	.998-0	.999-0	55
56	.969-0	.977-0	.983-0	.987-0	.990-0	.993-0	.995-0	.996-0	.997-0	.998-0	56

R	N=0700	N=0710	N=0720	N=0730	N=0740	N=0750	N=0760	N=0770	N=0780	N=0790	R	P=1/10
57	.959-0	.968-0	.976-0	.982-0	.986-0	.990-0	.993-0	.995-0	.996-0	.997-0	57	
58	.945-0	.958-0	.967-0	.975-0	.981-0	.986-0	.990-0	.992-0	.994-0	.996-0	58	
59	.929-0	.944-0	.956-0	.966-0	.974-0	.980-0	.985-0	.989-0	.992-0	.994-0	59	
60	.909-0	.928-0	.943-0	.955-0	.965-0	.973-0	.980-0	.985-0	.989-0	.992-0	60	
61	.886-0	.908-0	.926-0	.941-0	.954-0	.964-0	.973-0	.979-0	.984-0	.988-0	61	
62	.859-0	.884-0	.906-0	.925-0	.940-0	.953-0	.963-0	.972-0	.978-0	.984-0	62	
63	.827-0	.857-0	.882-0	.905-0	.923-0	.939-0	.952-0	.962-0	.971-0	.978-0	63	
64	.792-0	.826-0	.855-0	.881-0	.903-0	.922-0	.938-0	.951-0	.961-0	.970-0	64	
65	.753-0	.790-0	.824-0	.853-0	.879-0	.901-0	.920-0	.936-0	.949-0	.960-0	65	
66	.711-0	.752-0	.789-0	.822-0	.852-0	.877-0	.900-0	.919-0	.935-0	.948-0	66	
67	.665-0	.709-0	.750-0	.787-0	.820-0	.850-0	.876-0	.898-0	.917-0	.934-0	67	
68	.618-0	.664-0	.708-0	.748-0	.785-0	.819-0	.848-0	.874-0	.897-0	.916-0	68	
69	.569-0	.617-0	.663-0	.707-0	.747-0	.784-0	.817-0	.847-0	.873-0	.895-0	69	
70	.518-0	.568-0	.616-0	.662-0	.705-0	.746-0	.782-0	.815-0	.845-0	.871-0	70	
71	.468-0	.518-0	.568-0	.615-0	.661-0	.704-0	.744-0	.781-0	.814-0	.843-0	71	
72	.419-0	.468-0	.518-0	.567-0	.615-0	.660-0	.703-0	.743-0	.779-0	.812-0	72	
73	.371-0	.419-0	.469-0	.518-0	.567-0	.614-0	.659-0	.702-0	.741-0	.778-0	73	
74	.325-0	.372-0	.420-0	.469-0	.518-0	.566-0	.613-0	.658-0	.700-0	.740-0	74	
75	.282-0	.326-0	.372-0	.420-0	.469-0	.518-0	.566-0	.612-0	.657-0	.699-0	75	
76	.241-0	.283-0	.327-0	.373-0	.421-0	.469-0	.518-0	.565-0	.612-0	.656-0	76	
77	.205-0	.243-0	.284-0	.328-0	.374-0	.421-0	.470-0	.518-0	.565-0	.611-0	77	
78	.172-0	.206-0	.244-0	.286-0	.329-0	.375-0	.422-0	.470-0	.517-0	.565-0	78	
79	.143-0	.173-0	.208-0	.246-0	.287-0	.330-0	.376-0	.422-0	.470-0	.517-0	79	
80	.117-0	.144-0	.175-0	.210-0	.247-0	.288-0	.331-0	.376-0	.423-0	.470-0	80	
81	.948-1	.119-0	.146-0	.177-0	.211-0	.249-0	.289-0	.332-0	.377-0	.423-0	81	
82	.761-1	.963-1	.120-0	.147-0	.178-0	.213-0	.250-0	.291-0	.333-0	.378-0	82	
83	.603-1	.774-1	.978-1	.122-0	.149-0	.180-0	.214-0	.252-0	.292-0	.334-0	83	
84	.473-1	.616-1	.788-1	.993-1	.123-0	.151-0	.181-0	.216-0	.253-0	.293-0	84	
85	.366-1	.484-1	.628-1	.802-1	.101-0	.125-0	.152-0	.183-0	.217-0	.254-0	85	
86	.280-1	.376-1	.495-1	.641-1	.816-1	.102-0	.126-0	.154-0	.184-0	.218-0	86	
87	.212-1	.289-1	.386-1	.506-1	.653-1	.829-1	.104-0	.128-0	.155-0	.186-0	87	
88	.159-1	.219-1	.297-1	.395-1	.517-1	.665-1	.843-1	.105-0	.129-0	.157-0	88	
89	.118-1	.165-1	.226-1	.305-1	.405-1	.528-1	.678-1	.856-1	.107-0	.131-0	89	
90	.861-2	.122-1	.171-1	.233-1	.314-1	.415-1	.539-1	.690-1	.869-1	.108-0	90	
91	.623-2	.898-2	.127-1	.176-1	.241-1	.322-1	.424-1	.550-1	.702-1	.883-1	91	
92	.446-2	.652-2	.936-2	.132-1	.182-1	.248-1	.331-1	.434-1	.561-1	.714-1	92	
93	.315-2	.468-2	.682-2	.975-2	.137-1	.188-1	.255-1	.339-1	.444-1	.572-1	93	
94	.220-2	.333-2	.492-2	.713-2	.101-1	.142-1	.194-1	.262-1	.348-1	.454-1	94	
95	.152-2	.234-2	.351-2	.516-2	.744-2	.105-1	.147-1	.200-1	.269-1	.356-1	95	
96	.104-2	.162-2	.247-2	.369-2	.540-2	.776-2	.109-1	.152-1	.206-1	.277-1	96	
97	.705-3	.111-2	.172-2	.261-2	.388-2	.565-2	.808-2	.114-1	.157-1	.213-1	97	
98	.472-3	.757-3	.119-2	.183-2	.276-2	.407-2	.591-2	.841-2	.118-1	.162-1	98	
99	.312-3	.509-3	.811-3	.127-2	.194-2	.291-2	.427-2	.617-2	.875-2	.122-1	99	
100	.204-3	.338-3	.548-3	.868-3	.135-2	.205-2	.306-2	.448-2	.644-2	.909-2	100	
101	.132-3	.222-3	.366-3	.589-3	.927-3	.143-2	.217-2	.321-2	.469-2	.671-2	101	
102	.846-4	.145-3	.242-3	.395-3	.631-3	.989-3	.152-2	.228-2	.338-2	.490-2	102	
103	.536-4	.931-4	.158-3	.262-3	.425-3	.676-3	.105-2	.161-2	.241-2	.354-2	103	
104	.336-4	.593-4	.102-3	.172-3	.284-3	.457-3	.723-3	.112-2	.170-2	.254-2	104	
105	.208-4	.373-4	.654-4	.112-3	.187-3	.306-3	.491-3	.769-3	.119-2	.180-2	105	
106	.128-4	.233-4	.414-4	.719-4	.122-3	.203-3	.330-3	.524-3	.823-3	.126-2	106	
107	.775-5	.144-4	.259-4	.458-4	.790-4	.133-3	.220-3	.353-3	.564-3	.876-3	107	
108	.466-5	.876-5	.161-4	.288-4	.505-4	.865-4	.145-3	.235-3	.382-3	.602-3	108	
109	.277-5	.530-5	.988-5	.180-4	.320-4	.556-4	.946-4	.155-3	.257-3	.410-3	109	
110	.163-5	.317-5	.600-5	.111-4	.200-4	.354-4	.611-4	.100-3	.171-3	.277-3	110	
111	.949-6	.187-5	.361-5	.678-5	.124-4	.223-4	.391-4	.641-4	.112-3	.185-3	111	
112	.547-6	.110-5	.215-5	.410-5	.764-5	.139-4	.247-4	.402-4	.732-4	.122-3	112	
113	.312-6	.637-6	.127-5	.246-5	.465-5	.859-5	.155-4	.274-4	.473-4	.799-4	113	
114	.176-6	.366-6	.739-6	.146-5	.280-5	.525-5	.962-5	.172-4	.302-4	.518-4	114	
115	.985-7	.208-6	.427-6	.855-6	.167-5	.318-5	.591-5	.108-4	.191-4	.333-4	115	
116	.545-7	.117-6	.244-6	.497-6	.985-6	.191-5	.360-5	.664-5	.120-4	.212-4	116	
117	.299-7	.652-7	.138-6	.286-6	.576-6	.113-5	.217-5	.406-5	.744-5	.133-4	117	
118	.162-7	.360-7	.776-7	.163-6	.333-6	.665-6	.130-5	.246-5	.458-5	.832-5	118	
119	.871-8	.197-7	.431-7	.920-7	.191-6	.387-6	.766-6	.148-5	.279-5	.514-5	119	
120	.464-8	.106-7	.237-7	.514-7	.109-6	.223-6	.449-6	.879-6	.168-5	.315-5	120	
121	.244-8	.570-8	.129-7	.285-7	.611-7	.128-6	.260-6	.518-6	.101-5	.191-5	121	
122	.128-8	.302-8	.697-8	.156-7	.340-7	.722-7	.150-6	.302-6	.596-6	.115-5	122	
123	.659-9	.159-8	.372-8	.847-8	.188-7	.405-7	.852-7	.175-6	.349-6	.683-6	123	
124	.337-9	.827-9	.197-8	.456-8	.103-7	.225-7	.480-7	.100-6	.203-6	.403-6	124	
125	.171-9	.427-9	.103-8	.243-8	.556-8	.124-7	.268-7	.567-7	.117-6	.236-6	125	
126	.859-10	.218-9	.537-9	.128-8	.298-8	.675-8	.149-7	.319-7	.668-7	.136-6	126	
127	.428-10	.110-9	.276-9	.671-9	.159-8	.364-8	.815-8	.178-7	.378-7	.783-7	127	
128	.211-10	.553-10	.141-9	.348-9	.835-9	.195-8	.443-8	.981-8	.212-7	.445-7	128	
129	.103-10	.275-10	.711-10	.179-9	.436-9	.103-8	.239-8	.537-8	.118-7	.251-7	129	
130		.135-10	.356-10	.909-10	.225-9	.544-9	.127-8	.291-8	.647-8	.140-7	130	
131			.177-10	.459-10	.116-9	.283-9	.674-9	.156-8	.353-8	.777-8	131	
132				.229-10	.587-10	.146-9	.354-9	.832-9	.191-8	.426-8	132	
133				.113-10	.296-10	.747-10	.184-9	.439-9	.102-8	.232-8	133	
134					.147-10	.379-10	.946-10	.230-9	.543-9	.125-8	134	
135							.190-10	.483-10	.119-9	.286-9	135	
136								.245-10	.613-10	.149-9	136	
137								.123-10	.312-10	.773-10	137	
138									.158-10	.397-10	138	

R	N=0700	N=0710	N=0720	N=0730	N=0740	N=0750	N=0760	N=0770	N=0780	N=0790	R	P=1/10
139									•202-10	•501-10	139	
140									•102-10	•257-10	140	
141										•130-10	141	

R	N=0800	N=0810	N=0820	N=0830	N=0840	N=0850	N=0860	N=0870	N=0880	N=0890	R
55	•999-0	•999-0									55
56	•999-0	•999-0	•999-0								56
57	•998-0	•999-0	•999-0	•999-0							57
58	•997-0	•998-0	•999-0	•999-0	•999-0						58
59	•996-0	•997-0	•998-0	•998-0	•999-0	•999-0	•999-0	•999-0			59
60	•994-0	•996-0	•997-0	•998-0	•998-0	•999-0	•999-0	•999-0	•999-0	•999-0	60
61	•991-0	•994-0	•995-0	•997-0	•998-0	•998-0	•999-0	•999-0	•999-0	•999-0	61
62	•988-0	•991-0	•993-0	•995-0	•996-0	•997-0	•998-0	•998-0	•998-0	•998-0	62
63	•983-0	•987-0	•990-0	•993-0	•995-0	•996-0	•997-0	•998-0	•998-0	•998-0	63
64	•977-0	•982-0	•987-0	•990-0	•993-0	•995-0	•996-0	•997-0	•998-0	•998-0	64
65	•969-0	•976-0	•982-0	•986-0	•990-0	•992-0	•994-0	•996-0	•997-0	•997-0	65
66	•959-0	•968-0	•975-0	•981-0	•986-0	•989-0	•992-0	•994-0	•995-0	•996-0	66
67	•947-0	•958-0	•967-0	•975-0	•981-0	•985-0	•989-0	•991-0	•994-0	•994-0	67
68	•932-0	•946-0	•957-0	•966-0	•974-0	•980-0	•985-0	•988-0	•991-0	•993-0	68
69	•915-0	•931-0	•945-0	•956-0	•966-0	•973-0	•979-0	•984-0	•988-0	•990-0	69
70	•894-0	•913-0	•930-0	•944-0	•955-0	•965-0	•972-0	•978-0	•983-0	•987-0	70
71	•870-0	•892-0	•912-0	•929-0	•943-0	•954-0	•964-0	•971-0	•978-0	•982-0	71
72	•842-0	•868-0	•891-0	•910-0	•927-0	•941-0	•953-0	•963-0	•971-0	•976-0	72
73	•811-0	•840-0	•866-0	•889-0	•909-0	•926-0	•940-0	•952-0	•962-0	•969-0	73
74	•776-0	•809-0	•839-0	•865-0	•888-0	•908-0	•925-0	•939-0	•951-0	•960-0	74
75	•739-0	•775-0	•808-0	•837-0	•863-0	•886-0	•906-0	•923-0	•938-0	•949-0	75
76	•698-0	•737-0	•773-0	•806-0	•836-0	•862-0	•885-0	•905-0	•922-0	•936-0	76
77	•655-0	•697-0	•736-0	•772-0	•805-0	•834-0	•860-0	•883-0	•904-0	•920-0	77
78	•610-0	•654-0	•696-0	•735-0	•771-0	•803-0	•833-0	•859-0	•882-0	•901-0	78
79	•564-0	•610-0	•653-0	•695-0	•733-0	•769-0	•802-0	•831-0	•857-0	•880-0	79
80	•517-0	•564-0	•609-0	•652-0	•694-0	•732-0	•768-0	•800-0	•830-0	•856-0	80
81	•470-0	•517-0	•563-0	•608-0	•652-0	•693-0	•731-0	•766-0	•799-0	•828-0	81
82	•424-0	•470-0	•517-0	•563-0	•608-0	•651-0	•691-0	•730-0	•765-0	•797-0	82
83	•379-0	•424-0	•471-0	•517-0	•563-0	•607-0	•650-0	•690-0	•728-0	•763-0	83
84	•335-0	•379-0	•425-0	•471-0	•517-0	•562-0	•606-0	•649-0	•689-0	•727-0	84
85	•294-0	•336-0	•380-0	•425-0	•471-0	•517-0	•562-0	•606-0	•648-0	•689-0	85
86	•256-0	•295-0	•337-0	•381-0	•426-0	•471-0	•516-0	•561-0	•605-0	•647-0	86
87	•220-0	•257-0	•296-0	•338-0	•382-0	•426-0	•471-0	•516-0	•561-0	•605-0	87
88	•187-0	•221-0	•258-0	•297-0	•339-0	•382-0	•426-0	•471-0	•516-0	•561-0	88
89	•158-0	•189-0	•223-0	•259-0	•299-0	•340-0	•383-0	•427-0	•471-0	•516-0	89
90	•132-0	•160-0	•190-0	•224-0	•261-0	•300-0	•341-0	•383-0	•427-0	•472-0	90
91	•109-0	•134-0	•161-0	•192-0	•225-0	•262-0	•300-0	•341-0	•384-0	•428-0	91
92	•896-1	•111-0	•135-0	•162-0	•193-0	•227-0	•263-0	•301-0	•342-0	•385-0	92
93	•726-1	•909-1	•112-0	•136-0	•164-0	•194-0	•228-0	•264-0	•302-0	•343-0	93
94	•583-1	•738-1	•922-1	•113-0	•138-0	•165-0	•196-0	•229-0	•265-0	•304-0	94
95	•463-1	•594-1	•750-1	•935-1	•115-0	•139-0	•167-0	•197-0	•230-0	•266-0	95
96	•365-1	•473-1	•605-1	•762-1	•947-1	•116-0	•140-0	•168-0	•198-0	•232-0	96
97	•284-1	•373-1	•483-1	•616-1	•774-1	•960-1	•117-0	•142-0	•169-0	•200-0	97
98	•219-1	•291-1	•382-1	•493-1	•626-1	•786-1	•971-1	•119-0	•143-0	•171-0	98
99	•167-1	•225-1	•299-1	•390-1	•502-1	•637-1	•796-1	•983-1	•120-0	•145-0	99
100	•126-1	•172-1	•231-1	•306-1	•399-1	•512-1	•647-1	•807-1	•995-1	•121-0	100
101	•943-2	•130-1	•177-1	•238-1	•313-1	•407-1	•520-1	•657-1	•818-1	•101-0	101
102	•698-2	•978-2	•135-1	•183-1	•244-1	•321-1	•414-1	•529-1	•667-1	•832-1	102
103	•512-2	•726-2	•101-1	•139-1	•188-1	•250-1	•327-1	•422-1	•538-1	•680-1	103
104	•371-2	•534-2	•755-2	•105-1	•144-1	•193-1	•255-1	•334-1	•430-1	•550-1	104
105	•267-2	•389-2	•557-2	•784-2	•109-1	•148-1	•198-1	•261-1	•341-1	•441-1	105
106	•190-2	•280-2	•407-2	•580-2	•814-2	•112-1	•151-1	•203-1	•267-1	•351-1	106
107	•134-2	•200-2	•294-2	•425-2	•604-2	•842-2	•115-1	•155-1	•207-1	•276-1	107
108	•931-3	•141-2	•211-2	•308-2	•443-2	•626-2	•861-2	•118-1	•159-1	•215-1	108
109	•643-3	•989-3	•149-2	•221-2	•323-2	•461-2	•639-2	•887-2	•121-1	•167-1	109
110	•440-3	•685-3	•105-2	•158-2	•233-2	•336-2	•469-2	•659-2	•912-2	•128-1	110
111	•298-3	•470-3	•729-3	•111-2	•166-2	•242-2	•340-2	•484-2	•678-2	•968-2	111
112	•199-3	•320-3	•502-3	•775-3	•117-2	•173-2	•243-2	•351-2	•497-2	•728-2	112
113	•132-3	•215-3	•343-3	•536-3	•822-3	•122-2	•184-2	•268-2	•384-2	•543-2	113
114	•871-4	•143-3	•232-3	•367-3	•571-3	•856-3	•131-2	•193-2	•280-2	•401-2	114
115	•567-4	•947-4	•155-3	•249-3	•392-3	•591-3	•923-3	•138-2	•203-2	•293-2	115
116	•366-4	•619-4	•103-3	•167-3	•267-3	•403-3	•645-3	•976-3	•145-2	•213-2	116
117	•234-4	•401-4	•675-4	•111-3	•180-3	•270-3	•446-3	•684-3	•103-2	•153-2	117
118	•148-4	•257-4	•439-4	•734-4	•120-3	•194-3	•306-3	•475-3	•725-3	•109-2	118
119	•927-5	•164-4	•283-4	•480-4	•797-4	•130-3	•208-3	•327-3	•505-3	•768-3	119
120	•576-5	•103-4	•181-4	•311-4	•523-4	•865-4	•140-3	•223-3	•349-3	•537-3	120
121	•354-5	•643-5	•114-4	•199-4	•340-4	•570-4	•936-4	•151-3	•239-3	•372-3	121
122	•216-5	•398-5	•717-5	•127-4	•219-4	•372-4	•619-4	•101-3	•162-3	•256-3	122
123	•130-5	•244-5	•446-5	•798-5	•140-4	•241-4	•406-4	•671-4	•109-3	•174-3	123
124	•781-6	•148-5	•274-5	•498-5	•885-5	•154-4	•264-4	•442-4	•727-4	•118-3	124
125	•463-6	•890-6	•167-5	•308-5	•555-5	•980-5	•170-4	•288-4	•481-4	•786-4	125
126	•272-6	•531-6	•101-5	•189-5	•345-5	•618-5	•108-4	•186-4	•315-4	•522-4	126
127	•159-6	•314-6	•607-6	•115-5	•213-5	•386-5	•685-5	•119-4	•204-4	•343-4	127
128	•915-7	•184-6	•360-6	•691-6	•130-5	•239-5	•430-5	•759-5	•132-4	•224-4	128
129	•523-7	•107-6	•212-6	•412-6	•785-6	•146-5	•267-5	•478-5	•839-5	•144-4	129
130	•297-7	•613-7	•124-6	•244-6	•471-6	•890-6	•165-5	•299-5	•531-5	•925-5	130
131	•167-7	•349-7	•715-7	•143-6	•280-6	•536-6	•101-5	•185-5	•333-5	•588-5	131

R	N=0800	N=0810	N=0820	N=0830	N=0840	N=0850	N=0860	N=0870	N=0880	N=0890	R	P=1/10
132	.929- 8	.197- 7	.410- 7	.832- 7	.165- 6	.321- 6	.609- 6	.113- 5	.207- 5	.370- 5	132	
133	.513- 8	.111- 7	.233- 7	.480- 7	.233- 7	.965- 7	.190- 6	.366- 6	.690- 6	.128- 5	133	
134	.281- 8	.614- 8	.131- 7	.274- 7	.559- 7	.112- 6	.218- 6	.417- 6	.780- 6	.143- 5	134	
135	.152- 8	.338- 8	.734- 8	.155- 7	.321- 7	.650- 7	.129- 6	.249- 6	.473- 6	.879- 6	135	
136	.819- 9	.185- 8	.406- 8	.872- 8	.183- 7	.375- 7	.753- 7	.148- 6	.284- 6	.535- 6	136	
137	.437- 9	.100- 8	.223- 8	.486- 8	.103- 7	.215- 7	.437- 7	.870- 7	.169- 6	.323- 6	137	
138	.231- 9	.536- 9	.121- 8	.268- 8	.579- 8	.122- 7	.252- 7	.507- 7	.100- 6	.194- 6	138	
139	.121- 9	.285- 9	.655- 9	.147- 8	.321- 8	.687- 8	.144- 7	.294- 7	.587- 7	.115- 6	139	
140	.630-10	.151- 9	.351- 9	.798- 9	.177- 8	.384- 8	.813- 8	.168- 7	.341- 7	.678- 7	140	
141	.325-10	.788-10	.186- 9	.430- 9	.967- 9	.213- 8	.457- 8	.959- 8	.197- 7	.396- 7	141	
142	.166-10	.409-10	.981-10	.229- 9	.524- 9	.117- 8	.254- 8	.541- 8	.113- 7	.230- 7	142	
143		.210-10	.512-10	.122- 9	.281- 9	.636- 9	.140- 8	.303- 8	.639- 8	.132- 7	143	
144		.107-10	.265-10	.639-10	.150- 9	.344- 9	.769- 9	.168- 8	.360- 8	.753- 8	144	
145			.136-10	.333-10	.793-10	.184- 9	.418- 9	.927- 9	.201- 8	.426- 8	145	
146				.172-10	.416-10	.980-10	.225- 9	.507- 9	.111- 8	.239- 8	146	
147					.216-10	.517-10	.121- 9	.275- 9	.612- 9	.133- 8	147	
148					.111-10	.270-10	.640-10	.148- 9	.333- 9	.734- 9	148	
149						.140-10	.337-10	.788-10	.180- 9	.402- 9	149	
150							.176-10	.417-10	.968-10	.218- 9	150	
151								.219-10	.515-10	.117- 9	151	
152								.114-10	.272-10	.621-10	152	
153									.143-10	.324-10	153	
154										.165-10	154	

R	N=0900	N=0910	N=0920	N=0930	N=0940	N=0950	N=0960	N=0970	N=0980	N=0990	R
63	.999- 0										63
64	.999- 0	.999- 0	.999- 0								64
65	.998- 0	.999- 0	.999- 0	.999- 0							65
66	.998- 0	.998- 0	.998- 0	.999- 0	.999- 0						66
67	.997- 0	.998- 0	.998- 0	.999- 0	.999- 0	.999- 0					67
68	.995- 0	.996- 0	.997- 0	.998- 0	.998- 0	.999- 0	.999- 0				68
69	.993- 0	.995- 0	.996- 0	.997- 0	.998- 0	.999- 0	.999- 0	.999- 0	.999- 0		69
70	.991- 0	.993- 0	.995- 0	.996- 0	.997- 0	.998- 0	.998- 0	.999- 0	.999- 0	.999- 0	70
71	.987- 0	.990- 0	.993- 0	.995- 0	.996- 0	.997- 0	.998- 0	.998- 0	.999- 0	.999- 0	71
72	.983- 0	.987- 0	.990- 0	.992- 0	.994- 0	.996- 0	.997- 0	.998- 0	.998- 0	.999- 0	72
73	.977- 0	.982- 0	.986- 0	.989- 0	.992- 0	.994- 0	.996- 0	.997- 0	.998- 0	.998- 0	73
74	.969- 0	.976- 0	.981- 0	.985- 0	.989- 0	.992- 0	.994- 0	.995- 0	.997- 0	.997- 0	74
75	.960- 0	.969- 0	.975- 0	.981- 0	.985- 0	.989- 0	.991- 0	.994- 0	.995- 0	.996- 0	75
76	.949- 0	.959- 0	.968- 0	.975- 0	.980- 0	.985- 0	.988- 0	.991- 0	.993- 0	.995- 0	76
77	.936- 0	.948- 0	.958- 0	.967- 0	.974- 0	.980- 0	.984- 0	.988- 0	.991- 0	.993- 0	77
78	.920- 0	.935- 0	.947- 0	.958- 0	.966- 0	.973- 0	.979- 0	.984- 0	.988- 0	.990- 0	78
79	.901- 0	.919- 0	.933- 0	.946- 0	.957- 0	.966- 0	.973- 0	.979- 0	.983- 0	.987- 0	79
80	.880- 0	.900- 0	.917- 0	.932- 0	.945- 0	.956- 0	.965- 0	.972- 0	.978- 0	.983- 0	80
81	.855- 0	.878- 0	.898- 0	.916- 0	.931- 0	.944- 0	.955- 0	.964- 0	.971- 0	.978- 0	81
82	.827- 0	.854- 0	.877- 0	.897- 0	.915- 0	.930- 0	.943- 0	.954- 0	.963- 0	.971- 0	82
83	.796- 0	.826- 0	.852- 0	.876- 0	.896- 0	.914- 0	.929- 0	.942- 0	.953- 0	.962- 0	83
84	.763- 0	.795- 0	.824- 0	.851- 0	.874- 0	.895- 0	.913- 0	.928- 0	.941- 0	.952- 0	84
85	.726- 0	.762- 0	.794- 0	.823- 0	.849- 0	.873- 0	.894- 0	.912- 0	.927- 0	.940- 0	85
86	.688- 0	.725- 0	.760- 0	.793- 0	.822- 0	.846- 0	.872- 0	.892- 0	.910- 0	.926- 0	86
87	.647- 0	.687- 0	.724- 0	.759- 0	.791- 0	.820- 0	.847- 0	.870- 0	.891- 0	.909- 0	87
88	.604- 0	.646- 0	.685- 0	.723- 0	.758- 0	.790- 0	.819- 0	.846- 0	.869- 0	.890- 0	88
89	.560- 0	.604- 0	.645- 0	.685- 0	.722- 0	.757- 0	.789- 0	.818- 0	.844- 0	.868- 0	89
90	.516- 0	.560- 0	.603- 0	.644- 0	.684- 0	.721- 0	.755- 0	.787- 0	.817- 0	.843- 0	90
91	.472- 0	.516- 0	.560- 0	.602- 0	.644- 0	.683- 0	.720- 0	.754- 0	.786- 0	.815- 0	91
92	.428- 0	.472- 0	.516- 0	.560- 0	.602- 0	.643- 0	.682- 0	.719- 0	.753- 0	.785- 0	92
93	.385- 0	.429- 0	.472- 0	.516- 0	.559- 0	.601- 0	.642- 0	.681- 0	.718- 0	.752- 0	93
94	.344- 0	.386- 0	.429- 0	.472- 0	.516- 0	.559- 0	.601- 0	.641- 0	.680- 0	.717- 0	94
95	.305- 0	.345- 0	.386- 0	.429- 0	.473- 0	.516- 0	.559- 0	.600- 0	.641- 0	.679- 0	95
96	.268- 0	.306- 0	.346- 0	.387- 0	.430- 0	.473- 0	.516- 0	.558- 0	.600- 0	.640- 0	96
97	.233- 0	.269- 0	.306- 0	.346- 0	.388- 0	.430- 0	.473- 0	.516- 0	.558- 0	.599- 0	97
98	.201- 0	.234- 0	.270- 0	.308- 0	.347- 0	.388- 0	.430- 0	.473- 0	.516- 0	.558- 0	98
99	.172- 0	.202- 0	.235- 0	.271- 0	.308- 0	.348- 0	.389- 0	.431- 0	.473- 0	.516- 0	99
100	.146- 0	.173- 0	.203- 0	.236- 0	.272- 0	.309- 0	.349- 0	.389- 0	.431- 0	.473- 0	100
101	.123- 0	.147- 0	.174- 0	.205- 0	.238- 0	.273- 0	.310- 0	.349- 0	.390- 0	.432- 0	101
102	.102- 0	.124- 0	.148- 0	.176- 0	.206- 0	.239- 0	.274- 0	.311- 0	.350- 0	.391- 0	102
103	.844- 1	.103- 0	.125- 0	.150- 0	.177- 0	.207- 0	.240- 0	.275- 0	.312- 0	.351- 0	103
104	.690- 1	.855- 1	.104- 0	.126- 0	.151- 0	.178- 0	.208- 0	.241- 0	.276- 0	.313- 0	104
105	.560- 1	.701- 1	.865- 1	.106- 0	.128- 0	.152- 0	.180- 0	.210- 0	.242- 0	.277- 0	105
106	.450- 1	.570- 1	.710- 1	.878- 1	.107- 0	.129- 0	.153- 0	.181- 0	.211- 0	.243- 0	106
107	.358- 1	.459- 1	.578- 1	.722- 1	.889- 1	.108- 0	.130- 0	.155- 0	.182- 0	.212- 0	107
108	.283- 1	.366- 1	.466- 1	.588- 1	.732- 1	.900- 1	.109- 0	.131- 0	.156- 0	.183- 0	108
109	.221- 1	.289- 1	.372- 1	.475- 1	.598- 1	.742- 1	.911- 1	.110- 0	.132- 0	.157- 0	109
110	.171- 1	.227- 1	.295- 1	.381- 1	.484- 1	.607- 1	.752- 1	.922- 1	.112- 0	.134- 0	110
111	.131- 1	.176- 1	.231- 1	.302- 1	.388- 1	.492- 1	.616- 1	.763- 1	.933- 1	.113- 0	111
112	.100- 1	.135- 1	.180- 1	.238- 1	.309- 1	.396- 1	.501- 1	.626- 1	.773- 1	.943- 1	112
113	.754- 2	.103- 1	.139- 1	.186- 1	.244- 1	.315- 1	.403- 1	.509- 1	.635- 1	.783- 1	113
114	.563- 2	.781- 2	.106- 1	.143- 1	.190- 1	.249- 1	.322- 1	.411- 1	.518- 1	.645- 1	114
115	.417- 2	.585- 2	.799- 2	.110- 1	.147- 1	.195- 1	.255- 1	.329- 1	.418- 1	.526- 1	115
116	.306- 2	.434- 2	.598- 2	.835- 2	.113- 1	.152- 1	.200- 1	.261- 1	.335- 1	.426- 1	116
117	.223- 2	.320- 2	.443- 2	.629- 2	.863- 2	.117- 1	.156- 1	.205- 1	.266- 1	.342- 1	117
118	.160- 2	.233- 2	.324- 2	.469- 2	.651- 2	.891- 2	.120- 1	.160- 1	.210- 1	.272- 1	118
119	.115- 2	.168- 2	.235- 2	.347- 2	.487- 2	.674- 2	.919- 2	.124- 1	.164- 1	.215- 1	119

R	N=0900	N=0910	N=0920	N=0930	N=0940	N=0950	N=0960	N=0970	N=0980	N=0990	R	P=1/10
120	.812-3	.121-2	.168-2	.255-2	.361-2	.506-2	.697-2	.948-2	.127-1	.168-1	120	
121	.569-3	.857-3	.127-2	.185-2	.266-2	.376-2	.524-2	.721-2	.977-2	.131-1	121	
122	.396-3	.603-3	.904-3	.133-2	.194-2	.277-2	.391-2	.543-2	.744-2	.101-1	122	
123	.273-3	.421-3	.639-3	.953-3	.140-2	.203-2	.289-2	.406-2	.562-2	.769-2	123	
124	.187-3	.291-3	.447-3	.675-3	.100-2	.147-2	.212-2	.301-2	.421-2	.582-2	124	
125	.126-3	.200-3	.310-3	.474-3	.713-3	.106-2	.154-2	.221-2	.313-2	.437-2	125	
126	.849-4	.136-3	.214-3	.330-3	.502-3	.752-3	.111-2	.161-2	.231-2	.326-2	126	
127	.565-4	.915-4	.146-3	.228-3	.351-3	.532-3	.793-3	.117-2	.169-2	.241-2	127	
128	.373-4	.612-4	.985-4	.156-3	.243-3	.373-3	.562-3	.835-3	.122-2	.176-2	128	
129	.244-4	.405-4	.661-4	.106-3	.167-3	.259-3	.395-3	.594-3	.878-3	.128-2	129	
130	.158-4	.266-4	.439-4	.713-4	.114-3	.178-3	.275-3	.418-3	.626-3	.923-3	130	
131	.102-4	.173-4	.290-4	.476-4	.768-4	.122-3	.190-3	.293-3	.443-3	.660-3	131	
132	.650-5	.112-4	.189-4	.315-4	.514-4	.826-4	.130-3	.203-3	.310-3	.468-3	132	
133	.411-5	.717-5	.123-4	.207-4	.342-4	.555-4	.887-4	.140-3	.216-3	.329-3	133	
134	.258-5	.455-5	.790-5	.134-4	.225-4	.370-4	.598-4	.952-4	.149-3	.230-3	134	
135	.160-5	.287-5	.504-5	.868-5	.147-4	.245-4	.400-4	.644-4	.102-3	.159-3	135	
136	.989-6	.179-5	.318-5	.556-5	.953-5	.160-4	.265-4	.432-4	.692-4	.109-3	136	
137	.605-6	.111-5	.200-5	.353-5	.613-5	.104-4	.175-4	.288-4	.466-4	.743-4	137	
138	.367-6	.682-6	.124-5	.222-5	.390-5	.673-5	.114-4	.190-4	.311-4	.502-4	138	
139	.221-6	.416-6	.767-6	.139-5	.247-5	.431-5	.739-5	.125-4	.206-4	.337-4	139	
140	.132-6	.251-6	.469-6	.860-6	.155-5	.273-5	.474-5	.809-5	.136-4	.224-4	140	
141	.780-7	.151-6	.285-6	.529-6	.963-6	.172-5	.302-5	.522-5	.885-5	.148-4	141	
142	.458-7	.896-7	.172-6	.322-6	.595-6	.108-5	.191-5	.334-5	.573-5	.967-5	142	
143	.267-7	.528-7	.103-6	.195-6	.364-6	.667-6	.120-5	.212-5	.368-5	.628-5	143	
144	.154-7	.309-7	.608-7	.117-6	.221-6	.410-6	.746-6	.133-5	.234-5	.405-5	144	
145	.884-8	.180-7	.357-7	.697-7	.133-6	.250-6	.461-6	.834-6	.148-5	.259-5	145	
146	.503-8	.103-7	.208-7	.412-7	.798-7	.152-6	.282-6	.517-6	.930-6	.164-5	146	
147	.284-8	.591-8	.121-7	.241-7	.473-7	.911-7	.172-6	.318-6	.579-6	.103-5	147	
148	.159-8	.335-8	.693-8	.140-7	.279-7	.543-7	.104-6	.194-6	.358-6	.647-6	148	
149	.881-9	.189-8	.395-8	.810-8	.163-7	.321-7	.620-7	.118-6	.219-6	.401-6	149	
150	.486-9	.105-8	.223-8	.464-8	.944-8	.188-7	.369-7	.708-7	.133-6	.247-6	150	
151	.266-9	.583-9	.125-8	.264-8	.543-8	.110-7	.217-7	.422-7	.806-7	.151-6	151	
152	.144-9	.321-9	.698-9	.149-8	.310-8	.634-8	.127-7	.250-7	.483-7	.915-7	152	
153	.776-10	.175-9	.385-9	.832-9	.176-8	.364-8	.739-8	.147-7	.287-7	.550-7	153	
154	.414-10	.947-10	.211-9	.462-9	.989-9	.207-8	.426-8	.858-8	.170-7	.329-7	154	
155	.220-10	.509-10	.115-9	.255-9	.552-9	.117-8	.244-8	.497-8	.993-8	.195-7	155	
156	.116-10	.271-10	.621-10	.139-9	.306-9	.657-9	.138-8	.285-8	.578-8	.115-7	156	
157		.143-10	.333-10	.756-10	.168-9	.366-9	.780-9	.163-8	.334-8	.670-8	157	
158			.177-10	.408-10	.917-10	.202-9	.436-9	.922-9	.191-8	.389-8	158	
159				.218-10	.497-10	.111-9	.242-9	.518-9	.109-8	.224-8	159	
160				.116-10	.267-10	.604-10	.134-9	.289-9	.614-9	.128-8	160	
161					.143-10	.326-10	.731-10	.160-9	.345-9	.726-9	161	
162						.175-10	.397-10	.882-10	.192-9	.409-9	162	
163							.214-10	.481-10	.106-9	.229-9	163	
164							.115-10	.261-10	.582-10	.127-9	164	
165								.141-10	.317-10	.701-10	165	
166									.171-10	.384-10	166	
167										.209-10	167	
168										.113-10	168	

R	N=1000	N=1010	N=1020	N=1030	N=1040	N=1050	N=1060	N=1070	N=1080	N=1090	R
71	.999-0										71
72	.999-0	.999-0									72
73	.999-0	.999-0	.999-0								73
74	.998-0	.999-0	.999-0	.999-0							74
75	.997-0	.998-0	.999-0	.999-0	.999-0	.999-0					75
76	.996-0	.997-0	.998-0	.999-0	.999-0	.999-0	.999-0				76
77	.995-0	.996-0	.997-0	.998-0	.998-0	.999-0	.999-0	.999-0			77
78	.993-0	.995-0	.996-0	.997-0	.998-0	.998-0	.999-0	.999-0	.999-0		78
79	.990-0	.992-0	.994-0	.996-0	.997-0	.998-0	.999-0	.999-0	.999-0	.999-0	79
80	.987-0	.990-0	.992-0	.994-0	.996-0	.997-0	.998-0	.998-0	.999-0	.999-0	80
81	.982-0	.986-0	.989-0	.992-0	.994-0	.995-0	.997-0	.997-0	.998-0	.999-0	81
82	.977-0	.982-0	.986-0	.989-0	.992-0	.994-0	.995-0	.996-0	.997-0	.998-0	82
83	.970-0	.976-0	.981-0	.986-0	.989-0	.991-0	.993-0	.995-0	.996-0	.997-0	83
84	.962-0	.969-0	.976-0	.981-0	.985-0	.988-0	.991-0	.993-0	.995-0	.996-0	84
85	.951-0	.961-0	.969-0	.975-0	.980-0	.985-0	.988-0	.991-0	.993-0	.995-0	85
86	.939-0	.951-0	.960-0	.968-0	.975-0	.980-0	.984-0	.988-0	.991-0	.993-0	86
87	.925-0	.938-0	.950-0	.959-0	.967-0	.974-0	.979-0	.984-0	.987-0	.990-0	87
88	.908-0	.924-0	.937-0	.949-0	.959-0	.967-0	.973-0	.979-0	.983-0	.987-0	88
89	.889-0	.907-0	.923-0	.936-0	.948-0	.958-0	.966-0	.973-0	.978-0	.983-0	89
90	.867-0	.887-0	.906-0	.922-0	.935-0	.947-0	.957-0	.965-0	.972-0	.978-0	90
91	.842-0	.865-0	.886-0	.905-0	.921-0	.934-0	.946-0	.956-0	.965-0	.972-0	91
92	.814-0	.841-0	.864-0	.885-0	.904-0	.920-0	.934-0	.945-0	.955-0	.964-0	92
93	.784-0	.813-0	.839-0	.863-0	.884-0	.902-0	.919-0	.933-0	.945-0	.955-0	93
94	.751-0	.783-0	.812-0	.838-0	.862-0	.883-0	.901-0	.918-0	.932-0	.944-0	94
95	.716-0	.750-0	.782-0	.811-0	.837-0	.861-0	.882-0	.900-0	.917-0	.931-0	95
96	.678-0	.715-0	.749-0	.780-0	.809-0	.836-0	.859-0	.880-0	.899-0	.916-0	96
97	.639-0	.678-0	.714-0	.748-0	.779-0	.808-0	.835-0	.858-0	.879-0	.898-0	97
98	.599-0	.639-0	.677-0	.713-0	.747-0	.778-0	.807-0	.833-0	.857-0	.878-0	98
99	.557-0	.598-0	.638-0	.676-0	.712-0	.746-0	.777-0	.806-0	.832-0	.856-0	99
100	.515-0	.557-0	.598-0	.637-0	.675-0	.711-0	.745-0	.776-0	.805-0	.831-0	100
101	.473-0	.515-0	.557-0	.597-0	.637-0	.674-0	.710-0	.744-0	.775-0	.804-0	101



R	N=1000	N=1010	N=1020	N=1030	N=1040	N=1050	N=1060	N=1070	N=1080	N=1090	R	P=1/10
102	.432-0	.474-0	.515-0	.557-0	.597-0	.636-0	.674-0	.709-0	.743-0	.774-0	102	
103	.391-0	.432-0	.474-0	.515-0	.556-0	.596-0	.635-0	.673-0	.708-0	.742-0	103	
104	.352-0	.392-0	.432-0	.474-0	.515-0	.556-0	.596-0	.635-0	.672-0	.707-0	104	
105	.314-0	.352-0	.392-0	.433-0	.474-0	.515-0	.556-0	.596-0	.634-0	.671-0	105	
106	.278-0	.315-0	.353-0	.393-0	.433-0	.474-0	.515-0	.555-0	.595-0	.634-0	106	
107	.244-0	.279-0	.315-0	.354-0	.393-0	.433-0	.474-0	.515-0	.555-0	.595-0	107	
108	.213-0	.245-0	.280-0	.316-0	.354-0	.394-0	.434-0	.474-0	.515-0	.555-0	108	
109	.184-0	.214-0	.246-0	.281-0	.317-0	.355-0	.394-0	.434-0	.474-0	.515-0	109	
110	.158-0	.186-0	.215-0	.247-0	.282-0	.318-0	.356-0	.395-0	.434-0	.475-0	110	
111	.135-0	.159-0	.187-0	.216-0	.248-0	.283-0	.319-0	.356-0	.395-0	.435-0	111	
112	.114-0	.136-0	.161-0	.188-0	.217-0	.249-0	.284-0	.319-0	.357-0	.396-0	112	
113	.954-1	.115-0	.137-0	.162-0	.189-0	.219-0	.250-0	.284-0	.320-0	.358-0	113	
114	.793-1	.965-1	.116-0	.138-0	.163-0	.190-0	.220-0	.251-0	.285-0	.321-0	114	
115	.654-1	.803-1	.975-1	.117-0	.139-0	.164-0	.191-0	.221-0	.252-0	.286-0	115	
116	.535-1	.663-1	.813-1	.986-1	.118-0	.140-0	.165-0	.192-0	.222-0	.253-0	116	
117	.434-1	.543-1	.672-1	.823-1	.996-1	.119-0	.142-0	.166-0	.193-0	.223-0	117	
118	.349-1	.441-1	.551-1	.681-1	.833-1	.101-0	.120-0	.143-0	.167-0	.194-0	118	
119	.278-1	.355-1	.448-1	.560-1	.690-1	.843-1	.102-0	.122-0	.144-0	.168-0	119	
120	.220-1	.284-1	.362-1	.456-1	.568-1	.700-1	.852-1	.103-0	.123-0	.145-0	120	
121	.173-1	.225-1	.290-1	.369-1	.464-1	.576-1	.709-1	.862-1	.104-0	.124-0	121	
122	.134-1	.177-1	.230-1	.296-1	.375-1	.471-1	.585-1	.718-1	.872-1	.105-0	122	
123	.104-1	.138-1	.181-1	.235-1	.301-1	.382-1	.479-1	.593-1	.727-1	.881-1	123	
124	.793-2	.107-1	.142-1	.186-1	.240-1	.307-1	.389-1	.486-1	.601-1	.736-1	124	
125	.602-2	.818-2	.110-1	.145-1	.190-1	.245-1	.313-1	.395-1	.494-1	.609-1	125	
126	.453-2	.622-2	.843-2	.113-1	.149-1	.194-1	.250-1	.319-1	.402-1	.501-1	126	
127	.338-2	.470-2	.643-2	.869-2	.116-1	.153-1	.199-1	.256-1	.325-1	.409-1	127	
128	.251-2	.352-2	.486-2	.664-2	.894-2	.119-1	.156-1	.203-1	.261-1	.331-1	128	
129	.184-2	.261-2	.365-2	.503-2	.685-2	.920-2	.122-1	.160-1	.208-1	.266-1	129	
130	.134-2	.192-2	.271-2	.378-2	.520-2	.706-2	.947-2	.125-1	.164-1	.212-1	130	
131	.970-3	.140-2	.200-2	.282-2	.392-2	.538-2	.728-2	.973-2	.129-1	.168-1	131	
132	.695-3	.102-2	.147-2	.209-2	.293-2	.406-2	.555-2	.750-2	.100-1	.132-1	132	
133	.494-3	.731-3	.107-2	.153-2	.217-2	.304-2	.420-2	.573-2	.772-2	.103-1	133	
134	.349-3	.521-3	.769-3	.112-2	.160-2	.226-2	.316-2	.435-2	.592-2	.795-2	134	
135	.244-3	.369-3	.550-3	.807-3	.117-2	.167-2	.235-2	.327-2	.450-2	.610-2	135	
136	.169-3	.259-3	.390-3	.579-3	.847-3	.122-2	.174-2	.245-2	.339-2	.465-2	136	
137	.117-3	.180-3	.274-3	.412-3	.609-3	.888-3	.128-2	.181-2	.254-2	.351-2	137	
138	.797-4	.124-3	.192-3	.291-3	.434-3	.640-3	.930-3	.133-2	.189-2	.264-2	138	
139	.540-4	.853-4	.133-3	.203-3	.307-3	.458-3	.672-3	.974-3	.139-2	.196-2	139	
140	.363-4	.580-4	.913-4	.141-3	.216-3	.325-3	.482-3	.705-3	.102-2	.145-2	140	
141	.242-4	.392-4	.623-4	.975-4	.150-3	.229-3	.343-3	.507-3	.740-3	.106-2	141	
142	.160-4	.262-4	.421-4	.667-4	.104-3	.160-3	.242-3	.362-3	.533-3	.775-3	142	
143	.105-4	.174-4	.283-4	.453-4	.714-4	.111-3	.170-3	.256-3	.381-3	.560-3	143	
144	.687-5	.115-4	.189-4	.305-4	.486-4	.764-4	.118-3	.180-3	.271-3	.402-3	144	
145	.445-5	.751-5	.125-4	.204-4	.329-4	.522-4	.815-4	.126-3	.191-3	.286-3	145	
146	.285-5	.487-5	.819-5	.135-4	.221-4	.354-4	.559-4	.870-4	.133-3	.202-3	146	
147	.182-5	.314-5	.534-5	.892-5	.147-4	.238-4	.380-4	.598-4	.927-4	.142-3	147	
148	.115-5	.201-5	.345-5	.583-5	.970-5	.159-4	.257-4	.408-4	.639-4	.987-4	148	
149	.721-6	.127-5	.221-5	.379-5	.636-5	.105-4	.172-4	.276-4	.437-4	.682-4	149	
150	.449-6	.802-6	.141-5	.244-5	.414-5	.694-5	.114-4	.186-4	.297-4	.468-4	150	
151	.277-6	.501-6	.891-6	.156-5	.268-5	.453-5	.755-5	.124-4	.200-4	.319-4	151	
152	.170-6	.311-6	.559-6	.988-6	.172-5	.294-5	.495-5	.820-5	.134-4	.216-4	152	
153	.104-6	.192-6	.348-6	.622-6	.109-5	.189-5	.322-5	.539-5	.890-5	.145-4	153	
154	.626-7	.117-6	.215-6	.389-6	.691-6	.121-5	.208-5	.352-5	.587-5	.964-5	154	
155	.376-7	.711-7	.132-6	.241-6	.434-6	.767-6	.133-5	.228-5	.384-5	.638-5	155	
156	.224-7	.428-7	.805-7	.149-6	.270-6	.483-6	.848-6	.147-5	.250-5	.419-5	156	
157	.132-7	.256-7	.487-7	.910-7	.167-6	.302-6	.536-6	.938-6	.161-5	.273-5	157	
158	.776-8	.152-7	.292-7	.552-7	.103-6	.187-6	.336-6	.595-6	.103-5	.177-5	158	
159	.452-8	.895-8	.174-7	.333-7	.626-7	.116-6	.210-6	.374-6	.658-6	.114-5	159	
160	.261-8	.524-8	.103-7	.199-7	.378-7	.706-7	.130-6	.234-6	.416-6	.728-6	160	
161	.150-8	.304-8	.606-8	.118-7	.227-7	.429-7	.797-7	.145-6	.261-6	.461-6	161	
162	.855-9	.175-8	.353-8	.699-8	.136-7	.259-7	.486-7	.896-7	.163-6	.291-6	162	
163	.484-9	.100-8	.205-8	.409-8	.804-8	.155-7	.294-7	.549-7	.101-6	.182-6	163	
164	.272-9	.571-9	.118-8	.238-8	.473-8	.923-8	.177-7	.334-7	.619-7	.113-6	164	
165	.152-9	.322-9	.672-9	.138-8	.276-8	.545-8	.106-7	.201-7	.377-7	.696-7	165	
166	.841-10	.181-9	.381-9	.789-9	.160-8	.320-8	.627-8	.121-7	.229-7	.426-7	166	
167	.463-10	.101-9	.215-9	.449-9	.923-9	.186-8	.369-8	.719-8	.138-7	.259-7	167	
168	.253-10	.556-10	.120-9	.254-9	.528-9	.108-8	.216-8	.425-8	.823-8	.157-7	168	
169	.137-10	.305-10	.667-10	.143-9	.300-9	.620-9	.125-8	.250-8	.489-8	.940-8	169	
170		.167-10	.368-10	.797-10	.169-9	.353-9	.724-9	.146-8	.288-8	.560-8	170	
171			.201-10	.442-10	.949-10	.200-9	.415-9	.844-9	.169-8	.332-8	171	
172			.110-10	.243-10	.528-10	.113-9	.236-9	.486-9	.982-9	.195-8	172	
173				.133-10	.292-10	.630-10	.134-9	.278-9	.568-9	.114-8	173	
174						.160-10	.350-10	.750-10	.158-9	.326-9	174	
175							.193-10	.418-10	.890-10	.186-9	175	
176							.106-10	.232-10	.498-10	.105-9	176	
177								.128-10	.277-10	.592-10	177	
178									.153-10	.331-10	178	
179										.184-10	179	
180										.220-10	180	
181										.122-10	181	

R	N=1100	N=1110	N=1120	N=1130	N=1140	N=1150	N=1160	N=1170	N=1180	N=1190	R	P=1/10
79	.999- 0										79	
80	.999- 0	.999- 0									80	
81	.999- 0	.999- 0	.999- 0								81	
82	.999- 0	.999- 0	.999- 0	.999- 0							82	
83	.998- 0	.998- 0	.999- 0	.999- 0	.999- 0						83	
84	.997- 0	.998- 0	.998- 0	.999- 0	.999- 0	.999- 0					84	
85	.996- 0	.997- 0	.998- 0	.998- 0	.999- 0	.999- 0	.999- 0				85	
86	.994- 0	.996- 0	.997- 0	.998- 0	.998- 0	.999- 0	.999- 0	.999- 0			86	
87	.992- 0	.994- 0	.996- 0	.997- 0	.998- 0	.998- 0	.999- 0	.999- 0	.999- 0		87	
88	.990- 0	.992- 0	.994- 0	.995- 0	.997- 0	.997- 0	.998- 0	.999- 0	.999- 0	.999- 0	88	
89	.987- 0	.990- 0	.992- 0	.994- 0	.995- 0	.996- 0	.997- 0	.998- 0	.999- 0	.999- 0	89	
90	.982- 0	.986- 0	.989- 0	.992- 0	.994- 0	.995- 0	.996- 0	.997- 0	.998- 0	.998- 0	90	
91	.977- 0	.982- 0	.986- 0	.989- 0	.991- 0	.993- 0	.995- 0	.996- 0	.997- 0	.998- 0	91	
92	.971- 0	.977- 0	.982- 0	.986- 0	.989- 0	.991- 0	.993- 0	.995- 0	.996- 0	.997- 0	92	
93	.963- 0	.970- 0	.976- 0	.981- 0	.985- 0	.988- 0	.991- 0	.993- 0	.995- 0	.996- 0	93	
94	.954- 0	.963- 0	.970- 0	.976- 0	.981- 0	.985- 0	.988- 0	.991- 0	.993- 0	.994- 0	94	
95	.943- 0	.953- 0	.962- 0	.969- 0	.975- 0	.980- 0	.984- 0	.988- 0	.990- 0	.993- 0	95	
96	.930- 0	.942- 0	.952- 0	.961- 0	.969- 0	.975- 0	.980- 0	.984- 0	.987- 0	.990- 0	96	
97	.914- 0	.929- 0	.941- 0	.952- 0	.960- 0	.968- 0	.974- 0	.979- 0	.984- 0	.987- 0	97	
98	.897- 0	.913- 0	.928- 0	.940- 0	.951- 0	.960- 0	.967- 0	.974- 0	.979- 0	.983- 0	98	
99	.877- 0	.896- 0	.913- 0	.927- 0	.939- 0	.950- 0	.959- 0	.967- 0	.973- 0	.978- 0	99	
100	.855- 0	.876- 0	.895- 0	.912- 0	.926- 0	.939- 0	.949- 0	.958- 0	.966- 0	.973- 0	100	
101	.830- 0	.854- 0	.875- 0	.894- 0	.911- 0	.925- 0	.938- 0	.948- 0	.958- 0	.965- 0	101	
102	.803- 0	.829- 0	.853- 0	.874- 0	.893- 0	.910- 0	.924- 0	.937- 0	.948- 0	.957- 0	102	
103	.773- 0	.801- 0	.828- 0	.851- 0	.873- 0	.892- 0	.909- 0	.923- 0	.936- 0	.947- 0	103	
104	.741- 0	.772- 0	.800- 0	.827- 0	.850- 0	.872- 0	.891- 0	.908- 0	.922- 0	.935- 0	104	
105	.707- 0	.740- 0	.771- 0	.799- 0	.825- 0	.849- 0	.871- 0	.890- 0	.907- 0	.921- 0	105	
106	.671- 0	.706- 0	.739- 0	.770- 0	.798- 0	.824- 0	.848- 0	.870- 0	.889- 0	.906- 0	106	
107	.633- 0	.670- 0	.705- 0	.738- 0	.769- 0	.797- 0	.823- 0	.847- 0	.869- 0	.888- 0	107	
108	.594- 0	.632- 0	.669- 0	.704- 0	.737- 0	.768- 0	.796- 0	.822- 0	.846- 0	.867- 0	108	
109	.555- 0	.594- 0	.632- 0	.668- 0	.703- 0	.736- 0	.767- 0	.795- 0	.821- 0	.845- 0	109	
110	.515- 0	.554- 0	.593- 0	.631- 0	.666- 0	.702- 0	.735- 0	.766- 0	.794- 0	.820- 0	110	
111	.475- 0	.515- 0	.554- 0	.593- 0	.631- 0	.667- 0	.702- 0	.734- 0	.765- 0	.793- 0	111	
112	.435- 0	.475- 0	.515- 0	.554- 0	.593- 0	.630- 0	.666- 0	.701- 0	.733- 0	.764- 0	112	
113	.396- 0	.435- 0	.475- 0	.515- 0	.554- 0	.592- 0	.630- 0	.666- 0	.700- 0	.732- 0	113	
114	.358- 0	.396- 0	.436- 0	.475- 0	.514- 0	.554- 0	.592- 0	.629- 0	.665- 0	.699- 0	114	
115	.322- 0	.359- 0	.397- 0	.436- 0	.475- 0	.514- 0	.553- 0	.591- 0	.629- 0	.664- 0	115	
116	.287- 0	.322- 0	.359- 0	.397- 0	.436- 0	.475- 0	.514- 0	.553- 0	.591- 0	.628- 0	116	
117	.254- 0	.288- 0	.323- 0	.360- 0	.398- 0	.436- 0	.475- 0	.514- 0	.553- 0	.591- 0	117	
118	.224- 0	.255- 0	.289- 0	.324- 0	.361- 0	.398- 0	.437- 0	.475- 0	.514- 0	.553- 0	118	
119	.195- 0	.225- 0	.256- 0	.290- 0	.325- 0	.361- 0	.399- 0	.437- 0	.476- 0	.514- 0	119	
120	.169- 0	.196- 0	.226- 0	.257- 0	.290- 0	.325- 0	.362- 0	.399- 0	.437- 0	.476- 0	120	
121	.146- 0	.171- 0	.198- 0	.227- 0	.258- 0	.291- 0	.326- 0	.362- 0	.400- 0	.437- 0	121	
122	.125- 0	.147- 0	.172- 0	.199- 0	.228- 0	.259- 0	.292- 0	.327- 0	.363- 0	.400- 0	122	
123	.106- 0	.126- 0	.148- 0	.173- 0	.200- 0	.229- 0	.260- 0	.293- 0	.328- 0	.363- 0	123	
124	.091- 1	.107- 0	.127- 0	.149- 0	.174- 0	.201- 0	.230- 0	.261- 0	.294- 0	.328- 0	124	
125	.744- 1	.900- 1	.108- 0	.128- 0	.150- 0	.175- 0	.202- 0	.231- 0	.262- 0	.294- 0	125	
126	.618- 1	.753- 1	.910- 1	.109- 0	.129- 0	.151- 0	.176- 0	.203- 0	.232- 0	.262- 0	126	
127	.508- 1	.626- 1	.762- 1	.919- 1	.110- 0	.130- 0	.152- 0	.177- 0	.204- 0	.232- 0	127	
128	.415- 1	.516- 1	.634- 1	.771- 1	.929- 1	.111- 0	.131- 0	.153- 0	.178- 0	.205- 0	128	
129	.337- 1	.422- 1	.523- 1	.642- 1	.780- 1	.938- 1	.112- 0	.132- 0	.154- 0	.179- 0	129	
130	.271- 1	.343- 1	.429- 1	.531- 1	.650- 1	.789- 1	.947- 1	.113- 0	.133- 0	.155- 0	130	
131	.217- 1	.276- 1	.349- 1	.436- 1	.538- 1	.658- 1	.797- 1	.956- 1	.114- 0	.134- 0	131	
132	.172- 1	.221- 1	.282- 1	.355- 1	.442- 1	.546- 1	.666- 1	.806- 1	.967- 1	.115- 0	132	
133	.135- 1	.176- 1	.226- 1	.287- 1	.361- 1	.449- 1	.553- 1	.674- 1	.816- 1	.975- 1	133	
134	.106- 1	.138- 1	.180- 1	.230- 1	.292- 1	.367- 1	.456- 1	.560- 1	.684- 1	.823- 1	134	
135	.0818- 2	.108- 1	.142- 1	.184- 1	.235- 1	.297- 1	.373- 1	.462- 1	.569- 1	.690- 1	135	
136	.629- 2	.841- 2	.111- 1	.145- 1	.187- 1	.240- 1	.303- 1	.379- 1	.470- 1	.575- 1	136	
137	.480- 2	.648- 2	.864- 2	.114- 1	.149- 1	.191- 1	.244- 1	.308- 1	.386- 1	.476- 1	137	
138	.364- 2	.496- 2	.667- 2	.888- 2	.117- 1	.152- 1	.195- 1	.249- 1	.315- 1	.391- 1	138	
139	.273- 2	.376- 2	.511- 2	.687- 2	.912- 2	.120- 1	.155- 1	.199- 1	.253- 1	.319- 1	139	
140	.204- 2	.284- 2	.389- 2	.527- 2	.707- 2	.936- 2	.123- 1	.159- 1	.204- 1	.258- 1	140	
141	.151- 2	.212- 2	.294- 2	.402- 2	.544- 2	.727- 2	.960- 2	.126- 1	.162- 1	.208- 1	141	
142	.111- 2	.157- 2	.220- 2	.304- 2	.415- 2	.560- 2	.747- 2	.985- 2	.128- 1	.166- 1	142	
143	.0811- 3	.116- 2	.164- 2	.229- 2	.315- 2	.429- 2	.576- 2	.767- 2	.101- 1	.131- 1	143	
144	.588- 3	.849- 3	.121- 2	.170- 2	.237- 2	.326- 2	.442- 2	.594- 2	.788- 2	.104- 1	144	
145	.423- 3	.616- 3	.887- 3	.126- 2	.177- 2	.246- 2	.336- 2	.456- 2	.611- 2	.809- 2	145	
146	.302- 3	.444- 3	.646- 3	.927- 3	.131- 2	.184- 2	.254- 2	.348- 2	.470- 2	.628- 2	146	
147	.214- 3	.318- 3	.467- 3	.676- 3	.968- 3	.137- 2	.190- 2	.263- 2	.359- 2	.485- 2	147	
148	.150- 3	.226- 3	.335- 3	.490- 3	.708- 3	.101- 2	.142- 2	.198- 2	.273- 2	.371- 2	148	
149	.105- 3	.159- 3	.238- 3	.352- 3	.514- 3	.740- 3	.105- 2	.148- 2	.205- 2	.282- 2	149	
150	.727- 4	.111- 3	.169- 3	.251- 3	.370- 3	.538- 3	.773- 3	.110- 2	.154- 2	.213- 2	150	
151	.500- 4	.775- 4	.118- 3	.178- 3	.265- 3	.389- 3	.564- 3	.807- 3	.114- 2	.160- 2	151	
152	.342- 4	.534- 4	.824- 4	.125- 3	.188- 3	.279- 3	.408- 3	.590- 3	.842- 3	.119- 2	152	
153	.232- 4	.366- 4	.570- 4	.876- 4	.133- 3	.199- 3	.294- 3	.428- 3	.617- 3	.878- 3	153	
154	.156- 4	.249- 4	.392- 4	.608- 4	.931- 4	.141- 3	.210- 3	.309- 3	.449- 3	.645- 3	154	
155	.104- 4	.168- 4	.267- 4	.419- 4	.648- 4	.988- 4	.149- 3	.221- 3	.324- 3	.470- 3	155	
156	.693- 5	.113- 4	.181- 4	.287- 4	.447- 4	.689- 4	.105- 3	.157- 3	.233- 3	.341- 3	156	
157	.457- 5	.751- 5	.122- 4	.195- 4	.307- 4	.477- 4	.732- 4	.111- 3	.166- 3	.245- 3	157	
158	.299- 5	.497- 5	.813- 5	.131- 4	.209- 4	.328- 4	.509- 4	.778- 4	.117- 3	.175- 3	158	
159	.194- 5	.326- 5	.539- 5	.879- 5	.141- 4	.224- 4	.351- 4	.541- 4	.825- 4	.124- 3	159	
160	.125- 5	.213- 5	.355- 5	.585- 5	.950- 5	.152- 4	.240- 4	.374- 4	.576- 4	.874- 4	160	
161	.003- 6	.138- 5	.232- 5	.386- 5	.634- 5	.102- 4	.163- 4	.257- 4	.399- 4	.612- 4	161	
162	.511- 6	.884- 6	.151- 5	.254- 5	.420- 5	.682- 5	.110- 4	.175- 4	.275- 4	.425- 4	162	
163	.323- 6	.565- 6	.973- 6	.165- 5	.276- 5	.456- 5	.741- 5	.119- 4	.188- 4	.294- 4	163	

R	N=1100	N=1110	N=1120	N=1130	N=1140	N=1150	N=1160	N=1170	N=1180	N=1190	R	P=1/10
164	.203- 6	.358- 6	.623- 6	.107- 5	.181- 5	.301- 5	.494- 5	.800- 5	.128- 4	.201- 4	164	
165	.126- 6	.225- 6	.397- 6	.687- 6	.117- 5	.197- 5	.327- 5	.534- 5	.862- 5	.137- 4	165	
166	.782- 7	.141- 6	.251- 6	.438- 6	.756- 6	.128- 5	.215- 5	.355- 5	.578- 5	.928- 5	166	
167	.481- 7	.876- 7	.157- 6	.278- 6	.484- 6	.830- 6	.140- 5	.234- 5	.385- 5	.624- 5	167	
168	.293- 7	.541- 7	.980- 7	.175- 6	.308- 6	.533- 6	.911- 6	.153- 5	.255- 5	.417- 5	168	
169	.178- 7	.331- 7	.607- 7	.109- 6	.194- 6	.340- 6	.587- 6	.998- 6	.167- 5	.276- 5	169	
170	.107- 7	.202- 7	.373- 7	.680- 7	.122- 6	.216- 6	.376- 6	.645- 6	.109- 5	.182- 5	170	
171	.641- 8	.122- 7	.228- 7	.420- 7	.761- 7	.136- 6	.239- 6	.414- 6	.708- 6	.119- 5	171	
172	.381- 8	.732- 8	.138- 7	.257- 7	.471- 7	.850- 7	.151- 6	.264- 6	.456- 6	.776- 6	172	
173	.225- 8	.437- 8	.834- 8	.157- 7	.290- 7	.528- 7	.948- 7	.168- 6	.292- 6	.501- 6	173	
174	.132- 8	.259- 8	.499- 8	.949- 8	.177- 7	.326- 7	.591- 7	.105- 6	.186- 6	.322- 6	174	
175	.769- 9	.152- 8	.297- 8	.570- 8	.108- 7	.200- 7	.366- 7	.660- 7	.117- 6	.205- 6	175	
176	.445- 9	.891- 9	.176- 8	.340- 8	.649- 8	.122- 7	.225- 7	.410- 7	.736- 7	.130- 6	176	
177	.256- 9	.518- 9	.103- 8	.202- 8	.389- 8	.738- 8	.138- 7	.253- 7	.459- 7	.819- 7	177	
178	.146- 9	.299- 9	.602- 9	.119- 8	.232- 8	.444- 8	.837- 8	.155- 7	.284- 7	.513- 7	178	
179	.829-10	.171- 9	.349- 9	.697- 9	.137- 8	.265- 8	.505- 8	.948- 8	.175- 7	.319- 7	179	
180	.467-10	.977-10	.201- 9	.406- 9	.806- 9	.158- 8	.303- 8	.574- 8	.107- 7	.197- 7	180	
181	.262-10	.553-10	.115- 9	.235- 9	.471- 9	.930- 9	.181- 8	.346- 8	.651- 8	.121- 7	181	
182	.146-10	.311-10	.653-10	.135- 9	.273- 9	.545- 9	.107- 8	.207- 8	.393- 8	.737- 8	182	
183		.174-10	.369-10	.769-10	.158- 9	.318- 9	.630- 9	.123- 8	.236- 8	.447- 8	183	
184			.207-10	.436-10	.903-10	.184- 9	.368- 9	.726- 9	.141- 8	.269- 8	184	
185			.116-10	.246-10	.514-10	.106- 9	.214- 9	.426- 9	.836- 9	.161- 8	185	
186				.138-10	.291-10	.605-10	.124- 9	.249- 9	.492- 9	.960- 9	186	
187					.164-10	.344-10	.710-10	.144- 9	.288- 9	.567- 9	187	
188						.194-10	.405-10	.830-10	.168- 9	.333- 9	188	
189						.109-10	.229-10	.475-10	.970-10	.195- 9	189	
190							.129-10	.271-10	.557-10	.113- 9	190	
191								.153-10	.318-10	.652-10	191	
192									.181-10	.374-10	192	
193									.102-10	.213-10	193	
194										.121-10	194	

R	N=1200	R
88	.999- 0	88
89	.999- 0	89
90	.999- 0	90
91	.998- 0	91
92	.998- 0	92
93	.997- 0	93
94	.996- 0	94
95	.994- 0	95
96	.992- 0	96
97	.990- 0	97
98	.987- 0	98
99	.983- 0	99
100	.978- 0	100
101	.972- 0	101
102	.965- 0	102
103	.956- 0	103
104	.946- 0	104
105	.934- 0	105
106	.921- 0	106
107	.905- 0	107
108	.887- 0	108
109	.866- 0	109
110	.844- 0	110
111	.819- 0	111
112	.792- 0	112
113	.763- 0	113
114	.732- 0	114
115	.698- 0	115
116	.664- 0	116
117	.628- 0	117
118	.590- 0	118
119	.552- 0	119
120	.514- 0	120
121	.476- 0	121
122	.438- 0	122
123	.400- 0	123
124	.364- 0	124
125	.329- 0	125
126	.295- 0	126
127	.263- 0	127
128	.233- 0	128
129	.205- 0	129
130	.180- 0	130
131	.156- 0	131
132	.135- 0	132
133	.116- 0	133
134	.984- 1	134
135	.832- 1	135
136	.699- 1	136

R N=1200  
137 .583- 1  
138 .482- 1  
139 .397- 1  
140 .324- 1  
141 .263- 1  
142 .212- 1  
143 .169- 1  
144 .134- 1  
145 .106- 1  
146 .831- 2  
147 .646- 2  
148 .499- 2  
149 .383- 2  
150 .292- 2  
151 .221- 2  
152 .166- 2  
153 .124- 2  
154 .916- 3  
155 .674- 3  
156 .492- 3  
157 .357- 3  
158 .258- 3  
159 .184- 3  
160 .131- 3  
161 .926- 4  
162 .650- 4  
163 .453- 4  
164 .313- 4  
165 .215- 4  
166 .147- 4  
167 .999- 5  
168 .673- 5  
169 .451- 5  
170 .300- 5  
171 .198- 5  
172 .130- 5  
173 .849- 6  
174 .550- 6  
175 .354- 6  
176 .227- 6  
177 .144- 6  
178 .910- 7  
179 .571- 7  
180 .356- 7  
181 .221- 7  
182 .136- 7  
183 .833- 8  
184 .507- 8  
185 .306- 8  
186 .184- 8  
187 .110- 8  
188 .652- 9  
189 .384- 9  
190 .225- 9  
191 .131- 9  
192 .760-10  
193 .438-10  
194 .250-10  
195 .142-10

R P=1/10  
137  
138  
139  
140  
141  
142  
143  
144  
145  
146  
147  
148  
149  
150  
151  
152  
153  
154  
155  
156  
157  
158  
159  
160  
161  
162  
163  
164  
165  
166  
167  
168  
169  
170  
171  
172  
173  
174  
175  
176  
177  
178  
179  
180  
181  
182  
183  
184  
185  
186  
187  
188  
189  
190  
191  
192  
193  
194  
195

APPENDIX 5

**PLAINTEXT AND RANDOM MATERIAL FOR SAMPLING PURPOSES**

- A. 1000 Letters of English Plain Text
- B. 1000 Letters with Theoretical English Plaintext Frequencies
- C. 1000 Letters of Random Text
- D. 1000 Digits of Random Text
- E. 1000 Characters of Random Text (32-Element Alphabet)
- F. 25 Random 26-Letter Alphabets

* * * * *

In the study of a cryptographic system, the cryptanalyst often finds it expedient to encipher a known plain text and then examine the phenomena which arise. Or again, the analyst may use a certain kind of text as key and observe its effect in the resultant cipher text. This Appendix presents samples of the principal types of text useful in experimentation.

### PLAINTEXT AND RANDOM MATERIAL FOR SAMPLING PURPOSES

#### A. 1000 Letters of English Plain Text

T H E F A C T T H A T T H E S C I E N T I F I C I N V E S T  
 I G A T O R W O R K S F I F T Y P E R C E N T O F H I S T I  
 M E B Y N O N R A T I O N A L M E A N S I S C M A I T S E E  
 M S C M A Q U I T E I N S U F F I C I E N T L Y R E C O G N  
 I Z E D P D T H E R E I S W I T H O U T T H E L E A S T D O 5  
 U B T A N I N S T I N C T F O R R E S E A R C H C M A A N D  
 O F T E N T H E M O S T S U C C E S S F U L I N V E S T I G  
 A T O R S O F N A T U R E A R E Q U I T E U N A B L E T O G  
 I V E A N A C C O U N T O F T H E I R R E A S O N S F O R D  
 O I N G S U C H A N D S U C H A N E X P E R I M E N T C M A 10  
 O R F O R P L A C I N G S I D E B Y S I D E T W O A P P A R  
 E N T L Y U N R E L A T E D F A C T S P D A G A I N C M A O  
 N E O F T H E M O S T S A L I E N T T R A I T S I N T H E C  
 H A R A C T E R O F T H E S U C C E S S F U L S C I E N T I  
 F I C W O R K E R I S T H E C A P A C I T Y F O R K N O W I 15  
 N G T H A T A P O I N T I S P R O V E D W H E N I T W O U L  
 D N O T A P P E A R T O B E P R O V E D T O A N O U T S I D  
 E I N T E L L I G E N C E F U N C T I O N I N G I N A P U R  
 E L Y R A T I O N A L M A N N E R S E M I C O L O N T H U S  
 T H E I N V E S T I G A T O R F E E L S T H A T S O M E P R 20  
 O P O S I T I O N I S T R U E C M A A N D P R O C E E D S A  
 T O N C E T O T H E N E X T S E T O F E X P E R I M E N T S  
 W I T H O U T W A I T I N G A N D W A S T I N G T I M E I N  
 T H E E L A B O R A T I O N O F T H E F O R M A L P R O O F  
 O F T H E P O I N T W H I C H H E A V I E R M I N D S W O U 25  
 L D N E E D P D Q U E S T I O N L E S S S U C H A S C I E N  
 T I F I C I N T U I T I O N M A Y A N D D O E S S O M E T I  
 M E S L E A D I N V E S T I G A T O R S A S T R A Y C M A B  
 U T I T I S Q U I T E C E R T A I N T H A T I F T H E Y D I  
 D N O T W I D E L Y M A K E U S E O F I T C M A T H E Y W O 30  
 U L D N O T G E T A Q U A R T E R A S F A R A S T H E Y D O  
 P D E X P E R I M E N T S C O N F I R M E A C H O T H E R C  
 M A A N D A F A L S E S T E P I S U S U A L L Y S O O N D I  
 S C O V E R E D P D

#### Distribution:

A	81	G	15	L	27	Q	5	V	9
B	7	H	37	M	28	R	51	W	14
C	46	I	90	N	76	S	70	X	4
D	34	J	0	O	75	T	109	Y	14
E	112	K	4	P	25	U	33	Z	1
F	33								

B. 1000 Letters with Theoretical English Plaintext Frequencies

O	I	N	S	W	R	T	R	O	I	Y	D	N	P	D	A	T	T	L	S	C	V	U	E	A	T	Z	F	D	R
P	A	E	P	S	L	L	M	S	I	N	A	I	S	E	E	S	C	E	T	L	M	Y	E	D	N	D	P	W	D
P	R	I	C	M	T	G	A	S	C	S	E	L	M	R	E	T	E	R	N	T	I	O	H	T	S	L	O	P	S
I	L	T	O	V	I	U	L	M	D	A	Y	C	E	I	T	A	W	E	F	S	R	E	Y	C	I	O	G	O	E
G	L	N	I	H	N	O	F	S	E	A	E	T	L	N	R	W	E	O	O	E	R	S	R	R	S	P	E	R	E
M	A	I	E	W	A	T	E	X	I	F	C	R	E	N	S	A	U	I	E	U	R	S	T	I	M	N	S	D	T
E	N	T	T	N	F	S	X	N	U	N	R	U	L	M	O	R	O	G	I	E	I	A	R	E	R	E	E	N	N
R	D	E	A	E	T	S	P	E	R	L	T	A	N	E	I	R	R	N	O	E	C	Q	A	F	N	T	H	U	N
T	O	N	B	N	E	I	O	F	D	O	S	M	E	E	D	T	E	S	P	T	T	R	E	A	G	H	U	E	R
H	S	A	O	I	H	R	I	H	E	V	F	I	W	L	J	S	W	L	I	T	N	E	A	G	E	R	R	O	E
N	N	C	I	I	N	E	N	L	R	O	T	O	E	I	F	C	R	N	S	L	P	U	I	P	U	S	O	I	O
E	C	T	S	W	A	N	O	T	I	E	C	I	T	I	I	R	T	E	I	F	S	O	E	T	V	T	R	N	T
D	E	I	E	D	H	S	I	H	R	D	I	N	C	B	H	T	P	N	I	N	R	L	M	C	T	F	A	W	I
R	E	W	D	A	Y	A	A	O	S	N	N	I	O	G	M	R	K	O	F	F	T	S	D	O	H	T	A	I	A
A	B	E	T	T	O	N	T	N	F	O	I	T	H	F	L	M	N	Y	O	E	W	O	T	O	A	L	I	N	B
C	T	E	P	A	E	S	T	V	N	I	M	S	O	E	A	S	A	D	R	S	U	Y	N	R	D	I	C	I	V
S	S	M	E	O	I	E	A	H	F	U	C	Y	N	W	Y	E	N	A	T	R	D	T	A	D	M	A	D	E	E
M	E	H	E	E	T	E	P	A	C	Y	W	N	O	N	U	P	H	T	T	M	O	D	M	U	O	F	D	O	R
T	R	O	O	A	N	N	E	E	S	T	G	T	O	G	E	I	E	E	H	C	T	U	O	M	C	I	F	H	A
T	E	A	D	R	E	E	A	T	P	N	O	E	N	R	D	R	D	S	E	Y	L	E	S	Q	S	F	E	X	K
O	R	A	A	O	B	S	T	N	A	T	I	V	R	E	R	F	N	O	E	T	O	E	A	A	S	I	T	C	G
A	I	L	R	T	V	A	V	C	S	U	R	R	R	W	E	T	N	A	C	L	K	I	G	S	U	E	H	R	R
I	L	E	O	I	O	E	E	O	N	T	I	S	A	R	X	N	U	D	B	S	A	T	E	S	T	P	N	I	E
S	H	R	E	V	E	I	H	Y	N	A	S	I	S	B	L	N	R	S	A	G	I	L	G	E	S	O	U	E	H
D	A	U	E	L	H	O	T	D	S	T	O	H	E	G	R	U	E	A	U	I	H	G	O	I	U	E	D	S	E
F	D	R	E	L	J	L	F	A	E	R	T	T	A	I	R	H	N	L	E	T	R	N	E	T	T	E	F	A	C
I	L	C	P	I	A	N	O	U	V	I	U	N	R	G	R	R	R	E	T	E	E	O	P	E	E	P	R	D	E
O	E	B	P	A	E	T	I	R	S	D	T	S	N	H	W	A	T	S	W	P	A	A	R	R	N	A	O	E	E
D	F	O	N	D	T	F	D	M	E	S	R	N	O	O	T	C	A	N	E	Y	L	A	R	D	M	I	C	O	T
T	V	T	O	M	C	Y	T	T	X	N	Y	D	L	R	T	E	S	A	O	L	E	N	V	T	E	E	O	T	R
N	Q	N	T	N	Y	H	E	O	M	C	E	N	P	N	C	H	N	N	E	D	A	N	V	D	H	O	P	E	A
R	R	Y	A	O	B	I	P	T	D	V	A	R	E	E	M	D	H	F	E	O	A	Y	E	E	I	T	L	P	H
I	R	T	S	O	E	T	L	H	I	F	N	U	O	A	C	Y	H	N	E	M	N	I	I	T	P	T	O	H	A
O	A	A	L	F	O	E	I	E	S																				

Distribution:

A	74	G	16	L	36	Q	3	V	15
B	10	H	34	M	25	R	76	W	16
C	31	I	74	N	79	S	61	X	5
D	42	J	2	O	75	T	92	Y	19
E	130	K	3	P	27	U	26	Z	1
F	28								

C. 1000 Letters of Random Text

```

A G L Q O   Y P F J Y   Z R U F D   K F W F A   B V L T W   P P J Q V
R D F Y N   L Q G S D   F S P D Z   H O K Z B   B H A O S   L W K P G
G X J F B   A Z O L Z   G A A Z I   W Z I G Y   Q S F N O   U Z N S S
B Y L N N   V K L M S   G U R E J   U H X X Q   T N Q Z J   I A T I K
D H A W K   J Q W K W   H Z X P S   V F Q S U   Q V X S Z   G T J N B   5
B R F J N   C R O S W   Y N T D N   Y T U H C   G E O F L   X D V K Y
B Q S V X   V W C R J   G W N E O   R O L M L   S T Y T O   H S C J B
J O X W F   D S S P Q   O C C E X   K J A B Y   L M N Q H   K A L N W
S K N S M   H M O J H   U M D W Z   U L Y K X   A G S A P   W J V J H
J W J J N   M H F Z A   U G V M Z   W I Q U F   Q Z V E V   X C W Q N   10
Z V U F M   X F O U J   X B P R E   R S I W N   P F L O M   F H V S L
Z N Y X I   F W P K O   D L J I T   Y V D L V   P U M A R   H F Q V T
T R A H J   L J M U K   G W J A C   V Z C R U   E S G N B   D A W Z O
E U A B B   Z F R B G   N H Z N A   D K R B P   C E Y N A   P X M U I
L H X C X   N R X R M   C O Q M Y   H T T I O   N E F X H   J Y W F I   15
A N O T C   R K Y O U   M W Q V J   P R S H W   E K S M B   D K I A L
D F C Y N   H C W M U   X L S F W   G A D B R   Z V Y E T   U K Z M U
H H E B G   E K W F E   Y P T T B   I K C R M   I Y F A R   D V P U O
P F Y G V   Q C Z G O   L L J F B   C F S O C   Y B E D S   X P J G N
X V H T U   U Y P D P   U H P Z K   V U S F J   E W A T O   H W M X E   20
Z D X Z V   J X W U O   T U B J D   G R L P A   K G B H U   E B Y R A
L D M U J   N Y W V J   F S D C P   C G S T D   I O V Z Q   T U C I Y
F F H W I   G D P A U   C K H B X   P Q G S P   O O D E J   G C B G A
K N B A F   E F E Y U   P F B H S   E O O E P   Z Z W H P   L M I O J
S Z Y P D   B Z O E C   M U B P X   Q T V Q N   E G R D B   J V F T I   25
E J M O N   H R H Z K   A E B Q F   H P W W C   H F L B U   Q I Y R Z
R H Y H S   M S I K W   K N Z O U   Q G Y P F   A A Y G A   N Z T G V
O M G C T   Z G Y K Y   N Y R W W   W P D L V   T M P K U   R I A V K
D Q D L E   Z B K E S   Q V W E Q   P M Y T C   X O C O K   S N M S C
R L D G U   G P N Q Q   R F Y C N   X Z X G K   W K F A I   V A C U T   30
K A D L V   J O N X R   B Y V H I   W F H F N   I J T O H   J K V G F
Z A X A V   O K D X M   T O L E N   W Y X D L   C A A D G   U Y Z O K
J W O N R   Q G W E E   R T W S F   Y J E P X   S N K X V   X S X A D
U Q P K X   V F G Q R

```

Distribution:

A	43	G	40	L	33	Q	34	V	40
B	36	H	40	M	31	R	35	W	46
C	33	I	25	N	42	S	41	X	39
D	37	J	41	O	44	T	32	Y	42
E	35	K	41	P	40	U	41	Z	41
F	48								



D. 1000 Digits of Random Text

2 5 4 0 1	4 6 5 8 5	3 3 3 6 5	2 9 1 7 2	8 6 7 2 5	3 0 4 9 4	
4 6 6 7 5	0 3 2 7 8	3 0 6 8 0	0 0 2 2 0	1 4 9 8 4	6 6 3 1 2	
2 4 2 8 7	0 1 3 1 3	2 2 1 9 7	3 8 7 4 2	4 0 1 6 8	4 3 1 5 7	
8 9 3 7 6	0 2 8 6 9	2 4 7 9 4	7 8 8 3 4	5 8 4 4 6	5 1 8 6 0	
9 1 9 2 3	2 5 4 0 9	6 0 3 6 8	9 9 8 2 6	6 0 5 9 7	1 0 1 2 9	5
8 7 6 4 2	9 3 0 4 8	5 6 6 0 8	3 9 3 1 8	5 1 2 6 4	2 4 4 5 9	
0 1 6 7 4	5 2 5 0 8	9 1 4 1 4	8 5 4 2 4	9 1 5 5 5	7 2 7 6 9	
7 1 1 6 4	2 0 3 8 7	8 0 2 7 0	6 2 9 3 5	8 8 0 4 3	3 5 1 2 4	
0 6 5 1 1	3 4 6 2 2	2 7 8 5 1	2 3 6 2 2	5 4 1 2 5	2 5 5 0 2	
3 5 9 9 3	7 3 3 2 3	4 0 1 2 0	8 0 7 9 8	7 9 7 5 0	0 8 0 4 0	10
6 8 7 2 8	7 7 7 2 5	6 5 8 2 4	3 1 5 6 9	9 9 0 8 9	8 4 7 2 1	
3 6 3 7 5	6 2 9 6 2	9 0 4 3 0	4 0 7 8 4	0 0 9 2 5	9 5 5 4 8	
8 1 8 2 0	9 1 8 5 4	8 1 4 2 4	0 9 0 0 5	8 3 5 7 9	0 9 3 2 3	
7 4 8 5 4	3 7 3 1 0	1 2 8 2 2	0 3 0 3 3	1 2 9 4 9	8 9 2 1 0	
8 6 8 1 6	4 7 5 0 0	6 0 7 4 6	7 0 4 2 0	1 7 1 8 7	0 6 5 2 1	15
1 4 3 6 7	2 2 7 0 5	0 3 1 5 4	9 8 0 1 2	8 5 5 8 3	4 7 9 9 4	
2 4 1 4 9	5 2 3 7 3	4 2 1 0 1	0 3 4 7 4	4 3 9 6 0	9 2 6 5 1	
5 9 3 5 0	3 5 7 0 3	3 0 9 1 5	0 0 8 9 9	7 8 2 7 9	8 8 9 0 7	
2 3 3 1 0	8 1 4 8 1	4 1 2 1 3	4 1 6 4 7	0 9 5 3 7	8 4 0 7 3	
5 3 6 0 5	8 3 0 6 2	5 8 3 9 2	4 9 6 3 8	4 2 7 6 2	8 4 5 8 3	20
4 2 5 3 6	7 1 2 7 8	3 8 6 1 4	5 3 5 2 3	1 2 0 4 6	6 3 7 8 9	
4 5 1 2 9	8 9 6 5 1	9 6 2 6 4	0 0 2 9 0	0 1 4 2 3	7 9 6 8 9	
4 4 3 0 0	8 0 9 5 5	9 7 9 1 8	0 8 8 8 4	6 9 8 4 5	3 7 4 6 8	
2 0 1 4 1	8 6 9 1 8	4 1 3 9 3	4 8 7 0 7	6 8 7 9 0	7 1 8 1 3	
9 2 6 2 0	1 6 1 2 4	7 2 3 8 8	8 2 5 4 9	6 7 5 4 0	3 0 6 8 6	25
9 2 3 9 6	8 4 9 2 9	0 9 3 5 1	4 4 1 1 6	2 3 1 0 5	6 9 3 1 3	
8 9 6 9 8	9 8 6 7 8	0 1 1 5 4	2 6 1 1 7	6 8 9 4 7	4 6 0 2 4	
3 9 8 4 1	1 4 4 1 7	6 5 0 0 1	6 1 8 8 6	4 1 8 1 9	3 6 1 9 0	
7 9 5 5 7	5 1 5 8 9	8 2 3 9 4	8 8 3 9 1	5 6 2 8 8	7 2 9 0 2	
1 6 8 0 6	0 5 0 9 5	4 4 9 9 3	3 8 6 5 8	5 7 9 2 4	7 3 0 1 0	30
5 0 2 3 5	5 7 7 9 7	4 7 4 5 2	9 1 7 3 2	2 4 7 6 4	0 1 3 0 7	
7 9 8 1 8	5 1 7 5 2	2 3 6 0 4	2 6 9 6 9	6 3 2 8 2	9 7 9 0 7	
5 6 6 2 0	9 0 7 6 8	9 7 9 8 9	2 3 1 2 1	7 7 3 3 2	7 2 5 8 8	
9 1 5 1 1	9 3 2 3 4					

Distribution:

0	106	5	90
1	99	6	88
2	110	7	89
3	97	8	110
4	105	9	106

E. 1000 Characters of Random Text (32-Element Alphabet)

```

I H C Q N 7 Z G S K Y V J 3 P V 5 I Z V J 9 S P N E R A I C
8 7 W X K V U K X U N L P S V C O H 8 Z 5 G Z C R I N Q 8 U
T 3 3 V Y P A Z I W A T F R M S L E K 7 U B R T E J P 4 Z 9
W 8 3 U D F M 3 F E H L S B L I D F 8 S J 5 U Y U B K P B E
4 A D 5 R C X P E I H E 9 K C L V I 7 8 E M F 3 7 H 4 J S U 5
P 4 R J B G B Z 9 V F A 7 D H D T 9 W Q P R L M 3 U F I O U
G Z 7 X Q X D W 8 E C N E K F T 9 W Q C 8 E E N C 7 M L H 7
Z Q V R A C X B 4 C 8 N P W 3 P Y L R F S F 4 0 L G X N A Y
F Z W V 8 L 5 5 Y Q T J L R R K U 5 L T D Q D I S P E U Z C
A G U T S A 3 8 3 R L W T I S H F 8 Q 5 L E D B K P X F V F 10
9 P 5 B 9 J Q 4 9 H S T Y P B I G 0 5 D V L T W 9 U D 4 C Y
Q K 4 R O Q 5 A W K P I L K I 9 J B 9 U P B 9 N 4 A 5 G F A
I H V V G N T E L 8 E I J P P 5 S 5 Z 5 V W Q E I 4 3 M B Y
Z X N C G U L G T Y 9 8 7 U T V T 4 7 9 J K T C S W B F X X
A 9 X A E P B T 8 V E V D R 3 9 J R B C Y D L M N H L B G N 15
L Z 4 D T T T O W 4 F N G C O E W E Z 9 H 9 Y 5 Y N A Y Z C
M B A 9 K M D 9 3 8 8 V C W H T I T O T H O E 5 T E P Z P L
R 4 J C 3 B C C X Y L C Q P G 0 0 0 5 I P U I Z Z S Y G X 3
G I N N Q Y F R R E 3 R I E 4 H 7 G Q G 4 X D X Z U K R U 5
N D H 5 D S B Y I N 5 8 Q X K W J X 5 I 7 L I G 4 9 L N 7 I 20
U 4 F M T 7 D 4 X B H M F F L O R X U R 5 L E 5 K F F M K V
4 T 9 C G X J R M N Z E R Q Y Y I I Z 4 N C B 7 M S H Y D J
I T F S S L 8 I O X A Z X T G B K U Y F F Z 3 J D J Y Y B Q
Y U H 4 3 4 B 3 M 9 S Z V U N D A W D S F K V H H A K 4 X X
K Z E 9 C M P S H B T K G F X 9 V T 4 D J P W F C Z K 8 H V 25
G P O Q D 5 D S 3 Y X U E 9 T Q P 3 Q H Y N I Q N T G B M O
8 5 E S I B K 5 4 H Q S K E 3 H A M P 4 X Y A J D U O S Q P
M L O O W J 8 N P A Z L K T 3 8 I H K A 3 Q U X O N 9 O Z K
W G 5 A Y L 8 Q X D Z 4 Z 8 N Z B A N U G U M 5 R R O 8 E E
H P 5 W 5 O F 9 V B 4 U N Z P L K R Y K L M W 5 H A M E 3 L 30
C K 3 X N U 5 P I N Y A E F P L S B H 5 8 7 U 3 8 J W V Y H
U N E D L E 7 9 G Y N F K 3 K Y L H I A R A P V 9 3 C X 4 R
E 4 D 4 B X P B B M 8 3 C 9 Y 3 H 7 F 3 B B S U F W D D F V
M W H Y L Y T F A L

```

Distribution:

A	30	G	27	M	24	R	29	W	26	4	33
B	36	H	34	N	34	S	28	X	33	5	34
C	30	I	35	O	22	T	34	Y	37	7	19
D	32	J	22	P	38	U	35	Z	33	8	29
E	37	K	34	Q	27	V	28	3	32	9	32
F	37	L	39								

*F. 25 Random 26-Letter Alphabets*

1. A M Q N O D Z F R X I L K P E U Y C B G W V J S H T  
2. B S U G C Q P N Y E H M V L J K A F R Z I X O T D W  
3. C O M K Q A W V F Y L I U B T N R J H E S X D Z G P  
4. D M H T I U L N Z F Q K C R O S J E X A Y W P G V B  
5. E F L I S K O P R V T N J U Z Q C H W Y D M G X B A  
6. F Q N S K L R P H D M X Z Y E T W J U C A G I V B O  
7. G M Q L C T U V E N Z B O X H F J S K D R I A W P Y  
8. H M I W F A K X T V S B U Z D P E J C Y G L O Q N R  
9. I K G J V O W Y N X T M F L U P B S A R Q E Z H D C  
10. J X K P U C R Y D E I A W S H O T N G F Z M V L B Q  
11. K T H L O C P M G W N X E V S Z I F U B J Q A Y D R  
12. L R D E I O V W Q K X C B Y H M F A P Z N J U S T G  
13. M I W R K J L H E V G Q A U Y F Z S X P N C B D T O  
14. N F A K X W G V P C R I M L S D J E Q O Y H T Z U B  
15. O L Y B Q V P H U T E W J R D C X I M K Z S A G N F  
16. P H M L N A T Q K O Z Y G J F B E U X S I W C D V R  
17. Q W U L E X I V M O Z F B T Y P K C G A N H J S D R  
18. R E I F L V M N T J P W A K G Y S Q O B D H U X Z C  
19. S K A V O T R J H I Y Z G M Q W X U D B N P F C E L  
20. T I Z Q F J X V R S E H M K W O L N P U C B D Y G A  
21. U D W Z G B I E Y M V C H P J S N L O X F A K Q R T  
22. V L I C U D Y K R X Z A J Q W T F M G P E N B H O S  
23. W Z D N E J A T L M K V P R G Q U C S I O H Y X F B  
24. X I J F G Q E K C Y T U P W H O V R N D Z S L B A M  
25. Y B G F C L H Q X O R S I P A M W J E D U Z T K N V

## APPENDIX 6

## BASIC LETTER FREQUENCY DATA, 24 FOREIGN LANGUAGES

	Page
1. Albanian.....	563
2. Arabic.....	565
3. Bulgarian.....	567
4. Czech.....	569
5. Danish.....	571
6. Dutch.....	573
7. Finnish.....	575
8. French.....	577
9. German.....	579
10. Greek.....	581
11. Hungarian.....	583
12. Indonesian.....	585
13. Italian.....	587
14. Norwegian.....	589
15. Persian.....	591
16. Polish.....	593
17. Portuguese.....	595
18. Romanian.....	597
19. Russian.....	599
20. Serbo-Croat.....	601
21. Slovak.....	603
22. Spanish.....	605
23. Swedish.....	607
24. Turkish.....	609

These data are based on selected samples of newspaper text, communiqué style, of between 50,000 and 67,000 letters in each language, with but one exception (Slovak, with 46,026 letters.)

## BASIC LETTER FREQUENCY DATA, 24 FOREIGN LANGUAGES

### 1. ALBANIAN

1-a. *Absolute frequencies of single letters of Albanian plain text, arranged alphabetically, based on 57,851 letters of text.*

A	4,441	E	5,142	I	4,890	N	3,545	Rr	178	V	776
B	639	Ë	6,604	J	1,233	Nj	420	S	2,054	X	9
C	213	F	545	K	2,207	O	2,431	Sh	1,281	Xh	21
Ç	198	G	590	L	875	P	1,913	T	4,876	Y	296
D	1,161	Gj	325	Ll	381	Q	855	Th	207	Z	398
Dh	538	H	451	M	2,185	R	3,951	U	2,005	Zh	17

1-b. *Monographic kappa plain, Albanian language = .0604 (I.C. = 2.17)*

1-c. *Frequency distribution of single letters based on 57,851 letters of Albanian plain text reduced to 1,000 letters, and arranged according to their frequencies.*

Ë	114	N	61	P	33	V	14	Nj	7	Th	4
E	89	O	42	Sh	22	B	11	Z	7	Ç	3
I	85	K	38	J	21	G	10	Ll	7	Rr	3
T	84	M	38	D	20	F	9	Gj	6	Xh	∅
A	77	S	36	L	15	Dh	9	Y	5	Zh	∅
R	68	U	35	Q	15	H	8	C	4	X	∅

1-d. *Percentage of vowels, high-frequency consonants, medium-frequency consonants, and low-frequency consonants in 57,851 letters of Albanian plain text. Percentage of 7 most frequent letters in Albanian plain text.*

Vowels Ë, E, I, A, O, U, and Y = 44.6%

High-Frequency Consonants T, R, N = 21.4%

Medium-Frequency Consonants K, M, S, P, Sh, J, and D = 20.8%

Low-Frequency Consonants L, Q, V, B, G, F, Dh, H, Nj, Z, Ll, Gj, C, Th, Ç, Rr, Xh, Zh, and X = 13.2%

7 most frequent letters (in descending order of frequency) Ë, E, I, T, A, R, and N = 58%

1-e. *Absolute frequencies of single letters as initial letters of 13,249 words in Albanian plain text, arranged according to their frequencies. (One-letter words have been omitted.)*

T	1,252	Sh	571	Nj	338	J	187	Z	137	Rr	15
P	1,223	S	561	F	315	G	182	Ç	126	Y	10
K	1,050	Q	415	E	259	H	175	Ë	112	Xh	4
N	993	V	380	L	237	R	170	C	90	Ll	2
M	978	B	370	Gj	223	I	156	O	81		
D	605	A	351	Dh	221	U	138	Th	56		

2-a. Frequency distribution of digraphs based on 57,851 letters of Albanian plain text, reduced to 5,000 digraphs.

	A	B	C	Ç	D	Dh	E	Ë	F	G	Gj	H	I	J	K	L	Ll	M	N	Nj	O	P	Q	R	Rr	S	Sh	T	Th	U	V	X	Xh	Y	Z	Zh	
A	3	6	2	2	5	4	11	2	4	4	1	2	2	17	19	17	4	23	49	3	15	11	59	6	19	19	51	3	3	11			1	6	1		
B	17						6	11					4		4						4			3					7								
C	2						1	3				10									1																
Ç	4			2		1	3				2		1	1		1					1	1															
D	6						12	11				22	2								23			8					11						6		
Dh	3						35	3				1	3																	1							
E	8	6	2	4	13	20	8	1	9	6	4	3	4	15	32	10	5	27	42	5	2	26	9	47	2	26	17	72	2	3	14				4		
Ë	9	12	3	4	21	6	13	2	10	6	9	8	6	7	28	9	2	36	84	10	2	35	11	79	2	46	37	66	2	4	19				7		
F	11						4	1					5	2	2						4			3			1	6	6	1							
G	22							3				1		2							6			12					5								
Gj	2						12	1				11									1								1							1	
H	5						16	4					3							1		3								4					1		
I	16	4	3	2	7	6	10	2	4	4	2	4	13	8	38	12	5	34	54	5	8	31	4	12		40	18	49	8	5	6				10		
J	18	1			2	1	27	9	1		1	2	2				9	9	1	3	2	1	1			1	2	10	3								
K	29						14	47				13	1	1	1					3	1	1	14			3	6	1	27						1		
L	9						12	7				29								1	4	1							1							7	
Ll	8						1	4				12	1							1	3							1									
M	19	13			1	1	43	34				38	1	2			1	2	1	10	4	1	1			1	4	12	1								
N	16	1	5	1	32	2	35	84	4	20	3	1	30	1	5			4	5	1	6	5	2		2	4	2	21	11	3	1			1	1		
Nj	2						5	27													2							1									
O	1	2	1		2	1	1	1	3	2	1	1	1	1	23	7	7	5	12	27	4	1	11	3	29	1	11	1	32	1	1	4	1		2		
P	28						8	48				6	3	2	1			1	25			20			1	8	14										
Q	1						9	33				26									1						1	1								1	
R	44	4	1	2	3	1	47	37	3	6	4	3	75	2	12	1		11	6	3	15	9	4	1		8	5	17	1	1	2				5		
Rr	3						2	4				3									1							2									
S	12	1			2	2	26	26	1		1	33	2	7	1	1	3	5	1	12	5	1	1			7	1	20	5	1					1		
Sh	4				1		2	7				11	1	15				3	1		4	5	19				33	6	1								
T	40	1			3	2	43	140	2	1		1	45	10	5	1		9	9	2	25	9	4	20		4	2	17	19	2				4	1		
Th	4						2	5				2									2								1								
U	30	2			3	2	1		5	1		6	1	3	13	3	7	10	30			5	1	26	2	6	4	5		2					2		
V	8				1		28	10				9	3	1							5			2					1								
X																																					
Xh	1																																				
Y							5								3	1	1	1				1	1	5			1	1	2								
Z	4	2					5	3			1	4	1					2			9								2							1	1
Zh					1																																

2-b. Digraphic kappa plain, Albanian language=.0061 (I.C.=7.91)

2. ARABIC

1-a. Absolute frequencies of single letters of Arabic plain text, arranged alphabetically, based on 53,472 letters of text.

ا	10,391	ر	1,721	ض	355	گ	967
ب	1,725	ز	470	ط	535	ل	5,958
ث	3,411	س	2,526	ظ	93	م	3,204
ج	253	ش	341	ع	1,833	ن	2,771
ح	657	ص	1,330	غ	216	ه	1,935
خ	1,009	ق	463	ف	1,524	و	3,023
د	432	ك	533	ق	1,260	ي	4,536

1-b. Monographic kappa plain, Arabic language = .0811 (I.C. = 2.27)

1-c. Frequency distribution of single letters based on 53,472 letters of Arabic plain text reduced to 1,000 letters, and arranged according to their frequencies.

ا	194	و	57	ر	32	ح	19	ز	9	ث	5
ل	111	ن	52	ب	32	گ	18	ش	9	غ	4
ي	85	ر	47	ف	28	ج	12	خ	8	ظ	2
ت	64	ه	36	س	25	ط	10	ض	7		
م	60	ع	34	ق	24	ص	10	ز	6		

1-d. Percentage of vowels, high-frequency consonants, medium-frequency consonants, and low-frequency consonants, in 53,472 letters of Arabic plain text. Percentage of 8 most frequent letters in Arabic plain text.

Vowels ا, ي, and و = 33.6%

High-Frequency Consonants ل, ت, م, ن, and ر = 33.4%

Medium-Frequency Consonants ه, ع, ر, ب, ف, س, ق, ح, and گ = 24.9%

Low-Frequency Consonants ح, ط, ص, ز, ش, خ, ض, ز, ث, غ, and ظ = 8.1%

8 most frequent letters (in descending order of frequency) ا, ل, ي, ت, م, و, ن, and ر = 64.6%

1-e. Absolute frequencies of single letters as initial letters of 11,496 words of Arabic plain text, arranged according to their frequencies. (One-letter words have been omitted.)

ا	4,122	ل	549	ه	214	ج	140	ز	61	ض	27
م	905	ع	548	س	204	ر	133	ط	61	ز	25
و	880	ت	442	گ	203	ر	109	ص	56	ظ	7
ف	776	ي	334	ح	202	ش	76	ث	42		
ب	591	ق	223	ن	152	خ	70	غ	29		

2-a. Frequency distribution of digraphs based on 53,472 letters of Arabic plain text, reduced to 5,000 digraphs.

	ا	ب	ت	ث	ج	ح	خ	د	ر	ز	س	ش	ص	ض	ط	ظ	ع	غ	ف	ق	ك	ل	م	ن	ه	و	ي	
ا	78	27	49	6	10	17	9	25	9	39	4	27	7	10	7	8	26	1	24	18	12	348	50	86	12	35	32	
ب	41	3	8	1	4	4	1	14	3	1	1	1	1	12	3	2	5	1	11	4	6	8	7	19				
ت	75	14	8	2	5	11	6	5	1	13	1	8	4	6	1	3	1	17	1	17	9	6	13	23	6	14	31	17
ث	5		2						2								1		1			5	2	1	1	1	3	
ج	12	2	5		1		4	6	1								2					6	5	3	4	4	6	
ح	15	2	6	1	1		11	5	5	3		3	1	1				3	6	6	4	4	1	2	4	8		
خ	10	2	3				1	1	4				2	2					1			4	4			2	2	
د	37	3	17	1	1	2	2	3		7	1	2	1	1		1	5		3	3	2	4	11	5	9	16	25	
ر	16	1	1						2													2	6	1		8	1	5
ز	60	18	17		6	4	1	5		2	1	5	1	1	4	1	4	1	11	7	7	3	6	4	13	17	37	
س	11	4	1				1	2									1					1	2		1	2	6	
ش	23	7	24		2	1	1	1		2		1			7		6		4		4	7	6	4	3	7	17	
ص	9		3		1	1	1		11								3		1		4	1	1		1	1	5	
ض	9	3	2		4	4	7										1		2			6	1	1	2	5	3	
ط	9	1	1		1	1	4										2		1			2	3		1	3	5	
ظ	14	1	4						4								2		1	1		4	1	3	2	3	9	
ع	2								3										1							1	1	
غ	28	5	11		1		11	1	14	1	1	4		3	1	1	1		1	3	1	32	11	12	6	8	11	
ف	2	1	1				2	1	4													1	1			2	4	
ق	20	1	9		1	1	1	2		7		2	1	1	1		1	4		1	7	3	11	3	2	4	8	53
ك	25	7	9				21		6		1		2	3	2		4		3	1	1	6	3	1	2	13	10	
ل	19	4	4	2			1	1	5	1	1						1		2			7	14	6	1	12	7	
م	115	19	33	3	11	23	6	16	6	8	2	23	10	8	2	5	25	7	16	15	17	12	65	11	15	23	62	
ن	58	7	21	2	4	7	3	8	2	16		16	4	4	1	2	16	1	8	5	3	12	9	38	9	24	20	
ه	71	9	20		4	4	2	6	2	4	1	8	4	4	1	2	3	7	1	10	6	5	5	11	4	18	17	30
و	69	4	4	1	2	2	3	14	5		1			1			6		7	2	2	7	18	3	2	18	8	
ي	63	7	7	1	5	5	3	10	1	15	8	9	2	4	7	4	1	11	2	10	18	4	30	20	19	6	1	13
ي	79	10	49	2	8	7	3	16	2	27	4	13	2	2	2	9	15	1	12	10	8	13	22	42	37	21	8	

2-b. Digraphic kappa plain, Arabic language = .0101 (I.C. = 7.92).



## 3. BULGARIAN

1-a. Absolute frequencies of single letters of Bulgarian plain text, arranged alphabetically, based on 55,689 letters of text.

A	6,543	Ж	426	M	1,166	T	4,331	Ш	290
Б	849	З	1,203	H	4,226	У	750	Щ	344
В	2,579	И	5,245	O	4,950	Ф	161	Ъ	988
Г	816	Й	350	П	1,561	X	258	Ь	13
Д	1,949	К	1,723	P	2,799	Ц	422	Ю	111
Е	4,987	Л	1,829	C	2,993	Ч	722	Я	1,105

1-b. Monographic kappa plain, Bulgarian language=.0647 (I.C.=1.94).

1-c. Frequency distribution of single letters based on 55,689 letters of plain text, reduced to 1,000 letters and arranged according to their frequencies.

A	117	C	54	П	28	Г	15	Щ	6
И	94	P	50	З	22	У	13	Ш	5
Е	89	B	46	M	21	Ч	13	X	5
O	89	Д	35	Я	20	Ж	8	Ф	3
T	78	Л	33	Ъ	18	Ц	8	Ю	2
H	76	К	31	Б	15	Й	6	Ь	0

1-d. Percentage of vowels, high-frequency consonants, medium-frequency consonants, and low-frequency consonants in 55,689 letters of Bulgarian plain text. Percentage of 6 most frequent letters in Bulgarian plain text.

Vowels A, И, Е, O, Я, Ъ, У, Й, Ю and Ь=45.0%

High-Frequency Consonants T and H=15.4%

Medium-Frequency Consonants C, P, B, Д, Л, К, П, З, M, Б, Г, and Ч=36.2%

Low-Frequency Consonants Ж, Ц, Ш, X and Ф=3.4%

6 most frequent letters (in descending order of frequency) A, И, Е, O, T and H=54.4%

1-e. Absolute frequencies of single letters as initial letters of 10,421 words of Bulgarian plain text, arranged according to their frequencies. (One-letter words have been omitted).

H	1,284	O	611	T	433	P	304	A	117	Ф	93	Ш	25
C	1,191	K	518	Б	364	Г	232	У	114	Ц	82	Ю	18
П	1,022	B	488	M	340	Ч	197	Л	108	Ж	51	Я	13
Д	713	З	477	И	319	E	126	Щ	100	X	39		9,379

2-a. Frequency distribution of digraphs based on 55,689 letters of Bulgarian plain text.

	А	Б	В	Г	Д	Е	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ь	Ю	Я	
А	4	18	47	11	27	10	6	31	16	6	26	28	23	79	15	32	40	51	74	3	2	5	7	10	8	6			1	5	
Б	5		3		1	9		1	11			6		2	12		8	1		1		1				4	10			2	
В	53	2	3	2	2	32		2	29	1	3	3	2	10	30	4	8	15	3	2			1	2			20			5	
Г	18		1			6			5		1	6		3	21	1	8			1								1			
Д	38		5		1	30			24		2	2	1	18	19	2	7	6	1	9				1			7			1	
Е	3	8	18	13	45	3	7	15	13	3	12	32	21	83	13	22	25	45	36	3	1	2	4	10	5	7				1	
Ж	7	2			8	12			6		1			2																	
З	41	2	7	2	2	5		1	9		4	3	4	9	3	5	1	2	2	2		1					1			1	
И	8	5	21	7	14	25	4	28	14	3	20	15	17	44	15	18	13	38	69	2	1	3	11	21	3	4				48	
Й		1		1	1	1		1			3	1	1	5	1	2	1	5	4					1		1					
К	38	1	6		1	1		1	32			3		2	41		9	2	5	5			2				6				
Л	19	1	1	6	1	24	2	1	39		5			13	20	1		7	2	6				1	1		2		4	9	
М	17	1	3	1	2	22		1	18		1	1	1	5	16	2	1	2	1	4				1			3			1	
Н	139	1	2	3	5	40		3	85	1	5	1	1	5	46	2	1	13	11	2	1			4	2	1				5	
О	1	20	49	13	36	7	9	9	18	12	13	25	13	36	8	20	21	42	65	2	4	1	3	5	3	4				7	
П	12		1			10			7			5		1	42		52		1	4							4			1	
Р	65	1	2	4	5	50	3	1	33		1	1	2	6	38	2		6	6	8	1	3		1	2		5			5	
С	15	1	10	1	1	32		1	23		35	12	3	7	7	8	5	3	75	2				1			22			4	
Т	70	2	25	4	5	68		2	36	1	6	2	3	22	82	6	22	10	4	6	1	1		2			8		1	3	
У	1	3	7	2	5		4	1	1		2	3	4	4		3	6	9	2			3	1	4	1	1					
Ф	3					3			2						1	3															
Х	7		2		1				3					2	5						1										
Ц	6					5			23																						1
Ч	9		1			31			8		5	1		5	1		1		1	2											
Ш	4					9			5		1			4	1																
Щ	5					12			6					1	4								2								
Ъ		2	6	2	8		2	6		1	3	10	4	3	2	5	16	5	6					1	1		3			3	
Ь																1															
Ю		1		1				3						1	1									2	1						
Я	1	4	12	1	5	1		2	5	1	6	2	5	8	3	4	3	7	23		2	3	1	1	1	1					

2-b. Digraphic kappa plain, Bulgarian language=.0069 (I.C.=6.21).

4. CZECH

The frequencies of Ď, Ó, Ř, Ť, Ů, Ý, and Ž are included respectively with those of D, O, R, T, Ú, Y, and Z. The letter W is derived from the foreign words included in Czech plain text.

1-a. Absolute frequencies of single letters of Czech plain text, arranged alphabetically, based on 62,107 letters of text.

A 4,016	D 2,466	G 219	J 1,086	Ň 26	Š 434	W 39
Á 1,525	E 4,740	H 797	K 2,143	O 5,249	T 3,288	Y 2,091
B 1,251	É 728	Ch 528	L 2,847	P 2,050	U 1,988	Z 2,078
C 964	Ě 972	I 2,917	M 2,072	R 3,101	Ú 466	
Č 576	F 121	Í 1,697	N 4,285	S 2,771	V 2,576	

1-b. Monographic kappa plain, Czech language=.0465 (I.C.=1.53).

1-c. Frequency distribution of single letters based on 62,107 letters of Czech plain text, reduced to 1,000 letters and arranged according to their frequencies.

O 85	R 50	D 40	P 33	J 17	Č 9	F 2
E 76	I 47	K 34	U 32	C 16	Ch 8	W ∅
N 69	L 46	Y 34	Í 27	Ě 16	Ú 7	Ň ∅
A 65	S 45	Z 33	Á 25	H 13	Š 7	
T 53	V 42	M 33	B 20	É 12	G 4	

1-d. Percentage of vowels, high-frequency consonants, medium-frequency consonants, and low-frequency consonants of 62,107 letters of Czech plain text. Percentage of 4 most frequent letters.

Vowels O, E, A, I, Y, U, Í, Á, Ě, É, and Ú=42.5%

High-Frequency Consonants N, T, and R=17.2%

Medium-Frequency Consonants L, S, V, D, K, Z, M, P, B, and J=34.4%

Low-Frequency Consonants C, H, Č, Ch, Š, G, F, W, and N=5.9%

4 most frequent letters (in descending order of frequency) O, E, N, and A=29.5%

1-e. Absolute frequencies of single letters as initial letters of 11,696 words in Czech plain text, arranged according to their frequencies. (One-letter words have been omitted.)

P 1,354	B 614	O 446	Č 143	I 44	W 16
S 1,056	D 603	A 401	L 130	Ch 40	Z 3
N 948	M 572	R 349	C 106	G 33	Y 3
Z 908	J 490	U 181	Ú 87	Š 32	Ě 1
V 780	K 460	H 158	F 71	E 27	Í 1
T 630					

2-a. Frequency distribution of digraphs based on 62,107 letters of Czech plain text, reduced to 5,000 digraphs.

	A	Á	B	Č	D	E	É	Ě	F	G	H	Ch	I	Í	J	K	L	M	N	Ň	O	P	R	S	Š	T	U	Ú	V	W	Y	Z
A	5	15	8	5	24			1	2	5	1		14	25	31	19	36		5	14	14	19	2	26	4	1	28	1	1	17		
Á	1	3	3	1	13					2	1		2	5	9	5	20		3	9	10	3	10			16				7		
B	4			1		6		3				4	1			3	3		10		8	1			11				44			
Č	2		1			23				15	6		17			2	5	1					1		2	1						
Č	5	2				12				6	4		1	1		10								3	1	1						
D	16	9	1	1	1	123	1	10		1	9	4	1	3	9	3	28		33	4	8	4		1	6	5	4		12	1		
E	6	15	9	8	35			1	1	5	7	1	14	16	25	27	67		6	15	32	29		2	17	2	1	16	1	23		
É	2		2			2		1		8			1	2		8	3		2	6	2	6		4		1	3			6		
Ě	2		1	4	3					1	2		5	4	9	6	9		2	3	5	7		8			3			3		
F	1					1						2							3	2												
G	2	1				2				1			4						2	4					1							
H	5	2				3	1						12		1	29		6							2					2		
Ch	2	1	1	1	2				1	1		1	1	3	2	4		4	3	1	3		3	1	2	3				2		
I	7	1	5	20	9	9	6		1	1	2	3	3	1	5	14	24	8	29		5	11	4	19	2	24	2	1	14	10		
Í	5		3	7	2	6				4	6		3	8	3	15	8		4	12	7	12	1	7	1	1	9			13		
J	9	1				138						11	11		1	3	3		1	1		3	2		1	1						
K	15	7	2	1		9	4	15				1	1	1	8	2	3		33	2	9	2		17	12	3	4		20	2		
L	30	13	2	1		332	5		1	34	5	2	7	2	2	11		29	3	1	6	2	3	9	2	4		12	7			
M	15	7	3	2	1	2	17	1	12			14	8	1	3	5	3	7	21	6	3	3		3	17	2	2		4	6		
N	44	24	1	5	1	4	37	13	25	1	8	1	26	56	1	3	1	4	30	2	1	8	1	8	9	2	1		25	2		
Ň																																
O	5	23	8	6	44			1	1	13	2		16	13	22	23	24	1	5	21	23	38	2	23	36	1	47			28		
P	10	2		1		4	3					4	1		5				57	1	65	2	1	1	3	2						
R	36	16	1	1	1	3	39	5		1	3	1	24	12		2	1	4	5	51	1		5	1	3	15	5	4		9	3	
S	5	2				130				2	2	12	3	1	24	14	6	6	13	13	1	2		68	5	1	9		2	1		
Š	3					11						3	8		1	2	1							5								
T	32	9	1	1	1	130	8	9				38	9	1	3	2	1	12	44	3	22	4	2	1	12	1	8		9	1		
U	6		5	1	5	18				2	6	1		9	6	4	6	11	3	16	5	15	3	11	1		13			14		
Ú	2		1		1	1							1	1	2	6	2		1	3	3	3		1		3				4		
V	20	12	1	1	2	2	23	9	15			1	1	1	6	1	4	5	2	11	17	4	10	3	7	3	4	3		27	5	
W	1											1																				
Y	5	11	1	2	6	1				3	16	1	4	6	23	12	9		5	10	4	14	3	13	2		9			10		
Z	23	15	4	1	1	10	39			2	12	3	2	4	2	3	15		4	8	2	4	1	3	3	1	4			1	1	

2-b. Digraphic kappa plain, Czech language=.0042 (I.C.=4.57).

## 5. DANISH

NOTE: The letters W, X, and Z are derived from foreign words in Danish plain text.

1-a. Absolute frequencies of single letters of Danish plain text, arranged alphabetically, based on 56,176 letters of text.

A	4,434	G	2,358	M	1,755	S	3,452	X	1
B	747	H	807	N	4,370	T	4,098	Y	370
C	87	I	3,479	O	2,341	U	899	Z	8
D	3,906	J	339	P	624	V	1,379	Æ	472
E	9,021	K	1,727	R	4,739	W	13	Ø	511
F	1,459	L	2,780						

1-b. Monographic kappa plain, Danish language=.0730 (I.C.=1.97).

1-c. Frequency distribution of single letters based on 56,176 letters of Danish plain text reduced to 1,000 letters, and arranged according to their frequencies.

E	161	I	62	K	31	B	13	J	6
R	84	S	61	F	26	P	11	C	2
A	79	L	49	V	25	Ø	9	W	0
N	78	G	42	U	16	Æ	8	Z	0
T	73	O	42	H	14	Y	7	X	0
D	70	M	31						

1-d. Percentage of vowels, high-frequency consonants, medium-frequency consonants, and low-frequency consonants in 56,176 letters of Danish plain text. Percentage of 8 most frequent letters in Danish plain text.

Vowels A, E, I, O, U, Y, Æ, and Ø=38.3%

High-Frequency Consonants D, N, R, S, and T=36.6%

Medium-Frequency Consonants F, G, K, L, M, and V=20.4%

Low-Frequency Consonants B, C, H, J, P, W, X and Z=4.7%

8 most frequent letters (in descending order of frequency) E, R, A, N, T, D, I, and S=66.8%

1-e. Absolute frequencies of single letters as initial letters of 10,749 words in Danish plain text, arranged according to their frequencies. (One-letter words have been omitted.)

D	1,205	O	613	B	384	N	236	C	20
S	1,054	H	578	I	373	L	234	Y	11
A	881	T	543	P	310	R	186	W	8
F	822	V	493	G	269	J	74	Æ	8
E	713	K	407	U	247	Ø	51	Z	1
M	644								

2-a. Frequency distribution of digraphs based on 56,176 letters of Danish plain text, reduced to 5,000 digraphs.

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	R	S	T	U	V	W	X	Y	Z	Æ	ø
A	57	7		19	5	28	24	2	2	1	4	35	12	73	2	2	46	8	56	3	11						
B	5				26				3			10			5		6	1	1	2				3	1	2	
C					4			1	2																		
D	24	4		11	194	5	4	3	16		3	8	3	5	8	4	10	19	14	3	6			1	1	2	
E	18	11	1	66	13	24	17	12	15	12	16	49	32	142	12	91	75	57	97	7	18						2
F	8	1		4	7	5	2	2	7	1	1	5			47	1	12	3	11	2	1					3	8
G	18	3		9	68	4	5	7	11	2	2	2	5	5	7	3	8	21	19	2	3			1	1	5	
H	26				16				2	3					6		1				3	10				1	3
I	5	2	1	24	8	6	52	3	1		20	45	6	63	10	1	4	34	11	1	13						1
J	1			3	12							1			5		1	2	1	1				1	1		
K	21			1	44	1		1	3	1	16	4		3	15	1	11	7	7	12	1			1	1	3	
L	26	3		21	48	4	5	2	43	1	6	23	3	1	6	2	1	19	9	4	6			6	4	5	
M	28	2		4	44	3	1	3	19		1	2	15	1	8	3	1	5	4	5	1			1	2	3	
N	21	5	2	85	50	10	41	9	26	1	8	5	9	12	14	3	3	39	22	9	7			4	4	3	
O		2	1	9	1	3	34				2	11	32	18		9	68	3	2	1	11						
P	18				7	1	2	1	2			3			4	2	9	1	1	2							1
R	33	12		35	96	12	9	14	40	3	16	8	15	19	16	4	6	29	21	12	12			3	6	2	
S	29	3	1	6	39	6	1	3	24	1	45	10	10	3	18	9	2	15	62	3	7			3	3	5	
T	40	6		14	74	12	4	8	64	1	4	6	9	8	19	3	17	24	19	8	9			8	3	3	
U	2	1		18	2	1	2	1	1		2	11	1	20		1	6	5	3		1						
V	17			3	45	1			28			1		4	7		1	2	1	1						11	
W					1																						
X																											
Y		1		6	1		3				3	2		3			1	8	2		2						
Z																											
Æ				2		1	3				2	5		5		1	17	3	2		1						
ø		4		6			2			4	1	2	1	5			17	2			1						

2-b. Digraphic  $kappa$  plain, Danish language = .0094 (I.C. = 6.85).

### 6. DUTCH

1-a. Absolute frequencies of single letters of Dutch plain text, arranged alphabetically, based on 59,993 letters of text.

A	4,520	G	2,311	L	2,373	Q	77	V	1,663
B	955	H	1,046	M	1,299	R	4,159	W	844
C	892	I	4,077	N	6,039	S	2,541	X	9
D	3,154	J	482	O	3,738	T	3,850	Y	390
E	10,562	K	1,380	P	1,074	U	1,186	Z	813
F	599								

1-b. Monographic kappa plain, Dutch language=.0758 (I.C.=1.97).

1-c. Frequency distribution of single letters based on 59,993 letters of Dutch plain text reduced to 1,000 letters, and arranged according to their frequencies.

E	176	I	68	S	42	K	23	H	17	Z	14	Q	1
N	101	T	64	L	40	M	22	B	16	F	9	X	-
A	75	O	62	G	39	U	20	C	15	J	8		
R	69	D	53	V	28	P	18	W	14	Y	6		

1-d. Percentage of vowels, high-frequency consonants, medium-frequency consonants, and low-frequency consonants in 59,993 letters of Dutch plain text. Percentage of 8 most frequent letters in Dutch plain text.

- Vowels E, A, I, O, U, and Y=40.8%
- High-Frequency Consonants N, R, and T=23.4%
- Medium-Frequency Consonants D, S, L, G, V, K, M, P, and H=28.1%
- Low-Frequency Consonants B, C, W, Z, F, J, Q, and X=7.7%
- 8 most frequent letters (in descending order of frequency) E, N, A, R, I, T, O, and D=67.3%

1-e. Absolute frequencies of single letters as initial letters of 9,520 words in Dutch plain text, arranged according to their frequencies. (One-letter words have been omitted).

V	1,017	B	568	G	498	Z	406	P	248	L	158
D	739	S	515	E	481	H	376	C	205	F	83
A	708	T	512	M	440	N	371	U	169	J	38
O	571	I	511	W	436	R	251	K	168	Q	38

2-a. Frequency distribution of digraphs based on 59,993 letters in Dutch plain text, reduced to 5,000 digraphs.

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	83	3	11	10	1	8	15		3		13	34	12	90		4		40	8	34	3	4	1		1	1
B	9	2			37				9			6			4			6		1	1					3
C	2		2		3			31	4		1	1			17			2		7	3					
D	31	3	1	6	11		3	3	28		1	1	2	2	20	3		10	13	6	6	5	4			4
E	11	13	13	43	55	11	32	9	30	1	24	74	17	218	9	18	1	160	39	41	9	29	11	1		18
F	2			3	9	3	1	1	5					1	3			2	2	7		2	1			1
G	13	3	1	8	91		4	3	8		1	1	4	3	8	1		11	7	11	4	6	2			2
H	19				27				10					1	10			2		13	2					1
I	5		8	17	71	2	21			35	11	11	5	96	3	2	1	2	23	26		1				1
J	2			5	3	2	1				10	1		3	2				1		2	1	1			2
K	12	2		2	34		3	4	7		6	3	1	1	13	1		3	6	8	2	3	2			2
L	24	2	1	12	36	2	8	1	37		5	14	2	1	10	1		1	11	6	6	4	2		9	1
M	14	2	1	3	36		1		15				10		12	2			4	2	2	1				3
N	26	16	7	84	42	5	64	9	31	1	11	6	9	13	27	6	3	4	39	40	7	26	14			15
O	2	1	4	8	34	5	12		1		5	11	22	41	43	32		51	5	14	9	12	1			
P	9	2		2	12		2	3	4		1	3	1	1	9	3		16	2	3	8	5	2			1
Q																						6				
R	30	12	2	37	61	1	10	9	40		10	9	8	8	23	2		3	17	21	9	14	8		3	10
S	7	4	15	7	20	1	4	4	16	1	1	9	4	3	5	11		2	13	68	5	9	3		1	2
T	24	7	2	8	88	1	10	8	42		2	2	6	4	36	2		18	14	10	9	12	12		1	6
U	3	6	5	5	2		2		18		3	8	3	14	4			8	7	3	1	1	5			
V	26				60				8		3			33				6								3
W	17				28				9						11											4
Y				2	1	4	1	1			9	1	1	5					1	1		2				2
Z	9				22				17						11							4	2		3	

2-b. Digraphic kappa plain, Dutch language=.0094 (I.C.=6.35).



7. FINNISH

NOTE: The letters Q, W, X, and Z are derived from foreign words in Finnish plain text.

1-a. Absolute frequencies of single letters of Finnish plain text, arranged alphabetically, based on 62,261 letters of text.

A	7,367	L	3,442	S	5,241	Ö	360	G	71
E	5,232	M	2,240	T	6,603	B	44	Q	1
H	1,113	N	5,333	U	2,953	C	21	W	10
I	6,508	O	3,482	V	1,544	D	703	X	3
J	1,172	P	908	Y	1,705	F	55	Z	2
K	2,830	R	1,231	Ä	2,717				

1-b. Monographic kappa plain, Finnish language=.0737 (I.C.=2.11).

1-c. Frequency distribution of single letters based on 62,261 letters of Finnish plain text, reduced to 1,000 letters and arranged according to their frequencies.

A	118	O	56	V	25	D	11	C	0
T	106	L	55	R	20	Ö	6	W	0
I	105	U	47	J	19	G	1	X	0
N	86	K	45	H	18	F	1	Z	0
S	84	Ä	44	Y	17	B	1	Q	0
E	84	M	36	P	15				

1-d. Percentage of vowels, high-frequency consonants, medium-frequency consonants, and low-frequency consonants in 62,261 letters of Finnish plain text. Percentage of 6 most frequent letters in Finnish plain text.

Vowels A, E, I, O, U, 1, 2, and Y=47.7%

High-Frequency Consonants N, S, and T=27.6%

Medium-Frequency Consonants D, H, J, K, L, M, P, R, and V=24.4%

Low-Frequency Consonants B, C, F, G, Q, W, X, and Z=0.3%

6 most frequent letters (in descending order of frequency) A, T, I, N, S, and E=58.2%

1-e. Absolute frequencies of single letters as initial letters of 7,836 words in Finnish plain text, arranged according to their frequencies.

S	938	V	608	L	326	U	97	G	12
T	820	M	568	A	313	I	83	Ä	11
K	754	E	546	N	293	B	32	C	4
J	654	P	459	Y	153	D	28	W	4
O	613	H	329	R	132	F	28		

2-a. Frequency distribution of digraphs based on 62,261 letters of Finnish plain text, reduced to 5,000 digraphs.

	A	E	H	I	J	K	L	M	N	O	P	R	S	T	U	V	Y	Ä	Ö	B	C	D	F	G	Q	X	Z	
A	76	15	13	51	26	32	48	33	97	13	16	21	50	53	15	25	4			1		3	1	1				
E	5	34	14	30	4	13	39	18	113	5	3	20	38	52	12	10	2	1				8	1					
H	14	13		6	2	1		1	1	5				19	7		3	4	1			11						
I	22	24	7	40	7	31	32	28	80	11	5	10	114	72	1	18	1	4	1		1	13						
J	44	9		2						26					2			10										
K	47	24		27		13	1		1	32		4	35		23		6	12	1									
L	36	37	1	55	4	9	60	7		12	1		1	14	16	4	3	16	3									
M	40	26		41				20		9	3		1		18		7	14										
N	30	49	12	22	19	37	12	16	31	26	18	4	42	50	11	19	9	13	1	1		2	1	3				
O	4	1	10	42	6	17	42	20	43	5	9	6	28	20	8	8						7	1					
P	16	5		15						10	2	1	1		11		2	10										
R	21	7	2	22	8	7	1	2	1	4	1	3	1	5	4	6	1	4							1			
S	51	68	1	69	3	13	2	2	1	17	2		36	101	25	3	8	17										
T	118	60	2	43	5	10	2	4	2	46	3	2	11	79	47	3	23	61	9									
U	2	4	10	8	3	21	14	6	23	28	4	13	28	30	26	8							8					
V	53	6		20						15					6		1	22										
Y		1	9	3		9	4	7	4		1	2	11	12		4	6	1	12			3						
Ä	4	8	8	15	6	13	15	16	28	8	4	10	19	18	1	13	8	26										
Ö			1	2	1	2	3	2	4	1			5	4		2	1	1	1									
B	1	2								1																		
C			1																									
D	6	27		7						7					5		1	2										
F	1	1		2						1		1																
G	1	1		1			1					1																
Q																												
X																												
Z																												

2-b. Digraphic kappa plain, Finnish language = .0082 (I.C. = 6.44).

## 8. FRENCH

1-a. Absolute frequencies of single letters of French plain text, arranged alphabetically, based on 55,758 letters of text.

A	4,480	G	624	L	2,737	Q	616	V	801
B	406	H	276	M	1,617	R	4,117	W	6
C	1,944	I	4,230	N	4,406	S	4,564	X	317
D	2,198	J	184	O	3,255	T	4,057	Y	100
E	9,334	K	25	P	1,689	U	3,045	Z	84
F	646								

1-b. Monographic kappa plain, French language = .0777 (I.C. = 2.02).

1-c. Frequency distribution of single letters based on 55,758 letters in French plain text reduced to 1,000 letters, and arranged according to their frequencies.

E	167	T	73	C	35	G	11	J	3
S	82	O	58	P	30	Q	11	Y	2
A	80	U	55	M	29	B	7	Z	2
N	79	L	49	V	14	X	6	K	1
I	76	D	39	F	12	H	5	W	∅
R	74								

1-d. Percentage of vowels, high-frequency consonants, medium-frequency consonants, and low-frequency consonants in 55,758 letters of French plain text. Percentage of 8 most frequent letters in French plain text.

Vowels A, E, I, O, U, and Y = 43.8%

High-Frequency Consonants N, R, S, and T = 30.7%

Medium-Frequency Consonants C, D, L, M, and P = 18.3%

Low-Frequency Consonants B, F, G, H, J, K, Q, V, W, X, and Z = 7.2%

8 most frequent letters (in decending order of frequency) E, S, A, N, I, R, T, and O = 68.9%

1-e. Absolute frequencies of single letters as initial letters of 10,748 words in French plain text, arranged according to their frequencies. (One-letter words have been omitted).

D	1,445	L	784	I	315	U	250	H	67
P	929	S	664	F	313	O	177	Z	7
E	894	Q	394	T	305	G	146	K	5
A	866	R	389	N	278	B	115	W	3
C	816	M	337	V	263	J	98	Y	3

2-a. Frequency distribution of digraphs based on 55,758 letters of French plain text, reduced to 5,000 digraphs.

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	2	6	20	12	4	6	11		50	1		36	12	68	1	21	3	41	17	46	29	13			2	1
B	4			4				4			12			4			5	2	1	2						
C	15		6	47			11	20			5			48			4	1	8	8						
D	18			1	109			1	20	1		1	10	1		6	2		26							
E	30	4	49	48	30	15	14	3	13	5		56	58	105	4	38	12	89	154	58	27	17		8	3	
F	10		2	1	9	6		8			1			8	1		10	1		1						
G	6			16		1	2				3	1	7	6			8		4	2						
H	6			6				4						3			1			4						
I	9	3	12	10	41	4	4		1		27	8	49	51	5	12	27	52	47		9		7	1		
J	4			6											5						2					
K															1											
L	57		1	5	95	1		1	23			26		3	10	1			5	4	12				1	
M	22	9	1	1	52			23				13		8	9			1		4						
N	19	1	29	40	54	9	11	1	20	1		3	2	10	19	6	4	3	53	99	4	7				1
O		5	7	3	1	1	2	1	21	1		10	21	109		7		27	13	8	52	2			2	
P	30		1	1	13			2	3			11		35	9		34	1	6	4						
Q			1																		54					
R	62	2	10	13	127	2	6		24	1		16	11	8	27	5	3	7	14	19	6	7				1
S	42	2	16	32	75	5	2	1	36	2		15	8	6	22	24	11	8	41	33	24	4				1
T	40	1	7	22	78	4	1	2	67	1		12	4	4	14	11	7	44	23	10	11	2				
U	12	3	10	5	39	4	3	1	24	3		13	6	26	1	8	1	48	26	19	1	8		13	1	
V	9			24				16						16			5			2						
W																										
X	4		3	3	3			1	1			1	1		4	1	1	2	3	1						
Y	2				2										1				2							
Z				3				1							1											

2-b. Digraphic kappa plain, French language =.0093 (I.C. =6.29).

9. GERMAN

1-a. Absolute frequencies of single letters of German plain text, arranged alphabetically, based on 60,046 letters of text. (The letters X and Y are derived from foreign words contained in German plain text.)

A	3,601	G	1,921	L	1,988	Q	6	V	523
B	1,023	H	2,477	M	1,360	R	4,339	W	899
C	1,620	I	4,879	N	6,336	S	4,127	X	12
D	3,248	J	192	O	1,635	T	3,447	Y	24
E	10,778	K	747	P	499	U	2,753	Z	654
F	958								

1-b. Monographic kappa plain, German language = .0787 (I.C. = 2.05).

1-c. Frequency distribution of single letters based on 60,046 letters of German plain text, reduced to 1,000 letters, arranged according to their frequencies.

E	180	T	57	G	32	F	16	P	8
N	106	D	54	O	27	W	15	J	3
I	81	U	46	C	27	K	13	Y	∅
R	72	H	41	M	23	Z	11	X	∅
S	69	L	33	B	17	V	9	Q	∅
A	60								

1-d. Percentage of vowels, high-frequency consonants, medium-frequency consonants, and low-frequency consonants in 60,046 letters of German plain text. Percentage of 8 most frequent letters in German text.

Vowels A, E, I, O, U, and Y = 39.4%

High-Frequency Consonants D, N, R, S, and T = 35.8%

Medium-Frequency Consonants B, C, F, G, H, L, M, and W = 20.4%

Low-Frequency Consonants J, K, P, Q, V, X, and Z = 4.4%

8 most frequent letters (in descending order of frequency) E, N, I, R, S, A, T, and D = 67.9%

1-e. Absolute frequencies of single letters as initial letters of 9,568 words in German plain text, arranged according to their frequencies. (One-letter words have been omitted.)

D	1,716	U	550	Z	343	K	263	O	135
A	762	W	544	M	339	P	181	T	106
S	698	G	461	N	306	R	167	C	22
E	686	B	460	F	280	L	158	Q	2
I	581	V	408	H	265	J	135		

2-a. Frequency distribution of digraphs based on 60,046 letters in German plain text, reduced to 5,000 digraphs.

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	4	14	10	4	33	7	9	7	1	1	2	33	13	48		2		22	27	23	36	1	1			1
B	6				48		1	1	5			3			3			11	2	1	3		1			1
C								130			5															
D	29	2		8	127	1	2	2	60		1	3	2	2	4	1		5	8	2	9	2	2			2
E	13	22	10	31	13	12	32	24	90	2	6	28	25	235	3	6		195	68	28	24	9	15			7
F	7	1		3	15	7	2		2			2	1	1	3			10	2	10	12					
G	10	1		8	78	1	2	2	8		2	7	1	3	1			11	8	7	8	2	1			1
H	29	1		8	64	1	2	1	14		2	8	3	6	6	1		20	4	23	7	2	3			1
I	3	1	39	7	91	2	18	7	2		7	12	11	84	13	1		7	73	44	1	2	1			1
J	4				8																	3				
K	12	1		1	11		1	1	1			5			9			10	1	5	4					
L	26	3	1	6	27	1	2		37		3	20	1	2	4				10	12	6	1				1
M	16	3		4	26	2	2	1	14	1	2	1	11	1	8	5		1	3	3	9	1	1			1
N	39	12	1	118	58	9	57	8	35	4	10	6	10	18	8	5		4	36	27	20	10	17			14
O	1	3	5	3	11	3	3	3			1	18	6	33	1	5		18	12	4	1	1	5			1
P	10				5	4		1	2			1			7	2		7		1	1					
Q																					1					
R	34	11	5	35	60	9	12	9	37	2	11	6	8	12	19	3		6	22	18	26	6	8			5
S	14	6	55	13	46	3	7	3	30	1	5	4	7	3	16	6		2	40	57	9	5	5		1	5
T	25	3		17	88	2	4	6	40	1	3	7	3	4	4			14	20	7	16	2	10			13
U	1	2	8	2	37	15	5	1			2	2	11	76		2		18	28	14	1	1	2			1
V	1				19				3						21											
W	16				24				20	3					6						6					
X																										
Y																										
Z	1			1	8				5			1			2						4	27		4		

2-b. Digraphic kappa plain, German language = .0111 (I.C. =7.50).

## 10. GREEK

1-a. Absolute frequencies of single letters of Greek plain text, arranged alphabetically, based on 65,936 letters of text.

A	7,242	H	3,440	N	5,668	T	5,096
B	529	Θ	807	Ξ	277	Υ	2,871
Γ	915	I	6,176	O	6,263	Φ	481
Δ	1,256	K	2,494	Π	2,337	X	659
E	5,348	λ	1,842	P	2,705	Ψ	112
Z	213	M	1,961	Σ	5,232	Ω	2,012

1-b. Monographic kappa plain, Greek language = .0689 (I.C. = 1.65).

1-c. Frequency distribution of single letters based on 65,936 letters of Greek plain text reduced to 1,000 letters, and arranged according to their frequencies.

A	110	E	81	Υ	44	Ω	31	Γ	14	Φ	7
O	95	Σ	79	P	41	M	30	Θ	12	Ξ	4
I	94	T	77	K	38	λ	28	X	10	Z	3
N	86	H	52	Π	35	Δ	19	B	8	Ψ	2

1-d. Percentage of vowels, high-frequency consonants, medium-frequency consonants, and low-frequency consonants in 65,936 letters of Greek plain text. Percentage of 7 most frequent letters in Greek plain text.

Vowels A, O, I, E, H, T, and Ω = 50.6%

High-Frequency Consonants N, Σ, and T = 24.3%

Medium-Frequency Consonants P, K, Π, M, λ, and Δ = 19.1%

Low-Frequency Consonants Γ, Θ, X, B, Φ, Ξ, Z, and Ψ = 6.0%

7 most frequent letters (in descending order of frequency) A, O, I, N, E, Σ, and T = 62.2%

1-e. Absolute frequencies of single letters as initial letters of 11,850 words in Greek plain text, arranged according to their frequencies. (One-letter words have been omitted.)

T	2,359	Π	883	Σ	538	Γ	171	λ	108	P	60
E	1,696	Δ	730	N	370	B	156	I	95	Z	51
A	1,152	O	681	Θ	220	X	137	Φ	76	Ψ	23
K	896	M	548	Υ	193	H	129	Ω	70	Ξ	21

2-a. Frequency distribution of digraphs based on 65,936 letters of Greek plain text, reduced to 5,000 digraphs.

	A	B	Γ	Δ	E	Z	H	Θ	I	K	λ	M	N	Ξ	O	Π	P	Σ	T	Τ	Φ	X	Ψ	Ω
A	11	6	17	15	17	4	3	11	75	19	28	19	77	5	7	34	26	73	71	14	10	5	1	1
B	11				8		2		5		2				6		3			1				1
Γ	13		4		9		3		9	8	4	3	2		8		3			1		1		3
Δ	5				15		11		41						8		7			6				2
E	6	3	9	10	2	1	1	6	85	17	22	9	49	10	3	25	48	22	30	15	4	10	2	15
Z	2				4		4		1						3									1
H	6	1	4	4	9	1	4	6	1	8	6	21	61	1	4	6	10	77	20	1	4	2	1	1
Θ	15				16		13		1		1	1	3		4		2			3				1
I	86	4	4	15	20	4	8	4	1	69	7	8	45	2	43	14	7	68	36	2	2	4	1	13
K	70	1		1	12		21	1	3	2	4	2	1		35	1	11	1	8	8				10
λ	22			1	18		21	1	19	1	21	1			21	1			1	3	1			10
M	31	4			47		8		15			6	1		25	7				1	2			3
N	77	3	2	21	61	1	26	6	22	18	2	10	8	1	46	18	1	13	68	4	1	3	1	17
Ξ	4				5		2		4						2					2				2
O	4	8	8	8	9	1	3	3	39	10	22	25	68	1	4	28	15	52	33	120	6	4	2	1
Π	22				24		5		18		8		1		63		27		3	1				5
P	38	1	13	1	15		7	1	41	2		2	6		51		2		4	4	1	4		12
Σ	33	4	2	13	59	1	19	8	33	25	3	20	3		25	17	1	13	77	23	4	9		6
T	74				28	1	86		43			1			95		15	2	1	4				37
Τ	6	6	4	6	11	1	2	6	2	9	9	15	35	1	8	23	11	31	25	1	1	4	1	1
Φ	7				4		3	2	4		1				7		2			1				4
X	7				10		4	3	4				1		5		3			1				8
Ψ	1				2		3		2											1				
Ω	1		1	1	1		1	2		1	1	7	70		1	4	11	44	8		1	1		

2-b. Digraphic kappa plain, Greek language=.0080 (I.C.=4.61).



## 11. HUNGARIAN

1-a. Absolute frequencies of single letters of Hungarian plain text, arranged alphabetically, based on 50,787 letters of text.

A 4,579	E 5,414	I 2,427	M 1,738	Ö 417	T 4,277	V 1,082
Á 2,016	É 1,837	Í 229	N 2,626	P 489	Ty 3	W 13
B 937	F 391	J 667	Ny 309	Q 11	U 521	Y 15
C 198	G 1,261	K 2,557	O 2,178	R 2,261	Ú 111	Z 1,271
Cs 223	Gy 692	L 3,158	Ó 447	S 2,049	Û 394	Zs 22
D 1,057	H 889	Ly 220	Ö 503	Sz 1,056	Ü 62	

1-b. Monographic kappa plain, Hungarian language = .0523 (I.C. = 2.14).

1-c. Frequency distribution of single letters based on 50,787 letters of Hungarian plain text; reduced to 1,000 letters and arranged according to their frequencies.

E 107	I 48	M 34	B 18	P 10	Í 5	Zs 0
A 94	R 45	Z 25	H 18	Ó 9	Cs 4	Y 0
T 84	O 43	G 25	Gy 14	Ö 8	Ly 4	W 0
L 62	S 40	V 21	J 13	Û 8	C 4	Q 0
N 52	Á 40	D 21	U 10	F 8	Ú 2	Ty 0
K 50	É 36	Sz 21	Ö 10	Ny 6	Ü 1	

1-d. Percentage of vowels, high-frequency consonants, medium-frequency consonants, and low-frequency consonants in 50,787 letters of Hungarian plain text. Percentage of 11 most frequent letters in Hungarian plain text.

Vowels E, A, I, O, X, É, U, Ö, Ó, Ő, Ü, Í, Ú, Ű, and Y = 42.0%

High-Frequency Consonants T, L, N, and K = 24.8%

Medium-Frequency Consonants R, S, M, Z, G, V, D, Sz, B, H, Gy, and J = 29.5%

Low-Frequency Consonants P, F, Ny, Cs, Ly, C, Zs, W, Q, Ty = 3.7%

11 most frequent letters (in descending order of frequency) E, A, T, L, N, K, I, R, O, S, and Á = 66.4%

1-e. Absolute frequencies of single letters as initial letters of 8,130 words of Hungarian plain text, arranged according to their frequencies. (One-letter words have been omitted.)

M 724	É 329	L 215	Cs 132	C 48	Z 13
K 665	N 301	P 188	Á 100	G 39	Ó 13
A 636	Sz 298	R 169	O 66	Gy 34	Ó 11
E 513	F 275	J 152	U 61	Ö 32	Q 11
H 507	B 253	D 148	Ú 52	Ny 30	W 7
T 469	I 250	S 134	Û 50	Í 15	Y 2
V 372					

2-a. Frequency distribution of digraphs based on 50,787 letters of Hungarian plain text, reduced to 5,000 digraphs.

	A	Á	B	C	C _s	D	E	É	F	G	G _y	H	I	Í	J	K	L	L _y	M	N	N _y	O	Ó	Ö	Ő	P	Q	R	S	S _s	T	T _y	U	Ú	Ű	Ű	V	W	Y	Z	Z _s
A	12	112	1	5	17	5	3	5	6	22	10	16	10	42	46	32	48	2	1				16	34	11	14	51	2									11		35		
Á	1	8	5	1	1	1	1	23		1	1	3	18	19	2	6	18	10								25	25	1	19								6		3		
B	21	2	12			24	4			1	1	1	1	1												3	2	1				1	1			2	1	1			
C						1	1			2	1				1																										
C _s	4	1				1	1					1																													
D	7	5	1			1	27	12	1		2	7	3	3	1		2	3							9	2	4	2				1	1	1	4	3	1	1			
E	9	1	4	1	1	12	4	2	3	34	14	19	7		6	38	76	10	38	5	1	1				4	45	22	14	70			2	1			7	1	28		
É	1		4			3	1	19	1	1					9	14	2	3	9	1								8	23	48	6	13						3		3	
F	1	1				15	2					2													9	1	3										1				
G	17	11	3		1	1	16	6	2	2	1	3	7		2	4	3		4	5			13	1	1	1		4	1	2	5		2	1	1	3			1		
G _y	28		1			10	2			2	2				2	1	3	2				1	1	2	1		1	1	2	1		1	1	1	1	1					
H	24	4				15	1					6	2											25										9			2				
I	19	5	4	1	1	7	9	5	3	8	2	5	3		3	24	8	2	7	30			1	6	1	2		8	25	10	20		1	1	1	6		11	1		
Í						1	1			1	1																														
J	14	11				2	11	2							2	2										4	2	1								1		5	6	1	
K	35	5	5	1	1	2	39	18	3	1		5	24	1	2	13	3		10	4	1	26	1	17	1	2		8	3	3	6		2	1	7	4					
L	40	17	4		2	7	60	15	4	4		5	12	2	6	12	21		1	1	9		17	7	2	10	1	2	4	3	20		2	3	8						
L _y	2	1	1			7	1					1														1	1	2													2
M	32	16	4		1	4	11	1			1	2	1	1	1	3			3	1			1	1	2		1	1	4		6	1	1	1	2				4		
N	38	4	4	4	2	2	40	13	4	7	1	3	24	1	1	16	3		4	9	2	3		3	1	1		1	4	3	29		2	1	1	1	3			1	
N _y	2	1	1			5	1					1	3	1									1	1	1	3		1	1	3		1								3	
O	1	2	1	1	3			9	17	1					19	26	3	9	23	3							1	26	13	4	23						15		14	1	
Ó	1	2			2	1	1	1	1	1		1	2		2	3	10		1	2						2		1	3	1	5						2		1		
Ö		2			1			1							4	4			1	4								8	3	1	6					6		8			
Ő	1	1			4	1	1		1	1		1	4	6		1	1											2	4	1	3						2		3		
P	4	5			1	7	2					2	3	2	1								1	1	1		1	4									1	1	2		
Q																																									
R	22	13	2	2	1	10	31	6	1	1	2	2	20		3	6	2		10	3		14	5	2	6	1		4	4	9	20		1	1	7	1	9		1	1	
S	19	23	5		1	1	23	22	4	1		6	6	5	2	6	5		9	4		9	1	1	3	3	1	4	8	8	14		3	1	4		2				
S _s	8	14				19	4			1	4	1			2	14			1			7	3	1	1	1		1		15		1	3		1						
T	63	26	7	1	2	1	67	25	5	1	1	11	25		9	13	7		12	9		20	7	9	6	2		8	11	6	44		8	1	3	1	8				
T _y																																									
U	1					3			3	1					1	4	7		2	7		1						3	7	1	9										
Ú									1						3	1	2	1																							
Ű									1	4					4	2													1												1
Ű															1	1													1												
V	24	23				21	12					1	13		2																										
W	1																																								
Y															1																										
Z	17	7	1			3	23	8		1		1	7		2	2			3	3		14	4	3	3		1	1	14		2	1	1		1				3		
Z _s										1																															

2-b. Digraphic kappa plain, Hungarian language = .0043 (I.C. = 7.23).

## 12. INDONESIAN

NOTE: C and V are exclusively found in words of Dutch or English origin. F is used almost interchangeably with P, usually in words of Arabic origin. Q and X are used exclusively in words of occidental origin. Y is sometimes, though rarely, used for I or J. In the present text, however, it appears only in words of English origin. 2 is the sign of reduplication, either of the whole word or its root. W is used mostly in words of Arabic or Japanese origin, though it is sometimes used for consonantal U.

1-a. *Absolute frequencies of single letters of Indonesian plain text, arranged alphabetically, based on 56,653 letters of text.*

A	10,828	F	83	K	3,166	P	1,794	U	2,459	2	331
B	1,383	G	1,994	L	1,740	Q	6	V	40		
C	94	H	1,332	M	2,385	R	2,750	W	254		
D	3,082	I	4,073	N	5,670	S	2,085	Y	11		
E	4,968	J	1,542	O	1,277	T	3,299	Z	7		

1-b. *Monographic kappa plain, Indonesian language = .0833 (I.C. = 2.17).*

1-c. *Frequency distribution of single letters based on 56,653 letters of Indonesian plain text, reduced to 1,000 letters and arranged according to their frequencies.*

A	191	K	56	S	37	B	25	C	2	Q	∅
N	100	D	54	G	35	H	24	F	1		
E	88	R	49	P	32	O	23	V	∅		
I	72	U	43	L	31	2	6	Y	∅		
T	58	M	42	J	27	W	4	Z	∅		

1-d. *Percentage of vowels, high-frequency consonants, medium frequency consonants, and low-frequency consonants in 56,653 letters of Indonesian plain text. Percentage of 4 most frequent letters in Indonesian plain text.*

Vowels A, E, I, U, O and Y = 41.7%

High-Frequency Consonants N, T, K and D = 26.9%

Medium-Frequency Consonants R, M, S, G, P, L, J, B and H = 30.0%

Low-Frequency Consonants 2, W, C, F, V, Z and Q = 1.4%

4 most frequent letters (in descending order of frequency) A, N, E, and I = 45.1%

1-e. *Absolute frequencies of single letters as initial letters of 9,209 words of Indonesian plain text, arranged according to their frequencies. (One-letter words have been omitted.)*

D	1,532	S	795	J	344	L	141	E	33
M	969	A	447	R	240	N	126	V	13
K	893	I	418	H	234	G	66	Q	5
P	893	C	393	U	190	F	47	Z	3
T	837	B	348	O	170	W	46	Y	2

2-a. Frequency distribution of digraphs based on 56,653 letters of Indonesian plain text, reduced to 5,000 digraphs.

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	Y	Z	2
A	24	18	3	67	3	2	14	57	28	13	86	41	49	270	5	47		64	51	86	16		6			6
B	43	1		1	44				9	1	1	7			3	1		1	1		10					
C							3	1		1					2											
D	108	1		1	28	1		65	38	1	3	1	2	8	1		3	1	1	10						
E	7	14	1	12	1	1	11	11	3	1	24	40	51	92	2	21		106	20	19	1	1	2			
F	1			1	1				3																	
G	59	6		11	10		10	6	12	2	11	3	8	2	3	4		3	8	7	8					4
H	38	5		7	4			1	5	3	7	2	6	2	4	6		3	4	4	5		9			2
I	38	13	1	34	3	2	2	14	5	4	40	17	16	5	7	12		15	27	45	6		2			2
J	95				7		7		7			1			5							14				
K	112	4		8	43				21	7	8	1	12	3	22	6		4	9	7	12					1
L	71	1		5	16				26	1	2	2	5	1	4	2			2	2	11					2
M	43	20		3	74	1		1	16		5	1	2	1	6	17		2	2	2	15					
N	38	16	1	68	18	1	118	5	27	42	21	3	16	8	8	19		5	16	53	9	1	1			8
O	3	2	1	3	20		2	1	1		9	17	15	19	1	2		11	2	4						
P	49	1		3	53			1	12	1	3	1	2		7	1		6	2	2	14					
Q																						1				
R	67	5		13	28		2	6	44	1	8	4	3	6	9	3		1	8	14	18	1				2
S	40	3		6	44		1	1	34	3	4	1	4	2	7	1			3	8	20					1
T	77	2		8	42		2	1	37	15	17	1	5	4	7	2		4	5	16	45					1
U	23	8		17			6	8	3	1	29	9	16	33	1	9		13	21	18			1			1
V	1								1						1											
W	20								1																	
Y																										
Z																										
2	1	2		4					2	3	2	1	1	1	3			1	2	3	1					

2-b. Digraphic kappa plain, Indonesian language=.0111 (I.C.=7.50).

## 13. ITALIAN

NOTE: In all calculations, accented letters have been combined with the corresponding unaccented letter.

1-a. Absolute frequencies of single letters of Italian plain text, arranged alphabetically, based on 57,906 letters of text.

A	6,771	G	1,168	L	3,592	Q	227	V	1,024
B	527	H	493	M	1,441	R	4,037	W	13
C	2,367	I	6,568	N	4,094	S	2,967	X	9
D	2,258	J	18	O	5,022	T	4,139	Y	14
E	6,784	K	28	P	1,616	U	1,547	Z	527
F	655								

1-b. Monographic kappa plain, Italian language = .0745 (I.C. = 1.94).

1-c. Frequency distribution of single letters based on 57,906 letters in Italian plain text, reduced to 1,000 letters and arranged according to their frequencies.

E	117	R	70	P	28	F	11	K	∅
A	117	L	62	U	27	B	9	J	∅
I	113	S	51	M	25	Z	9	Y	∅
O	87	C	41	G	20	H	9	W	∅
T	72	D	39	V	18	Q	4	X	∅
N	71								

1-d. Percentage of vowels, high-frequency consonants, medium-frequency consonants, and low-frequency consonants in 57,906 letters of Italian plain text. Percentage of 8 most frequent letters in Italian plain text.

Vowels A, E, I, O, U, and Y = 46.1%

High-Frequency Consonants L, N, R, and T = 27.4%

Medium-Frequency Consonants C, D, G, M, P, S, and V = 22.2%

Low-Frequency Consonants B, F, H, J, K, Q, W, X, and Z = 4.3%

8 most frequent letters (in descending order of frequency) E, A, I, O, T, N, R, L = 07.8%

1-e. Absolute frequencies of single letters as initial letters of 10,481 words in Italian plain text, arranged according to their frequencies. (One-letter words have been omitted.)

D	1,381	L	500	T	337	U	217	J	13
C	1,041	R	403	G	333	Q	172	W	9
S	885	N	396	F	298	B	153	K	6
P	830	E	374	V	263	H	69	Y	3
A	822	M	371	O	235	Z	29	X	2
I	685								

2-a. Frequency distribution of digraphs based on 57,847 letters of Italian plain text, reduced to 5,000 digraphs.

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	18	9	39	41	14	12	22	1	19			76	24	78	5	24	4	57	36	63	6	24				12
B	10	7			7				10			1			4		4				2					
C	32		10		20			33	33			2			64		1	5			6					
D	31			1	65				64						23			2			9					
E	23	7	31	53	15	8	22	2	25			66	18	73	6	22	4	96	62	27	6	17				4
F	9				11	7			11			1			10			6			3					
G	9				11		8	2	20			17		8	9			11			6					
H	6				27				9																	
I	66	8	52	30	31	11	11	2	11			35	31	62	44	20	3	20	48	45	15	16				7
J																					1					
K																										
L	62	3	8	6	49	2	7		56			52	4	2	21	5	1	3	6	15	7	3				
M	31	5			35				17				4		18	13					2					
N	32	1	15	26	51	6	11	1	37			3	1	10	50	4	5	2	11	66	8	4				11
O	17	4	22	27	10	5	10	1	20			45	24	86	4	25	2	55	40	14	3	18				2
P	23				30				14			2			28	11		23			7					
Q																						20				
R	64	1	8	8	71	1	7		63			4	13	9	45	2		12	9	16	10	3				3
S	20		15	1	32	2			45			2	3		25	9			31	58	12	1				
T	83		1		65	1			59			1		1	56				43	1	37	10				
U	12	2	4	3	15	1	3		10			6	3	24	8	6		9	11	15						1
V	26				23				23						10			2			2	2				
W																										
X																										
Y																										
Z	13				4				20						3											5

2-b. Digraphic kappa plain, Italian language = .0081 (I.C. = 5.48).

## 14. NORWEGIAN

NOTE: The letter Q is derived from foreign words in Norwegian plain text.

1-a. Absolute frequencies of single letters of Norwegian plain text, arranged alphabetically, based on 56,190 letters of text.

A 3,228	G 2,211	M 1,841	S 3,572	Z 4
B 739	H 830	N 4,666	T 4,497	Æ 154
C 20	I 3,298	O 2,702	U 718	Ø 505
D 2,714	J 487	P 846	V 1,505	Å 957
E 9,119	K 2,077	Q 1	W 5	
F 1,287	L 3,043	R 4,813	Y 351	

1-b. Monographic kappa plain, Norwegian language =.0712 (I.C. =1.98).

1-c. Frequency distribution of single letters based on 56,190 letters of Norwegian plain text reduced to 1,000 letters, arranged according to their frequencies.

E 162	A 57	M 33	B 13	C 0
R 86	L 54	V 27	U 13	W 0
N 83	D 48	F 23	Ø 9	Z 0
T 80	O 48	Å 17	J 9	Q 0
S 64	G 39	P 15	Y 6	
I 59	K 37	H 15	Æ 3	

1-d. Percentage of vowels, high-frequency consonants, medium-frequency consonants, and low-frequency consonants in 56,190 letters of Norwegian plain text. Percentage of 8 most frequent letters in Norwegian plain text.

Vowels A, E, I, O, U, Y, Æ, Ø, and Å =37.4%

High-Frequency Consonants N, R, S, and T =31.2%

Medium-Frequency Consonants D, F, G, H, K, L, M, P, and V =29.1%

Low-Frequency Consonants B, C, J, Q, W, and Z =2.3%

8 most frequent letters (in descending order of frequency) E, R, N, T, S, I, A, and L =64.4%

1-e. Absolute frequencies of single letters as initial letters of 11,678 words in Norwegian plain text, arranged according to their frequencies. (One-letter words have been omitted.)

S 1,233	V 669	I 367	R 184	W 4
D 1,099	M 646	P 340	J 76	Z 2
F 922	H 637	N 322	Ø 55	Æ 1
E 853	T 562	G 287	Å 34	
O 712	B 483	L 278	Y 8	
A 677	K 420	U 207	C 6	

2-a. Frequency distribution of digraphs based on 56,190 letters of Norwegian plain text, reduced to 5,000 digraphs.

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	Y	Z	Æ	ø	Å	
A	1	2		11	2	6	16	1	1		13	32	14	61	2	4		47	17	30	2	24							
B	8			22					3			12			2			8			2			4			1	2	
C								1																					
D	16	2		9	135	3	1	2	14		1	4	2	4	4	1		15	11	9	3	3		1			1	2	
E	11	12		44	13	21	25	13	21	1	21	58	23	178	13	8		157	55	110	4	20					1	2	
F	9			8	3			5	2		8			44			14		3	2			1				9	6	
G	15	4		8	54	6	8	8	9	12	2	3	5	6	7	2		8	18	7	3	5	1				1	7	
H	30			16				2	2						10			1			2	7	1				2	1	
I	3	2		25	10	7	38	4	2		29	43	5	55	3	4		9	31	14	1	7					1		
J	2			21											13						1							7	
K	22	1		1	50	1		1	5	6	24	4	1	2	18	1		8	10	14	10	3	2				1		
L	22	4		21	58	4	4	2	42	1	5	34	3	1	12	2		1	17	13	4	7	4		1	3	4		
M	16	3		5	54	4	1	4	14		3	2	14	1	7	3		2	8	5	3	2	1				2	8	
N	17	6		49	70	13	47	8	24	1	11	7	8	39	21	5		3	38	23	3	8	3		2	2	8		
O	1	1		5	4	1	33	1	1		4	18	51	17	1	11		68	10	5		9							
P	5			1	10		2	1	2			3	1	1	4	12		8	2	2	1						2	18	
Q																													
R	36	12		32	92	16	9	12	39	2	13	7	15	10	21	4		7	36	31	10	10		3			5	7	
S	18	2	1	3	51	5	1	2	15	13	39	11	7	4	27	8		2	17	61	3	9	3		1	3	11		
T	32	6		13	96	13	3	9	53	2	4	6	9	9	23	4		18	26	41	8	12	5		1	5	4		
U	2	1		2	1	1	1				5	10	2	15		1		4	5	15									
V	19	1		5	38	2	2	1	36		1	1	1	3	5	1		1	3	2		1				8	2		
W																													
Y				2	4		2				3	1		4		1		4	4	4		1							
Z																													
Æ																		14											
ø		2		2		1					3	2	1	3		1		20	2	2		3	3						
Å	3	4		6	4	7	3	4	3	1	3	4	3	2	2	3		12	8	9	1	4						1	

2-b. Digraphic kappa plain, Norwegian language = .0087 (I.C. = 6.82).



## 15. PERSIAN

1-a. Absolute frequencies of single letters of Persian plain text, arranged alphabetically, based on 55,322 letters of text.

ا	9,186	ج	765	ز	173	ش	1,090	ع	909	گ	484	و	3,612
ب	2,238	چ	167	ر	4,910	ص	376	غ	87	ل	1,681	ي	4,263
پ	177	ح	498	ز	1,009	ض	259	ف	822	م	3,319		
ت	2,929	خ	788	ژ	13	ط	492	ق	1,026	ن	3,747		
ث	41	د	3,997	س	1,478	ظ	160	ک	1,534	ه	3,102		

1-b. Monographic kappa plain, Persian language =.0713 (I.C. =2.28).

1-c. Frequency distribution of single letters based on 55,322 letters of Persian plain text, reduced to 1,000 letters and arranged according to their frequencies.

ا	166	و	65	ل	30	ز	18	ح	9	پ	3	ث	∅
ر	89	م	60	گ	28	ع	16	ط	9	ز	3	ژ	∅
ي	77	ه	56	س	27	ف	15	ک	9	چ	3		
د	72	ت	53	ش	20	خ	14	ص	7	ظ	3		
ن	68	ب	40	ق	19	ج	14	ض	5	غ	2		

1-d. Percentage of vowels, high-frequency consonants, medium-frequency consonants, and low-frequency consonants in 55,322 letters of Persian plain text. Percentage of 9 most frequent letters in Persian plain text.

Vowels ا, ي, and و =30.8%

High-Frequency Consonants ر, د, ن, م, ه, and ت =39.8%

Medium-Frequency Consonants ب, ل, ک, س, ش, ق, ز, ع, ف, خ, and ج =24.1%

Low-Frequency Consonants ح, ط, گ, ص, ض, ن, پ, چ, ظ, غ, ث, and ژ =5.3%

9 most frequent letters (in descending order of frequency) ا, ر, ي, د, ن, و, م, ه, and ت =70.6%

1-e. Absolute frequencies of single letters as initial letters of 13,793 words of Persian plain text, arranged according to their frequencies. (One-letter words have been omitted.)

ا	2,650	ن	810	ه	314	ح	202	ص	124	ل	71	ژ	8
م	1,381	ت	673	س	291	ع	173	چ	113	غ	22	ث	5
ب	1,341	ر	585	و	272	ف	168	ي	105	ض	21		
د	1,056	خ	444	ج	251	پ	158	ز	84	ن	21		
گ	814	ش	390	ق	249	ک	142	ط	74	ظ	11		

2-a. Frequency distribution of digraphs based on 55,322 letters of Persian plain text, reduced to 5,000 digraphs.

ی و ه ن م ل گ گ ق ف غ ع ظ ط ض ص ش س ژ ز ر ز ر خ ح ج ش ت پ ا

ا	29	39	2	36	2	11	2	7	13	40	4	86	46	41	20	6	4	8	4	19	11	14	17	14	6	33	62	107	30	19	117		
ب	58	2	1	8		2		2	2	8		28	2		4	3	1		3		7		2	3	3	1	8	6	7	12	19	14	
پ	4											2			2	1													1		1	5	
ت	36	18	1	4		3		7	12	13	1	14	1		5	9	4	2		2	7	1	5	8	9	1	7	21	14	23	22	14	
ث	1											1																				1	
ج	17	2								5		4	2								4						3	3	8	12	4	2	
ح	1																							1					3	5	2	1	
خ	5	1		4						3		4	1		2		2	4					1	3	2		2	3		1	4	2	
د	17	3		4						1		4			2	1	4		1								5				23	4	
ذ	74	18	1	11		1	2	1	3	15		52	1		7	4	1				2	1	1	2	14	4	2	19	22	46	40	16	
ر	7											3				1								1								2	
ز	136	14	3	26		13	3	5	7	40		7	2		11	6	3	2	2		3	1	18	2	16	4	1	24	12	11	30	43	
س	26	5	1	2		2		3	1	4		3			2	2	1		3		1			3	1		1	9	4	4	4	10	
ش	19	5		48		1			2	2		5			1	1			2		1		9		2		4	4	3	9	4	10	
ص	11	1		11					2	19		9			1							1		6	1		5	5	2	23	1		
ض	4	1					1		3	4													1				4	1	2	1	8	2	
ط	8											3											1				2				5	3	
ظ	3	3										7			1								2				7	1	1	15	3	1	
ع	2											5																			1	3	2
غ	11	5		6		1			1	8		4	3			1		7	1		1		1	3	1		8	7	3	4	3	7	
ف	1											1															1					1	2
ق	14	1		10		1				2		16			1	2	1					4		6	1		1	1	1	2	5	6	
ک	18	5		6						8		7			2	2	1	1	16		3		1				3	2		1	8	8	
گ	28	2		5								19	1		2	4											2	8	16	37	7	4	
ل	5		1									2	18	2		1							1				3	1			3	5	
م	36	7	1	19		1	1	2	1	3		2	1		3	2			1		2	2	2	1	4	5	3	8	6	8	8	25	
ن	46	9	1	13		6	1	6	7	11		4	26	3	10	6	2	1	4		7		2	8	8	1	13	7	16	10	36	36	
و	42	15	2	14		9	2	2	7	6		9	2		9	6	1		1	6	3		7	19	11	11		37	11	19	15	21	
ه	69	19	2	10		3	2	2	5	29		1	20	3		5	10	2		1	2		4	4	7	2	1	34	16	6	15	9	
ی	55	12	1	9		7	2	2	2	47		1	38	17		11	5	3	6	1	1	10		2	10	4	2	28	17	16	4	2	11
	48	15	1	17		7	1	4	4	40		4	5		13	12	1		1		3	1	2	3	33	4	10	20	65	16	1	4	

2-b. Digraphic kappa plain, Persian language=.0065 (I.C.=6.66).

## 16. POLISH

NOTE: The letters Q and V are derived from foreign words appearing in Polish plain text.

1-a. Absolute frequencies of single letters of Polish plain text, arranged alphabetically, based on 53,845 letters of text.

A	4,695	E	4,232	J	1,362	Ń	161	S	2,414	Y	2,146
Ą	582	Ę	558	K	1,776	Ō	4,314	Ś	264	Z	2,906
B	753	F	164	L	1,125	Ó	542	T	1,872	Ż	489
C	2,330	G	746	Ł	900	P	1,789	U	1,035	Ź	39
Ć	189	H	675	M	1,309	Q	1	V	4		
D	1,902	I	4,323	N	2,980	R	2,541	W	2,727		

1-b. Monographic kappa plain, Polish language = .0528 (I.C. = 1.80).

1-c. Frequency distribution of single letters based on 53,845 letters of Polish plain text, reduced to 1,000 letters and arranged according to their frequencies.

A	87	W	51	T	35	U	19	Ę	10	Ń	3
I	80	R	47	P	33	Ł	17	Ó	10	Ż	∅
O	80	S	45	K	33	B	14	Ź	9	V	∅
E	79	C	43	J	25	G	14	Ś	5	Q	∅
N	55	Y	40	M	24	H	13	Ć	4		
Z	54	D	35	L	21	Ą	11	F	3		

1-d. Percentage of vowels, high-frequency consonants, medium-frequency consonants, and low-frequency consonants in 53,845 letters of Polish plain text. Percentage of 4 most frequent letters in Polish plain text.

Vowels A, I, O, E, Y, U, ą, ę, and ó = 41.7%

High-Frequency Consonants N, Z, W, R, S, and C = 29.5%

Medium-Frequency Consonants D, T, P, K, J, M, and L = 20.7%

Low-Frequency Consonants Ł, B, G, H, Ż, Ś, Ć, F, Ń, Ź, V, and Q = 8.1%

4 most frequent letters (in descending order of frequency) A, I, O, E = 32.6%

1-e. Absolute frequencies of single letters as initial letters of 8,451 words of Polish plain text, arranged according to their frequencies. (One-letter words have been omitted.)

P	1,196	Z	521	T	335	C	254	U	160	F	54	Ł	4
S	729	D	500	R	283	A	213	G	142	E	33	Ż	2
N	626	O	436	M	275	J	215	I	118	Ś	32	Ą	1
W	606	K	391	B	265	Ź	179	L	108	H	21	Y	1

2-a. Frequency distribution of digraphs based on 53,845 letters of Polish plain text, reduced to 5,000 digraphs.

	A	Ą	B	C	Ć	D	E	É	F	G	H	I	J	K	L	Ł	M	N	Ń	O	Ó	P	Q	R	S	Ś	T	U	V	W	Y	Z	Ż	Ź
A	3		9	35	6	27			2	8		4	22	21	18	26	23	53	9	6		20	33	24	2	23	3	31	17	8	1			
Ą	1		2	10	1	8			2		2		1		1	1	2		2		4	1	5		2		4		4	2				
B	6					6	4				9		1	2			2		7		1	10	1		4		15	1						
C	7	1			1	15	1			60	26	18	8		1	3		1	3	6	3	1	1	1	1	2	2	1	13	48	1			
Ć			1			1					1				1	2		1	2		3	1	1		3	1	1	1	2					
D	15	2	3	3		2	14	1			1	1	3	8	3	2	15		36	3	3	5	3	1	6	4	9	33		2				
E	3		7	24	1	26	1		2	29	4	35	13	19	2	29	39	5	6		19	32	31	4	11	3	22	20	6					
É			1	4		10			1		1	1	3	1		4		2		6		4	1	4	1	3	3	2						
F	2					2				4									2		2					1		1						
G	11	1				4	2				4			2	3	1		26	2		10				2	1								
H	4		1	3		2		1	1		3	2	3	1	1	2	5		9	1	6	1	3	2	2	6	1	4	1					
I	47	8	2	27	3	10	32	26	1	2	4	4	11	6	8	8	17		12		13	3	16	1	9	6	14	9	5					
J	17	13	1	3		3	22	4	1	1	17	1	3	1		3	5		3	1	4	2	11		5	4	2							
K	26	3		2		1	2			45	1	1	1	2	1	1		33	6	1	11	4		12	8	2	1							
L	12	1	1	1		19	2		1	23			5			10		8			14		1	6	1									
Ł	19	1	1			1	3	1		1			2			4		18	1	4	1	3	1	6	2	10	1	2						
M	13		2	2		2	8			35	2	2	1		1	4		18	4	6	1	3	1	6	3	5	2	1						
N	52	4		5		5	26	1	3	4	96	2	4			6		21	1	1		4	10	3	2	26								
Ń						3															9													
O	2		19	14		40			3	6	3	11	13	29	7	16	36	2	4		19	22	32	13	16	2	67	18	6					
Ó			2	2		2					1		2	1							10		1		28		1							
P	14					5				10		2	2	1		70	2		53	1		4		1										
Q																																		
R	47	1		2		4	23	1		1	4	2	1		1	3	3		39	9	2		6	4	5	3	18	55	1					
S	10	3		6		6				25	4	35		7	1	2		10	2	15	1		52	4	5	4	30							
Ś				11	3									2		1	2				1				4									
T	33	2	1	1		1	20	4			1	1	7	1		8		15	11	1	19	1	1	11	12	23	1							
U	3		3	7		8			5		21	6	4	3	1	4	8		2		9	5	11	1	4	4	4	4						
V																																		
W	40	2	1	5		4	17	2	1	1	53	2	5	1	5	2	12		22	3	10		7	15	1	3	1	5	28	6				
Y	1		7	38	3	9			1	4	2	9	12	4	8	15	11		4		12	4	16	2	10	1	14	8	5					
Z	41	8	4	6		5	54	3		2	23	4	6	1	4	16	18		16	1	6	2	3	4	5	10	39	1						
Ż	3	2				1	16						2	1		4		3		1		2		1	1	7	1							
Ź				2													1																	

2-b. Digraphic kappa plain, Polish language = .0055 (I.C. = 6.36).

## 17. PORTUGUESE

1-a. Absolute frequencies of single letters of Portuguese plain text, arranged alphabetically, based on 45,106 letters of text.

A	5,362	G	724	L	1,245	Q	348	V	737
B	470	H	304	M	1,699	R	3,292	W	24
C	2,285	I	3,314	N	2,912	S	3,409	X	166
D	1,900	J	160	O	5,001	T	2,679	Y	22
E	5,441	K	17	P	1,377	U	1,491	Z	207
F	520								

1-b. Monographic kappa plain, Portuguese language = .0746 (I.C. = 1.94).

1-c. Frequency distribution of single letters based on 45,106 letters of Portuguese plain text, reduced to 1,000 letters, and arranged according to their frequencies.

E	121	N	65	U	33	F	11	X	4
A	119	T	59	P	30	B	10	J	3
O	111	C	51	L	28	Q	8	W	1
S	76	D	42	V	16	H	7	Y	∅
I	73	M	38	G	16	Z	5	K	∅
R	73								

1-d. Percentage of vowels, high-frequency consonants, medium-frequency consonants, and low-frequency consonants in 45,106 letters of Portuguese plain text. Percentage of 8 most frequent letters in Portuguese plain text.

Vowels A, E, I, O, U, and Y = 45.8%

High-Frequency Consonants N, R, and S = 21.3%

Medium-Frequency Consonants C, D, L, M, P, and T = 24.8%

Low-Frequency Consonants B, F, G, H, J, K, Q, V, W, X, Y, and Z = 8.1%

8 most frequent letters (in descending order of frequency) E, A, O, S, I, R, N, and T = 69.7%

1-e. Absolute frequencies of single letters as initial letters of 7,058 words in Portuguese plain text, arranged according to their frequencies. (One-letter words have been omitted.)

P	847	M	405	I	264	B	113	Z	14
C	731	T	348	F	222	G	111	W	11
E	608	R	316	Q	222	J	92	K	7
S	601	N	299	O	187	U	77	Y	4
A	597	V	271	L	143	H	60	X	2
D	506								

2-a. Frequency distribution of digraphs based on 45,106 letters of Portuguese plain text, reduced to 5,000 digraphs.

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	11	11	52	60	15	9	14	2	18	2		38	36	56	49	23	8	68	72	22	8	16	1			5
B	11			1	10				5			2	1		9			9	2	1	2					
C	60		2		30			4	39			5		1	85			7		8	12					
D	45				61				33				1		61			2	1	1	5					
E	15	5	48	22	11	11	23	1	27	6	1	31	44	97	6	18	6	76	95	20	7	12	1	15		5
F	9				14				13			1			15			2			3					
G	15				14				4			1		1	14			14			15					
H	10				8				3						11						1					
I	41	3	34	31	6	7	9		1			16	22	53	26	5	2	25	39	27	2	10		2		7
J	7				2										2						7					
K																										
L	24	1	4	4	24	1	5	9	21			2	4	2	14	4	2	1	4	7	6	2				
M	41	10	3	4	51	1			26	1		1	2	1	16	15	1	3	5	2	6	2				
N	31		29	35	14	7	8	12	18						25	1			19	114	4	4				1
O	21	9	32	25	27	10	7	3	20	4		20	36	79	5	35	8	71	85	18	12	22	1	1	1	1
P	26		2		25				2			4		1	60	1	1	28	1	1	3					
Q					1																37					
R	75	2	14	9	86	3	7	1	46	1		2	18	8	34	7	3	11	8	18	4	6				1
S	41	6	22	10	62	6	3	2	23	2		3	12	5	23	35	7	4	40	47	18	5				
T	65		1	1	69	1			26					1	88			33		1	13					
U	22	5	5	7	26	1	4		18	1		14	11	17	2	4		9	6	11		1				2
V	11				37				23						9			1								
W	1																									
X	10		3		1				2							3				1						
Y																										
Z	7		1		9				2				1		1		1	1								

2-b. Digraphic kappa plain, Portuguese language = .0084 (I.C. = 5.68).

## 18. ROMANIAN

NOTE: The letters K, Q, W, X, and Y are derived from foreign words.

1-a. *Absolute frequencies of single letters of Romanian plain text, arranged alphabetically, based on 56,370 letters of text.*

A	5,143	D	1,933	I	6,251	M	1,628	R	4,279	U	3,261
Ă	1,896	E	6,828	Î	610	N	3,753	S	2,308	V	623
Â	337	F	619	J	124	O	2,627	Ș	685	W	3
B	509	G	577	K	9	P	1,706	T	3,830	X	69
C	2,883	H	146	L	2,655	Q	1	Ț	693	Y	3
										Z	381

1-b. *Monographic kappa plain, Romanian language = .0670 (I.C. = 2.08).*

1-c. *Frequency distribution of single letters based on 56,370 letters of Romanian plain text, reduced to 1,000 letters and arranged according to their frequencies.*

E	121	U	58	D	34	Ș	12	B	9	X	1
I	111	C	51	Ă	34	V	11	Z	7	K	∅
A	91	L	47	P	30	F	11	Â	6	W	∅
R	76	O	47	M	29	Î	11	H	3	Y	∅
T	68	S	41	Ț	12	G	10	J	2	Q	∅
N	67										

1-d. *Percentage of vowels, high-frequency consonants, medium-frequency consonants, and low-frequency consonants in 56,370 letters of Romanian plain text. Percentage of 6 most frequent letters in Romanian plain text.*

Vowels E, I, A, U, Ă, Î, Â, and Y = 43.1%

High-Frequency Consonants R, T, and N = 21.1%

Medium-Frequency Consonants C, L, O, S, D, P, and M = 27.9%

Low-Frequency Consonants Ț, Ș, V, F, G, B, Z, H, J, X, K, W, and Q = 7.9%

6 most frequent letters (in descending order of frequency) E, I, A, R, T, and N = 53.4%

1-e. *Absolute frequencies of single letters as initial letters of 10,655 words of Romanian plain text, arranged according to their frequencies. (One-letter words have been omitted.)*

D	1,168	M	467	T	370	V	239	Z	52	Ă	1
C	1,167	N	449	F	369	O	200	J	31	Q	1
P	979	I	415	E	314	G	174	H	20	W	1
A	907	L	395	R	277	B	117	Â	5	X	1
S	862	Ș	392	U	249	Ț	62	K	2	Y	1
Î	508										

2-a. Frequency distribution of digraphs on 56,370 letters of Romanian plain text, reduced to 5,000 digraphs.

	A	Ă	Â	B	C	D	E	F	G	H	I	Î	J	K	L	M	N	O	P	Q	R	S	Ș	T	Ț	U	V	W	X	Y	Z
A	10			6	39	22	4	8	6		20	6	3		48	18	29	3	18		72	28	8	60	18	17	7			7	
Ă	11			1	14	15	2	4	2		6	6	1		6	7	8	3	12		25	13	5	14	6	3	3			3	
Â											1				1	1	18				2			7							
B	5	2	1				3				11				4			2	1		3	1			1	11					
C	33	29	9		2	2	48			6	28	2			4	2		30			10	1	1	11	5	34					
D	13	3			2	1	87			1	27	1			1	1	1	7	1		4	4	1	1		15	1				
E	73			8	57	38	9	10	14	1	30	11	3		45	25	48	13	35		54	60	18	19	4	8	13		5	7	
F	8	6					8				16				2			8			3					3					
G	6	5	1				9			3	6				1		1	2			8					8					
H	1						3				5							1	1												
I	43			8	47	29	34	9	9	1	32	7	2		38	29	87	13	20		17	34	12	43	6	18	12			7	
Î	1				1						1				1	3	43	1						1	1						
J	1						1				1				1			1									5				
K																															
L	30	7		1	5	6	65	1	1		29	3			2	3	2	27	5		2	4	2	11	1	28	2				
M	33	7	6	6	2	2	23				21	1			1	1	3	7	13			2	1	1	1	14					
N	27	9	1	1	26	26	40	5	7		40	2	1		3	4	2	17	6		2	19	2	52	12	26	4			1	
O	20			6	14	7	2	2	3		7				13	20	28		9		62	12	1	10	1	5	6			3	
P	14	8	1		1		32				5				7			19			42	2		6	14						
Q																															
R	36	21	2	2	9	7	102	4	5		78	4			3	10	8	27	5		2	6	3	15	3	27	2			1	
S	18	22	1	1	17	1	29	2			18	2			2	1		7	9			2		57	18						
Ș	2				1		3				39													13	2						
T	40	29	4		6	7	76	3			46	6			3	2	2	33	4		44	4	2	1	28						
Ț	6	7					6				39														1	1					
U	13	2		3	14	7	5	4	2		27	3			50	16	52	1	13		28	14	3	19	3	1	5			3	
V	9	5	1				13				12							9			2				1						
W																															
X	1						1				2								2					1							
Y																															
Z	5	4	1	1			7				11							1								3					

2-b. Digraphic kappa plain, Romanian language = .0068 (I.C. = 6.53).



## 19. RUSSIAN

1-a. Absolute frequencies of single letters of Russian plain text, arranged alphabetically, based on 67,850 letters of text.

А	5,122	З	1,280	Н	4,463	У	1,578	Щ	257
Б	1,095	И	4,923	О	8,078	Ф	127	Ы	1,421
В	3,543	Й	961	П	1,815	Х	941	Ь	960
Г	1,141	К	2,324	Р	3,427	Ц	369	Э	173
Д	2,076	Л	2,747	С	3,917	Ч	902	Ю	455
Е	5,537	М	1,936	Т	4,041	Ш	554	Я	1,185
Ж	502								

1-b. Monographic kappa plain, Russian language = .0568 (I.C. = 1.76).

1-c. Frequency distribution of single letters based on 67,850 letters of Russian plain text reduced to 1,000 letters, and arranged according to their frequencies.

О	119	В	52	П	27	Б	16	Ж	7
Е	82	Р	50	У	23	Й	14	Ю	7
А	75	Л	40	Ы	21	Ь	14	Ц	5
И	73	К	34	З	19	Х	14	Щ	4
Н	66	Д	31	Я	17	Ч	13	Э	3
Т	60	М	29	Г	17	Ш	8	Ф	2
С	58								

1-d. Percentage of vowels, high-frequency consonants, medium-frequency consonants, and low-frequency consonants in 67,850 letters of Russian plain text. Percentage of 10 most frequent letters in Russian plain text.

Vowels А, Е, И, Й, О, У, Ы, Э, Ю, and Я = 43.4%

High-Frequency Consonants В, Н, Р, С, and Т = 28.6%

Medium-Frequency Consonants Б, Г, Д, З, К, Л, М, П, Х, Ч, and Ъ = 25.4%

Low-Frequency Consonants Ж, Ф, Ц, Ш, and Щ = 2.6%

10 most frequent letters (in descending order of frequency) О, Е, А, И, Н, Т, С, В, Р, and Л = 67.5%

1-e. Absolute frequencies of single letters as initial letters of 10,601 words in Russian plain text, arranged according to their frequencies. (One-letter words have been omitted.)

П	1,210	Д	496	И	321	Х	120	Ф	58
С	983	М	446	Г	292	А	116	Ц	47
Н	800	Р	429	У	229	Е	92	Я	41
В	731	Т	418	Ч	182	Ж	72	Ю	34
О	650	З	404	Э	147	Ш	63	Щ	2
К	555	Б	344	Л	146				

2-a. Frequency distribution of digraphs based on 67,850 letters of Russian plain text, reduced to 5,000 digraphs.

	А	Б	В	Г	Д	Е	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ы	Ь	Э	Ю	Я		
А	2	12	35	8	14	7	6	15	7	7	19	27	19	45	5	11	26	31	27	3	1	10	6	7	10	1			2	6	9		
Б	5					9	1		6			6		2	21		8	1		6						1	11				2		
В	35	1	5	3	3	32		2	17		7	10	3	9	58	6	6	19	6	7		1	1	2	4	1	18	1	2		3		
Г	7				3	3			5		1	5		1	50		7			2													
Д	25		3	1	1	29	1	1	13		1	5	1	13	22	3	6	8	1	10			1	1	1		5	1			1		
Е	2	9	18	11	27	7	5	10	6	15	13	35	24	63	7	16	39	37	33	3	1	8	3	7	3	3			1	1	2		
Ж	5	1			6	12			5					6					1														
З	35	1	7	1	5	3			4		2	1	2	9	9	1	3	1		2							4				4		
И	4	6	22	5	10	21	2	23	19	11	19	21	20	32	8	13	11	29	29	3	1	17	3	11	1	1		1	3	17			
Й	1	1	4	1	2		1	2	4		5	1	2	7	9	7	3	10	2				1	3	2								
К	24	1	4	1		4	1	1	26		1	4	1	2	66	2	10	3	7	10			1										
Л	25	1	1	1	1	33	2	1	36		1	2	1	8	30	2		3	1	6		4		1			2	30		4	9		
М	18	2	4	1	1	21	1	2	23		3	1	3	7	19	5	2	5	3	9	1			2			5	1	1		3		
Н	54	1	2	3	3	34			58		3		1	24	67	2	1	9	9	7	1		5	2			36	3			5		
О	1	28	84	32	47	15	7	18	12	29	19	41	38	30	9	18	43	50	39	3	2	5	2	12	4	3			2	3	2		
П	7					15			4			9		1	46		41	1		6							2				2		
Р	55	1	4	4	3	37	3	1	24		3	1	3	7	56	2	1	5	9	16		1	1	1	2		8	3			5		
С	8	1	7	1	2	25			6		40	13	3	9	27	11	4	11	82	6		1	1	2	2		1	8			17		
Т	35	1	27	1	3	31		1	28		5	1	1	11	56	4	26	18	2	10				1			11	21			4		
У	1	4	4	4	11	2	6	3	2		8	5	5	5	1	5	7	14	7			1		8	3	2				9	1		
Ф	2					2			2					1		1	1																
Х	4	1	4	1	3	1		2	3		4	3	3	4	18	5	3	4	2	2	1			1									
Ц	3					7			10		2				1					1							1						
Ч	12					23			13		2			6					7	1					1			1					
Ш	5					11			14		1	2		2	2					1								1					
Щ	3					8			6					1						1													
Ы		1	9	1	3	12		2	4	7	3	6	6	3	2	10	3	9	4	1		16		1	2								
Ь		2	4	1	1	2		2	2		6		3	13	2	4	1	11	3					1	4				1	3	1		
Э										1			1					1	9														
Ю		2	1	2	1			3	1		1		1	1	1	3	1	1	7					1	1		4						
Я	1	3	9	1	3	3	1	5	3	2	3	3	4	6	3	6	3	6	10			2	1	4	1	1			1	1	1		

2-b. Digraphic kappa plain, Russian language = .0052 (I.C. = 5.00).

## 20. SERBO-CROAT

NOTE: The letter W is derived from foreign words appearing in Serbo-Croat plain text.

1-a. Absolute frequencies of single letters of Serbo-Croat plain text, arranged alphabetically, based on 61,915 letters of text.

A 7,161	Dj 271	J 2,370	N 3,424	S 3,246	H 389
B 847	E 5,625	K 2,283	Nj 509	T 2,541	C 512
V 2,467	Ž 416	L 1,750	O 5,773	Ć 42	Č 577
G 1,122	Z 1,108	Lj 361	P 1,858	U 2,802	Š 577
D 2,413	I 5,875	M 1,772	R 3,382	F 123	W 3

1-b. Monographic kappa plain, Serbo-Croat language=.0617 (I.C.=1.85).

1-c. Frequency distribution of single letters based on 61,915 letters of plain text, reduced to 1,000 letters and arranged according to their frequencies.

A 116	R 55	D 39	L 28	Š 9	H 6
I 95	S 52	J 38	G 18	C 8	Lj 6
O 93	U 45	K 37	Z 18	Nj 8	Dj 4
E 91	T 41	P 30	B 14	Ń 7	F 2
N 55	V 40	M 29	Č 9	Ć 7	W 0

1-d. Percentage of vowels, high-frequency consonants, medium-frequency consonants, and low-frequency consonants in 61,915 letters of Serbo-Croat plain text. Percentage of 4 most frequent letters in Serbo-Croat plain text.

Vowels A, I, O, E, and U=44.0%

High-Frequency Consonants N, R, S, and T=20.3%

Medium-Frequency Consonants V, D, J, K, P, M, L, G, Z, and B=29.1%

Low-Frequency Consonants Č, Š, C, Nj, Ž, Ć, H, Lj, Dj, F, and W=6.6%

4 most frequent letters (in descending order of frequency) A, I, O, and E=39.5%

1-e. Absolute frequencies of single letters as initial letters of 11,460 words of Serbo-Croat plain text, arranged according to their frequencies. (One-letter words have been omitted.)

S 1,401	K 676	T 353	G 249	C 84	H 38
P 1,250	J 527	B 338	A 184	F 78	Nj 38
D 818	Z 437	U 319	Ć 133	E 76	Lj 27
N 760	V 436	M 314	Š 119	Ž 73	Dj 23
O 760	I 430	R 313	Č 116	L 66	W 1

2-a. Frequency distribution of digraphs based on 61,915 letters of Serbo-Croat plain text, reduced to 5,000 digraphs.

	A	B	V	G	D	Dj	E	Ž	Z	I	J	K	L	Lj	M	N	Nj	O	P	R	S	T	Ć	U	F	H	C	Č	Š	W	
A	6	10	50	10	43	4	2	7	21	20	31	34	29	3	24	50	15	24	30	37	45	30	5	16	2	2	12	11	8		
B	8						5			17	2		4	1	2		10		12					5							
V	42						33			37	8	1	6	5	11		32		13	2				4			1		1		
G	13	1	1		1	1	5		1	6		1	9		1	2		22	2	14	2	1		6							
D	46	2	5	2	1		14		1	26	1	1	2		1	22	3	25	2	22	8	1		11							
Dj	2						11																		4						
E	4	10	16	12	56	6	1	3	15	16	6	24	19	5	23	54	9	18	25	25	43	25	12	17	2	2	4	5	6		
Ž	11	2					9			7						2	1								1						
Z	36	2	6	3	2		7			8	4		2		3	6		2	1	3	1			4							
I	4	4	18	6	15	1	1	2	28	8	55	26	20	2	38	45	6	21	18	13	45	25	5	11	2	24	12	13	9		
J	25	1	2		1		10	7		16		1			1	3		5	2		6			18	1						
K	33		3		1		17			18	1	1	3	1		1	1	68	1	11	2	3		17			1				
L	42	1					19			36		1			1	6		25	1		1	2		6							
Lj	8						10			2						1						2			5						
M	34	2	1	1	3		17		2	15	7	3	1	4	2	6		16	7	3	8	1		7			1	1			
N	78			4	5		37		1	65	1	2				1		53	2	1	8	6		10	1		4		1		
Nj	8						20			5								1			1			6							
O	1	23	54	30	50	3		5	9	6	49	15	12	5	35	25	1	5	18	30	46	18	3	4	1		2	7	8		
P	13						5			7	1		6	1				54		50	2	1		7						3	
R	77	2	4	5	2		43	10	1	40	1	2	1		2	7	1	38	1		8	2		19		1		1	6		
S	22		17				29			12	10	37	17	1	2	7		8	10	4	1	65		21			1				
T	45		12	1	2		18		1	50	3	3				6		28	3	20	5		1	8							
Ć	5						16			6						1		1				1			2						
U	2	7	8	15	12	1	1	7	9	9	10	12	5	1	9	13	2	8	23	8	24	10	5	7	1	1	2	9	4		
F	1						3			2								2		2											
H	1	1	2	1	4		1		1	4		1			1	2		3	2	2	2	1		1							
C	5						7			22	1							1		2				2							
Č	6						8			9	1	13	2			3		1						2							
Š	4						9			6	1	3	2			1	2		1				14	1	2						
W																															

2-b. Digraphic kappa plain, Serbo-Croat language = .0062 (I.C. = 5.58).

## 21. SLOVAK

1-a. *Absolute frequencies of single letters of Slovak plain text, arranged alphabetically, based on 46,026 letters of text.*

A	4,694	F	110	K	1,816	R	2,428	W	23
B	810	G	124	L	1,892	S	2,238	X	12
C	732	H	596	M	1,512	Š	338	Y	1,343
Č	424	Ch	515	N	2,903	T	2,294	Z	935
D	1,666	I	3,251	O	4,827	U	1,656	Ž	349
E	3,848	J	849	P	1,487	V	2,354		

1-b. *Monographic kappa plain, Slovak language = .0585 (I.C. = 1.70).*

1-c. *Frequency distribution of single letters based on 46,026 letters of Slovak plain text, reduced to 1,000 letters and arranged according to their frequencies.*

O	105	R	53	K	40	Y	29	H	13	G	3
A	102	V	51	D	36	Z	20	Ch	11	F	2
E	84	T	50	U	36	J	18	Č	9	W	0
I	71	S	49	M	33	B	18	Ž	8	X	0
N	63	L	41	P	32	C	16	Š	7		

1-d. *Percentage of vowels, high-frequency consonants, medium-frequency consonants, and low-frequency consonants in 46,026 letters of Slovak plain text. Percentage of 5 most frequent letters in Slovak plain text.*

Vowels O, A, E, I, U, and Y = 42.6%

High-Frequency Consonants N, R, V, T, and S = 26.6%

Medium-Frequency Consonants L, K, D, M, P, Z, J, B, and C = 25.4%

Low-Frequency Consonants H, Ch, Č, Ž, Š, G, F, W, and X = 5.4%

5 most frequent letters (in descending order of frequency) O, A, E, I, and N = 42.5%

1-e. *Absolute frequencies of single letters as initial letters of 7,882 words of Slovak plain text, arranged according to their frequencies. (One-letter words have been omitted).*

P	960	Z	378	D	350	R	263	Ž	110	Š	64	G	24
S	745	K	368	M	330	U	232	Č	108	C	59	Ch	19
V	602	T	361	B	313	J	144	H	108	F	54	W	11
N	577	O	356	A	297	L	127	I	89	E	39	Y	1

2-a. Frequency distribution of digraphs based on 46,026 letters of Slovak plain text, reduced to 5,000 digraphs.

	A	B	C	C	D	E	F	G	H	Ch	I	J	K	L	M	N	O	P	R	S	Š	T	U	V	W	X	Y	Z	Ž	
A	8	11	16	9	40	1	2	1	10	6	3	19	30	39	30	54	9	28	31	40	6	39	6	42			1	20	7	
B	6				7				3	5		2	4	1	4	23		11	1				9				10			
C	5				9						25		20			2	7	1		1		3	4	1				1		
Č	9				4						12		1	1		10	4		3	1		1								
D	24	5	2	2	2	23					8	1	4	7	2	21	36	3	5	5	1	1	10	4			8	7		
E	10	12	9	5	32		2	1	21	2	3	27	12	31	26	61	9	23	31	27	4	26	6	22	1	1	12	5		
F	2				2					1						2		2					1							
G	3				3					1			1		1	1		1				1	1							
H	3				2					2			6		2	38		5				1	2				2			
Ch	4	1	1	1	2	1			1			1	2	3	2	3	11	4	3	3		3	2	5			1	3		
I	50	6	25	6	8	54	1	2	1	8	4	4	16	23	13	30	7	11	5	25	2	25	4	14			9	3		
J	9	1		1	3	22			1		3		1	1	3	8	5	4	1	5	2	2	14	3			1			
K	24	1	2	1	2	26	1			4		1	4	1	2	50	1	10	2			14	19	4			28	1		
L	44	2	1	1	1	25			1		32	1	6	2	3	13	30	2	1	8	2	2	13	4			10	2		
M	21	3	1	1	2	26			1		31	1	3	2	2	7	18	6	2	6	1	3	11	6			6	3	1	
N	63	1	6	2	3	68	2	4			63		5	1		4	31	1		10	1	9	15	3			27	2		
O	4	27	8	9	48		2	1	11	5	2	23	22	35	42	24	4	18	43	45	2	17	11	90			22	8		
P	12		1			7				4			8		1	60		61	1	1		3								
R	51	1	1	1	4	46		2	2		47		1	2	6	8	53	2		7	1	3	11	6			7	1	1	
S	27	1				9			2	2	16	1	39	16	4	5	16	16	3	5		66	8	8			1			
Š	3					8			1		10		1	1		1	1	1				7	1	1						
T	35	1			1	26	1		1		35		8	3	1	13	50	2	25	9		2	13	14			8	1	1	
U	10	4	6	5	19	1	1		5	1	1	11	9	5	6	7	4	18	8	19	3	14	2	10			6	7		
V	47	3	1	1	4	33			1		22	1	4	6	2	12	42	6	7	5	6	4	5	2			35	7		
W	1										1																			
X																		1												
Y	6	4	1	1	3				1	3	27	1	2	5	2	17	8	4	9	5	16	4	5	2	11			4	2	
Z	30	2			4	5			4		8	1	3	2	4	9	7	3	4	3	1	1	4	5			1	1		
Ž	1	1			2	13					10		1	1		5	1			1	1		1							

2-b. Digraphic kappa plain, Slovak language = .0056 (I.C. = 4.71).

## 22. SPANISH

1-a. Absolute frequencies of single letters of Spanish plain text, arranged alphabetically, based on 60,115 letters of text.

A	6,681	G	823	L	2,174	Q	346	V	602
B	799	H	367	M	1,740	R	4,628	W ²	36
C	3,137	I	4,920	N ¹	4,823	S	4,140	X	127
D	2,687	J	190	O	5,859	T	3,180	Y	413
E	7,801	K	22	P	1,785	U	2,172	Z	182
F	481								

1-b. Monographic kappa plain, Spanish language = .0747 (I.C. = 1.94).

1-c. Frequency distribution of single letters based on 60,115 letters in Spanish plain text, reduced to 1,000 letters, and arranged according to their frequencies.

E	130	S	69	U	36	V	10	J	3
A	111	T	53	P	30	F	8	Z	3
O	97	C	52	M	29	Y	7	X	2
I	82	D	45	G	14	H	6	W	1
N	80	L	36	B	13	Q	6	K	∅
R	77								

1-d. Percentage of vowels, high-frequency consonants, medium-frequency consonants, and low-frequency consonants in 60,115 letters of Spanish plain text. Percentage of 7 most frequent letters in Spanish plain text.

Vowels A, E, I, O, U, and Y = 46.3%

High-Frequency Consonants N, R, and S = 22.6%

Medium-Frequency Consonants C, D, L, M, P, and T = 24.5%

Low-Frequency Consonants B, F, G, H, J, K, Q, V, W, X, and Z = 6.6%

7 most frequent letters (in descending order of frequency) E, A, O, I, N, R, and S = 64.6%

1-e. Absolute frequencies of single letters as initial letters of 10,129 words in Spanish plain text, arranged according to their frequencies. (One-letter words have been omitted.)

P	1,128	L	435	Q	286	V	183	Y	27
C	1,081	R	425	I	281	F	177	W	19
D	1,012	M	403	H	230	O	169	Z	2
E	989	N	346	U	219	B	124	K	1
S	789	T	298	G	206	J	47	W	∅
A	761								

¹ Includes Ñ throughout all tables.

² From foreign words appearing in Spanish plain text.

2-a. Frequency distribution of digraphs based on 60,115 letters of Spanish plain text, reduced to 5,000 digraphs.

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	
A	12	14	54	64	15	5	8	4	10	8		41	30	64	4	24	5	81	62	18	9	9			11	4	
B	11				5				14	1		12			5			12	2	1	3						
C	39		5	17			8	80				3			69			6		13	18						
D	32		1	2	84			1	30					1	59	2	1	3	1		6				1		
E	20	5	47	26	17	8	21	6	9	3		44	26	126	5	23	4	94	119	17	5	10	1	8	2	3	
F	2				9				12			1			7			4			5						
G	12				12				5			1		2	15			11		1	11						
H	15				3				5						6						1						
I	43	8	42	29	40	5	8			1		14	16	50	67	4	1	16	27	24	1	8				5	
J	4				5										3						3						
K					1																						
L	44		5	5	35	1	3		28			9	5	1	17	5	1	2	4	5	5	3			1		
M	32	10			42				30						15	10					6						
N	41	2	33	37	41	10	6	2	28	1		5	4	3	43	10	2	4	21	91	12	6			1	1	
O	19	17	28	26	16	6	5	5	4	1		22	33	104	4	29	7	58	73	12	3	5			2	9	1
P	30		1	16					5			8			31			34	1	3	19						
Q																					29						
R	74	1	12	10	94	1	12		45	1	1	6	15	11	43	7	3	10	10	15	9	6			1	1	
S	32	2	18	15	57	3	2	4	41	1		5	7	5	22	26	4	6	10	57	23	2			4		
T	60		1		67				35						56			34			11						
U	13	6	11	5	52	1	3		9			9	6	34	1	3		9	10	4		1			2		
V	12			1	15				15						7												
W	1				1																				1		
X			1						4							3				2							
Y	5	1	3	2	5	1	1					1	1	1	5	2	1	1	3	1	1						
Z	6		1	1											3						2						

2-b. Digraphic kappa plain, Spanish language = .0091 (I.C. = 6.15).



## 23. SWEDISH

NOTE: The letters Q, W, and Z are derived from foreign words in Swedish plain text.

1-a. Absolute frequencies of single letters of Swedish plain text, arranged alphabetically, based on 53,302 letters of text.

A	5,073	G	1,835	M	1,749	S	3,400	Y	354
B	697	H	961	N	4,784	T	4,694	Z	11
C	612	I	3,059	O	1,938	U	854	Å	938
D	2,483	J	289	P	835	V	1,183	Ä	996
E	5,401	K	1,760	Q	3	W	22	Ö	828
F	1,238	L	2,749	R	4,512	X	44		

1-b. Monographic kappa plain, Swedish language = .0626 (I.C. = 1.78).

1-c. Frequency distribution of single letters based on 53,302 letters of Swedish plain text reduced to 1,000 letters, and arranged according to their frequencies.

E	101	I	57	M	33	U	16	J	5
A	95	L	52	F	23	P	16	X	1
N	90	D	47	V	22	Ö	16	W	-
T	88	O	36	Ä	19	B	13	Z	-
R	85	G	34	H	18	C	11	Q	-
S	64	K	33	Å	18	Y	7		

1-d. Percentage of vowels, high-frequency consonants, medium-frequency consonants, and low-frequency consonants in 53,302 letters of Swedish plain text. Percentage of 9 most frequent letters in Swedish plain text.

Vowels A, E, I, O, U, Y, Å, Ä, and Ö = 36.5%

High-Frequency Consonants N, R, and T = 26.2%

Medium-Frequency Consonants D, F, G, H, K, L, M, P, S, and V = 34.1%

Low-Frequency Consonants B, C, J, Q, W, X, and Z = 3.2%

9 most frequent letters (in descending order of frequency) E, A, N, T, R, S, I, L, and D = 67.9%

1-e. Absolute frequencies of single letters as initial letters of 9,603 words in Swedish plain text, arranged, according to their frequencies. (One-letter words have been omitted.)

S	1,094	H	465	P	354	N	217	Å	68
F	766	V	433	I	304	G	188	C	25
A	741	E	418	U	291	Ä	153	Y	15
D	723	B	417	L	261	Ö	96	W	10
M	594	T	415	R	251	J	82	Z	3
O	555	K	357						

~~SECRET~~

2-a. Frequency distribution of digraphs based on 53,302 letters of Swedish plain text, reduced to 5,000 digraphs.

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	Å	Ä	Ö	
A	7	7	2	36	5	13	20	4	6	2	15	29	21	84	8	9		82	30	64	4	23						2	1	
B	8	2			24				3			9			4			6			1				1		2	2	2	
C					4			28	4		20																			
D	31	2		7	117	4	1	2	11	1	2	4	2	5	6	1		9	10	2	3	3				1		4	4	2
E	7	6	2	32	3	15	8	7	6	1	11	32	14	126	6	5		101	34	75	3	8			2			1	1	1
F	11				7	5			7			4			6			21		9	2				1		4	2	38	
G	33	1		3	40	4	6	5	8	1	2	3	3	4	9	2		8	11	10	2	2					7	3	5	
H	25	2		3	15	2		1	3	1	1	2	1	1	6	1		2	2	2	3	2	1				4	6	5	
I	3	3	8	18	10	6	40	1	1		15	29	3	72	9	2		5	30	21	1	10				1				
J	9			1	2							1			3						1	3						5	1	
K	44				21	2		2	4			1	6	1	7	19	1	13	9	16	11	2			2		1	3	2	
L	35	3		8	25	4	2	3	35	5	6	55	5	4	8	2		1	16	9	6	3			6		3	12	3	
M	24	4		4	38	5	2	3	14	1	3	3	13	4	9	4		3	6	5	2	2			3		6	4	3	
N	50	7	1	60	23	15	47	9	40	2	11	7	9	21	16	6		4	53	27	8	9			4		7	7	2	
O		2	31	3	1	5	4				2	11	46	24		3		31	4	10	1	2								
P	9				6	1	1		2			6	1	1	6	11		13	2	1	2							17		
Q																														
R	73	10		24	48	12	6	10	46	2	12	10	13	23	17	6		9	30	23	10	8			3		14	11	4	
S	24	4	2	4	25	6	1	2	22	3	48	11	8	5	26	8		3	18	58	4	12			3		10	9	4	
T	53	8	1	10	64	13	6	9	51	4	5	7	10	9	19	5		20	35	67	9	11			8		4	10	4	
U		2		2	2	1	1	1	1		3	7	3	19		8		5	6	19		2								
V	25	1		5	23	1	1	1	22		1	2	1		2	1		1	5	2	2	1					4	11		
W	1				1																									
X					1											1								1						
Y	1		7	2	1		3	1			1	1	1	2	1			3	6	3										
Z																														
Å	3	1		8	3	2	13	1	1		3	7	2	15	1	1		8	7	8	1	1								
Ä			1	2		1	9				4	10	5	21				29	2	7		2		1						
Ö			1	2			2			2	3	3	1	2		1		48	3	2		8								

2-b. Digraphic kappa plain, Swedish language = .0070 (I.C. = 5.89).

~~SECRET~~

## 24. TURKISH

NOTE: Letters W and X are derived from foreign words.

1-a. *Absolute frequencies of single letters of Turkish plain text, arranged alphabetically, based on 55,206 letters of text.*

A	6,303	F	339	J	27	Ö	276	U	1,698	Z	629
B	1,408	G	614	K	2,360	P	431	Ü	923		
C	535	Ğ	489	L	3,623	R	3,978	V	772		
Ç	382	H	777	M	2,381	S	1,774	W	3		
D	2,296	İ	5,314	N	4,015	Ş	975	X	1		
E	5,839	I	2,060	O	1,117	T	2,480	Y	1,387		

1-b. *Monographic kappa plain, Turkish language = .0622, (I.C. = 1.93).*

1-c. *Frequency distribution of single letters based on 55,206 letters of Turkish plain text, reduced to 1,000 letters and arranged according to their frequencies.*

A	114	R	72	K	43	U	31	Ş	18	Z	11	P	8	J	0
E	106	L	66	D	42	B	25	Ü	17	G	11	Ç	7	W	0
İ	96	T	45	I	37	Y	25	H	14	C	10	F	6	X	0
N	173	M	43	S	32	O	20	V	14	Ğ	9	Ö	5		

1-d. *Percentage of vowels, high-frequency consonants, medium-frequency consonants, and low-frequency consonants in 55,206 letters of Turkish plain text. Percentage of 6 most frequent letters in Turkish plain text.*

Vowels A, E, İ, I, U, O, Ü, and Ö = 42.6%

High-Frequency Consonants N, R, L, T, M, K, and D = 38.3%

Medium-Frequency Consonants S, B, Y, Ş, H, and V = 12.8%

Low-Frequency Consonants Z, G, C, Ğ, P, Ç, F, J, W, and X = 6.3%

6 most frequent letters (in descending order of frequency) A, E, I, N, R, and L = 52.0%

1-e. *Absolute frequencies of single letters as initial letters of 8,016 words of Turkish plain text, arranged according to their frequencies. (One-letter words have been omitted.)*

B	1,078	A	508	H	404	Ç	123	C	84	Ö	44
M	571	S	442	E	366	N	119	Z	74	I	9
İ	565	T	434	Y	339	Ş	110	Ü	72	J	5
D	541	G	416	O	298	R	102	L	55	W	2
K	513	V	409	P	148	F	97	U	46		

2-a. Frequency distribution of digraphs based on 55,206 letters of Turkish plain text, reduced to 5,000 digraphs.

	A	B	C	Ç	D	E	F	G	Ğ	H	I	İ	J	K	L	M	N	O	Ö	P	R	S	Ş	T	U	Ü	V	W	X	Y	Z
A	7	23	10	3	30	3	10	7	8	18	9		1	56	42	28	90	4		11	89	29	16	24	1		12			27	14
B	25	1	1		14					42	4							3	2		1				28	6					
C	12				18				1	7	1			3				1							3	1					
Ç	5	1			6					11	3			1	1			2							1	2					
D	53				4	62				41	18							6	1		1				12	8				1	
E	8	18	15	7	32	5	5	10	8	8	7	1	1	43	31	31	47	4	1	3	99	34	11	62	1	1	16		19	4	
F	6				5					5	5			1							3			2	1						
G	6				15					13	1							2	10		2				1	6					
Ğ	2			3						14	11				3						3				7	1					
H	28				1	9				1	7	1		1	2	1					2	2		2	4	6	1				
İ	6	17	4	10	13	4	4	5	9	10	8			29	61	21	88	3	1	3	71	30	26	16		1	4		26	14	
I	3	5	1	2	5		1	2	7	3	4			12	14	9	57	2		1	18	8	14	4		1	3		6	6	
J	1										1																				
K	44	5		1	4	19		1		1	27	11		8	14	5	1	15	2	1	7	4	1	19	13	5	2		3		
L	77	4	2	1	16	106		3		2	32	13		4	12	26	1	4		1		2		7	10	3	1		1		
M	46	2	1		2	54		1		1	43	14		3	8	2	1	6		1	1	2	1	1	12	13	1		1		
N	33	20	9	3	56	29	3	12		8	43	24		9	19	15	3	6	1	1	3	16	2	9	17	5	7		12	2	
O		1	1		1		1	1	3					9	27	6	19			4	14	4	1	3			3		2	1	
Ö									1						2	1	3				9	1		1					5	2	
P	13	1			1	2				1	1	4			6	2		2			2	1		1	1						
R	58	16	2	3	26	37	3	5		5	62	22		10	18	18	4	6		2	3	7	4	18	14	6	4		6	2	
S	19	1			20					33	21			3	5	2	1	10	4	3	1	2		17	10	3	1		3		
Ş	8	3		1	5		1			7	6			5	9	11		3			1			17	2	3	3				
T	42	3		1	2	39		1		2	48	16		2	18	14		7	1	3	4	1		8	6	5	2				
U	4	4	1	1	5		1	4	7	6	2	1		6	14	14	30	1		3	15	10	5	7	1		4		3	5	
Ü		1	1	1	2	1	1		1	1	1			11	3	5	19			1	8	4	6	3			2		6	8	
V	12				39					2				1	2	1					2				2	4		3			
W																															
X																															
Y	43	1			3	26	1	1		6	7			1	9	1	1	12			3				6	5			1		
Z	12	2	1	1	5	8		1		1	7	4		1	4	3		1				1		1	2	1	1		1		

2-b. Digraphic kappa plain, Turkish language = .0065 (I.C. = 6.25).

## APPENDIX 7

**PROBLEMS—MILITARY CRYPTANALYTICS, PART III**

The problems in this appendix are grouped into ten sections, paralleling the sequence of the text, with scopes as follows:

- Section A—Simpler varieties of aperiodic substitution systems
- Section B—Ciphertext autokey systems
- Section C—Plaintext autokey systems
- Section D—Systems with long or continuous keys
- Section E—Cylindrical cipher devices and strip cipher systems
- Section F—The Wheatstone cipher device
- Section G—The Kryha cipher machine
- Section H—Key analysis
- Section I—Teleprinter key analysis
- Section J—Cryptodiagnosis

The portion of the text which should be read by the reader prior to solving the problems in each section is indicated in the section heading.

This set of problems is also available as a separate publication in a loose-leaf book of ten lessons. This book, entitled "Problem Book—Course, Military Cryptanalytics, Part III," contains the cryptograms which for the most part have been arranged in a form suitable for worksheet use, obviating the necessity of recopying; frequency distributions and other aids, where applicable, are also appended to reduce the amount of time spent on the purely clerical labor incidental to solution.

* * * * *

DO NOT WRITE ON OR OTHERWISE DEFACE THESE PAGES!

DO NOT WRITE ON THIS PAGE

**PROBLEMS—MILITARY CRYPTANALYTICS, PART III***A. Simpler varieties of aperiodic substitution systems*  
(Embracing Chapters I–III, inclusive)

1a. Solve the following cryptogram and recover all keys:

LQRSR	EGEAT	PDMZL	KAHPB	BTNPF	EQPRU	KNCCU	IHOSE	MVQGX	NDRCB
QPUTL	ARTQE	POLBV	UMFAL	KKLNV					

b. Solve the following cryptogram and recover all keys:

UWDSU	BYNPZ	QAWLY	NSLVP	MILCU	DLLUM	VYDHR	LMLBW	GWCJL	FCRPV
NYZRF	FRAIG	TPFST	ZOUPC	RPYDN	ZPMRJ				

2. Solve the following cryptogram and recover all keys:

XQGZO	IDQDE	LSHUD	HTGBZ	AWGVG	ABNUW	ZNKET	ZKTEY	ZIWYX	LVJSJ
AAFAJ	BAFEB	ATCJR	FTWPC						

3. Solve the following cryptogram and recover all keys:

DPPWJ	VAOYO	APVUZ	NXACE	ZAWTP	EAHQD	NBRPQ	DLUDE	IDRCZ	KLNYQ
CGGWZ	OQXIE	QRCCH	MQUAD	SVQMJ	EDWIX	LWTZL	NXKMA	SIZBD	YZVIM
SLYYP	XFXXX								

4. Solve the following cryptogram and recover all keys:

MMKWV	IDQGW	WXGRF	XZBGN	WNNRD	FUVPX	CHOXC	EXKYK	HBXWA	NODJB
GWXLY	LAILM	HZHSY	JGOBA	ATYZU	VSFVA	KGJUN	VHQWV	XJFTI	ZZNYH
ZLIWX	BBXQM	NQAYZ	YVSBG						

5. Solve the following cryptogram and recover all keys:

ZXUSL	UHKTG	CQSWR	YZLIG	KBSAX	GXSAA	LWCNL	MAZWU	GOFJU	XTTUX
LITJZ	OAWYX	LIRXU	XEZZE	ZGWUL	ASBMN	IJJAJ	BPEGJ	LSJKZ	RTSUX
URQCU	ABOUT	LIHYV	INVMO	BDGYD	QFHNA	PHWTV	JGTXX		

6. Solve the following cryptogram and recover all keys:

LDQUR	PIWIIYCNF	BCM	QFPSOAX	YQP	RCVDWPNE	ZIGAO	MGRKQSBDK	XW	WOJL
DHCS	RJUQQJUODQ	OKRDB	IHAHD	ACDO	TRHP	ZTBPN	QYUB	JRDUUFTGE	

7. Solve the following cryptogram and recover all keys:

NAZAE	ZANWJ	FWBWR	JKPVS	EOLJC	XJNZI	MAMBC	ONCME	VJLKL	VRTSQ
XLJWA	BMPHJ	ZXAII	JKAIA	UJBSP	YBJAZ	SJOXO	TJBYI	YHDYQ	JFDJD
ALAZT	JAIQV	EQPIP	JIDUM	JXATM	HSCUW				

DO NOT WRITE ON THIS PAGE

8. Solve the text of the first of the following six messages and recover all keys:

Message No. 1

KZUSM	APEIL	BIJUT	JQPAX	TDHOG	SFGRU	WRRML	FXHGV	WYAFP	QEHUI
SYXAJ	ZOOYH	MDXAY	IEYUZ	DCIGW	QBKAD	ERIJU	TNNAP	XYBSJ	LYZCW
ZBXAG	SHVQT	NWGVY	VGABF	ZYLFV	BLXLV	GAXXX			

Message No. 2

BZRVG	DABMH	JKXTJ	VPRCO	DTCHZ	IGLPZ	ZUURE	GFZXG	YZLGO	VYRZA
SPSHE	UGAVA	XAWJO	BZXYI	IYEUZ	GBKDD	MDPUJ	ANPBU	BNZPX	IPYBL
VOAEA	KUVCF	GVYXX							

Message No. 3

YUDLV	AZGSD	MODJZ	TIIPM	CGPYU	GKKGC	AFJRX	TGPZY	VATPQ	EHUEH
BLLOK	YTNXZ	XTXRR	XSGXK	ICPDF	EIVBI	HJCNM	YXZYL	RVHFN	ZXZDA

Message No. 4

KVBXL	NZAQB	LIESZ	JFKTI	IPYAZ	DBC GP	YUXZG	XFLEI	ZGQZB	XAGSU
JLTEW	JOXXX								

Message No. 5

MVWAV	GSSJO	VCOWM	QPZXG	YTLHG	YUXNM	FLXDH	GOVYR	ZBALP	HEULQ
LMLJE	XONEX	ZQDRK	GCKGW	KIETD					

Message No. 6

LG AID	QS UJK	DPPXE	RGRTK	KCQTU	NIUQG	ZFXHC	GZLIK	XAKHG	XUISJ
JWE00	NGIXN	XIDZD	XHGQX	LNDSE	MCDIJ	QZGYP	PXAWI	YFLXY	VVFBA
GHUVI	NHMSL	TYLGA	PYLYZ	FNURZ	HZGXB	AFEIJ	DGJPU	XIICI	

9. Solve the first 100 letters of the following cryptogram and recover all keys:

BYDEL	VRTFG	BZNTG	SUCXC	WNFYK	LCQPB	EXIJN	QZHIW	QXVPN	ZKMDA
GFLML	ZEHIF	BJBHZ	VBYHR	BGHSI	FXCCW	RHQJQ	BXTSG	QMCFG	IKOHB
IFLIQ	RUF RP	YKJJD	NPGIE	KMMFB	YDELV	UDANS	SCCKW	YCDNQ	JJQP B
QMSMI	WMHUJ	QPMSX	HEDVJ	NREQD	HFRJT	VD TNS	SCAKE	WJQOK	BGTIJ
RNJHS	UQPWS	ENZVE	DSTWN	PMGLM	LZEPQ	HSFKW	YAXJB	WAVDR	RNDTS
UAYYA	KEWKD	BGCDV	IOJRR	PMHUF	PQSEE	VANDW	LWAHE	SMKIP	FRJTV
FZHNZ	HFBZG	SLIZM	WNDRY	GQKQB	SMZTS	GIKOH	XUAWX	PLEKM	FAVED
MLPWF	FGZJP	MGLEZ	HMMHD	PFIZV	GRNKF	DESJC	LLCKE	CXWJK	DYBHS
CKDMB	ISNLH	ZFSPC							

10. Solve the first 100 letters of the following cryptogram and recover all keys:

GVFGO	PIBEV	IIPOF	BHHIG	CWCPG	WXBTH	VKGUC	UBTXS	PWVEE	VCLOV
LLMQX	FXNQZ	XEEPG	GQLVP	BMGVV	KDJHH	MGXYC	RKPTJ	XSRCC	WEVMR
ZMCOS	SHNBZ	BMNXE	RABKV	PGKVU	BAKCU	GFBXF	UWDPC	GWSKR	GWWAH
TXTKH	ZKCVQ	FXFVQ	TUMQO	VQDNF	PWCPG	BQOOV	GNUVP	RVCZZ	IKOHC
JXXRG	THBTV	YOVBV	GEOZT	VEENG	BYEJ	FKSBQ	AKDGQ	TPNBW	AFXPS
CTFWN	XFFZT	ICPXK	OLSGU	BTGTG	NEXQK				

DO NOT WRITE ON THIS PAGE

11. The cryptograms below were enciphered with the same cipher component as that used in Problem 10, but with a different plain component.

a. Solve the following and recover all keys:

ODQYC	JSTOE	WRMYT	LYCVW	JZHDX	HNJXP	DEZDD	VGSYH	DDLQG	XEOIL
LIMIX	VUYWC	ZMTJS	ZXCEP	V TSAI	GTVJI	DQTRT	WZVRT	QDYNH	OYSOR
ELIMS	YYFBB	SZGOZ	IYNET	ZMGAM	OCUZF	LBFUF	WTJMN	WARCB	ZNLRQ

b. Solve the following and recover all keys:

QOOEF	JBQFF	OVNWQ	ZZKDU	THYQB	KYMLR	RORLD	ZBYMB	FESFY	LQYXQ
JVPEX	PHQVW	JAWBT	HLYRT	HYZDK	WMQGO	LINOL	CRREZ	GCOQU	EQIHQ
EXZAZ	WWZIM	ORSAE	XQONE	SRJFY	SLNSZ	TQQSM	UMQUF	WTARB	FPGBN

12. The inventor of a cipher device submitted the following partially deciphered message produced by his device. Solve the remainder of the message and reconstruct the principles of the device.

TGVCX	GDDAG	HDYAE	OFXVL	VKPUJ	DZWLS	LJWBA	BLAZO	OQQGP	UWHCQ
WAR*D	EPART	MENT*	U*S*A	*WASH	INGTO	N*D*C	*IF*S	PEED*	IS*NO
OUNQI	TXKFK	PFFOF	WAGIF	RYWOJ	VQGXF	ZPHGJ	ZJLPD	GZXQZ	KTMRT
T*THE	*FEAT	URE*T	HAT*O	UT*WE	IGHS*	ALL*O	THER*	CONSI	DERAT
PUTNX	HMXNH	LQDNT	JERCW	XQLFS	IQGNW	IGEKG	EKVEG	ZMSVX	YTDLL
IONS*	IN*A*	CODE*	MAKIN	G*DEV	ICE*I	*THIN	K*I*H	AVE*A	*LITT
MPJIT	YLZPU	STPCM	LBUKK	HXQAE	KWWRP	FJIFV	LDCOW	FNBEW	AKNVJ
LE*MA	CHINE	*THAT	*WILL	*COMP	ARE*F	AVORA	BLY*I	N*SIZ	E*WEI
CYJVC	ILXND	TDLAD	RHYTT	DBZCT	VXSTW	CHRSU	KIQJL	HWCNW	CTNFK
GHT*D	URABI	LITY*	SECRE	CY*AN	D*COS	T*OF*	PRODU	CTION	*WITH
NAVNI	KYGOY	ETJDY	DQGJW	YNXCP	QLMZP	FSJHF	MVLFR	IWNJO	KUUCZ
*ANY*	KNOWN	*METH	OD*OF	*DEVE	LOPIN	G*COD	ED*ME	SSAGE	S*YOU
MBFMQ	KEAFO	IFJNJ	GCRDF	AWEQE	FQZEA	HJLPB	LKDPZ	HSRPM	TXHTX
*MAY*	TEST*	ITS*S	ECURI	TY*BY	*DECI	PHERI	NG*TH	E*POR	TION*
TJPCM	TEUAI	VVEZK	RWOVE	CGVLA	KVBWQ	YTJIV	LASZS	CGXBO	AHFXP
OF*TH	IS*ME	SSAGE	*THAT	*REMA	INS*U	NDECI	PHERE	D*AND	*AFTE
UBJXG	ZPQER	LGMRC	PKRHT	UXCLG	BRKNV	KNOCE	TNRVD	WIGQJ	KYLGJ
R*YOU	*HAVE	*DONE	*SO*I	*WOUL	D*THA	NK*YO	U*FOR	*YOUR	*OPIN
YDBYP	UAXZD	SPRBC	TDGRX	TSLOM	YPNAW	KOKSQ	GCWMQ	EWCGG	LCOTB
ION*A	S*TO*	ITS*S	ECURI	TY*AN	D*ADA	PTABI	LITY*	TO*AR	MY*US
YWYFF	LETZK	AYBZG	DTALB	PDHPR	VCUSP	ALNRF	CONEH	PNKWF	TOXMW
E									
TGEVN	ZVFN	DGUWF	KMJPG	BTSVY	VDPQX	AHGYL	IROLC	PMFLI	TVQQT
URJUQ	LTWWF	YRBGD	HVOYF	HIBFH	AYFFA	QFJYL	SGKDM	MAKBO	HBMCC
SUXRT	LPIXG	CKTNN	JTRNM	ERTIZ	ECZGO	IFUIP	DOVfy	JFBKK	SXSYU
HLXNA	FSSYL	BYXXN	MLFQC	XPYOE	MIWBV	ITBNK	YQWWF	OLGDV	IYFJA
ECAMB	SFWSL	SPDSA	GZLWZ	HZPHC	ZUMHR	CXJQN	CBINE	TJETR	WIKCW
UTJGV	NGEKB	WAGES	ECZSL	SYLVL	XZXJ				



DO NOT WRITE ON THIS PAGE

B. Ciphertext autokey systems  
(Embracing Chapter IV)

1. The following cryptograms have been enciphered with introductory keys up to 10 letters in length. Solve them and recover all keys.

- a. UCVOM ESLVR VFMKJ LKYNJ UQQEL YXNLQ DHYGK RLRRL
- b. GBBRP CPCTE EOYZS QLBTB XHANN UJGNW BXMEL GJDPK FNSJQ GPMLN
- c. GDKCN BNIGQ OJHJI UCEPY WHRFC PGIXM KJIKT RFCEP AUBDU IFFTK  
YNLCE MNYWA

2. Solve the first of the following administrative messages and recover all keys:

Message No. 1

TRXPA	AXOAC	IMCGA	QMJGE	HFBEZ	BUWPJ	DIEJH	LZPEG	VAXRH	CIIUY
PODTG	EAGKT	ONPIS	DJOTO	DYYKN	MVYWQ	PIBIO	EIIOT	MUSME	MBPND
IPIPP	YVSVK	TVUBT	OSXBU	KWDZW	UBUMA	CCWZH	ZKFVT	RLCFS	VNRNB
MILLY	WIMVV	XSNWQ	QMGX	QSLQS					

Message No. 2

LRDJG	CGFUB	BGGTL	OEXHQ	ZPOUY	GHFSS	DACGF	KWZHZ	XSFFF	IYDGS
DGHNH	RTPOS	MEVRL	TTRQP	YZPEQ	WVYKI	WYNRR	XQNWG	KKJUW	VTKTX
XGLSW	RQBUT	VSTPO	GBBWS	EMJHU	VHLJX	BUKWD	ZWUBU	MAJLO	ORXYN
SACLO	BUMIX	XSFFF	JLVTM	RXDVA	IDYDB	BMSBU	MMVTW		

Message No. 3

XXPPB	WZTYC	DMMZA	DEQBY	PKDZT	LJOSM	MBFCX	CDYCC	DDQHC	WZXGJ
HLEOR	XSVKT	OCUVM	MQCGR	ONXAV	AIPPZ	DJFDD	PNWXX	YKXXH	JLWXR
HFKVF	YPZRR	POUYG	HFCUM	SXCGQ	PZVVK	TLTRC	YDLIM	AVJWW	UIMJI
MAONG	UCYUU	CBTMX							

Message No. 4

PISDF	PNROO	NWOOR	QAYXQ	SXHKK	FMOAL	EQLSG	CFUCW	ZKZHZ	NWVOI
VJPIX	ASEUV	JPEVS	UBUZH	YVVFU	ONNPB	FYKNO	PKQKA	ONIMO	SMMLR
LCFDR	OTGEB	FGDAA	YVYPZ	PUBFC	FZPOT	TCQAL	JKXAN	CXAAC	

3. Solve the first five of the following message beginnings and recover all keys:

- |           |       |       |       |       |           |       |       |       |       |
|-----------|-------|-------|-------|-------|-----------|-------|-------|-------|-------|
| 1. BFRJV  | WOAPR | ALFSV | EAAHC | . . . | 14. BZVSZ | DOHSC | FXBOB | ZDFCR | . . . |
| 2. ZPTQI  | UEEGD | PYENI | UBZZZ | . . . | 15. RADHI | UZFJF | JZPHP | MBLME | . . . |
| 3. RAEJF  | UZTFL | RLUEZ | GYBYK | . . . | 16. VMPHE | UMIBF | FORRY | KIHJS | . . . |
| 4. JPQTS  | WWCXL | XXYAD | WPGTH | . . . | 17. RAQHI | OERZT | XWCJG | APOFS | . . . |
| 5. BWRJK  | ZJHDW | OGQEJ | NWRXV | . . . | 18. IWGNP | ZEOVP | RGVLY | EIRER | . . . |
| 6. RACMZ  | AYJAT | UBBWO | WGJON | . . . | 19. THPMZ | YJTHK | QQPAQ | XDYZM | . . . |
| 7. JAUWP  | DPRZM | RWEEQ | KZTKW | . . . | 20. RAIBW | VIFVV | BMSMD | SQCGR | . . . |
| 8. BZFJK  | BCSKL | SORIO | NXYEA | . . . | 21. KWCQE | ZBBOD | GGVUF | JDVLY | . . . |
| 9. UPTQK  | SIWLJ | QCXXT | JUGZJ | . . . | 22. PVRQT | WHOZK | KPNQM | IQZGU | . . . |
| 10. TACMZ | EEJEK | QNUQL | XXYVK | . . . | 23. MMUTS | KPRLK | NRIGN | BMKXH | . . . |
| 11. GPTBK | UMWLA | QJNNG | FAWFF | . . . | 24. OVCIS | AAZDP | IHRRU | QRNKE | . . . |
| 12. GPSFE | AEGHD | NMGHK | CCOHD | . . . | 25. KWRHI | JLAYU | XKTMM | TNZKD | . . . |
| 13. TAVHZ | HJJLI | STUSF | ORUHP | . . . |           |       |       |       |       |

## DO NOT WRITE ON THIS PAGE

4. Solve the following messages and recover all keys:

## Message No. 1

OHGWX	HRLDM	HJQMV	TKJLZ	QJNHE	WPEOB	GTUSI	RGAEI	WPEXE	ZFQST
CBIAO	RLNLI	PRGIA	HLNDF	EQJEX	ZRLXB	ZVAXE	CZYEC	VJSDY	AGYRA
KPVXX									

## Message No. 2

CFENB	GJUQF	WKWUA	DZQEX	ZPSKP	YTXFH	TENOD	MOCUV	OSIKJ	KZHCB
GWJYT	CAJNX	MRJPB	XQSAH	DVZQM	FNSOD	HMKUW	KTCHJ	TPCIA	HCAJT
SKZHT	EZBGJ	NPBAH	DRXDY	MAKYQ	MBIGH	SCZQZ			

## Message No. 3

HSFRM	GGPNG	ENKQX	ODAQM	ICWIV	ZLOQM	LVAMQ	MKTCTI	XPCWK	CICLW
ZSLXI	GYEOB	YPYHR	UYHXD	JCUWL	UNWBF	XXXXX			

5. Solve the following isologs and recover all keys:

## Message "A"

ETGTU	DVUAF	HDLPT	URNGK	ZNNSY	OQPHP	DINHW	ESWCV	FHJYK	UAKBK
AYCAK	SIEWB	UPWYH	HJXPO	YJUTM	FIDOH	BXIML	XZNHI	WZRBX	SNUID

## Message "B"

FIKKK	YWRWD	LJJTP	IEYZH	JFVRG	CYEMW	SHLYS	XJCQR	KGJSF	VLEGR
DCGHY	LFBBE	PKGTP	HIHJW	TSGAJ	FYROJ	PTLXN	XLPSB	RRUZF	XDYRO

6. The following isologs have been enciphered by two different pairs of primary components and with introductory keys of from 1 to 6 letters in length. Solve them and recover all keys.

## Message "A"

FAPDH	VDHVV	WSKZT	FNPNR	IDSXP	BVHIQ	ZHWKP	WNQJD	ORPSU	XQQNQ
EPLYJ	HXBTK	VEGAP	WWTGQ	SQIRV	YDPEE	MVFYR	UPZKX	GMTAU	XVJSQ
LUAAA	BNOGX	XOJGU	QESNP	KKNUQ	DQWKY	SBHRY	ZWYIR	KKXQC	ISEYC
WNPJV	CLCVZ	IBJWD	ZWJJE	NJTNW	PNCUA	XPJPF	UANMZ	QXJDL	AXEJL

## Message "B"

TNSDI	ZPSVU	IEGMJ	AAKND	WRERC	TCXKR	TYROK	SCWRU	LFCQA	HIFMF
EHMQL	ZRUBQ	CDIQL	QMPEQ	ZLMBP	PWATF	QZMZZ	KLZEE	YLYHR	FAZYU
AQRZI	LDTXT	RLFME	UABLO	MAETL	QZLFP	OSWQT	YRVAH	VSRHF	QBVID
XTHGP	JAVOV	AZFVE	WZOXV	IDWCH	PGTEF	FGRZM	UDVSZ	WEZEX	DNBQQ

7. The following cryptogram has been enciphered with an introductory key up to 15 digits in length. Solve it and recover all keys.

33168	07421	39672	85642	55456	53024	12093	91140	52025	54945
16501	86151	71625	84239	07039	62410	25357	14058	22910	37974
40108	39549	08168	25141	70324	09859	53483	05604	61895	00807
00537	14239								

## DO NOT WRITE ON THIS PAGE

8. The following teleprinter intercepts have been enciphered with introductory keys up to 15 elements in length. Solve them and recover all keys.

- a. 8EN55 MT5QH MUHHQ 5QM4F B7ES0 OCDC5 CMKDY CD97Q CL9D5 05CP5  
4D7KK UBOUG IXCKG UVCEP QMNPB BM4BF UVW53 WAXW9
- b. K8AZE J7GQK GYV7Y CSBA0 V7VFP XA8RM UY7U9 8HRP7 3TNBP 3XUM5  
3WRBP 3XHE8 TN3HH AHDH5 4SPFR OARF7 B34BV FP5SB 0IM05 57NU5  
HKPNQ OWFP7 VVKSE UU0U0

## C. Plaintext autokey systems

(Embracing Chapter V)

1. The following cryptograms have been enciphered by standard alphabets and with introductory keys from 5 to 10 letters in length. Solve them and recover all keys.

- a. YEZSM ACHYE OVSES CGREK UVMCW OKUTS ATRAG SSSMQ QGHPD AGWIV  
PNGKH QVMCU JXOXJ LIGYE BFPZL
- b. MAAAA CRFHX ZSHBM KKVAH UHMZW VLWPS QEGWZ VANDG WFHAN OZJWJ  
ZLBJU BKPVH DNAMJ AAQEL MASCA GSLBF RDIKV IUAEG
- c. GYGJN BKGCN BYYPX KYRSN TYLTY LXWDG WZEZQ IAADN PLMQO SYSKB  
NFQRC BMHBH CCCCC HYKCM PSIFF SQSLJ YRCQF WBNBZ WTKVI ZPVJH  
URPEM VTREM DDJMU PVTDF SLPGT JFFTA HXVQC INRQN QYRQH SZGEM
- d. UNFLK BXYTG NNOMC JXHJE IAOMZ CRRAN XGDPG HEDML CIQRL VFDRM  
CZNGW EZRVC ELKDX KMFHL LRPNQ TKXYQ SGVFH PFXDT QWDCG NPVMC  
EEZZO XQDPD FNJPS GRRCH GMOHR JVWVG DMWZS PLXXH LSPYB GNMJR  
EQGIF UYCNT

2. Solve the first of the following messages and recover all keys.

## Message No. 1

FLZPS RKVPB WMBHZ ANVDD DVAID WCDHX DOORS AHCNT TRLUJ MTKOL  
RZSKJ HUUQB AVAYJ OMMTB TIKHU ZQMIU UTIUP IDYBV FFWMR KQEBW  
KINQI QDRUC TQQST SKTKM PFTSS

## Message No. 2

CDTJS TCUIN OSUZB ERDVS PLZSY FFSDL VDFDL ZPSRK VPBWM DHCZU  
PSRQQ VHZDF GZHIH LILIF OPUHB YOCEU SAHCW OQQIL UJMTK OLRZS  
KNRFA DGZDS ROQDM OLYPB PJHKC

## Message No. 3

CDTJS TCUIN OSUZB ERDVS PLZSY FFSBP YFIZO QILCZ UPSRQ QMAOI  
HLILI NTBBQ ISBOP UHBYO CERCC DXONE ZMFAD GZDSR OQDFT UQKTC  
JJQNM OLDDU KXDMI UZUKQ SBTKO APYED VSQQS TSKTK MPFTS

DO NOT WRITE ON THIS PAGE

3. Solve the first five of the following message beginnings and recover all keys.

- 1. UONEK NUCSJ XLKNX UVXHF CWRGL . . .
- 2. SHCEX RHETR QIDRO ZOHEN CKWCK . . .
- 3. LHIWI OYQSE EYRXZ RGNIB ONNFP . . .
- 4. VMUPF IGMEE YRXVC ENCRD DSTTK . . .
- 5. UONEK JSDSC ZISCH DITLX CZAKN . . .
- 6. HJRDT BEDRG ULWRA IDXEK ORHBB . . .
- 7. PJFLR ZPPVP JLXMP BXERB ILRYP . . .
- 8. SHIFI UQQXG BXBOT GPJLX MCSRE . . .
- 9. SHCEX RHETR QIDRV PGZWE IAHPD . . .
- 10. NSCZW BEPJS BCVSZ DLKCY BLGEC . . .
- 11. KOKBB OXKDE FCHDL ONYQI EIXIQ . . .
- 12. NJIQO CQRES BLRMV REXYJ ZVWIO . . .
- 13. PHSFF JYVXN OMFXE DSJXL KNYFD . . .
- 14. NSUPY DDOYF VREXJ XQEMJ PDZFY . . .
- 15. GJUDQ OOSOX CFEPD HNHZF NCPSU . . .
- 16. HJMCQ RENSO UCPGX JSWYB LUEUV . . .
- 17. JRDSJ XLKNZ RJCSR CAQID RVPGZ . . .
- 18. LIUWW TEILU RHBXS OIUJM OUVHH . . .
- 19. ZXUQD LCYUO VQOZW HITWH SKVMV . . .
- 20. SHKBD XIVZK VHVOH MFNOR QFEVH . . .
- 21. VMZXR BMNCQ MOTYX LYGLQ HWCYY . . .
- 22. BJAAR PNHBH WJBBV IJMVV GRWEN . . .
- 23. KODLH ZMTXV KLWRA TEJYF VREXP . . .
- 24. HARUL WUCXW IKWYB IHYSH VVGRW . . .
- 25. JUMMR CIQRW FERBE WLROO QSBWZ . . .

4. Solve the first of the following messages and recover all keys.

Message No. 1

TSGYX	EHEOP	EFYNJ	WBKFB	FGRUV	IMCWH	WLXXG	PBQQX	PKHHN	AZGSZ
XAYQX	YSHXM	NJPXX	BIGOP	PSSUS	AJZND	JUKWR	UYFYN	JWBKF	BFRGU
VIXMR	QDDVE	UFPKL	ELXVP	VLAUL	TXDVL	BWPVW	YZWHJ	MFQIV	GFHYB
KIHJX	MZXFk	BFRGU	VIIUP	QCVGS	QOFKK	AYCDL	BOCZV	FIXIK	DBQFT
RYGWU	OTNMZ	UHDOA	QZMFS	HEJZL					

Message No. 2

BQGYG	MEQMZ	KMXYX	ZFBHJ	ZZNXO	YDAGX	EBPRY	GFUTL	FIAHQ	FJBFG
RUVIZ	ARBEZ	LHOZA	SYETQ	ACQKB	TIHFH	AZFYU	DVPKZ	BMLQX	OLAQC
RTLfy	NJWBK	FBFGR	UVIYV	QSIzN	NOFNJ	ZFLXR	DUCAS	YETQA	CQKBT
IHTZZ	IFMFI	MTSBA	HLGFI	XEBHX	FZQFP	MFQXX	BDCTY	FTGOP	PSJWY
NHKIB	UMYWQ	ZGTZQ	KBTIH	KCZWW	FIEAO	MPZAS	YXNPY	ZVNUM	TFGBU
GQTRL	WDZPZ	OXMMF	QEHUY	YXUGQ	ROVNW	YBOYW	SDNVQ	BTIMY	WZMZU
HDOAQ	ZMFSH								

Message No. 3

TSGYX	EHEOP	EFYNG	TRSVU	YWAFa	HDDYP	BYIIH	MUCZQ	UVQBT	IMYWI
IWYAG	CRRDG	VOYFJ	DLYAO	FYASD	IGASC	AWESE	LFNYY	TFBHI	ICUFS
GFIFS	WIIEY	WQZWW	EXSBD	IPNMZ	UPCAR	WBTZU	UPLSU		

DO NOT WRITE ON THIS PAGE

5. Solve the following message with its compromised plain text, and recover all keys.

QSOGL GMXWM YGVVF MHWOL IQBKM RDTHK CCTNX IWSTX HIGCX DNMYJ  
MORNI NGREP ORTFO RFRID AYSIX TEEND ECEMB ERHAS BEENS ENTYE

XZZTH UQTUY HAVZN AEZEJ LUWWR  
STERD AYTOY OURHE ADQUA RTERS

6. The following two message beginnings are suspected of containing the opening crib indicated. Solve them, recover all keys, and reconstruct the plain texts of the 10th group of each message.

Message No. 1

JQHBT JECFL LQHBH CYKEU QARID MODXV MFBHY VZQKE KRNSH USQES . . .  
MORNI NGREP ORTFO RSATU RDAYE EVENT EENDE CEMBE RSTOP

Message No. 2

BQZQO XTLWR XCCBT SRWFV FOJPT DKPOY DQKWZ VOOGT CXEDH ZAMTR . . .  
MORNI NGREP ORTFO RSATU RDAYE EVENT EENDE CEMBE RSTOP

7. The following cryptogram has been enciphered in an additive system with an introductory key up to 10 digits in length. Solve it and recover all keys.

69517 50891 63848 42537 44276 24220 18799 65167 15251 60727  
83342 97642 09067 07673 63920 07287 00072 44040 22166 84144  
00631 13844 08604 03551 88204 38282 40100 41101 06711 38523  
20147 28192 66211 62282 78362 58083 86127 23459 73226 41762  
31742 61378 48093 48606 88625 07070 61132 92945 11100 07109  
65238 68252 48629 82383 09012 89824 79894 07748 42123 21873  
04110 10671 13892 32534 97432 98676 58227 64061 12268 66058  
28731 62986 88045 67221 40642 62528 33096 40770 07922 50015  
62562 78475 63808 38618 98006 67158 56777 84561 15586 01162  
28272 08420

8. The following teleprinter transmission was enciphered with an introductory key up to 10 characters in length. Solve it and recover all keys.

FIW8A CHN8Y DSX8L 87W89 NONN8 CZXGR XT00V EPMJH 8BVVY ZADMB  
NFEEC VVA9A LBSY5 VVQTU PEOXQ WUMV4 YGXDM RN8YO D3M84 XR3UR  
X8QGI KC4GJ 88BQN NXPID LBZNC Z3G8R JDSXN TWNMJ DH40B TTCBL  
UTQLQ S9VY3 Z8BGU SIXGP R8LAY V5MDI 8M3TQ V4WEU VX7TJ GNNQA

9. The enemy is using a plaintext autokey system with a multiplicity of five-letter introductory keys in conjunction with an unchanging pair of enciphering components, the plain component being the CARBON . . . XYZ keyword-mixed sequence, and the cipher component the HYDROGEN . . . WXZ keyword-mixed sequence. Solve the following cryptogram and recover the particular introductory key used.

IGLKI USMSB SSFPU XBOWT VPKSN ZGMZU ADIHM WCWBE IWDCA YGUFB

## DO NOT WRITE ON THIS PAGE

## D. Systems with long or continuous keys

(Embracing Chapter VI)

1a. The following cryptogram, suspected of beginning with the word STRONG, has been enciphered with direct standard alphabets and a key from a literary source. Solve it and recover the key sequence.

SFV FV IXOMK FSQLN PHUSS ZKIAW IIWAF ALNAP ZVCBO AZLQM WEQPF  
KQWCU TSDMX SGQXD HBTZR OYKVR TKSIR UCUDK XIFFJ SDUBM RKBEM

b. Recover the plain texts of the following two messages which were enciphered on the Hagelin C-38 machine in flush depth. The probable word NUMBER is suspected to be present in the first message.

## Message "A"

YRWLY MYIEE QDJZF WFDXK CXZLG ZRRJD MSRVW KIBVL NGOOV WSIGL  
FUWLM LFYMG ATLMQ BQIQJ WHPAM UKCDK PPFUM PRZKD

## Message "B"

XUNEO CCDRV NDJXA ABPVU JMKJS FWXIF QSMBX QGBYP LABOM WHLGC  
PHCJO LFXMV MKWBB LDRFK CTPQK EKFW S PPJVM ENVWD

2. Recover the plain text of the following Gronsfeld cipher, suspected of beginning with the word SUPPLY.

WCWVU BVWBK SGJRF YZLUO NYVOQ NWWYUS ECTPN XFWNQ JVVVL KVGJP  
URAIT TRDRQ LITKS LLPDL TPJRY WCUJQ WDVWF PVKSG JYJRH JDHYO

3. The following matched plain and cipher beginnings of two messages were enciphered in flush depth in a cryptosystem employing a mixed sequence sliding against itself in reverse for the primary components. Reconstruct the original mixed sequence and derive all keys.

## Message "A"

KQMHV OVWOJ KIRGQ PVMO RFPYM JCN GP YPKOI UQCFT ZTJAY QOWPZ . . .  
REFER ENCEZ YOURZ MESSA GEZNU MBERZ NINEZ FIVEZ DATED ZONEZ

## Message "B"

FAYVY JOESY GYNTT SOWYQ GOPEE UTRVX IHFPV EGHV GPJDJ XQHEZ . . .  
TOZCO MMAND INGZO FFICE RSZAL LZSUB ORDIN ATEZU NITSZ STOPZ

DO NOT WRITE ON THIS PAGE

4. The following messages with their matched plain texts were enciphered in flush depth in a cryptosystem employing two different primary components. Reconstruct the original components and derive all keys.

Message "A"

QQDJA	JPXCY	NKQOU	RXLRW	PJUCN	VDDAS	SBLIT	BZJUF	OXDLP	ETHPQ
REFER	ENCEZ	YOURZ	MESSA	GEZNU	MBERZ	SIXZF	IVEZD	ATEDZ	ONEZS
JXTKI	VPLFR	VGOEQ	IDPSV	WMLQN	NGBEB	JZWLX	DQNYI	NNVMO	XFEOK
EVENZ	DECEM	BERZS	TOPZL	TZAND	REWSZ	CONFI	NEDZT	OZHOS	PITAL

Message "B"

KNUGV	VMPKF	DJNEM	JZWBS	YOVOL	XPITN	MFMRs	KXOVN	MREBC	HJIXH
TOZCO	MMAND	INGZO	FFICE	RZSEC	ONDZR	EGIME	NTZST	OPZYO	URZRE
MBBCV	GBZYC	MTCDI	D000J	UGWBP	RUVNR	QYTJO	ZGBNG	OZDKY	UXBOD
GIMEN	TZWIL	LZBEZ	READY	ZTOZM	OVEZF	ORWAR	DZATZ	NOONZ	TODAY

5a. The following are the beginnings of 25 messages in flush depth. Solve the first three beginnings and recover the components.

1. YHWKW RVTTP THRLV GZXEE JNSAS HDVSW GZZVP . . .
2. YHGPL BPHDH CCTMD TOUHU GLDGI GTBJE HZFKO . . .
3. SXKIW WKKKW CQRUV LWYYC KIOFH TMLUQ AZXKP . . .
4. LXWYW EBGKW QAADX VWKNE SMTNP MCYWF MFQKW . . .
5. XXDWM ISKGP FRROV VXYYK VFHYV JSMLM VUWKW . . .
6. LXWYW EBGKW QAADX TKLTJ SQZTI GTBJE HZWJD . . .
7. LXHQI OZZAV XQVDK GCCWK KOLYU LOVLC ZZFGF . . .
8. DTOHP QPZBI KHQXQ LSURA JJXHE QOLYS KKBXF . . .
9. VBIHL GVJCI JZXXS FUQIS JMSYM GALYS KKBBA . . .
10. WPUYA WQUMW ERRKQ MIFUI KNRYU LESPO QUWYW . . .
11. WMYAX EVTTP THRLV GZXEE JNSAS HFCLC VHIZI . . .
12. LXHQI OZZFL FDWZC UIOCJ JEZMX ZILNO VTIDP . . .
13. MLZZP COZVP MAXBP UPNBP HAFYH LXIAU TVEJV . . .
14. QEKYO UZNDC GLCOV LCQWZ KUCGT HEAEF SEYDU . . .
15. KUEKI FZKCR XCEZS GNFTK SJZMI ZIYSX GOGDH . . .
16. DRKRE YVDKE CDRXA UVYUA UVWVT QGDPG PZXXW . . .
17. LXKKW WAZBA NLJYC CKKUI KVWFT WUADC AZIFW . . .
18. KLGHD RFVMN EYBAY HPGFA JJXHX LALWE OFCKD . . .
19. DPDJH OVKKE CSYAY HOPZC KOOEM GNNNW QUWYW . . .
20. VLI GP MFVGR CYRDV KSBNQ FHTFD HWXPL RTBHU . . .
21. NXIYW QPZOI CAFQX SUQUP QMUMR SGJDF SKGJO . . .
22. ZUAYW OVYCO ICGZV LOGNH NMGYD ZZLVZ JZGKF . . .
23. QVWYC WQAKW SEVQX BKFUP HAFYE QHQPO QTOBD . . .
24. PUESP OQUMC NAKAS GNPPR HYMYL XZYLF DYAVU . . .
25. VNDZK EVTPI IHRBY UKLXD UBEME WUATE VKTTL . . .

b. Extrapolate additional key from the foregoing problem, and recover the complete plain text to Message No. 1, which is given below.

YHWKW	RVTTP	THRLV	GZXEE	JNSAS	HDVSW	GZZVP	OLLZX	RIUUP	TUTRE
LCYIE	FGIEJ	IYDDT	NOEJ	TCEYS	KLRSQ	PQBCI	FOJUV	VWOIH	KDZLR
HAOYA	FFVYK	WRAXA	TUZBI	HBFQF	HBIWS	WRUGB	WZWAA	PSYMJ	EJZVT
HVDHP	GQTOK	CNXQO	KKQTK	ZACPX	GYGIS	KQBOG	WSARN	YTCQB	AMGGE

DO NOT WRITE ON THIS PAGE

6. The following four messages were enciphered on a machine employing reversed standard alphabets for the primary components. Place the messages in depth, and recover the first five words of one of the messages.

Message "A"

XTEKJ	EWPSG	IDJUO	GDZEI	KVGGC	YRWVX	YHACQ	WYDJB	GHULC	NARXN
OVWOQ	VMIAQ	FZJJK	CHNQP	HJWUU	IEZUN	MGTXS	VFECJ	EHCKB	SYXCB
MCXOK	RPOXV	YYZOK	KIHHS	DFGFU	PZXGS	TDJMI	BNLPO	SRCAP	SGUEA
JWPFQ	PHGUG	WCXOV	ZLQQQ	AYTLM	FBRCA	CSEOH	OGURD	FAAUT	MPCWK
VMHDA	IAEAS	ORFXI	TNWAU	ZDLHU	YJTCG	CKAVO	PGZSR	PNIPJ	TRNGD
TGQLC	RWHSI	EFPEB	UZGDL	NIADE	LXRGU	ZTTVK	BTWNW	NAXMH	ELFEY
NRQGT	JBTDK	AYWEF	PCAUM	WSEJU	PTQHN	YSCZI	YZXGG	LOIHC	FNYPE
XCZKC	SUYID	WSKRL	LHPYZ	UXWTQ	QFSLW	XLEHF	VGUPP	XVSIY	UGKBR
RRRGE	LVNUV	FKQGX	LTZLD	NZIHT	OVBQK	DHWGB	NISNV	AEPBF	

Message "B"

LKGZE	OQXIF	AOPOB	ASRBE	GCXMX	RHLYT	APRLX	PCUSP	GDVFW	LGLNH
BCMIZ	UAEPW	QKBQA	KKZUA	XFMSF	TVZTS	WOGSO	OZYIV	TCPWN	NWPFI
NCGPF	DKUNG	FYSQX	RXERR	RCHOW	QKKCU	RAECB	XAEDB	UCKIV	YONUJ
SOXIZ	LRFTD	AFRYY	BTCSS	AHIMW	RGFZB	QTKGI	LMQWD	HIKSN	LTMFB
MLQZF	FSNPH	DSPGT	YVDTG	RKZRF	SWOBN	KHVPV	POVYF	XDLAL	RIJVT
VEGNB	DSBCA	LFWQM	XOQSC	YLVSW	RTYTO	QZWVQ	AUZSK	COFRG	DHNCC
XXBPQ	PIYNH	JUPFT	MVQES	WIUFG	NNUTZ	BDRNH	JBFBY	WJOUB	BRKVV
RBVIR	LKDLE	TVCWQ	AQHGO	TFGXF	IDQQK	VYNQI	DTDBY	UYJHY	QAPVJ
LCZPO	XDHZS	HWPYU	ZYLNW	CACTJ	AWJKR				

Message "C"

OIZHM	QOQJW	YXBEC	QHZGV	LZZVG	UIZPL	QQXDW	RKCWH	GYUHT	RBXQR
GKKNE	IWXYG	TKVEO	RUIWN	OKMXD	YNIKV	GOQHG	OOJXN	LTEMX	MPLNQ
AOICK	XINEK	RANYV	GJFWJ	YFOLF	WRWWX	YPHBU	CRMSB	WJHAF	BLQYY
LIOMU	KXAXG	URTHR	RQVZV	JPAHN	RHGOI	GVPMW	LODRV	OTBIY	QPWCJ
QJKNG	EOVTB	FADRW	WJNGZ	UHUKL	ZIAQD	DYYPK	ZHJMJ	MYGVP	QDPOV
EIZTB	JRVQN	YXMBB	ZRRAF	IPXBZ	NQMSK	VMAQO	DSWGF	DYPUF	OBYNL
LDBFI	LZYXD	PMMEE	OGEFI	ECRRR	MJHVL	CFTJO	TLGSG	MEIQS	XBHXC
XFDYD	LVXFV	TFGGE	ZQYRL	TMHLW	DCLDR	NVIEI	DHAJY	GTNYP	WCHNS
BLUNI	VLXGW	EBTOS	BNGVW	KPEOM	YLUDO				

Message "D"

PIVLV	OPJIO	BYJEA	ESOPC	XYVRF	VSSZZ	ZPCZX	VZMML	LRLUI	LTFRG
QBLXE	ZDKBI	VNCSV	OBLXS	REEPU	PZBZX	CLUYN	WTJNB	VEJGO	NNXGT
OKRLO	MEVXG	LBXSG	OYBLA	CQZKB	OYLSL	BAUXJ	SKFLW	LUTKP	KHNFA
OISFT	XQIRH	YKXOI	NZKID	FABFY	BZIAZ	CSLHY	IBTXN	AQICB	KBBAZ
EEBTP	HCBXY	EMHQE	ISAWP	YHFIG	VJHGR	NETUX	OSLXK	LPMVM	TPLSL
PDDCJ	PUIHT	RJXKW	HDSVL	LRDMI	QXPDE	ZMYNM	VFHBK	PQJSY	OIAJM
CCDZG	CUIVC	TMIDZ	MPQVT	DMXKO	QBDQY	JOKIX	FWZDR	YBPPK	HRBVI
CLEHL	YWQLF	QMFHZ	DQOZM	SUGLW	JVTAG	GQGVK	CHIFH	YCSAV	YSFMP
AGEOO	FNBBH	QQZER	KHIBJ	EKHVI	OSZET				



## DO NOT WRITE ON THIS PAGE

7a. The following are the beginnings of 30 messages in offset depth, each successive message being displaced one position further to the right on the key. Solve the first three beginnings and recover the components.

- |     |                |                      |       |       |       |        |       |       |       |       |
|-----|----------------|----------------------|-------|-------|-------|--------|-------|-------|-------|-------|
| 1.  | BIVMR<br>BFTWR | PRFLL<br>JEPPR . . . | LUBPZ | NQUCM | EPCHR | VHHMI  | CMKXF | GGQQB | ZSRZG | MIYLW |
| 2.  | OUACG<br>QMFXL | XGQBL<br>ZBHRC . . . | USJZV | DJBUS | FWKTK | MMNRC  | ATKNU | YHPZW | MUYEP | MEDBO |
| 3.  | VXYFF<br>NCMHL | UXGTQ<br>CADHQ . . . | KYYNX | IIANO | TTNUN | KVFPL  | QPNPY | XIGWR | VTUNJ | QLQET |
| 4.  | MWTVU<br>VMHLS | HUZPW<br>PAGRU . . . | PZCIL | NISQN | YIWHY | WLEAD  | RBTZH | AGVKX | ALYME | OYUQD |
| 5.  | YFFVG<br>DAMXG | JDGZP<br>YKIGP . . . | OZDQO | ANTHZ | NJFBR | JXCDO  | BWLQE | ARHNZ | LKJEO | ZOKTW |
| 6.  | GEOMV<br>ZRCKI | PQSYH<br>IQXRL . . . | SCYYR | NKWEJ | GVDNA | NAQPA  | OIWOB | AHRZQ | YKBRW | DQVWX |
| 7.  | PCZUG<br>LRRNL | XPMWS<br>LEEQH . . . | TTNDL | PJDKU | MYKQM | AXUPB  | HCFGG | MKPUG | AXLMW | QDVVG |
| 8.  | FTUZP<br>FXIYD | WIDDW<br>TKZSP . . . | XMFFX | XOKDB | NJFXX | OJWXP  | ITEZS | BSDCC | XBCDL | XCEBA |
| 9.  | VJLUO<br>JYLJQ | CGMDQ<br>ZOGTK . . . | ZUUQA | WIFOT | RENXX | ONSWQ  | AJUII | NBCQY | PPZCD | KQMAL |
| 10. | LSIKK<br>JYJHP | LQNXO<br>TDHEH . . . | DPOHK | FVTWY | FMSJN | SFGQQ  | BMHPF | VUJLM | ROKVV | OWVJH |
| 11. | JBBPT<br>AVDPG | CHYHK<br>CTYDQ . . . | QXADK | KMHAV | CMKWV | HYRXG  | SXULB | IKXMW | WTHEM | NRLQX |
| 12. | CDZRW<br>SVGJH | AIHYH<br>GQYRK . . . | JNNIW | SXRGX | LKLGX | YLHJH  | PLJOR | IBMRO | VTVEH | KCXAY |
| 13. | YYZTI<br>ERXYE | UEXQG<br>CBHBO . . . | AEJVP | CDGTP | DPQVI | QZFOP  | UZEPZ | EHZHX | TEXAQ | CENAF |
| 14. | GNDGJ<br>UTSGG | LDVGD<br>NUVLZ . . . | TMVVY | YSEFM | QBGGF | XXWPP  | DBPNE | EWNID | EUUHR | VDGOU |
| 15. | IDGQI<br>LGTUB | SCVWW<br>JJXQJ . . . | ZKMMN | RCATK | NUYHA | ZKXTZ  | ESNQW | GOGKS | ONJSE | MHFGR |
| 16. | CAXIY<br>DDLVO | FTVQK<br>KGFGK . . . | BBKDF | BZQJA | WGCQX | OCNTT  | OZYLW | YJNWT | WNPJT | GVUCV |
| 17. | AIHYH<br>CSMEW | JNNIW<br>RPTSW . . . | SXRJC | HDOVU | KNEGR | AXJDK  | NHMPZ | FDRPI | UDQDQ | JUUOD |
| 18. | TBKQX<br>ARWWG | ADVFF<br>PNPAH . . . | BRICA | MFUWM | SGWAM | GTECW  | ZWWHI | NEEZN | PDRQP | VPNHF |
| 19. | IUNHY<br>MMUAO | NKUUD<br>WYIJH . . . | DLTPD | PQVSQ | AZAGR | ZJZRC  | MAOQM | AMJAP | OLZQU | TQRCV |
| 20. | UNKVE<br>WJRCJ | IFLTR<br>QRJDW . . . | BDRIJ | QWBQO | YWIQG | UASGR  | WGIXE | PTUCI | HWLZV | ZUTSV |
| 21. | HJNNI<br>GUHSY | WSBQF<br>QFSFI . . . | PNBKO | TCDIG | CXCNB | AF ECS | CRDLM | NLZMM | AQERJ | SPTMW |

DO NOT WRITE ON THIS PAGE

- 22. TVOJG BKUST PDPQV SQAZA GRZJZ RCMAO AWMFN KNTVG LVIEI ESMOF  
WTLKZ KFFDT . . .
- 23. VOPWO YWRCA YVPWK HGJOV SZLJQ EFFWJ ZNMZY MVWCF IPWIJ FXCOQ  
BLYKL ZCKKY . . .
- 24. UJGVW ATCXK UCVNA OZHQQ AOMZJ XKPID AMRDY FVKLV IEFJL LZKUB  
OQIUG WPJZG . . .
- 25. KUMNV WNPXK GVTIJ XHDRT IMTYX DEUFF FNKNT VGLGB BQUFY RWGRN  
ZKJHF QEGQA . . .
- 26. GBPIS MKKIG UFHTQ AHVNJ CAWXB CXQYO NGJGA YJHPR QESSA YGNQD  
KTTWQ DGIOE . . .
- 27. EWIUT ZMXNU NHXBH MNZTY XGOFQ LYZXB MSWVO XVGHS FNMUR AWJSV  
JRFGR CMJGE . . .
- 28. CAFJU JHYVN IQCMA EZJZR CMAOC CWXAN PQCHQ DTEIE SMRFB ZBNXI  
LNEEP CZBEA . . .
- 29. QLOMK ONSWQ AJHUQ RUMZE PRQXY SEZZJ QHMIU JVCUU BSVNB MYXSZ  
ZUKUD QGQTT . . .
- 30. YDUXE VYYIT EOWNZ JZRCM AOJKF XIOSQ LAHDP QSNQV WVPYB DURIT  
XZOTX TTVSF . . .

b. Extrapolate additional key from the foregoing problem, and recover the complete plain text to Message No. 30, which is given below.

YDUXE VYYIT EOWNZ JZRCM AOJKF XIOSQ LAHDP QSNQV WVPYB DURIT  
 XZOTX TTVSF YONAI WTAHK LFFLC CVHJH HLHFR LYZNB OZMEB ATIWO  
 PLZEJ RQEQB FCDIW BJQST

8. The following cryptogram is suspected of having been enciphered with a key derived by some sort of Fibonacci method. Solve it and recover all keys.

84360 89843 23654 99422 11271 04823 25759 41545 81196 65525  
 45773 93577 69960 67340 88260 13590 51375 06770 62070 38254  
 09178 84673 93453 29051 71193 42329 56490 07497 59137 78351  
 50745 28901 84105 44839 74867 34591

*E. Cylindrical cipher devices and strip cipher systems*  
(Embracing Chapter VII)

1. The cipher message given below was followed by its original plain text two days later during World War II. Reconstruct the cryptosystem involved.

MCSGO HKXVS QFFKW TFIUO ODLLZ SQSVM KWOLY HBXFO GJGGW YTXUP  
 QQUPC XCSDJ EJZUZ UPBSA NEZLE ATKNF IFCMI MFWNM CXWRK TTWKF  
 NJGIM FKJNZ KTXCQ RBWLW KDMWH LTKHZ GE AFC MGKDA LICUD IPXHJ  
 OLCKC CWZJM FPAQL QWQSE RDREI AEOJO NAXEV GZRPG YKLRX XOKVY  
 DCQJK HWKGD RGQIK ZSGNQ DOVRW LXNDF XHCCP YJRNM VZIAJ XOHRU  
 ZPPXQ MHTIU IPSUM XSITS IQKLX BCIUF MPXZB CWLVC QZAZJ NDWTE  
 MKNNA LN ZIF NVHUT KHPTD CDBXV LYBQV ZZBUL NXBOC KWTCF OFEZF  
 FKNWU QFZFD YYVNK XKKPU YQWCV PVHUP WJBXM ABYVW KMIGM ZXGKS  
 RBYOM KDCHR QDBMI XCRYU HXKMF TYELW MPXZL CEVNV KQPQW TWF GK  
 QKEMK ONUKD MQLCT DEXIA AXFLP HWPEW EPVDH IZQFJ PAMRE ZYCXT

DO NOT WRITE ON THIS PAGE

XOYSV	NUSJK	TUVQQ	WDSHC	EEZKV	OLJQR	KHIMO	XVFRS	VJXCX	PNTZP
IGHTF	OURSE	VENZE	ROATS	FONEF	DRTCO	DSYIT	EHMKJ	IWUKX	YWVNG
XQMDM	FNHIX	NBGOV	HDNRG	EPPJQ	LXIVM	EIFLV	WXOLX	UTAQE	LDEWB
LFMTQ	AOYUX	VXHLH	RHPFO	NHMWB	CMKZS	MLVNT	ZENEO	TZQGG	ENDCY
MBNJY	AKQMA	FJVSK	XKKPA	USJLO	XLANT	JVPRE	QKSFZ	NWCYY	XLNPW
KBUGM	KAWAS	DRLIQ	YZGJA	SACXT	WSRDG	WVAKG	MJJPW	DXEVT	VESHK
RVBLK	QDQHE	ZQLQA	YMVUY	IWMRK	ONFPG	WYAEG	UKLSC	AJBGJ	WHSZA
RHMTQ	YHUTP	WUZPM	CMHKV	JLHLE	HMMLN	SQWOQ	KJEQB	HZZWX	BGFFC
PDMSL	MULWG	MIWFA	TYZXU	VWVRG	ATQLP	RMABF	VXVNR	WNVFK	LHQYL
MCPBI	DOTBI	KXMTX	NCIRR	QEAUH	KOTZY	OKVFD	FHBWD	KVBQT	XL00Y
PCLJU	WTVBW	VXSBU	YNIPG	GYFJW	PGJFB	YPHDM	IQPYP	QFCJK	RSIPL
EXPTB	FLEIE	ZUHDP	YINCX	AZGSU	ZAGAE	IULFC	VODSM	KMQIM	BPIAA
UQGHT	SKSOP	SEZJC	EEFKL	HJXPL	MTQOM	EKXAJ	GOAMF	CFTEU	HFQMW
YGJFN	RIVTT	MYDGP	GLPBN	NIZCL	KBUGX	KTFZN	DDUWZ	YOHDB	JMFCF
CMKFM	NJUTZ	LKSWM	THLKL	SBDCY	SEMPU	KAVOT	GBIEY	ZDNEZ	EHDIU
PWYJR	QCQHF	GONUJ	OHTTC	JNEUK	UNQSL	RJSJT	MDVWC	JAEJT	GSZZZ
BMMSC	VQWOQ	YXCGE	PPMHG	VUSJC	IXMWL	HOIVY	YCHPG	ELTMA	AJAWJ
GOPZB	RHWUY	BYCYG	OWNCX	AZGWU	WKAPJ	ZIRVV	WJSJB	KVPKJ	GXGML
NSCUJ	WHKDM	UHLZQ	ENVSO	TBVMZ	SJGMC	GMYYK	NJMIJ	RJEGQ	UTAKP
XEASN	KVGPL	GCEUI	CKTCZ	FAKXW	MOXDP	GQYWX	LSOJZ	KELUC	ZGQNJ
PEFQB	MKMRX	SHFLG	MMICF	GKVPC	SGDXZ	YUDYK	WLHWB	LUSUM	XDUFG
WSRDH	FKZBE	DLZSE	NVPUN	RIMLS	TGWZB	OIXHW	WHJCX	UTAQA	QCDWM
AUHSJ	EDBCZ	LBWQL	KFFEJ	RDJWA	AAMLU	GKABS	HLFVP	IMNPO	YTAXL
UBZPQ	QNNNS	ZPVMP	IBJTO	LFMSJ	GYXSE	BHQHR	HALKN	AHRQI	ZAWHE
VXKVE	KLRLP	KESPZ	VKSPE	ESSAN	SVHAK	XZPQD	KGWSA	IJZYJ	VKGSJ
CUNLO	HHKDM	UMQGN	OQCQX	QPEOY	WULEX	YQYAS	JIPIW	WPXHK	LHQYL
QQEAK	XZPQD	KGJVO	UIPEZ	ENGHY	IVMWQ	ABNAJ	YNSYV	FLAXD	URLWV
PKUYS	YXETY	WWYNX	VFAUJ	JRNEI	OQZFX	YQPGZ	AXOKL	IJFGG	BQPZQ
GPBJC	MXHRE	TTTNM	YUGJT	LDHHO	BFTYP	KRSGI	CQNUS	QEKCI	KMQSE
HXTIW	EDNCV	OKWAY	ATAOP	MRCAG	LAHAM	YAHFD	MBGOY	UYHJV	DPPMP
XJEDM	FNHCU	XGNQT	OGGJG	GHQJL	OPVYE	QVXCP	IUSOM	EWBWS	HCPOV
MNIYX	OBNAP	ATYTC	VJCCU	CINBH	BJRZJ	HETXO	FACDV	EOFGC	OTUFJ
LYOTW	ESPAJ	QQXDN	VXGGI	WXLVC	TTLLY	ABDWM	EKFZE	GBWVS	YAQVY
SNKYJ	TUFMC	LQKVY	BOGXD	HHZAS	KHBNM	KPJXO	DKCZZ	RGIRX	SUYKD
GKSEL	LDMOV	HDJDE	AIVNS	YKWBW	ASLOT	TNGJE	JRSGA	HYXZD	GMXDN
AUHMD	WFYOJ	EPORY	LXHGI	WAQTW	LBPEX	PPKFM	JUVFL	TAUPD	SONSZ
EUJED	XTETK	MXQJX	GOLIX	SMSTV	HMIZD	JQKHW	SKMID	FTHBX	UCTIS
QFJKF	YTZUM	YNNZR	PGHGE	IAKJD	CGSLI	MIOVY	YCHPG	ELWHS	YJXQH
LKPXZ	AKOAC	BCPFR	YQZLD	TKGEE	AVNPG	CFAFU	VPZDY	ATRYZ	YCXGL
FCRDC	XXNVO	EUGBT	CCTWX	EILLG	CYULK	IWXTF	OXWFC	FGNLN	RXDOT
NUSKU	UVSZY	DLVGY	NKZDH	UWRHU	OJDTH	GINBO	SMCOM	MXNHP	QUWHR
PKEYG	SQQVV	MSNCR	SKSLL	UGKJZ	BMEAV	PGHPQ	QTCAM	VZOZO	KNJTE
WOHXH	JGMNR	QVYTR	JDIOC	BZMBD	TXXCS	WJADZ	ASXBQ	KGWIO	YVSIF
QSGAU	FXYLW	EHXIV	KMOEN	ELFCU	PPFWR	PYMIJ	DXJAP	BJSAX	IZWEE
SNSUG	AERQG	GXALQ	WLWDF	VCLOY	GVROU	WSEOH	UBDSE	PWQAQ	TNVSO
DGZYW	KYSPC	LWFMS	NXEBS	TQAWY	SQCHU	GWWMS	JWVAZ	CTLQB	MCQIH
PDFYK	FQGIT	GANWC	CJTIT	YXABU	TWLJR	DOSTY	LGJZO	XQANF	PXACJ
XSEZO	QWJIB	IDEYL	OQRJW	WYXGD	DBAMN	WVGYZ	SGBEW	DXTCZ	FASMZ
MIPUO	OPSSS	SEPCI	XNHSC	LOMNY	TEFUT	CFNTD	PNUVS	SQAKS	NWLOM
BLSKL	TZERD	ECQMF	DCKKE	VGVEY	SQZLS	NKZEY	HDYIW	YTCPB	GTVOI
XRSIK	UIKYQ	ZEKSI	ALASY	QDHAQ	HGHCO	HYCZT	EKHKF	WLJZT	VBFMA
YOBSY	DQYGG	ZUIUS	GWUTY	IWMRC	WTEGW	MMWIR	MUTTX	WPVFJ	WBBYX

DO NOT WRITE ON THIS PAGE

QEJAP	JWYST	FYBXN	LWEGO	KPMDI	NQZYQ	JOCHK	VSOEB	JJYTG	ZNREV
LCELQ	KTFSH	OPAJA	LAHVX	XSLEP	ZBZV	NWOPX	FBUXF	BBZWR	SFSHZ
KDWJB	AKVKO	UZFUU	WCDWS	TMGQR	EUPAG	ZOLVV	QMIIA	IIBKQ	DEAUQ
AJENO	COHOQ	UJNIF	OZXRG	PDKBP	KOIWL	VVUMQ	RSVJC	QZAZB	RLLDL
GLMKU									

The original plain text of the foregoing cipher message, as it appeared in the teletypewriter copy:

RE TELEPHONE CONFERENCE 32 CARS AS FOLLOWS COLON

B&O	380083	4005593	470	199200	15980	82700	1833
PRR	78708	4005594	470	201-2	15980	82800	1833
MILW	18844	4005595	470	203-4	15980	82300	1833
MILW	19647	4005596	470	205-6	15980	82900	1833
C&NW	73692	4005597	470	207-8	15980	82900	1833
C&O	4167	4005598	470	209-10	15980	82200	1833
B&O	380579	4005600	470	211-12	15980	82900	1833
B&O	379021	4005601	470	213-14	15980	82600	1833
T&O	54682	4005602	470	215-16	15980	82600	1833
MILW	6442	4005607	376	217-18	12784	66500	1466
MILW	18081	4005608	470	219-20	15980	82600	1833
MILW	18470	4005609	470	221-2	15980	82800	1833
ATSF	143641	4005610	470	223-4	15980	82300	1833
RDG	103285	4005611	564	225-6	19176	99000	2199
SOU	306570	4005612	470	227-8	15980	82200	1833
RDG	19102	4005613	470	229-30	15980	83200	1833
MILW	19545	4005626	470	239-40	15980	82900	1833
GW	45019	4005627	470	237-38	15980	82700	1833
UP	75308	4005628	455	231-32	15470	80200	1774
WAB	83552	4005629	470	233-34	15980	82300	1833
NYC	132442	4005630	440	236-45	14960	77000	1760
MP	42680	4005631	445	241-42	15130	79100	1735
SOU	261700	4005632	470	243-44	15980	82700	1833
NYC	151707	4005670	470	246-47	15980	82800	1833
WAB	83350	4005671	470	248-49	15980	83100	1833
B&M	73104	4005672	425	250-51	14450	82600	1657
B&M	72108	4005677	440	252-53	14960	77100	1716
SSW	33571	4005678	470	254-55	15980	81100	1833
CB&Q	42072	4005679	352	256-57	11968	65600	1372
CCC&STL	48835	4005680	430	258-59	14620	78000	1677
WAB	82452	4005681	440	260-61	14960	77000	1716
C&O	2418	4005682	369	262-63	12546	67900	1439

## DO NOT WRITE ON THIS PAGE

2. The cryptogram below, enciphered with the M-94, is suspected of beginning with the word ENEMY. Reconstruct the plain text, and recover the sequence of disks and the literal key upon which it is based.

GDYUB ZIBHN IUJGQ ZUXTC ZBDRO DRRZM LCXTO LPBOR JELHM GYGAU  
AODLH CNBTU ZJRVL HQUNW DQHZB ATUPF VRLHL RFKUV UAAHG BEZHU

3. The cryptogram below, enciphered with the M-94, is suspected of containing the word HEAD-QUARTERS. Reconstruct the plain text, and recover the sequence of disks and the literal key upon which it is based.

NEKYL SRQXV EEZHP VGTUT YJXBY APKVI RPZNJ WWFXE OBXDB VQAYZ  
ZDJGM MFQGX LKHIW BVDJK YARBK LLOLO OYOVD FARUX ZVXBT GMAUV

4. The cryptograms below have been enciphered with the M-94. Reconstruct the plain texts, and recover the sequence of disks and the literal key upon which it is based.

YXI DE RBV 0405 26 DEC Message "A"

QVQQK YMYRK FEOPM

Message "B"

YXI DE RBV 0501 26 DEC

GNNSF IDOOX HQFQQ

Message "C"

YXI DE RBV 0612 26 DEC

RKNSG QPNIS OBWHC AWLZU ZIVCB DRUFW WMRQK GDCXU DIFKB OSTZN  
FCLCM ADOEO EHAAX JGAWP NRKZH NGPRG HCBSL RSJCR WGZBI NVABP

*F. The Wheatstone cipher device*

(Embracing Chapter VIII, pars. 49-51)

1. Solve the following cryptograms and recover all keys:

Message "A"

PIBRQ HOCDP VKIKZ XKTLZ WYPFL LYEQO NBVKX VWXTT

Message "B"

KIMLP CAGHX PKXLR UZLGM SVMMC KWKMO

2. The following cryptogram is suspected of containing the word HEADQUARTERS. Solve it and recover all keys.

GUGVD YVCOM NPHT E MXZED HIOWA SNXYT SULEI XQNTQ GTHYH WRVFR  
ZLRBA FUPSJ DSCTF HFUJY SBSLC RWCAO OPDL D EIPXH WWYTZ UWEEY

DO NOT WRITE ON THIS PAGE

3. Solve the first five of the following message beginnings and recover all keys:

- |           |       |       |       |           |       |       |       |
|-----------|-------|-------|-------|-----------|-------|-------|-------|
| 1. DMOMW  | GSVRO | HDKBD | . . . | 14. EQRKC | QYRES | TBRHR | . . . |
| 2. ZODFF  | JDUVC | XZNHE | . . . | 15. PQOFS | RJIBR | OYKGI | . . . |
| 3. QODFF  | RDCUT | YRKNJ | . . . | 16. JXZRK | CYSZD | BUHZW | . . . |
| 4. GGZZI  | KADGX | QUYAN | . . . | 17. QOJKM | YPTIX | IYZQT | . . . |
| 5. PPRVT  | NQQDR | NYNHC | . . . | 18. AMROC | QVKAQ | JKOVL | . . . |
| 6. ZOUYR  | JIYOB | WYQWP | . . . | 19. AMYPZ | XIUCZ | ZOBNM | . . . |
| 7. JOSBE  | SOQQJ | KZLBJ | . . . | 20. QOFFR | TTIAF | OZYWP | . . . |
| 8. OXHZH  | KSHAV | CFKZL | . . . | 21. SXXRV | YJHDO | PKOYA | . . . |
| 9. QODYV  | BNFVD | CVJSO | . . . | 22. QOKXJ | FROJP | AQBBO | . . . |
| 10. JOSOZ | UIHUA | TUDRN | . . . | 23. DBHYP | HNLAD | AYZJM | . . . |
| 11. DMOMW | GQIUT | RQLYK | . . . | 24. MXEYT | RTVAT | DMZNH | . . . |
| 12. IATKR | VFFID | TBMFT | . . . | 25. NXIST | NQQDR | NYWGB | . . . |
| 13. QQQTY | HTSNF | KZTQY | . . . |           |       |       |       |

4. Solve the first five of the following message beginnings and recover all keys:

- |           |       |       |       |           |       |       |       |
|-----------|-------|-------|-------|-----------|-------|-------|-------|
| 1. FUTJY  | VPFAR | RRNVT | . . . | 14. DLWTK | FFZHL | RVITG | . . . |
| 2. WWZMP  | GRGUC | QCPLC | . . . | 15. WVVHA | WHANV | YSSTD | . . . |
| 3. IBVEB  | TXCMR | TOXEY | . . . | 16. CSLBZ | DILSQ | MFMFB | . . . |
| 4. HRLQA  | CWAYB | STCHD | . . . | 17. ZCJQC | YODQX | BSPVE | . . . |
| 5. GRFRF  | WDHLG | YJPVH | . . . | 18. WOUIK | RCTEV | ZFRKD | . . . |
| 6. DDRZL  | OYQAE | KELSN | . . . | 19. QFCIG | NWPTU | WLFHZ | . . . |
| 7. LDLIP  | LIPJU | JYLIY | . . . | 20. QSDUK | BHSCH | BCNQB | . . . |
| 8. BXQKC  | QSWUT | XUYNK | . . . | 21. NLGQT | FMAVT | RDHVR | . . . |
| 9. CXHMX  | WKSEI | AGHGO | . . . | 22. DMGMR | UFCQW | UADVI | . . . |
| 10. CDMZE | KWCHQ | MQVUW | . . . | 23. LSQDG | XGNXI | CHABL | . . . |
| 11. GIHCN | JYIOI | KFKNQ | . . . | 24. VFUAO | QJOSZ | IRQSF | . . . |
| 12. CSLBZ | DILSQ | FKBEX | . . . | 25. ZQYQV | BAHCM | BXZTS | . . . |
| 13. FOWYT | OYEZX | DVTXN | . . . |           |       |       |       |

5. Recover all keys from the following matched plain and cipher text:

WAHJJ	MTOVL	LHTEX	JCWQC	WLJHZ	WQZPX	AOLHS	ORYKH	KCDAG	DNKPZ
REFER	ENCE*	YOUR*	LAST*	MESQA	GE*SE	COND*	REGIM	ENT*C	OMQAN
OHJOP	ESPQH	SYONH	EWXBV	CADWX	BEMOE	EOSFE	RZOWH	NCXFU	IMMVD
DPOST	*NOW*	LOCAT	ED*IN	*SCHO	QLHOU	SE*TH	REQ*H	UNDRE	D*YAR
ROESP	JYRPL	FGLGX	QEBIA	RAVSX	QXGZP	XRILU	NRQRD	ZKEGS	WLDDY
DS*NO	RTHEA	ST*OF	*ROAD	JUNCT	ION*S	EVEN*	NINE*	EIGHT	*STOP

6. Solve the following cryptogram and recover all keys:

GDRYL	RDTVO	AHRHO	KGETG	YZCAL	BPMLJ	DEJKW	GCOFB	MZBOU	GJHNH
UKVUQ	HAFZU	BNWZN	ULLAS	NUMQS	TNXC B	JVMWP	QERKZ	POETC	MHOGD
VYUEF	XAVAF	JWTUW	OPNXB	RQDTJ	CMISE	MDAGJ	PRSAR	LORNH	HPKRN
ISKCR	QBSIC	GYVKJ	FINYO	EGVWV	HGJPH	UHOJH	ZEYAH	ZDELV	KFTTE
FYHIH	OJTLO	SPSUM	QLBHI	ZSIDA	QPQNI				

7. Solve the following cryptogram and recover all keys:

WOVAC	XPLDV	KZGZU	ZDAOD	ANTQI	EPIUA	QUMAR	WOXFH	PLHMM	FQKDG
BARXF	TGOZV	RQMCY	MPLSV	CQCPH					



DO NOT WRITE ON THIS PAGE

3. The following cryptogram, known to have been enciphered on the original Kryha machine, is available with its compromised plain text. Reconstruct the components and determine the disk setting.

		5		10		15	17
Q	D	N	W	Q	Q	F	J
R	E	F	E	R	E	N	C
O	A	S	C	D	Q	N	X
A	G	E	N	U	M	B	E
M	R	W	S	Y	W	G	N
H	T	D	A	T	E	D	O
A	B	U	T	W	H	O	Q
C	E	M	B	E	R	S	T
K	P	W	V	K	G	V	K
I	S	I	T	I	O	N	S
G	W	M	H	W	M	X	N
O	N	I	C	S	S	U	P
T	A	V	I	T	N	Q	M
B	E	S	U	B	M	I	T
C	D	E	A	E	H	J	H
R	U	P	L	I	C	A	T
I	W	T	T	T	J	O	L
O	R	M	A	L	S	U	P
G	Q	O	N	B	K	P	R
L	S	T	O	T	H	E	P
D	M	S	J	T	L	X	O
D	E	P	O	T	S	T	O
X	W	U	O	C	D	X	X
E	S	P	E	C	I	A	L



DO NOT WRITE ON THIS PAGE

4. The message below was enciphered with the improved Kryha machine. The I.C. of vertical digraphs on a width of 21 of a volume of homogeneous traffic (see distribution on p. 634) is found to be 1.04, whereas the I.C.'s of other trial widths are in the vicinity of 1.00; therefore it has been determined that 21 screws have been activated. Solve the message and recover all keys.

	5	10	15	20	21															
C	S	T	W	I	Z	Y	Z	X	I	Y	M	V	R	M	Z	T	X	Q	S	B
Q	T	Y	N	R	D	Q	V	P	U	X	O	Q	U	O	F	B	M	D	A	O
F	T	H	O	C	B	O	L	Z	V	F	N	I	S	H	O	Y	S	U	B	T
B	V	B	M	U	D	O	Q	V	R	B	L	P	X	B	J	Z	R	Y	U	L
F	P	J	V	S	W	W	O	E	C	N	R	E	A	L	S	J	J	I	V	A
R	E	G	Q	Q	Y	A	P	P	C	S	K	F	T	L	S	V	E	G	M	N
A	F	X	X	T	Z	I	T	Y	W	T	U	U	I	L	L	M	Y	G	C	C
C	Z	C	T	C	R	F	L	F	X	R	V	Q	O	M	E	I	R	R	W	Y
N	I	Q	O	G	P	Q	T	V	Q	K	F	G	T	M	V	K	X	C	D	P
Y	O	U	T	K	I	F	N	M	I	X	K	K	F	F	Z	L	C	N	K	I
L	W	X	F	S	F	J	M	F	F	N	L	D	R	C	P	E	N	S	W	V
K	A	L	G	L	P	Z	I	U	O	P	Z	X	P	S	S	L	B	S	I	T
K	T	H	W	N	S	D	H	Q	A	B	D	T	N	H	G	W	R	M	Y	B
D	V	C	P	W	X	E	D	T	A	B	Q	L	C	W	E	E	R	A	Z	A
H	J	Z	H	X	U	R	M	P	J	S	F	J	M	W	H	B	F	D	Q	N
S	U	Y	M	Z	Z	S	P	M	L	S	C	N	W	Z	O	B	C	R	X	X
M	H	U	G	I	K	P	S	Y	Y	C	X	X	I	P	D	D	U	X	P	P
E	R	W	K	J	O	S	D	O	N	A	O	R	Q	I	A	G	V	I	R	P
P	F	D	S	A	Z	E	U	B	J	V	J	P	Z	E	N	C	F	D	K	W
K	C	J	T	A	F	F	N	T	K	N	W	Q	L	J	O	A	H	V	B	R
M	N	T	T	C	M	H	K	N	T	V	Y	Q	N	K	O	C	J	B	I	W
Y	D	W	K	G	L	O	I	X	I	K	X	T	I	Y	D	Z	D	I	Z	H
Q	T	L	X	Z	Z	T	Q	N	A	D	X	L	Z	R	F	J	Q	K	P	U
I	E	C	M	G	X	N	S	V	D	R	I	Y	R	H	N	U	I	U	V	L
L	Z	S	R	V	U	U	S	F	L	I	N	U	V	V	G	H	X	Q	Q	F
I	P	M	A	X	Q	M	N	J	V	N	P	M	Q	V	X	Y	X	S	G	F
T	S	O	F	D	H	C	K	D	Q	Z	P	E	R	Q	Q	L	L	S	W	P
E	A	Q	R	N	O	Z	D	T	O	T	P	J	R	I	A	I	Q	L	H	D
F	D	J	S	W	Z	K	I	I	Z	D	A	B	G	P	G	O	F	L	I	R
O	Z	G	N	E	G	A	J	O	T	F	E	D	C	A	D	M	I	Q	V	P
H	Q	Q	V	E	T	W	S	X	L	X	W	M	V	D	S	W	E	V	X	G
L	K	F	I	M	W	F	D	C	S	R	I	N	L	E	B	F	E	G	N	C
L	M	A	G	C	O	D	B	Q	T	D	W	Z	P	E	U	Y	C	H	C	D
E	J	Y	H	P	M	Q	H	U	J	F	U	Y	H	M	U	J	M	R	C	M
V	B	Q	W	Z	V	F	J	V	Q	A	I	Q	B	Y	Y	I	X	O	K	U
V	V	S	T	O	Y	M	L	F	C	Z	T	F	L	C						

## DO NOT WRITE ON THIS PAGE

5. The following two messages were enciphered with the same components as in Problem No. 4, but with a different screw pattern of width between 18 and 25. Solve them and recover all keys.

## Message "A"

MXBJW	SBSSO	VLULG	ZBJVD	JQTBI	KIEBG	UWOYT	JDSFL	HKVCR	LGKLF
NCKNG	GILGT								

## Message "B"

MXBJW	SBSSX	JHXRF	VHGKN	KLUJT	XHUAW	QNZNR	UUWUF	OQAOV	ZVPZV
KNIYT	HJLGT	FGPEP	VIIXW	VZDQW	HVPZX	EDJRP	PBDMA	FXBOL	JKBNA
NEUCF	PHTVL	HNAKV	VBXYW	NLZXB	BREFV	KIVSK	CYQLH	JCZNT	BWNDE
ESEDF	ZZKEM	FZSDN	DNDOI	YKVJD	XDGSD	IECY Y	HJZEM	OAXHD	

6. The following message beginnings were enciphered on the improved Kryha machine. Solve the first five beginnings, recover the original enciphering components, and determine the screw settings.

- |     |       |       |        |        |       |       |       |
|-----|-------|-------|--------|--------|-------|-------|-------|
| 1.  | IZZKK | FSCHU | RASBD  | BMEED  | ZMRSL | SNVIF | . . . |
| 2.  | YZNDD | CLZCE | WLSXD  | BNEEC  | ZHSMR | SMNVQ | . . . |
| 3.  | PDNUG | ZEXBO | SFMDI  | ITCSA  | ZERAL | SHMHZ | . . . |
| 4.  | ZULDD | YXJBM | EBNKL  | QDWXJ  | PFYMV | TNNWW | . . . |
| 5.  | WDFPK | PMXUW | KELGH  | TGFXH  | UHSCL | DOSME | . . . |
| 6.  | PDTIS | OLXBO | CFSCW  | JTBQD  | SBXQH | AZRTM | . . . |
| 7.  | ZMCDH | VXTCY | LHRTD  | BVT LJ | TIKYP | HAJFF | . . . |
| 8.  | WVJXP | WXDXL | VWF CN | JZWSM  | UAGSZ | BEXJW | . . . |
| 9.  | PDKRR | ZEIXM | LWVDY  | BUIQO  | COQDJ | UHFGV | . . . |
| 10. | IZZKK | HMIGE | ZCAQV  | GGWYB  | TIKYH | SNRBV | . . . |
| 11. | QDNUD | JXRPP | KWWQM  | ITAAF  | YUXAT | TZJAF | . . . |
| 12. | YZNNG | PMIPE | KNRVN  | WGAHR  | BABMO | TATPY | . . . |
| 13. | HVLUR | ZEIAB | CFRDL  | YZCMM  | CMJJU | LHRRF | . . . |
| 14. | YZNDD | CLZGY | WEWFK  | SJJSM  | KXXVW | YPUIL | . . . |
| 15. | PDYND | XMLLD | RFANY  | YTDLK  | NUIDF | BNWWD | . . . |
| 16. | ZYPVD | TKMAP | EBVUF  | INWLU  | RACWF | NZEXV | . . . |
| 17. | KVXCB | XKCXL | AWYRW  | IZJGG  | CMXIE | EHKXS | . . . |
| 18. | ZRYNG | ISOML | BIGQK  | SMEER  | ZTFJX | TNBGS | . . . |
| 19. | MTTTA | XXCLL | RQRJV  | BHJAR  | ZMCHF | EXVIP | . . . |
| 20. | PDDVP | JSIPE | KVIRO  | HDSST  | FTBZE | OYXGF | . . . |

7. The following cryptogram was enciphered by the machine of Problem No. 6, but with different components. Solve it, reconstruct the components, and determine the initial screw setting.

TNFDL	XHDCJ	DFKDP	PIEVS	IWOSJ	XQRJB	EPLMC	KFXIC	VYVQY	QBUGH
IDFFM	PINYY	NAIYI	MJR XO	BBYRB	WVYBL	DURMG	RIHRS	SXYLB	XEQBG
BDQNQ	YHECI	PRERA	ZVPKV	EDFNT	WJHVT	QQULC	UNOUD	DKZIR	KGERC
WEGZG	MMNPL	RFSYT	BKNAF	THRFR	GFLZQ	VBSNT	UXRDT	VDKCK	KGPKS
XMUPH	YSVFW	QBOUY	XVZFY						

DO NOT WRITE ON THIS PAGE

Problem No. 4: Vertical digraphic distribution, width 21

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	20	22	14	23	23	18	19	25	17	20	24	39	16	18	22	18	22	26	24	23	17	35	30	26	20	16
B	16	21	34	16	27	24	24	24	18	30	24	18	20	12	29	16	15	15	17	21	18	13	23	25	25	21
C	31	21	19	17	20	15	21	21	15	23	22	15	21	27	26	27	20	26	20	20	22	16	24	25	15	40
D	30	23	16	41	28	31	18	13	17	22	25	25	32	13	24	26	19	24	13	35	15	30	26	25	24	22
E	19	27	18	33	17	21	21	35	27	28	23	15	19	34	22	22	14	25	19	32	26	23	22	19	20	23
F	25	18	22	18	18	23	33	20	31	22	34	32	21	19	16	20	12	17	18	25	17	27	18	21	11	33
G	11	26	13	18	19	17	24	16	17	19	16	19	25	27	21	17	15	31	39	21	22	37	27	15	26	11
H	21	20	28	43	20	16	24	29	17	23	25	26	26	31	21	23	24	27	22	27	22	15	19	19	13	20
I	18	15	25	19	16	26	31	48	15	26	20	37	21	31	23	26	31	25	23	16	22	39	21	16	13	17
J	20	41	11	15	19	24	23	15	17	13	22	18	28	27	16	20	16	21	09	27	19	13	22	23	24	21
K	19	23	19	16	21	41	20	31	32	16	16	18	30	25	27	19	22	22	20	20	30	14	18	17	24	13
L	17	20	31	12	19	21	23	17	27	19	17	17	14	26	23	16	18	20	25	22	38	22	12	19	27	26
M	28	17	31	31	19	15	30	24	52	16	25	11	25	37	17	17	22	19	15	16	20	19	20	13	21	17
N	17	29	32	12	18	20	20	17	26	16	22	31	20	18	19	16	13	19	32	34	24	30	26	23	29	19
O	25	17	21	14	23	16	26	16	23	13	28	13	16	31	20	13	17	33	18	17	25	25	27	21	20	33
P	24	17	22	16	21	19	22	22	21	42	19	19	31	21	15	23	13	19	25	20	17	22	21	18	20	40
Q	18	18	16	35	19	11	22	11	36	16	35	30	27	28	22	24	37	12	20	14	22	16	26	19	20	17
R	28	12	27	21	13	21	18	17	16	22	28	12	34	23	24	18	31	30	21	28	21	18	32	15	24	19
S	38	30	20	24	22	14	17	36	24	19	24	16	09	14	30	16	15	21	19	19	19	19	18	18	17	21
T	21	21	10	18	30	11	14	27	24	23	32	20	20	33	12	21	13	21	27	25	24	22	22	18	13	20
U	19	22	28	24	21	22	18	10	24	17	27	15	31	13	23	24	18	21	26	26	11	27	26	39	19	27
V	18	17	27	23	27	26	24	17	21	23	37	27	44	21	21	20	20	22	27	22	22	22	20	22	21	20
W	16	20	41	17	19	14	24	18	26	33	18	18	14	25	20	16	18	23	27	21	21	15	17	17	20	17
X	16	19	26	11	27	17	20	13	25	17	18	34	19	19	15	30	22	31	24	24	25	21	16	18	20	19
Y	21	21	17	35	17	26	27	36	23	27	20	27	10	21	17	14	36	29	13	20	22	13	28	20	18	14
Z	17	24	15	26	22	26	31	24	31	22	08	16	17	18	31	28	19	24	30	16	32	43	25	22	22	18

H. Key analysis

(Embracing Chapter IX)

1a. Determine the source or method of generation of the following key:

38549	40853	51895	56813	14525	40990	25353	59453	59918	56585
45655	62505	49995	22508	56529	09312	21449	38938	81253	54453
05408	53390	81450	85814	40519	91351	35470	85653	58956	08551
80808	59561	81051	44571	12901	09540	53893	80852	13956	41018

b. Determine the source or method of generation of the following key:

69424	34901	07748	11480	43778	07703	42047	67437	49034	80664
97876	97369	47845	44569	45947	43689	09649	49941	06732	64694
54849	70335	03867	43745	03449	20375	94173	43736	94594	74368
90964	90334	38456	07594	17343	73096	78146	84114	80480	04948

c. Determine the source or method of generation of the following key:

07453	85663	28647	76529	46394	72266	26147	84030	67151	25768
01691	65848	23023	61754	31080	30949	41597	03271	79723	35042
51247	32718	80433	47419	13607	50476	20615	22505	37215	53510
06115	34462								

DO NOT WRITE ON THIS PAGE

2a. Determine the source or method of generation of the following key:

78131	76784	31174	50078	76343	47807	41346	53334	01331	01799
78318	76441	31917	92478	74179	10834	76033	55723	40178	31347
46554	65323	41305	86131	34767	30345	77787	48763	77689	76072
76747	88123	11278	31788	76503	47753	17807	67921	07276	07310
17997	88878	74703	05323	15777	71034	76371	33764	47117	37607
88390	00666	33300	03985	79531	31533	78342	47800	17230	75560
34850	74547	83189							

b. Determine the source or method of generation of the following key:

VOPVJ	AKDXA	MTQUG	QMOSF	SOPXF	AEBTA	NXHIY	RNAQF	KIDUF	USLLO
KYLYV	HCOMH	SAQBK	UHWBA	SSPIU	GDAVT	XOYCG	YPFKE	ASNEN	BSYGN
TUFMV	ORXXY	FHPYR	AQUOX	ZYPQG	AHDPY	HRNYL	VJEUN	XIFLD	EXUBI
IGXUN	QNOBO								

3a. Determine the source or method of generation of the following key:

64748	25986	81202	65617	94252	60376	46908	04349	57970	71582
19145	35989	40208	18269	32025	64609	05138	69604	71080	34248
78391	19293	70431	36757	10162	45363	71487	57019	15450	68758
59360	97923	13767	28020	30481	54247	86821	27353	14159	26535
89793	23846								

b. Determine the source or method of generation of the following key:

ENKZU	HNZXN	ZPCTJ	CCHLD	BFXHB	DURKD	HRXNL	EZJPV	BYJVD	JVQGH
XGGYC	UEKDY	EUBFP	UYFDJ	CZKBG	PRDBP	ZBPSA	XEAAD	IVFCZ	DFVRL
GVDLZ	BIKSK	OWCRK	WQKWT	NVPNN	RYLGM	QRGLC	AOLRA	QKYSX	OZDNA
ODHOD	VKITK	KAFYJ	EHAJY	NBZYA	BHOFX	PESQF	UEQVE	QWMDZ	MMUAR

4. Determine the source or method of generation of the following key:

FWNEV	MDUPG	XOFWN	DULCT	KBSHY	PGXOF	WNEVM	DULEV	MDULC	TKBSJ
ARIZQ	HYPGX	OCTKB	SJARO	FWNEV	MLCTK	BSJGX	OFWNE	VARIZ	QHYPY
ZQHYP	GXBSJ	ARIZQ	JARIZ	QHYPD	ULCTK				

5a. Determine the source or method of generation of the following key:

82490	31675	06393	47325	69227	10571	51498	15286	65379	67042
18065	37463	98618	01092	74798	11919	11679	20000	27361	20002

b. Determine the source or method of generation of the following key:

59326	42580	91806	33386	24182	57468	71540	28908	99448	17346
06784	13020	19704	22724	31428	53142	84560	37602	11162	48764

c. Determine the source or method of generation of the following key:

79246	61603	77639	43926	72180	93987	22756	49218	31392	44215
86369	49957	38421	12634	38975	17628	83809	11897	29768	16340

d. Determine the source or method of generation of the following key:

43518	20967	29410	15258	54526	82587	41366	55092	80576	04190
32830	54025	33189	96701	72864	23880	76829	39653	16941	80490

## DO NOT WRITE ON THIS PAGE

e. Determine the source or method of generation of the following key:

93471	49565	94930	51871	29765	96392	99213	49961	94992	37013
45361	94330	99457	49943	94994	51875	67389	30338	71219	03585

f. Determine the source or method of generation of the following key:

59438	43712	45956	94412	14613	50719	32522	57484	93703	27465
44339	57299	09066	25701	91606	32318	25467	91874	39212	27979

g. Determine the source or method of generation of the following key:

48057	17417	70473	63098	82865	99303	71229	72305	84242	15552
59966	37418	90486	83133	03352	25763	61288	62953	70379	62954

h. Determine the source or method of generation of the following key:

01360	14961	53576	88234	60570	65276	17932	47206	19267	01837
14718	01898	19779	06461	80079	80767	87335	08980	87788	54563

i. Determine the source or method of generation of the following key:

77364	40908	89071	79788	37225	09475	63860	91469	17084	87822
56335	19686	16296	78153	90085	90834	70844	78281	63319	96408
62521	87739	06271	68987	60829	68015	33153	64689	25830	73137
68792	45616	66090	26992	93972	22694	58983	37716	83522	18743
24782	61508	59962	48586	41855	59300	31405	45459	07204	79241

j. Determine the source or method of generation of the following key:

37259	97499	61385	74132	15453	37259	09749	96385	74325	45369
37590	97499	61385	74131	54536	72590	97499	61857	41215	45699
37259	09799	61385	71321	55369	37290	97499	61387	41321	43699

6a. Determine the source or method of generation of the following key:

61901	84775	03315	98714	41689	52248	75012	75379	04305	58005
30558	00429	53770	12548	72951	84265	88103	35678	00234	56789
10325	47596	18396	08101	22436	38404	24456	58504	24446	48302
22416	07998	17365	57492	11294	76684	02203	85674	92092	74562

b. Determine the source or method of generation of the following key:

16202	61340	37100	06781	01056	66149	57520	04962	76405	42033
96082	62023	21603	21620	57130	08910	81289	27175	81022	96523
62535	51245	76973	91019	32602	82450	49196	07816	41121	39153
12320	09803	11810	44969	26106	14800	59401	64960	24372	04329
70672	46098	21213	31851	74147	27312	43901	05532	92569	58328
78749	02156	10374	49058	37308	43201	15280	15122	42351	86340
16146	01396	05125	76011	29477	82020	58703	74690	57392	08333
91132	94148	23523	31963	35168	44514	75911	32748	11993	01071
12117	01880	70327	00050	58707	75021	00436	13035	22032	90294
25040	52195	21195	65217	58021	60986	12102	99660	45805	06569

## DO NOT WRITE ON THIS PAGE

## 7. Determine the source or method of generation of the following keys:

Key "A": 0360 5418 2657 7302 4153 9819 7756 6948 6742 0202  
 9041 9518 5476 4038 8210 3693 2054 7294 8568 2762  
 1618 8319 7203 5344 9538 2549 1309 0917 4875 6553  
 1034 6532 9990 0583 2829 4269 5176 4702 9655 9494  
 6155 9784 6788 9676 3253 2448 6450 2894 7151 9040  
 8084 2032 1419 6829 6585 2536 4605 5039 0337 1881  
 9906 4552 1251 2952 8488 9676 3423 8167 7692 3139  
 6720 3413 8802 3129 0401 5426 0236 4235 6883 5719  
 0773 8664 3279 7886 5302 8461 0505 3415 7248 6932  
 7992 8699 9840 8715 3015 3136 0764 6223 8430 7514

Key "B": 0178 9820 6584 9519 0528 7505 1416 5361 1302 9790  
 1984 1229 6931 5508 3256 9723 4841 7747 1068 6030  
 8647 7831 2036 4022 4975 1066 8941 9490 1855 7320  
 4612 6241 1580 8703 8192 7996 1243 2165 3995 8140  
 5984 3906 6223 2581 7164 1896 0359 3502 8341 7424  
 4739 5318 6042 4081 2715 0115 1662 1150 3587 4623  
 6827 1599 9784 6237 5416 8534 0850 0731 5832 3491  
 0115 7096 8765 0388 2584 7051 9037 0264 1113 9257  
 3805 1920 3398 1015 8734 4764 7565 0151 6238 6582  
 2043 3347 2409 7672 1891 2470 7351 3541 9510 1735

Key "C": 4690 8476 9635 0542 3377 9486 7831 7821 5808 2212  
 9751 6654 3857 0575 0016 6036 8509 4800 9294 7378  
 1046 5789 9409 0077 3663 7282 4784 5992 8817 5105  
 0488 2566 9952 0739 5080 8771 1796 0230 6212 4155  
 9227 4510 8793 4506 6188 7166 8734 9448 9964 0321  
 3548 5335 6071 3071 8099 4526 3453 6268 2389 8607  
 6866 6963 6770 1201 9931 3059 2987 2283 4597 1112  
 3403 4886 6660 7388 1792 9578 1412 3398 3065 7543  
 1319 4425 1740 2093 8709 6743 0226 7411 8905 9918  
 2679 1344 6823 5669 7940 1562 4853 8907 8373 5210

Key "D": 5747 9978 6432 5811 6197 3433 3229 1217 5960 0438  
 7296 3593 3858 3697 1121 7780 5328 4640 7746 4622  
 9153 9413 7904 6340 1196 4786 0132 4583 0225 6728  
 2520 9878 0283 6765 3378 1340 5143 4411 9799 3562  
 3618 8212 0326 6042 9888 5031 9301 5704 8074 5539  
 1499 6404 2699 5730 2309 1790 7611 6716 1948 4373  
 0331 6688 0822 4471 0513 7079 7197 5004 5623 5945  
 0022 6076 9019 1624 7129 2897 6598 3592 0481 6840  
 0029 1149 5536 4861 5640 1967 4925 6575 7023 2499  
 3080 6720 5365 0931 1924 5619 2242 5477 4781 8363

## DO NOT WRITE ON THIS PAGE

## 8. Determine the source or method of generation of the following keys:

Key "A": 0812 6092 9531 2226 8481 9995 4063 4408 6270 4094  
 5311 1618 1943 9084 4327 5981 3985 8256 2901 7826  
 2629 6521 4171 4591 6203 7992 6538 8706 3145 8384  
 1924 4243 1755 3259 7617 8296 7119 2093 0033 2726  
 1654 5289 1861 9112 9156 4452 6425 3644 4436 9350  
 3673 5257 3574 0572 2430 0074 1682 1964 7311 6116  
 0405 3916 1602 2580 9311 8562 4476 3821 3015 8953  
 1844 0409 6643 5139 7001 1963 1121 8573 3741 0243  
 8989 6508 7091 4031 9312 4957 1657 8239 8005 7362  
 1285 1558 2160 6363 2449 3473 1741 5655 7737 7015

Key "B": 3787 2422 8189 2952 6960 3105 2815 7233 4589 8513  
 4741 3066 0730 3809 9431 4675 2401 8297 9501 3913  
 9954 8723 8327 4399 6284 9018 2385 6632 7202 9223  
 0528 6052 3704 2876 2889 2399 5486 4892 1652 1187  
 2941 2358 2324 8891 9172 3799 9770 2173 6783 6957  
 5998 6699 4268 4326 3426 8668 6797 5757 8626 2240  
 6317 6377 5944 7832 2200 3594 9332 2073 0861 9720  
 6886 0507 2626 8841 2415 8985 4660 8821 9181 5589  
 5946 9543 0184 6745 4950 5355 6423 4165 8512 6002  
 5482 6628 6135 8558 7240 6746 3929 7516 4464 1533

Key "C": 2009 7085 2534 0907 1764 1666 1962 5290 3713 6750  
 5522 3430 1749 8358 1142 6236 3539 9774 1431 3225  
 8963 7979 3801 8095 5901 7976 1616 8898 4241 9270  
 5776 4620 5485 2359 8984 3078 7133 2851 9499 5699  
 8657 1388 2887 9174 4639 2454 9946 5920 6004 5023  
 5028 9265 4512 8618 7652 1850 2083 1157 7320 2480  
 1400 2477 3973 8517 1408 7033 1863 0804 9894 9248  
 1306 7082 5246 6032 9323 0353 1252 8396 8574 9216  
 6554 3319 3820 9496 5845 6022 4146 2036 2092 2024  
 1794 4770 4446 4494 3625 9545 9771 8805 9612 1501

Key "D": 1594 5519 6177 5152 8388 1681 0658 2593 3124 0736  
 5363 7475 4252 4546 4231 0624 3377 9908 3540 1987  
 9290 5188 7932 9886 2628 7172 1046 1912 0777 6875  
 2601 9710 7731 4201 0965 5381 4813 4762 4972 3483  
 4909 0351 7054 0202 4740 5667 8543 2603 6907 6847  
 3474 1846 6803 4656 5200 5282 8911 1080 6918 8607  
 4360 1867 3737 7017 3062 0425 7839 3493 3032 1425  
 0740 6461 0853 4199 7142 2297 3651 2948 9269 0109  
 6586 3269 2871 6083 6358 6703 5396 5484 6594 5024  
 9042 8295 9580 5848 0848 3731 5971 0229 4110 8651

DO NOT WRITE ON THIS PAGE

Key "E": 8668 2240 4326 6699 5998 6797 8626 5757 3426 4268  
 6746 1533 8558 6628 5482 3929 4464 7516 7240 6135  
 2399 1187 2876 6052 0528 5486 1652 4892 2889 3704  
 4675 3913 3809 3066 4741 2401 9501 8297 9431 0730  
 3105 8513 2952 2422 3787 2815 4589 7233 6960 8189  
 3594 9720 7832 6377 6317 9332 0861 2073 2200 5944  
 5355 6002 6745 9543 5946 6423 8512 4165 4950 0184  
 8985 5589 8841 0507 6886 4660 9181 8821 2415 2626  
 3799 6957 8891 2358 2941 9770 6783 2173 9172 2324  
 9018 9223 4399 8723 9954 2385 7202 6632 6284 8327

Key "F": 2009 3430 3801 2359 4639 1850 1863 8396 2092 1501  
 1594 7457 7932 4201 4740 5282 7839 2948 6594 8651  
 7085 1749 8095 8984 2454 2083 0804 8574 2024 1794  
 5519 4252 9886 0965 5667 8911 3493 9269 5024 9042  
 2534 8358 5901 3078 9946 1157 9894 9216 6554 4770  
 6177 4546 2628 5381 8543 0801 3032 6010 6586 8295  
 0907 1142 7976 7133 5920 7320 9248 1306 3319 4446  
 5152 4231 7172 4813 2603 6918 1425 0740 3269 9580  
 1764 6236 1616 2851 6004 2480 1400 7082 3820 4494  
 8388 0624 1046 4762 6907 8607 4360 6461 2871 5848

Key "G": 1666 3539 8898 9499 5023 5028 2477 5246 9496 3625  
 1681 3377 1912 4972 6847 3474 1867 0853 6083 0848  
 1962 9774 4241 5699 8657 9265 3973 6032 5845 9545  
 0658 8066 0777 3483 4909 1846 3737 4199 6358 3731  
 5290 1431 9270 5776 1388 4512 8517 9323 6022 9771  
 2593 3540 6875 2601 0351 6803 7017 7142 6703 5971  
 3713 3225 8963 4620 2887 8618 1408 0353 4146 8805  
 3124 1987 9290 9710 7054 4656 3062 2297 5396 0229  
 6750 5522 7979 5485 9174 7652 7033 1252 2036 9612  
 0736 5363 5188 7731 0202 5200 0425 3651 5484 4110

9. Determine the source or method of generation of the following keys:

Key "A"

10097 13586 80959 48056 96248 40372 42268 96450 20902 90190  
 67071 65886 79997 36147 23665

Key "B"

97325 86346 59091 56489 48052 72063 68953 50930 02560 90252  
 71538 86767 97080 47640 65398 65747 50366 13398 54557 53034  
 48679 77602 16569 74818 33213 04890 84682 75303 78358 28260

Key "C"

13586 80959 74945 48052 36104 08229 30323 25601 76435 07153  
 58867 36276 76403 98951 71217 76850 65813 29170 53034 99074  
 34030 69268 48187 24718 70489



DO NOT WRITE ON THIS PAGE

Key "D"

33765	73548	17392	47429	40372	61040	19645	32320	15953	90937
31131	43970	15736	32366	95116	17340	97361	85111	18240	26148
90743	02051	26866	73053	50532	55357	87098	52964	08342	93520

Key "E"

46735	80959	92927	29624	06361	29166	09025	33476	80336	53831
16588	70443	36147	98951	76833	66973	65813	11992	40635	67990
30973	65748	38524	23885	89055	54828	98349	64778	60935	88435

Key "F"

35863	54876	91173	89474	40372	20082	03232	01595	64350	67071
31131	67439	80157	36653	12171	68503	36170	98851	57182	26148
92340	92686	87305	47186	54704	55357	82870	03529	34282	35273

Key "G"

08422	09303	15953	25290	15383	11658	80799	01573	03236	60657
27685	70658	01080	82406	34261	85269	65692	73053	21350	48905
75482	79645								

Key "H"

53376	67354	11739	94742	24037	36104	31964	03232	01595	29093
83113	74397	01573	03236	89511	71734	69736	88511		

Key "I"

72768	70658	99291	63530	67990	92340	65692	57481	85247	54704
54828	34912	77835	82609	34435	20135	76809	92749	62480	06361
20082	09303	90256	34764	67071	16588	44362	14764	53989	87712
72768									

Key "J"

40323	98951	21717	85036	58133	92917	03426	90743	03097	26866
81873	71862	47048	28468	25624	58083	60935	52738	58634	09590
27494	05240	61040	22916	32320	56015	43508	70715		

Key "K"

65201	48768	92927	29624	72063	40200	45093	20902	53347	37670
31165	70443	36147	66539	16877	40727	61706	11992	40635	48679

Key "L"

89531	09303	25601	01902	07153	58867	70801	76403	53989	57471
07276	73617	31060	82406						

10. The following key was recovered from a depth of two in a Hagelin C-38 machine cipher cryptosystem. Reconstruct the pin and lug settings.

		5			10			15			20			25										
1	16	7	2	19	12	10	19	15	6	0	17	19	21	12	7	23	9	21	7	22	14	18	24	11
1	7	6	15	8	12	12	2	5	15	10	7	19	20	23	18	24	19	24	20	9	1	20	25	24
1	19	19	16	11	21	25	18	20	1	11	6	3	7	24	6	21	9	10	5	8	1	5	25	8
21	15	21	7	23	7	10	6	18	0	20	19	4	20	24	21	6	23	11	6	22	4	15	13	12

DO NOT WRITE ON THIS PAGE

I. Teleprinter key analysis

(Embracing Chapter X)

1a. A certain cipher teleprinter has four wheels with the following patterns and rules of motion:

	1	2	3	4	5	6	7	8	9	
Wheel A:	x	x	o	o	o	x	x	x	o	, moves one step at each operation
Wheel B:	o	x	x	x	o	o	x	x		, moves when A is "x" (CCM motion)
Wheel C:	x	o	o	x	o	x	o			, moves when B is "o"
Wheel D:	o	x	o	x	o					, moves when A+C is "x" (xx, oo=x)

The following wheel combinations are used for the five key levels:

KL1:	A+B,	Vernam (xx, oo=x)
KL2:	A+C,	" " " " "
KL3:	B+C+D,	" " " " "
KL4:	B+D,	mod 2 (xx, oo=o)
KL5:	A+D,	Boolean (xx, xo, ox=x)

With the wheels aligned at their initial positions as shown above, complete the diagram below and decipher the remainder of the cipher text:

		5		10		15		20		25		30																					
A:	x	x	o	o	o	x	x	x	o	x	x	o	o	o	x	x	x	o	x	x	o	o	o	x	x	x	o	x	x	o			
B:	o	x	x	x	x	x	x	o	o	o	x	x	x	x	x	o	x	x	x	x													
C:	x	o	o	o	o	o	o	o	x	o	o	o	o	o	o	x	x	x	x														
D:	o	x	x	o	x	o	o	o	o	o	x	x	o	x	o	o	o	o	o	x													
KL1:	o	x	o	o	o	x	x	o	x	o	x	o	o	o	x	o	x	o	x	x													
KL2:	x	o	x	x	x	o	o	o	x	x	o	x	x	x	o	o	x	o	x	x													
KL3:	x	o	o	x	o	x	x	o	o	x	o	o	x	o	x	o	o	o	o	x													
KL4:	o	o	o	x	o	x	x	o	o	o	o	o	o	x	o	x	o	x	x	x	o												
KL5:	<u>x</u>	<u>x</u>	<u>x</u>	<u>o</u>	<u>x</u>	<u>x</u>	<u>x</u>	<u>x</u>	<u>x</u>	<u>o</u>	<u>x</u>	<u>x</u>	<u>x</u>	<u>x</u>	<u>o</u>	<u>x</u>	<u>x</u>	<u>x</u>	<u>x</u>	<u>o</u>	<u>x</u>	<u>x</u>	<u>o</u>	<u>x</u>	<u>x</u>	<u>o</u>	<u>x</u>	<u>x</u>	<u>o</u>	<u>x</u>	<u>x</u>		
K:	P	Z	L	C	L	X	X	T	A	P	Z	L	C	L	X	T	5	3	5	Q													
C:	S	P	V	Y	Z	G	M	D	T	W	R	3	D	R	L	5	7	U	M	N	5	U	G	M	U	S	K	C	I	3			
P:	N	O	W	9	M	O	V	I	N	G	9	S	O	U	T	H	9	T	O	9													

b. The following bit stream is the result of a Vernam or mod-2 combination of two cyclically stepping wheels, one of which is of size 11, 12, or 13. Recover the pin patterns of the two wheels.

		5		10		15		20		25		30		35																			
x	x	o	o	x	o	o	x	x	o	x	o	x	x	x	o	x	x	o	x	o	x	o	o	o	o	o	o	x	o	x	o	x	
o	x	x	x	x	x	x	x	x	o	o	o	o	o	o	o	o	o	o	o	x	x	o	x	o	x	x	o	x	x	x	o	o	x

c. The following bit stream is the result of a Boolean combination of two cyclically stepping wheels, one of which is of size 11, 12, or 13. Recover the pin patterns of the two wheels.

		5		10		15		20		25		30		35																				
x	x	o	x	x	x	x	x	x	x	o	x	x	o	x	o	o	x	x	x	x	o	x	x	x	x	o	x	x	o	x	x	o	x	
x	x	x	x	x	x	x	x	x	o	x	x	o	o	x	x	o	x	x	x	x	o	x	o	o	x	x	x	x	x	x	x	x	x	x



DO NOT WRITE ON THIS PAGE

3. The following is key from a cipher teleprinter, one of whose wheels is of size 19. Recover all elements of the machine.

⁵ 3-U 9 3 Y T E Y ¹⁰ 9 E 3 M T Y ¹⁵ 9 9 3 U C E P T B ²⁰ 9 4 M C M C E ²⁵ 3 F 8 8 Y ³⁰ 8 M G G Y ³⁵ 8 M G G Y ⁴⁰

O X O O X O X X O X O O O X O O O X O X O O X O O O O O X O X X X X X O O O X  
 O X O O O O O O O O O O O O O X X O X O O O X O X O X O O O X X O X O X X O  
 O X X O X O O X X O O X O X X X O X X O X O O X O X X X X O O X X X X X X O O X  
 X O O X O O O O O X X O O O O X O X O O O X O O X X X X O X X X X O X X X X O  
 O O O X X O X O O O X X X O O O O O O X X X O O X O X O O O O X X X X X X X X

⁴⁵ P W 3 W C 8 F G P ⁵⁰ 8 W M G U ⁵⁵ 3 Y 4 F F E ⁶⁰ 9 Y G C G ⁶⁵ 3 3 9 J ⁷⁰ 9 3 J T G M E W P C T ⁷⁵ 8 M E W P C T ⁸⁰

O X O X O X X O O X X O O X O X O X X X O X O O O O O X O O X O O X X O O O  
 X X O X X X O X X X O X X O O X O O O O O X X X O O O X O O X O X O O X X X O  
 X O O O X X X O X X O X O X O X O X X O X X O X O O O X O X O O O O X O O X X O  
 O O X O X X X X O X O X X O X O O X X X X X O X O X X O X X O O O X O  
 X X O X O X O X X X X X O O X O O O O X X O X O O O O O O O X X X O X X O X

⁸⁵ 4 E M U M E E 4 E T T U ⁹⁰ 3 3 W 4 4 U 8 P G 8 8 F T Y 8 T P B J J 8 C B M P 3 9 C ¹⁰⁰ 8 8 F T Y 8 T P B J J 8 C B M P 3 9 C ¹⁰⁵ 8 8 F T Y 8 T P B J J 8 C B M P 3 9 C ¹¹⁰ 8 8 F T Y 8 T P B J J 8 C B M P 3 9 C ¹¹⁵ 8 8 F T Y 8 T P B J J 8 C B M P 3 9 C ¹²⁰

O X O X O X X O X O O X O O X O O X X O O X X X O X X O O X X X X O X O O O O O  
 X O O X O O O X O O O X O O X X X X X X X X X O O O X O X O X X X X O O X O O X  
 O O X X X O O O O O O X O O O O O X X X O X X X O X X O X O O O X X O X X O X X  
 O O X O X O O O O O O O X X O O O O X O X X X X O O X O O X X X X X X X O X O X  
 O O X O X O O O O X X O O O X O O O X X X X X O X X X X X X O O X O X X X O O O

4. The following is key from a cipher teleprinter involving a combination of three wheels for each key level. Reconstruct all elements of the machine.

⁵ D W R B 8 J S H ¹⁰ 3 A S K U ¹⁵ 5 X U J U F Z J D E D ²⁰ W 3 M O S Y R K I T Z ²⁵ 7 M 3 U C ³⁰ 7 M 3 U C ³⁵ 7 M 3 U C ⁴⁰

X X O X X X X O O X X X X X X X X X X X X X X X O O O X X O X O O X O O O X O  
 O X X O X X O O O X O X X X O X X X O O X O O O X O O O O O X X X O O O O O X X  
 O O O O X O X X O O X X X O X X O X X O O O O O O O X O X X O X X O O O X O X X  
 X O X X X X O O X O O X O X X O X O X O X X O X O X X X O O X X O O O X X O X  
 O X O X X O O X O O O O O O X X O O O O X O O O O X O X X O X O O O X X O O O

⁴⁵ N 9 Z Y 5 9 Y W I Q ⁵⁰ 8 7 S R F K S G T ⁵⁵ 4 9 L T V 9 I J Y G N ⁶⁰ 0 3 L I Q T R X E ⁶⁵ 4 9 L T V 9 I J Y G N ⁷⁰ 0 3 L I Q T R X E ⁷⁵ 4 9 L T V 9 I J Y G N ⁸⁰

O O X X X O X X O X X O X O X X X O O O O O O O O X X O O O O O O X O O X X O  
 O O O O X O O X X X X O O X O X O X O X O X O X X O X O O O X X X O X O O X  
 X X O X O X X O X X X O X O X X X O O O X O O X X X O X O X O O O X X O O X O O  
 X O O O X O O O O O X O O X X X O X O O O O O X O O X O X X X X O O O O X X O O  
 O O X X X O X X O X X O O O O O O X X O O X X X O O O X X O X O X X O X O O

⁸⁵ E J 5 G 5 C 7 G 8 J V R Y Z A L F L N E F W M X T S E N T Y E O N Y R V K 8 N A ⁹⁰ 8 J V R Y Z A L F L N E F W M X T S E N T Y E O N Y R V K 8 N A ⁹⁵ 8 J V R Y Z A L F L N E F W M X T S E N T Y E O N Y R V K 8 N A ¹⁰⁰ 8 J V R Y Z A L F L N E F W M X T S E N T Y E O N Y R V K 8 N A ¹⁰⁵ 8 J V R Y Z A L F L N E F W M X T S E N T Y E O N Y R V K 8 N A ¹¹⁰ 8 J V R Y Z A L F L N E F W M X T S E N T Y E O N Y R V K 8 N A ¹¹⁵ 8 J V R Y Z A L F L N E F W M X T S E N T Y E O N Y R V K 8 N A ¹²⁰

X X X O X O O O X X O O X X X O X O O X X X O X O X X O O X X O O X O O X X O X  
 O X X X X X O X X X X X O O X X O X O O O X O O O O O O O O O O O O X X X X O X  
 O O O O O X O O X O X O X O O O X O X O X O X X O X O X O X O O X X O X X X X O  
 O X X X X X O X X X X X O O O O X O X O X O X X O O O X O O O X X O X X X X X O  
 O O X X X O O X X O X O X X O X O X O O O X X X X O O O X X O X O X O X O O

DO NOT WRITE ON THIS PAGE

5. The following two key streams were recovered by exploiting a "bust" situation. Recover all elements of the cipher teleprinter involved.

Key "A"

	5		10		15		20		25		30		35		40																																	
P	B	K	Y	Y	Q	I	J	4	H	H	T	G	T	D	B	X	Z	F	Z	I	7	N	5	E	U	T	K	8	M	M	U	A	5	9	H	J	G	G	N									
O	X	X	X	X	X	O	X	O	O	O	O	O	O	X	X	X	X	X	O	O	O	X	X	X	O	X	X	O	O	X	X	X	O	O	X	X	O	O	X	O	O	O	O					
X	O	X	O	O	X	X	X	X	O	O	O	X	O	O	O	O	O	O	X	O	O	X	O	X	O	X	X	O	O	X	X	X	O	O	X	X	X	O	O	X	X	X	O					
X	O	X	X	X	X	X	O	O	X	X	O	O	O	O	X	O	X	O	X	O	O	X	O	O	X	O	X	X	X	X	X	O	O	X	X	O	O	O	X	O	O	O	X					
O	X	X	O	O	O	X	O	O	O	O	X	O	X	X	X	O	X	O	O	O	X	X	O	O	O	X	X	X	X	O	O	X	O	O	X	X	X	X	O	O	X	X	X	X				
X	X	O	X	X	X	O	O	O	X	X	X	X	O	X	X	X	O	X	X	X	O	X	O	O	X	O	X	X	X	O	O	X	O	X	X	X	O	O	X	O	X	O	X	X	O			
A	A	Y	W	W	E	7	I	B	V	H	F	K	8	8	3	H	V	C	F	7	9	W	W	D	D	Y	S	9	T	U	5	9	J	I	5	D	R	G	Z									
X	X	X	X	X	X	O	O	X	O	O	X	X	X	X	O	O	O	X	O	O	X	X	X	X	X	X	O	O	X	X	O	X	O	X	X	O	O	X	X	O	O	X	O	O	X			
X	X	O	X	X	O	O	X	O	X	O	O	X	X	X	O	O	X	X	O	O	O	X	X	O	O	O	O	O	X	X	O	X	X	X	O	X	X	O	X	X	O	X	X	O	X	O		
O	O	X	O	O	O	O	X	O	X	X	X	X	X	X	O	X	X	X	X	O	X	O	O	O	X	X	X	O	X	O	X	O	X	O	X	O	X	O	X	O	O	O	O	O	O	O		
O	O	X	X	X	O	O	O	X	X	X	O	O	X	X	O	O	X	X	O	O	O	X	X	O	O	X	O	X	O	O	O	X	O	X	O	O	O	X	O	O	X	O	O	X	X	X		
U	U	N	D	D	Z	D	S	N	E	Y	P	J	4	T	G	H	H	K	F	B	N	5	Z	Z	N	N	J	T	8	X	H	L	9	Y	G	L	B	B	J									
X	X	O	X	X	X	X	X	O	X	X	O	X	O	O	O	O	X	X	X	O	X	X	X	O	O	X	O	X	X	O	O	O	X	O	X	O	O	X	O	O	X	X	X	X	X	X	X	
X	X	O	O	O	O	O	O	O	O	X	X	X	O	X	O	O	X	O	O	O	X	O	O	O	X	O	X	O	O	X	O	O	X	O	O	X	O	O	X	X	O	O	X	X	O	X	O	
X	X	X	O	O	O	X	X	O	X	X	O	O	O	X	X	X	X	O	X	O	O	X	X	O	O	X	X	O	X	X	X	O	X	X	O	X	X	O	O	O	X	O	X	X	X	O	O	
O	O	X	X	X	O	X	O	X	O	O	X	O	O	X	X	X	X	O	O	X	X	X	X	O	O	X	X	X	O	X	X	O	O	O	X	O	X	X	O	O	O	X	O	X	X	X	X	
O	O	O	O	O	X	O	O	O	X	X	O	O	X	X	X	X	O	O	X	O	X	X	X	O	O	X	X	X	X	O	X	X	X	X	O	X	X	X	X	O	X	X	X	X	O	X	X	X

Key "B"

	5		10		15		20		25		30		35		40																																		
M	8	A	M	8	V	C	D	E	B	O	H	H	L	9	Y	W	H	U	P	D	J	C	X	F	9	B	U	Y	Y	B	D	E	T	K	V	7	L	V	R										
O	X	X	O	X	O	O	X	X	X	O	O	O	O	X	X	O	X	O	X	X	O	X	X	O	X	X	X	X	X	X	X	X	O	X	O	O	O	O	O	O	O	O	O	O	O	O			
O	X	X	O	X	X	X	O	O	O	O	O	O	X	O	O	X	O	X	X	O	X	X	O	O	O	O	X	O	O	O	O	O	X	X	O	X	X	O	X	X	X	X	X	X	X	X	X		
X	X	O	X	X	X	X	O	O	O	X	X	O	X	X	O	X	X	X	O	O	X	X	X	O	X	X	X	O	O	O	O	X	X	O	O	X	X	O	O	X	O	O	X	O	O	X	O		
X	X	O	X	X	X	X	O	X	X	O	O	O	O	O	O	X	X	X	X	O	X	O	O	O	X	X	O	O	X	X	O	O	X	X	X	X	O	O	O	X	X	X	X	X	X	X	X	X	
X	X	O	X	X	X	X	O	O	O	X	X	O	O	O	O	X	X	X	X	O	X	O	O	O	X	X	X	O	O	X	X	X	X	O	O	X	X	X	X	O	O	O	X	X	X	X	X		
O	O	X	X	X	O	O	X	X	X	X	O	X	X	O	O	O	X	X	O	O	O	X	X	O	O	X	O	X	O	O	X	O	X	O	O	X	O	O	X	O	O	X	O	O	X	X	X		
K	A	A	4	D	Z	A	S	A	K	8	X	D	D	Z	Z	O	O	E	7	O	R	Y	V	P	I	R	I	B	Y	O	O	T	C	M	G	W	Q	8	4										
X	X	X	O	X	X	X	X	X	X	X	X	X	X	X	O	O	X	O	O	O	O	O	O	O	X	X	O	O	O	O	O	O	O	O	O	O	O	O	O	O	O	X	X	X	O	X	X	X	
X	X	X	X	O	O	X	O	X	X	X	O	O	O	O	O	O	O	O	O	O	X	X	X	X	X	O	O	O	O	O	O	X	O	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	
X	O	O	O	O	O	X	O	X	X	X	O	O	O	O	O	O	O	O	O	O	X	X	X	X	O	X	O	O	O	X	X	O	O	X	X	O	O	X	X	O	O	X	X	O	X	O	X	O	
X	O	O	X	O	O	O	X	X	X	X	O	X	X	O	X	X	O	X	X	O	X	O	X	O	X	O	X	O	X	X	O	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	
O	O	O	O	O	X	O	O	O	X	X	O	O	X	X	X	X	O	X	O	X	X	X	X	O	O	X	X	X	X	X	O	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X

*DO NOT WRITE ON THIS PAGE*

6. From the following key, recover all elements of the cipher teleprinter involved.

	5		10		15		20		25		30		35		40
<u>D</u>	<u>L</u>	<u>G</u>	<u>R</u>	<u>L</u>	<u>5</u>	<u>4</u>	<u>R</u>	<u>G</u>	<u>A</u>	<u>E</u>	<u>K</u>	<u>M</u>	<u>F</u>	<u>3</u>	<u>M</u>
<u>3</u>	<u>Y</u>	<u>W</u>	<u>B</u>	<u>U</u>	<u>S</u>	<u>4</u>	<u>A</u>	<u>D</u>	<u>H</u>	<u>T</u>	<u>M</u>	<u>O</u>	<u>S</u>	<u>S</u>	<u>A</u>
<u>J</u>	<u>D</u>	<u>Z</u>	<u>8</u>	<u>C</u>	<u>V</u>	<u>K</u>	<u>X</u>	<u>V</u>	<u>C</u>	<u>K</u>	<u>X</u>	<u>D</u>	<u>V</u>	<u>C</u>	<u>8</u>
<u>4</u>	<u>R</u>	<u>4</u>	<u>A</u>	<u>D</u>	<u>Q</u>	<u>H</u>	<u>Z</u>	<u>M</u>	<u>3</u>	<u>H</u>	<u>Z</u>	<u>X</u>	<u>R</u>	<u>G</u>	<u>L</u>
<u>5</u>	<u>A</u>	<u>D</u>	<u>N</u>	<u>M</u>											

x o o o o x o o o x x x o x o o o x x x x x o x x o o o o x x x x x x x o x x x  
 o x x x x x x x x o x o o o o o o x o x o x x o o o o o o o x x o o x x x o x  
 o o o o o o o o o o x x x o x o x o o x x o o o x o x o x x o o o o x x x x o  
 x o x x o x o x x o o x x x x x x o o x o o o o x o o x x o o o x x o x x x x x  
 o x x o x x o o x o o o x o o x o x x x o o o o o x x x x o o o o o x x o x o x

	45		50		55		60		65		70		75		80
<u>7</u>	<u>3</u>	<u>O</u>	<u>S</u>	<u>I</u>	<u>I</u>	<u>I</u>	<u>U</u>	<u>S</u>	<u>4</u>	<u>4</u>	<u>R</u>	<u>R</u>	<u>W</u>	<u>B</u>	<u>9</u>
<u>7</u>	<u>3</u>	<u>O</u>	<u>S</u>	<u>I</u>	<u>I</u>	<u>I</u>	<u>U</u>	<u>S</u>	<u>4</u>	<u>4</u>	<u>R</u>	<u>R</u>	<u>W</u>	<u>B</u>	<u>9</u>
<u>7</u>	<u>3</u>	<u>O</u>	<u>S</u>	<u>I</u>	<u>I</u>	<u>I</u>	<u>U</u>	<u>S</u>	<u>4</u>	<u>4</u>	<u>R</u>	<u>R</u>	<u>W</u>	<u>B</u>	<u>9</u>
<u>7</u>	<u>3</u>	<u>O</u>	<u>S</u>	<u>I</u>	<u>I</u>	<u>I</u>	<u>U</u>	<u>S</u>	<u>4</u>	<u>4</u>	<u>R</u>	<u>R</u>	<u>W</u>	<u>B</u>	<u>9</u>
<u>7</u>	<u>3</u>	<u>O</u>	<u>S</u>	<u>I</u>	<u>I</u>	<u>I</u>	<u>U</u>	<u>S</u>	<u>4</u>	<u>4</u>	<u>R</u>	<u>R</u>	<u>W</u>	<u>B</u>	<u>9</u>
<u>7</u>	<u>3</u>	<u>O</u>	<u>S</u>	<u>I</u>	<u>I</u>	<u>I</u>	<u>U</u>	<u>S</u>	<u>4</u>	<u>4</u>	<u>R</u>	<u>R</u>	<u>W</u>	<u>B</u>	<u>9</u>
<u>7</u>	<u>3</u>	<u>O</u>	<u>S</u>	<u>I</u>	<u>I</u>	<u>I</u>	<u>U</u>	<u>S</u>	<u>4</u>	<u>4</u>	<u>R</u>	<u>R</u>	<u>W</u>	<u>B</u>	<u>9</u>
<u>7</u>	<u>3</u>	<u>O</u>	<u>S</u>	<u>I</u>	<u>I</u>	<u>I</u>	<u>U</u>	<u>S</u>	<u>4</u>	<u>4</u>	<u>R</u>	<u>R</u>	<u>W</u>	<u>B</u>	<u>9</u>
<u>7</u>	<u>3</u>	<u>O</u>	<u>S</u>	<u>I</u>	<u>I</u>	<u>I</u>	<u>U</u>	<u>S</u>	<u>4</u>	<u>4</u>	<u>R</u>	<u>R</u>	<u>W</u>	<u>B</u>	<u>9</u>
<u>7</u>	<u>3</u>	<u>O</u>	<u>S</u>	<u>I</u>	<u>I</u>	<u>I</u>	<u>U</u>	<u>S</u>	<u>4</u>	<u>4</u>	<u>R</u>	<u>R</u>	<u>W</u>	<u>B</u>	<u>9</u>
<u>7</u>	<u>3</u>	<u>O</u>	<u>S</u>	<u>I</u>	<u>I</u>	<u>I</u>	<u>U</u>	<u>S</u>	<u>4</u>	<u>4</u>	<u>R</u>	<u>R</u>	<u>W</u>	<u>B</u>	<u>9</u>
<u>7</u>	<u>3</u>	<u>O</u>	<u>S</u>	<u>I</u>	<u>I</u>	<u>I</u>	<u>U</u>	<u>S</u>	<u>4</u>	<u>4</u>	<u>R</u>	<u>R</u>	<u>W</u>	<u>B</u>	<u>9</u>
<u>7</u>	<u>3</u>	<u>O</u>	<u>S</u>	<u>I</u>	<u>I</u>	<u>I</u>	<u>U</u>	<u>S</u>	<u>4</u>	<u>4</u>	<u>R</u>	<u>R</u>	<u>W</u>	<u>B</u>	<u>9</u>
<u>7</u>	<u>3</u>	<u>O</u>	<u>S</u>	<u>I</u>	<u>I</u>	<u>I</u>	<u>U</u>	<u>S</u>	<u>4</u>	<u>4</u>	<u>R</u>	<u>R</u>	<u>W</u>	<u>B</u>	<u>9</u>
<u>7</u>	<u>3</u>	<u>O</u>	<u>S</u>	<u>I</u>	<u>I</u>	<u>I</u>	<u>U</u>	<u>S</u>	<u>4</u>	<u>4</u>	<u>R</u>	<u>R</u>	<u>W</u>	<u>B</u>	<u>9</u>
<u>7</u>	<u>3</u>	<u>O</u>	<u>S</u>	<u>I</u>	<u>I</u>	<u>I</u>	<u>U</u>	<u>S</u>	<u>4</u>	<u>4</u>	<u>R</u>	<u>R</u>	<u>W</u>	<u>B</u>	<u>9</u>
<u>7</u>	<u>3</u>	<u>O</u>	<u>S</u>	<u>I</u>	<u>I</u>	<u>I</u>	<u>U</u>	<u>S</u>	<u>4</u>	<u>4</u>	<u>R</u>	<u>R</u>	<u>W</u>	<u>B</u>	<u>9</u>
<u>7</u>	<u>3</u>	<u>O</u>	<u>S</u>	<u>I</u>	<u>I</u>	<u>I</u>	<u>U</u>	<u>S</u>	<u>4</u>	<u>4</u>	<u>R</u>	<u>R</u>	<u>W</u>	<u>B</u>	<u>9</u>
<u>7</u>	<u>3</u>	<u>O</u>	<u>S</u>	<u>I</u>	<u>I</u>	<u>I</u>	<u>U</u>	<u>S</u>	<u>4</u>	<u>4</u>	<u>R</u>	<u>R</u>	<u>W</u>	<u>B</u>	<u>9</u>
<u>7</u>	<u>3</u>	<u>O</u>	<u>S</u>	<u>I</u>	<u>I</u>	<u>I</u>	<u>U</u>	<u>S</u>	<u>4</u>	<u>4</u>	<u>R</u>	<u>R</u>	<u>W</u>	<u>B</u>	<u>9</u>
<u>7</u>	<u>3</u>	<u>O</u>	<u>S</u>	<u>I</u>	<u>I</u>	<u>I</u>	<u>U</u>	<u>S</u>	<u>4</u>	<u>4</u>	<u>R</u>	<u>R</u>	<u>W</u>	<u>B</u>	<u>9</u>
<u>7</u>	<u>3</u>	<u>O</u>	<u>S</u>	<u>I</u>	<u>I</u>	<u>I</u>	<u>U</u>	<u>S</u>	<u>4</u>	<u>4</u>	<u>R</u>	<u>R</u>	<u>W</u>	<u>B</u>	<u>9</u>
<u>7</u>	<u>3</u>	<u>O</u>	<u>S</u>	<u>I</u>	<u>I</u>	<u>I</u>	<u>U</u>	<u>S</u>	<u>4</u>	<u>4</u>	<u>R</u>	<u>R</u>	<u>W</u>	<u>B</u>	<u>9</u>
<u>7</u>	<u>3</u>	<u>O</u>	<u>S</u>	<u>I</u>	<u>I</u>	<u>I</u>	<u>U</u>	<u>S</u>	<u>4</u>	<u>4</u>	<u>R</u>	<u>R</u>	<u>W</u>	<u>B</u>	<u>9</u>
<u>7</u>	<u>3</u>	<u>O</u>	<u>S</u>	<u>I</u>	<u>I</u>	<u>I</u>	<u>U</u>	<u>S</u>	<u>4</u>	<u>4</u>	<u>R</u>	<u>R</u>	<u>W</u>	<u>B</u>	<u>9</u>
<u>7</u>	<u>3</u>	<u>O</u>	<u>S</u>	<u>I</u>	<u>I</u>	<u>I</u>	<u>U</u>	<u>S</u>	<u>4</u>	<u>4</u>	<u>R</u>	<u>R</u>	<u>W</u>	<u>B</u>	<u>9</u>
<u>7</u>	<u>3</u>	<u>O</u>	<u>S</u>	<u>I</u>	<u>I</u>	<u>I</u>	<u>U</u>	<u>S</u>	<u>4</u>	<u>4</u>	<u>R</u>	<u>R</u>	<u>W</u>	<u>B</u>	<u>9</u>
<u>7</u>	<u>3</u>	<u>O</u>	<u>S</u>	<u>I</u>	<u>I</u>	<u>I</u>	<u>U</u>	<u>S</u>	<u>4</u>	<u>4</u>	<u>R</u>	<u>R</u>	<u>W</u>	<u>B</u>	<u>9</u>
<u>7</u>	<u>3</u>	<u>O</u>	<u>S</u>	<u>I</u>	<u>I</u>	<u>I</u>	<u>U</u>	<u>S</u>	<u>4</u>	<u>4</u>	<u>R</u>	<u>R</u>	<u>W</u>	<u>B</u>	<u>9</u>
<u>7</u>	<u>3</u>	<u>O</u>	<u>S</u>	<u>I</u>	<u>I</u>	<u>I</u>	<u>U</u>	<u>S</u>	<u>4</u>	<u>4</u>	<u>R</u>	<u>R</u>	<u>W</u>	<u>B</u>	<u>9</u>
<u>7</u>	<u>3</u>	<u>O</u>	<u>S</u>	<u>I</u>	<u>I</u>	<u>I</u>	<u>U</u>	<u>S</u>	<u>4</u>	<u>4</u>	<u>R</u>	<u>R</u>	<u>W</u>	<u>B</u>	<u>9</u>
<u>7</u>	<u>3</u>	<u>O</u>	<u>S</u>	<u>I</u>	<u>I</u>	<u>I</u>	<u>U</u>	<u>S</u>	<u>4</u>	<u>4</u>	<u>R</u>	<u>R</u>	<u>W</u>	<u>B</u>	<u>9</u>
<u>7</u>	<u>3</u>	<u>O</u>	<u>S</u>	<u>I</u>	<u>I</u>	<u>I</u>	<u>U</u>	<u>S</u>	<u>4</u>	<u>4</u>	<u>R</u>	<u>R</u>	<u>W</u>	<u>B</u>	<u>9</u>
<u>7</u>	<u>3</u>	<u>O</u>	<u>S</u>	<u>I</u>	<u>I</u>	<u>I</u>	<u>U</u>	<u>S</u>	<u>4</u>	<u>4</u>	<u>R</u>	<u>R</u>	<u>W</u>	<u>B</u>	<u>9</u>
<u>7</u>	<u>3</u>	<u>O</u>	<u>S</u>	<u>I</u>	<u>I</u>	<u>I</u>	<u>U</u>	<u>S</u>	<u>4</u>	<u>4</u>	<u>R</u>	<u>R</u>	<u>W</u>	<u>B</u>	<u>9</u>
<u>7</u>	<u>3</u>	<u>O</u>	<u>S</u>	<u>I</u>	<u>I</u>	<u>I</u>	<u>U</u>	<u>S</u>	<u>4</u>	<u>4</u>	<u>R</u>	<u>R</u>	<u>W</u>	<u>B</u>	<u>9</u>
<u>7</u>	<u>3</u>	<u>O</u>	<u>S</u>	<u>I</u>	<u>I</u>	<u>I</u>	<u>U</u>	<u>S</u>	<u>4</u>	<u>4</u>	<u>R</u>	<u>R</u>	<u>W</u>	<u>B</u>	<u>9</u>
<u>7</u>	<u>3</u>	<u>O</u>	<u>S</u>	<u>I</u>	<u>I</u>	<u>I</u>	<u>U</u>	<u>S</u>	<u>4</u>	<u>4</u>	<u>R</u>	<u>R</u>	<u>W</u>	<u>B</u>	<u>9</u>
<u>7</u>	<u>3</u>	<u>O</u>	<u>S</u>	<u>I</u>	<u>I</u>	<u>I</u>	<u>U</u>	<u>S</u>	<u>4</u>	<u>4</u>	<u>R</u>	<u>R</u>	<u>W</u>	<u>B</u>	<u>9</u>
<u>7</u>	<u>3</u>	<u>O</u>	<u>S</u>	<u>I</u>	<u>I</u>	<u>I</u>	<u>U</u>	<u>S</u>	<u>4</u>	<u>4</u>	<u>R</u>	<u>R</u>	<u>W</u>	<u>B</u>	<u>9</u>
<u>7</u>	<u>3</u>	<u>O</u>	<u>S</u>	<u>I</u>	<u>I</u>	<u>I</u>	<u>U</u>	<u>S</u>	<u>4</u>	<u>4</u>	<u>R</u>	<u>R</u>	<u>W</u>	<u>B</u>	<u>9</u>
<u>7</u>	<u>3</u>	<u>O</u>	<u>S</u>	<u>I</u>	<u>I</u>	<u>I</u>	<u>U</u>	<u>S</u>	<u>4</u>	<u>4</u>	<u>R</u>	<u>R</u>	<u>W</u>	<u>B</u>	<u>9</u>
<u>7</u>	<u>3</u>	<u>O</u>	<u>S</u>	<u>I</u>	<u>I</u>	<u>I</u>	<u>U</u>	<u>S</u>	<u>4</u>	<u>4</u>	<u>R</u>	<u>R</u>	<u>W</u>	<u>B</u>	<u>9</u>
<u>7</u>	<u>3</u>	<u>O</u>	<u>S</u>	<u>I</u>	<u>I</u>	<u>I</u>	<u>U</u>	<u>S</u>	<u>4</u>	<u>4</u>	<u>R</u>	<u>R</u>	<u>W</u>	<u>B</u>	<u>9</u>
<u>7</u>	<u>3</u>	<u>O</u>	<u>S</u>	<u>I</u>	<u>I</u>	<u>I</u>	<u>U</u>	<u>S</u>	<u>4</u>	<u>4</u>	<u>R</u>	<u>R</u>	<u>W</u>	<u>B</u>	<u>9</u>
<u>7</u>	<u>3</u>	<u>O</u>	<u>S</u>	<u>I</u>	<u>I</u>	<u>I</u>	<u>U</u>	<u>S</u>	<u>4</u>	<u>4</u>	<u>R</u>	<u>R</u>	<u>W</u>	<u>B</u>	<u>9</u>
<u>7</u>	<u>3</u>	<u>O</u>	<u>S</u>	<u>I</u>	<u>I</u>	<u>I</u>	<u>U</u>	<u>S</u>	<u>4</u>	<u>4</u>	<u>R</u>	<u>R</u>	<u>W</u>	<u>B</u>	<u>9</u>
<u>7</u>	<u>3</u>	<u>O</u>	<u>S</u>	<u>I</u>	<u>I</u>	<u>I</u>	<u>U</u>	<u>S</u>	<u>4</u>	<u>4</u>	<u>R</u>	<u>R</u>	<u>W</u>	<u>B</u>	<u>9</u>
<u>7</u>	<u>3</u>	<u>O</u>	<u>S</u>	<u>I</u>	<u>I</u>	<u>I</u>	<u>U</u>	<u>S</u>	<u>4</u>	<u>4</u>	<u>R</u>	<u>R</u>	<u>W</u>	<u>B</u>	<u>9</u>
<u>7</u>	<u>3</u>	<u>O</u>	<u>S</u>	<u>I</u>	<u>I</u>	<u>I</u>	<u>U</u>	<u>S</u>	<u>4</u>	<u>4</u>	<u>R</u>	<u>R</u>	<u>W</u>	<u>B</u>	<u>9</u>
<u>7</u>	<u>3</u>	<u>O</u>	<u>S</u>	<u>I</u>	<u>I</u>	<u>I</u>	<u>U</u>	<u>S</u>	<u>4</u>	<u>4</u>	<u>R</u>	<u>R</u>	<u>W</u>	<u>B</u>	<u>9</u>
<u>7</u>	<u>3</u>	<u>O</u>	<u>S</u>	<u>I</u>	<u>I</u>	<u>I</u>	<u>U</u>	<u>S</u>	<u>4</u>	<u>4</u>	<u>R</u>	<u>R</u>	<u>W</u>	<u>B</u>	<u>9</u>
<u>7</u>	<u>3</u>	<u>O</u>	<u>S</u>	<u>I</u>	<u>I</u>	<u>I</u>	<u>U</u>	<u>S</u>	<u>4</u>	<u>4</u>	<u>R</u>	<u>R</u>	<u>W</u>	<u>B</u>	<u>9</u>
<u>7</u>	<u>3</u>	<u>O</u>	<u>S</u>	<u>I</u>	<u>I</u>	<u>I</u>	<u>U</u>	<u>S</u>	<u>4</u>	<u>4</u>	<u>R</u>	<u>R</u>	<u>W</u>	<u>B</u>	<u>9</u>
<u>7</u>	<u>3</u>	<u>O</u>	<u>S</u>	<u>I</u>	<u>I</u>	<u>I</u>	<u>U</u>	<u>S</u>	<u>4</u>	<u>4</u>	<u>R</u>	<u>R</u>	<u>W</u>	<u>B</u>	<u>9</u>
<u>7</u>	<u>3</u>	<u>O</u>	<u>S</u>	<u>I</u>	<u>I</u>	<u>I</u>	<u>U</u>	<u>S</u>	<u>4</u>	<u>4</u>	<u>R</u>	<u>R</u>	<u>W</u>	<u>B</u>	<u>9</u>
<u>7</u>	<u>3</u>	<u>O</u>	<u>S</u>	<u>I</u>	<u>I</u>	<u>I</u>	<u>U</u>	<u>S</u>	<u>4</u>	<u>4</u>	<u>R</u>	<u>R</u>	<u>W</u>	<u>B</u>	<u>9</u>
<u>7</u>	<u>3</u>	<u>O</u>	<u>S</u>	<u>I</u>	<u>I</u>	<u>I</u>	<u>U</u>	<u>S</u>	<u>4</u>	<u>4</u>	<u>R</u>	<u>R</u>	<u>W</u>	<u>B</u>	<u>9</u>
<u>7</u>	<u>3</u>	<u>O</u>	<u>S</u>	<u>I</u>	<u>I</u>	<u>I</u>	<u>U</u>	<u>S</u>	<u>4</u>	<u>4</u>	<u>R</u>	<u>R</u>	<u>W</u>	<u>B</u>	<u>9</u>
<u>7</u>	<u>3</u>	<u>O</u>	<u>S</u>	<u>I</u>	<u>I</u>	<u>I</u>	<u>U</u>	<u>S</u>	<u>4</u>	<u>4</u>	<u>R</u>	<u>R</u>	<u>W</u>	<u>B</u>	<u>9</u>
<u>7</u>	<u>3</u>	<u>O</u>	<u>S</u>	<u>I</u>	<u>I</u>	<u>I</u>	<u>U</u>	<u>S</u>	<u>4</u>	<u>4</u>	<u>R</u>	<u>R</u>	<u>W</u>	<u>B</u>	<u>9</u>
<u>7</u>	<u>3</u>	<u>O</u>	<u>S</u>	<u>I</u>	<u>I</u>	<u>I</u>	<u>U</u>	<u>S</u>	<u>4</u>	<u>4</u>	<u>R</u>	<u>R</u>	<u>W</u>	<u>B</u>	<u>9</u>
<u>7</u>	<u>3</u>	<u>O</u>	<u>S</u>	<u>I</u>	<u>I</u>	<u>I</u>	<u>U</u>	<u>S</u>	<u>4</u>	<u>4</u>	<u>R</u>	<u>R</u>	<u>W</u>	<u>B</u>	<u>9</u>
<u>7</u>	<u>3</u>	<u>O</u>	<u>S</u>	<u>I</u>	<u>I</u>	<u>I</u>	<u>U</u>	<u>S</u>	<u>4</u>	<u>4</u>	<u>R</u>	<u>R</u>	<u>W</u>	<u>B</u>	<u>9</u>
<u>7</u>	<u>3</u>	<u>O</u>	<u>S</u>	<u>I</u>	<u>I</u>	<u>I</u>	<u>U</u>	<u>S</u>	<u>4</u>	<u>4</u>	<u>R</u>	<u>R</u>	<u>W</u>	<u>B</u>	<u>9</u>
<u>7</u>	<u>3</u>	<u>O</u>	<u>S</u>	<u>I</u>	<u>I</u>	<u>I</u>	<u>U</u>	<u>S</u>	<u>4</u>	<u>4</u>	<u>R</u>	<u>R</u>	<u>W</u>	<u>B</u>	<u>9</u>
<u>7</u>	<u>3</u>	<u>O</u>	<u>S</u>	<u>I</u>	<u>I</u>	<u>I</u>	<u>U</u>	<u>S</u>	<u>4</u>	<u>4</u>	<u>R</u>	<u>R</u>	<u>W</u>	<u>B</u>	<u>9</u>
<u>7</u>	<u>3</u>	<u>O</u>	<u>S</u>	<u>I</u>	<u>I</u>	<u>I</u>	<u>U</u>	<u>S</u>	<u>4</u>	<u>4</u>	<u>R</u>	<u>R</u>	<u>W</u>	<u>B</u>	<u>9</u>
<u>7</u>	<u>3</u>	<u>O</u>	<u>S</u>	<u>I</u>	<u>I</u>	<u>I</u>	<u>U</u>	<u>S</u>	<u>4</u>	<u>4</u>	<u>R</u>	<u>R</u>	<u>W</u>	<u>B</u>	<u>9</u>
<u>7</u>	<u>3</u>	<u>O</u>	<u>S</u>	<u>I</u>	<u>I</u>	<u>I</u>	<u>U</u>	<u>S</u>	<u>4</u>						

## DO NOT WRITE ON THIS PAGE

*J. Cryptodiagnosis*  
(Embracing Chapter XI)

One of the difficulties in attacking real-life problems in the initial diagnostic stages, especially when the volume of data might be insufficient, is that the analyst usually does not know just how much information he can glean from the particular data under study: he may be content with uncovering and explaining a phenomenon, or obtaining a partial solution of a technical detail, without realizing perhaps that he could have gone on and made further progress, even without additional data. Therefore, in order to give the analyst some idea of the amount of information he should be looking for (implying thereby some estimate of the time necessary) in each of the message logs below, there is appended a coding indicating the diagnostic aspects in each problem, thus eliminating the wasting of time in searching for nonexistent aspects. This coding is the following:

- A. Preamble information
- B. Enciphered discriminants or indicators
- C. Indicator information
- D. Distributional phenomena
- E. Repetitive phenomena
- F. Other textual characteristics
- G. Further manipulation of text
- H. Nature of general cryptosystem
- I. Identity, source, or generation of key
- J. Plain text recovery

1a. Analyze the following message log: (B)

<i>To</i>	<i>From</i>	<u>NR</u>	<u>FDT</u>	<u>GR</u>	<u>A1</u>	<u>A2</u>	<u>A3</u>	<u>A4</u>	<u>A5</u>	<u>Z1</u>	<u>Z0</u>
MKR	GNU	563	160905	46	29700	30248	55624	56951	62396	58645	73021
MKR	GNU	564	160947	72	81060	80946	20160	63159	81931	95167	35381
MKR	GNU	565	161023	87	70908	17452	94814	29741	67729	47867	24229
MKR	GNU	566	161112	53	22607	35330	02452	24654	36680	09806	76928
MKR	GNU	567	161130	69	38114	58064	76495	23828	06899	64004	82435

b. Analyze the following message log: (BC)

<i>To</i>	<i>From</i>	<u>NR</u>	<u>FDT</u>	<u>GR</u>	<u>A1</u>	<u>A2</u>	<u>A3</u>	<u>A4</u>	<u>A5</u>	<u>Z1</u>	<u>Z0</u>
PHO	ZFC	111	231406	85	22222	46753	40370	14163	14965	89794	09243
PHO	ZFC	112	231415	60	22222	92568	23789	69079	69779	42236	25082
PHO	ZFC	113	231435	64	22222	29886	21688	95738	37986	23001	59377
PHO	ZFC	114	231451	59	22222	86479	64716	51228	93578	60158	81617
PHO	ZFC	115	231510	78	22222	23348	55782	97352	33446	04281	51262

c. Analyze the following message log: (BC)

<i>To</i>	<i>From</i>	<u>NR</u>	<u>FDT</u>	<u>GR</u>	<u>A1</u>	<u>A2</u>	<u>A3</u>	<u>A4</u>	<u>A5</u>	<u>Z1</u>	<u>Z0</u>
CFB	NWL	719	271224	61	33455	90579	72037	34314	65319	77774	16031
CFB	NWL	720	271239	58	33455	12603	99066	55418	76397	92933	44195
CFB	NWL	721	271250	97	33455	40865	21541	34189	94854	44734	56738
CFB	NWL	722	271318	83	33455	56843	31624	99341	91318	14809	27777
CFB	NWL	723	271345	80	33455	30367	10386	38773	43177	20754	56545

## DO NOT WRITE ON THIS PAGE

d. Analyze the following message log: (B)

<u>To</u>	<u>From</u>	<u>NR</u>	<u>FDT</u>	<u>GR</u>	<u>A1</u>	<u>A2</u>	<u>A3</u>	<u>A4</u>	<u>A5</u>	<u>Z1</u>	<u>ZØ</u>
VKF	RNZ	262	031812	48	77477	81523	32207	94592	77092	12019	05166
VKF	RNZ	263	031827	53	77477	79047	09628	91025	04909	26360	19759
VKF	RNZ	264	031834	54	77477	00157	88281	45103	61332	31666	36528
VKF	RNZ	265	031856	67	77477	66723	61932	70782	66863	36062	73567
VKF	FNZ	266	031917	42	77477	55795	63035	69754	44776	28035	04507

e. Analyze the following message log: (BCH)

<u>To</u>	<u>From</u>	<u>NR</u>	<u>FDT</u>	<u>GR</u>	<u>A1</u>	<u>A2</u>	<u>A3</u>	<u>A4</u>	<u>A5</u>	<u>Z1</u>	<u>ZØ</u>
BLV	FTW	489	180918	69	LDSQS	GDOZE	LSRPR	FWOKL	KMVYY	FOZNU	BKURD
BLV	FTW	490	181232	60	BFMPR	CDAWH	ODDFY	VYIJK	GMHOF	VLOJZ	JTGRL
BLV	FTW	491	181550	71	MCLLR	WIRSA	DATGL	GVHFK	ARXPR	YIBCZ	WELPY
BLV	FTW	492	181702	57	UUOOL	GKBCY	KACTM	ONKIE	KTGCR	YPZSA	RADMS
SDM	FTW	724	181019	87	LILQH	POQRD	FTGLY	FBHKA	APRMZ	BFJFT	PZNUG
SDM	FTW	725	181046	74	DLNZQ	ARQAC	NZGXU	XEJTJ	KRQXU	PVJLT	FXHRG
SDM	FTW	726	181625	45	BQXCF	DMIAJ	NVXAA	VJTWY	NMHAA	ASXFO	UMIYZ
WJW	FTW	019	180836	51	ZVSFO	ECECV	NMPQD	TOOZH	GHRVQ	UQLIO	EWKAP
WJW	FTW	020	180850	73	XXRFI	ZQRXF	DYBQQ	RQNZB	BVDVC	YSKDR	WNNVY
WJW	FTW	021	180927	42	ZINKI	FCWRA	QKGD	TBJEB	HHIIX	OFNDY	NYDAP

f. Analyze the following message log: (B)

<u>To</u>	<u>From</u>	<u>NR</u>	<u>FDT</u>	<u>GR</u>	<u>A1</u>	<u>A2</u>	<u>A3</u>	<u>A4</u>	<u>A5</u>	<u>Z1</u>	<u>ZØ</u>
IHI	KTL	431	141152	58	ZTYBZ	DADZH	YDRRP	EDXUZ	JAXCR	JVXBC	BHKFS
IHI	KTL	432	141306	72	ZUFMB	LZGOX	XAYKB	XTLGA	LSTKW	RGVLT	BIRQU
LIZ	KTL	572	141239	71	QXWPX	SCMWH	DARGQ	DVLYL	SXGOC	GBXRD	SLITQ
IHI	KTL	426	150814	49	RDUFM	MJKHL	PVRNR	XHHBJ	UVAVD	GOVBU	TRGJF
LIZ	KTL	576	151602	63	QTHMK	ZHAWL	JSDTE	PGTAF	FVQDM	ICNDK	SHTQD
IHI	KTL	425	161108	82	PGQHA	VNLLS	KUBUG	MLPHY	XEZYK	NBWZB	RUCLT
IHI	KTL	426	161427	74	BYDUX	JPTJV	ZRBRD	RGSRD	BEKJV	BXSEL	DMPYQ
IHI	KTL	430	161628	87	IQDQF	AYFXM	HIROO	RBUID	KRIRB	PLTYQ	KEPUY
LIZ	KTL	574	160915	43	LYPAR	IMQTS	XZNBS	DWGOQ	OJJGQ	CSDGR	NMBEK
LIZ	KTL	575	161021	50	ERJAP	JMWUA	MJANN	MRAUG	JUWBT	IXSXV	GFVEI

g. Analyze the following message log: (ABC)

<u>To</u>	<u>From</u>	<u>NR</u>	<u>FDT</u>	<u>GR</u>	<u>A1</u>	<u>A2</u>	<u>A3</u>	<u>A4</u>	<u>A5</u>	<u>Z1</u>	<u>ZØ</u>
EFS	EMW	872	200740	51	HPLSC	HYIKW	EYRKZ	CCDVC	BEZTW	MVNKL	IZJLX
EFS	RTM	875	201039	67	GIMWT	UFYSN	DRSOQ	HLZIW	VNOHU	BSJGG	VGZTO
EFS	CBQ	876	201057	48	SWBBE	FNCHY	FUAKO	PFHTB	UANTF	TSZCG	GODIZ
EFS	TOK	880	201402	51	NRFCO	WAWII	KALUL	ROXGJ	KVJCC	UFEGP	XBXJJ
EFS	UIO	881	201535	72	HRVTY	XUATS	DSCQR	EABLV	NBEQU	UWIOU	YVBUT
EFS	VES	870	210916	75	FJXTA	YQELU	CSDLX	MKDMR	YFBMX	ARFFC	ZRFMV
EFS	ZQT	871	211140	68	ZZTCE	CCFSY	ECTHE	WIZUB	PVWFG	OWEUN	DDGTZ
EFS	LJN	873	211305	87	GIJAJ	OVZMD	DRPSG	UKJYC	SCHMD	VVYPM	PWANE
EFS	ZEK	876	211326	40	ITHEF	CQWQZ	ETKPN	FCNWC	UXQYD	FHJRX	DRXRA
EFS	VIJ	879	211611	62	AHCBJ	YUVXD	WGJCX	XQITG	RPTJH	ACPQA	ZVWYE



## DO NOT WRITE ON THIS PAGE

h. Analyze the following message log: (ABC)

<u>To</u>	<u>From</u>	<u>NR</u>	<u>FDT</u>	<u>GR</u>	<u>A1</u>	<u>A2</u>	<u>A3</u>	<u>A4</u>	<u>A5</u>	<u>Z1</u>	<u>Z0</u>
ARX	NNA	490	190600	64	35701	18339	89693	14177	01595	80756	16855
ARX	NNA	192	190842	66	91175	29984	05187	84552	70971	50132	04144
HIS	NNA	963	190857	83	06712	04331	93924	83705	78125	59386	23988
ARX	NNA	670	191015	80	65000	54336	68077	33709	27120	09381	24045
HIS	NNA	688	191029	72	10565	67184	76969	55331	48753	21914	84831
HIS	NNA	014	191141	64	19676	86281	49637	98047	80460	64621	01473
ARX	NNA	460	191306	81	11188	32192	34137	13597	94921	89182	51010
ARX	NNA	576	191419	82	45912	44566	39458	24211	44705	90967	73869
ARX	NNA	632	191427	79	51695	14491	48616	30993	59488	06640	41589
HIS	NNA	103	191443	53	55004	28665	95676	07962	25458	73610	47643

i. Analyze the following message log: (BC)

<u>To</u>	<u>From</u>	<u>NR</u>	<u>FDT</u>	<u>GR</u>	<u>A1</u>	<u>A2</u>	<u>A3</u>	<u>A4</u>	<u>A5</u>	<u>Z1</u>	<u>Z0</u>
WRP	JVM	981	171102	62	61865	98903	67654	08586	17697	99036	23755
MRP	JVM	982	171305	60	91514	28652	63757	33763	04680	52696	93443
WRP	JVM	984	171636	64	27362	54400	47306	71988	88231	68901	96814
WRP	JVM	985	181050	63	47149	74287	67790	08626	86697	96885	22501
WRP	JVM	987	181312	63	36556	63694	98567	39495	30217	52313	25292
WRP	JVM	988	181632	60	38237	65375	89641	51714	20570	75995	53878
WRP	JVM	989	191108	62	15646	42784	99866	30706	45630	28788	31962
WRP	JVM	990	191315	63	72845	09983	04945	19874	45886	39636	90706
WRP	JVM	992	191628	60	55624	82762	65748	58104	06681	39112	23261
WRP	JVM	993	191646	63	00802	37940	59941	90885	55406	32701	31989

j. Analyze the following message log: (BC)

<u>To</u>	<u>From</u>	<u>NR</u>	<u>FDT</u>	<u>GR</u>	<u>A1</u>	<u>A2</u>	<u>A3</u>	<u>A4</u>	<u>A5</u>	<u>Z1</u>	<u>Z0</u>
OKH	ULO	401	081014	78	69158	62316	99237	72652	16948	55420	09145
OKH	ULO	401	091037	48	26219	30140	37135	13567	45329	66206	39210
OKH	ULO	401	120925	53	92327	54798	24392	07724	12517	25401	32314
OKH	ULO	401	151142	60	81761	90274	05858	73601	92063	21758	94943
OKH	ULO	401	180926	57	51047	45489	06846	89287	39931	37570	91034
OKH	ULO	401	191057	91	88068	63327	14153	46760	16223	28055	22972
OKH	ULO	401	211123	52	19086	97953	80188	70390	01628	59073	57295
OKH	ULO	401	231000	55	34199	54162	78867	37513	64982	74186	16421
OKH	ULO	401	241045	67	51864	87898	85741	68194	07164	90691	91851
OKH	ULO	401	260956	59	49079	16281	52854	35200	86754	17363	89066

## DO NOT WRITE ON THIS PAGE

k. Analyze the following message log: (BDFGHIJ)

<u>To</u>	<u>From</u>	<u>NR</u>	<u>FDT</u>	<u>GR</u>	<u>A1</u>	<u>A2</u>	<u>A3</u>	<u>A4</u>	<u>A5</u>	<u>Z1</u>	<u>ZØ</u>
FLC	BUG	317	020900	49	89108	27704	66181	03417	22745	11635	33769
SLY	BUG	892	020917	48	23062	60022	74850	16163	48145	53539	27123
ZBJ	BUG	724	021021	62	64527	14424	45932	04392	42625	93094	18483
ZBJ	BUG	725	021037	59	87118	47047	81605	35392	14046	11655	01878
BUG	FLC	027	021013	60	20276	60309	41766	15086	35338	50763	24734
ZBJ	FLC	946	021145	58	75087	27705	70442	21153	52511	02524	09643
BUG	SLY	375	020941	75	37157	02828	64004	91086	27705	61634	81712
BUG	ZBJ	421	021052	43	25073	50541	70382	25401	00302	52500	39334
FLC	ZBJ	803	021108	67	65729	02826	83500	78244	14450	94276	49183
SLY	ZBJ	514	021121	81	31534	02822	73910	36125	01615	64011	15392

l. Analyze the following message log: (BFGHIJ)

<u>To</u>	<u>From</u>	<u>NR</u>	<u>FDT</u>	<u>GR</u>	<u>A1</u>	<u>A2</u>	<u>A3</u>	<u>A4</u>	<u>A5</u>	<u>Z1</u>	<u>ZØ</u>
DOM	KLS	501	130816	63	86284	89703	98576	07737	93244	61746	23577
DOM	KLS	502	131139	48	59911	11594	16667	99528	02606	36289	96768
DOM	KLS	504	131406	46	02889	54220	06677	37543	22356	95153	40600
DOM	KLS	501	141000	52	39080	48214	88104	42145	85639	39712	79416
DOM	KLS	502	141027	51	13198	42412	25116	01346	22642	85453	59870
DOM	KLS	501	150902	60	78513	87031	46483	35751	66336	01998	13004
DOM	KLS	503	151345	58	11539	67932	88399	97555	65640	62505	51464
DOM	KLS	502	161125	49	40554	84220	73220	73133	86796	99002	83346
DOM	KLS	503	161152	62	76068	34450	80745	35618	47627	38807	18402
DOM	KLS	505	161308	54	20098	42604	91590	03999	49087	54236	69572

m. Analyze the following message log: (BDEFH)

<u>To</u>	<u>From</u>	<u>NR</u>	<u>FDT</u>	<u>GR</u>	<u>A1</u>	<u>A2</u>	<u>A3</u>	<u>A4</u>	<u>A5</u>	<u>Z1</u>	<u>ZØ</u>
WKN	JNT	704	101402	58	53044	50667	62274	96641	98885	74944	62773
WKN	JNT	705	101421	72	49984	72827	69484	48865	58234	13460	60282
WKN	JNT	706	101450	63	80772	32975	21872	44544	55012	68041	82906
WKN	JNT	707	101505	65	18134	90656	23444	34820	39266	64489	13489
WKN	JNT	708	101532	84	73966	40205	05796	82983	69404	22854	19425
WKN	JNT	709	101555	60	39910	36522	20270	70988	42494	56460	64431
WKN	JNT	710	101619	73	31066	24325	83306	22543	83015	14532	02581
WKN	JNT	712	101647	81	51120	98139	83690	89249	51096	58642	40243
WKN	JNT	715	101723	55	87978	46272	88758	73924	69614	14128	38066
WKN	JNT	719	101830	47	29770	28725	23430	66944	15032	95690	64190

## DO NOT WRITE ON THIS PAGE

n. Analyze the following message log: (BDFHIJ)

To	From	NR	FDT	GR	A1	A2	A3	A4	A5	Z1	Z0
ESW	PTB	336	010930	59	BFCUB	QPDFI	OJFRV	GEFCB	XWDAK	DHSEK	DDGTK
ESW	PTB	337	010956	62	NPYRS	DMWVY	DETHD	IBRFD	BHINH	RGOGP	PAUWH
ESW	PTB	338	011010	63	FAGQT	SERVY	LKFBU	DCPQY	NAFZD	ABCNH	HSGHD
ESW	PTB	339	011036	58	GCARQ	OLCQF	UNTRD	JIKTQ	MQVYK	QHQCQ	IZUKK
ESW	PTB	340	011055	60	OKXKJ	ZNYBC	IPNGR	GWDFY	OVHSF	NTIQR	QBOWF
ESW	PTB	342	011130	71	NERJH	TYVBM	DHAFQ	ADPRQ	VWHQU	AJKHD	PMBIU
ESW	PTB	343	011216	76	GHOQR	YXCSF	YNWCN	OQFBT	VUWTD	UDPBT	ILXSD
ESW	PTB	344	011242	54	YNCSR	DRIQH	STOJW	PNOQZ	AGRJT	JUWTD	AFPHT
ESW	PTB	347	011350	82	QCGMY	YBPRS	GUFBK	VEFRN	QTORG	FOGBH	SPGIG
ESW	PTB	348	011607	73	SZFSE	FNIXP	WALRB	UPBCD	RDJRA	NPDIC	UBMTA

o. Analyze the following message log: (BCDFHIJ)

To	From	NR	FDT	GR	A1	A2	A3	A4	A5	Z1	Z0
IXN	YBB	936	051032	67	XGLFZ	MVJNS	ERKXU	BHFUX	ODMRX	AVGJR	18965
IXN	YBB	939	051517	82	AHMEA	GNJNN	AYGDL	XJXDO	PDVGI	RVHLO	73421
JFH	YBB	272	050820	49	AMMLA	LSGKS	ACENM	HACMW	UNDNA	YOJJP	98265
JFH	YBB	273	050835	58	WIOIA	NQFHG	QAXNE	AUHHM	NDUKN	RXGIV	46328
JFH	YBB	274	051141	52	YKNIZ	HREGN	FREVB	PEZTB	JLAVS	UTCOS	58742
PWC	YBB	708	050856	79	RHIEY	HTFKH	XDAWI	LQSJX	GOUDO	VXF00	04597
PWC	YBB	710	051539	80	SHFJU	IQHMV	BZOTR	AFZBJ	ZRVVT	UVHNQ	76150
XGD	YBB	564	050925	63	YLLIX	IQCEP	HUAGY	ASHZL	YHUSF	WPHJR	87429
XGD	YBB	565	051017	75	WNNMR	IUIMC	PXVNF	WASLB	TDJKS	UTFJT	49683
XGD	YBB	566	051445	56	WIFHS	NRFIM	HZZEJ	ERVTE	IWAEC	YRBMV	25831

p. Analyze the following message log: (BFHIJ)

To	From	NR	FDT	GR	A1	A2	A3	A4	A5	Z1	Z0
YWR	TFE	439	220752	56	62711	26977	42197	32966	09424	23634	14492
YWR	TFE	440	220812	59	16887	75144	78023	12322	68913	32481	74368
YWR	TFE	441	220827	60	37128	82143	54217	21876	62125	16463	73569
YWR	TFE	442	220855	55	81022	06272	63327	94223	70649	28321	86693
YWR	TFE	443	221024	57	09999	10261	16332	39077	48187	18726	51680
YWR	TFE	445	221107	68	67498	93465	73427	71972	99223	44773	03789
YWR	TFE	446	221241	73	33522	56732	19211	72518	44228	71063	54553
YWR	TFE	447	221305	51	66387	77578	88244	61620	37148	99778	43598
YWR	TFE	450	221428	79	21280	11837	82264	47612	73982	87668	89551
YWR	TFE	451	221443	70	35532	17201	04767	16776	27492	61721	38023

q. Analyze the following message log: (BHIJ)

To	From	NR	FDT	GR	A1	A2	A3	A4	A5	Z1	Z0
HUE	AZI	124	300955	48	PMCVC	XULRR	MFPLN	SNOIF	KJHUU	59721	95723
HUE	AZI	125	301026	73	ZFZPG	TGTVM	WYMVO	NMLBU	MESQY	84856	37365
HUE	AZI	126	301324	56	MBEGU	AVVMO	JUXAO	IXQSU	ILLFM	33577	22088
HUE	AZI	128	301502	52	JZOJN	VMMNV	GSIEH	VVAHV	ASIIF	40890	71321
HUE	AZI	129	301525	85	WPGDX	CBVIS	TIUWN	SOSZN	ZFMCP	57113	20664
HUE	AZI	130	301548	69	YUWNI	KOLHL	VNXGJ	TTIGQ	EULMA	97903	91985
HUE	AZI	131	301617	78	JZOHP	ZIGLV	GSKFE	VXATH	SUGGH	44016	11549
HUE	AZI	132	301730	71	PZMTN	EDMIQ	MSTUH	XIYEN	IPRSF	31919	02424
HUE	AZI	133	301803	67	UBQIX	EEOJL	RUIVD	HUCWL	WJRHP	75925	13963
HUE	AZI	136	301842	58	BUVVX	VGTVP	YNXQR	OBHPV	SVSUP	77583	33527

DO NOT WRITE ON THIS PAGE

r. Analyze the following message log: (BFGHIJ)

To	From	NR	FDT	GR	A1	A2	A3	A4	A5	Z1	ZØ
GSM	MNS	847	070712	98	37777	70995	39344	99967	86507	05503	59983
GSM	MNS	848	070806	87	86348	99941	00594	99901	02009	57780	89582
GSM	MNS	849	070831	99	26998	46760	11696	02921	89997	68770	90684
GSM	MNS	850	070916	93	55766	94356	66959	85899	97792	49580	45947
GSM	MNS	851	071014	82	81859	79121	11987	73199	93108	77400	60847
GSM	MNS	852	071052	95	90839	91030	03997	99932	44689	55705	70028
GSM	MNS	853	071107	88	56675	94003	35888	41664	79995	78029	35663
GSM	MNS	854	071328	86	46776	82272	01472	10195	89991	21108	61260
GSM	MNS	855	071545	90	17958	86380	21188	07499	90987	81120	00176
GSM	MNS	856	071619	91	54896	67788	03737	99932	53002	67093	33884

s. Analyze the following message log: (BCGHIJ)

To	From	NR	FDT	GR	A1	A2	A3	A4	A5	Z1	ZØ
SHF	CVG	501	150756	83	AVUXB	OPRVJ	NIFTH	MWQPD	DOUSN	59326	19072
SHF	CVG	502	150835	90	UHIPC	PGVXX	NTZUM	BBJVT	CNFUC	27758	87583
SHF	CVG	503	150941	48	VMMRL	NBMYN	KBBOL	TCGHC	XKAGG	61083	21924
SHF	CVG	504	151037	62	PQHCZ	BXUHV	XOKQP	SCXSQ	SJJRK	15746	76773
SHF	CVG	505	151052	56	WTIJP	HUXAV	WJTOV	UJMES	BIFRW	32188	93130
SHF	CVG	506	151126	59	UJWBX	WZQXI	VHUIR	IQIUA	ZUDGL	94392	55418
SHF	CVG	507	151153	78	YZXSB	UJXHW	HGNPO	AMPRH	KCELC	57911	18064
SHF	CVG	508	151210	85	ANPEV	KKZPJ	JQQFI	DEQJS	BURJG	80647	41857
SHF	CVG	509	151421	73	VOEJW	SYMSI	TLIOP	FSHLZ	DWZZW	03469	64880
SHF	CVG	510	151650	69	WJVHV	FBMBL	KPDMP	TQFHN	FVSDS	47530	08180

t. Analyze the following message log: (BDHIJ)

To	From	NR	FDT	GR	A1	A2	A3	A4	A5	Z1	ZØ
OJP	ZKM	251	040810	62	QMUYE	RCBDX	MNSFW	GBTXA	IXROY	YWVPE	NFGFW
OJP	ZKM	252	040846	88	YVGHK	LAXDY	NACXF	UMNAE	PGBWQ	LTREX	ITJKQ
OJP	ZKM	253	040915	74	CXIDT	WUFHB	SRGJB	CMLQQ	NJANC	AAAAE	PKSQT
OJP	ZKM	254	040942	86	UNUHX	TKZTO	MKULO	WUESA	NXGZC	RIBHW	TNQZS
OJP	ZKM	255	041005	99	PMGRV	LBOQE	NZXGG	OTWKR	TRAZC	PJRMJ	QKMGU
OJP	ZKM	256	041028	60	LWRUM	BVYVL	WNSQB	KIMUJ	WEAHS	VLJUG	IPDBE
OJP	ZKM	257	041052	98	GTLSE	MTBDU	WRSFZ	OTKGQ	VCBMX	AJQDX	JMNKM
OJP	ZKM	259	041121	89	JMJXA	SIFEE	NYXSN	GKAHM	AGHIM	JHQHO	DDMOE
OJP	ZKM	260	041143	65	KHUHZ	YPLQI	LQUEA	JYNYT	PXFSN	MZIWO	MQRZF
OJP	ZKM	262	041200	87	EMRUM	LPOUT	SQYPA	GZJQL	WOZMR	SAAAP	IIABL

2. Diagnose the following, reconstruct all elements of the cryptosystem, and recover the plain text:

ZUBBK	AZUJM	OMVZO	NDUPX	XCNQZ	OKAET	WRGUX	BGVUZ	UPEVC	XLAZO
MQVPO	IFIKE	TKAIZ	OJRRW	KAPBV	ZUPQE	NSEPL	KILKI	HVOBJ	KEBIZ
OJLCZ	UFKEB	NKIBK	ALGJT	XGAIR	TAFNV	KAYJU	GJRYB	ESBNZ	UZYEG
KAGKI	LYGXH	PPDYZ	YQZUJ	IZOQA	DHBGH	KESBI	LMRGR	WKEHR	ZOJDK
ITKIZ	UKEKA	CZURC	KEMXB	IKAKE	IXZOW	FPGXM	LMJVK	EMOQI	ISKEG
DPZYM	BWBKA	CGZUS	JHWZO	JPOYF	OJTQO	OKAPA	DCXTE	VUVNX	VXZUY
TZOXL	LTOOU	ONJJS	KITKE	UDXKA	VKIJJ				

DO NOT WRITE ON THIS PAGE

3. Diagnose the following, reconstruct all elements of the cryptosystem, and recover the plain text:

AAUMQ	AGNYD	HOFXV	ETMQH	SLDON	EXOWQ	RVHAW	KAMNX	NPCGQ	DLMPS
XAIUB	QDWXU	PLDED	OJIAR	OQEER	MOXMY	LHQGU	GDCXF	HHZQE	CVEMX
BVVEQ	ORWDX	TMWPW	HQMLM	WXRAR	OMDIF	GQEER	MOBWX	ULWUS	EWOQP
CXFIH	PMNRW	LQOYD	KZSOX	MOLBO	QSPEI	ORPUH	XERTF	HAIUB	QDWXJ
TPEID	KSAVQ	VVAOX	NDRWA	AHUQH	IGTXD	LQBFY	GOXFJ	AYHGU	QWPXZ
ERQLG	WDKXN	PNAOM	FQHIX	TUPES	MWCKH	QJLZX	EEPMO	QMYLH	

4. Diagnose the following, reconstruct all elements of the cryptosystem, and recover the plain text:

BSZXG	YMPSX	QAHOL	YCDSF	IQAWQ	MYMEX	BRRWN	ZPWWC	KQAHF	OBYCW
LTYVO	QXMEZ	PPCGN	ZTJBR	YYLER	JTDQW	AOYUZ	EDFSZ	DBUKD	FFQLZ
IBDZB	MLCJH	QKJHI	KOWTG	KLASG	LKUY	KNJCP	HRBIX	QUAOC	NELLY
HNAPH	IISYP	DNJKR	MVBHJ	QVFXG	TVLLQ	HTJQQ	WESUY	BQOLE	GNCUP
WIWXH	QEIJL	ZSUQS	DWZVW	TRODL	IVZAP	RVREH	PZZWC	MQWBT	GDXTF
TLEIM	OAAGN	ZDSRL	XXUVP	WZPNS	TTREI	YGLQP	RELZV	BTPIV	NXHUN
PLNYE	ISUWD	XWGPV	IRCKP	JCSRJ	VVSMI	UVNOG	UEABV	CRRJF	YSFIO
YFDMK	SGEQJ	LHJUD	JCMQM	BVLSS	FIVXH	JDZLE	RJTDK	ZSWCQ	EPGNN

5. Diagnose the following, reconstruct all elements of the cryptosystem, and recover the plain text:

CFLOL	ACABJ	GGCFD	DCGAB	ACOJA	DOACG	ACAHN	OEACA	GMOIA	CLLFI
JLNOG	JLIEA	CCDIO	JADOH	LACAC	GALFA	GAGAC	ODEJB	DOABC	AHJAK
ADAGC	HACMO	CLIFA	GAGAC	LNOAI	JDFIF	JGDOK	ACFGH	OAILA	CAICL
ACMOF	GOKAG	CABAF	OADJL	ACDIO	DIJAI	OABCD	EFGHO	ABJAG	OFGAD

6. Diagnose the following cryptogram, suspected of dealing with agent activity in Greece, and recover as much plain text as possible:

ANLSL	GSGLN	SYSLD	LSAUS	ALASG	SLLPS	AOSYG	LSLSN	SYGSL	ULSAA
SLLGS	ASLSL	SYRYS	YDSLY	LSYSD	PSOSA	PRSLG	SADUS	YYSYO	USLNS
YGLSL	SLAYS	YOSLY	USAYS	GLNSY	SLLNS	ADSDP	SOSAD	USYYS	YRYSY
DSOPS	LASLG	USLNS	YOLSD	SAYOS	USLSL	SAPRS	LGSYU	SLNSD	PSOSA
LRSAA	SLYUS	YRSLD	USLOS	YGLSL	SLONS	ALSDP	SOSAU	ASLLS	YRYSY
DSGSO									

7. Diagnose the following, reconstruct all elements of the cryptosystem, and recover the plain text:

SMFXB	MNEIB	ESLPR	CMEXP	UIKKS	MCSRZ	NBIWX	FENFX	PNBEI	YZXBP
QPJEC	JSVZD	LVCRA	YYOZS	ODAKV	DLOCR	AYJDA	YMODD	JZDVA	ZDL0D
QPTAK	UIOCS	XOKAH	OXWTS	PIFHS	HIODH	RUKOV	OOEJH	OXVSH	FDOQZ
UPYXL	VTTJL	VUXYP	YZYPU	OJXEI	PVZXA	PVSJY	PVUVN	IEOZS	JYPVU
XQLMJ	UPJXM	VEIDM	JIAJG	EICRR					

8. Diagnose the following, reconstruct all elements of the cryptosystem, and recover the plain text:

XXSDR	RUFTS	IRPIH	ZENWK	HSWPW	ZIEWM	VKHCK	VFSBL	GEMUW	TDSPU
HTIKY	ZGHKL	UOWDD	UYRNW	QBJED	AEMFC	JSBWP	IJGKB	BUKUM	DWDZP
GYOCT	PDCKX	UDFCW	DHRTT	DSGXR	ZQVOT	YOLUW	FKWKW	XAXVW	FBYHM
TCLVK	MNCQH	NCFBL	UTZPY	UMPDC	XBKKC	EQHBI	GYNKV	NULXX	EMIQW
VJFPD	BPPZK	QZATA	DVBQZ	ATRAF	PKCDX				

**INDEX**

(b) (1)  
 (b) (3)-18 USC 798  
 (b) (3)-50 USC 3024(i)  
 (b) (3)-P.L. 86-36

## INDEX

The entries contained herein have been indexed down to sub-subparagraph wherever possible. Entries from footnotes are indexed by showing the paragraph location followed by a dagger (†), and the footnote number; for example, footnote 50 out of subparagraph 77f(5) is indexed by the notation "77f(5)†50."

	Paragraphs	Pages
Absent letters (J, K, Q, W, X, Z)	78c	402
[Redacted]		
Affinities of letter contacts	77g(7)	386
Alphabets, 26-letter random	App. 5	553
Amalgamation of generatrices, strip cipher solution	48e	167
Aperiodic digraphic substitution systems	81b, c	415
Aperiodic systems:		
[Redacted]		
Cryptographic principles of	5	4
Practical definition of	1a	1
Art of cryptanalysis vs. science of cryptanalytics	1a†1	1
[Redacted]		
Autokey systems:		
Characteristics of	35b, c	115
Enciphering conventions in	35g, h	117
Autokeying:		
Ciphertext	21b	41
Plaintext	21c	42
Autokeying trials:		
Ciphertext	76n(4)	351
Plaintext	76n(5)	352
[Redacted]		
Average I.C.	24c	52
Base letter	23b	49
Basic letter frequency data, 24 foreign languages	App. 6	561
Basic steps in diagnosis	72	325
Baudot:		
Combination tables	64a	263
Teleprinter code	63	263
Blank cells in transposition matrices	77f(3)	370
Book key:		
Expected distribution of cipher	77e(6)	364
Sources	7b; 56a, b	7, 227
[Redacted]		
Characteristic uniliteral frequency distributions	77e	360
[Redacted]		
Check indicators	76g(3)	340
Chemical analogy in diagnosis	71b(2)	323
Chi-square:		
Interpretation of delta I.C.	77b†33	358
Table	77h	390
Test, applications of	77h	390
Test, use of Poisson tables in	77h(5)†67	398

(b) (1)  
(b) (3) -18 USC 798  
(b) (3) -50 USC 3024 (i)  
(b) (3) -P.L. 86-36

Chi test:	Paragraphs	Pages
Applications of	76n	355
Formula for	76p	355
Cipher devices:		
Cylindrical	45a	151
Early	49	173
Geared disk cryptomechanisms	55b-d	222
Kryha	52-54	184
Strip ciphers	48c	166
Wheatstone	50, 51	173
Cipher square with arbitrary key letters	28a	70
Cipher teleprinters:		
Baudot code	63	199
Baudot combination tables	63	199
Key generation in	64	263
Ciphertext autokey systems:		
Cryptography of	21b	41
Digital	28c	72
Digraphic I.C. in	24c	52
Enciphering conventions in	35h	119
Generatrix methods in	22b	44
Probable-word method in	22c, d	46
Solution by frequency analysis	23, 24	48
Solution by means of isologs	26, 27	59
Solution by means of isomorphs	25	55
Trial decipherments on hypothesis of	76n(4)	351
Ciphertext digraphic autokey systems	81b, c	415
Ciphertext interruptor systems:		
Cryptography of	16	29
Cleartext indicators	78f(7)	409
Code books as sources of key	59h	240
Code text enciphered by M-94, analysis of	48h	168
Coincidences, intermittent	13d(2)	22
Combinations, formula for number of	65d†12	277
Combined plaintext-ciphertext autokey system	82	416
Combined substitution-transposition	77e(9)	366
Completing the plain-component sequence:		
Example of	9b	8
Incomplete components in	11c(1)	11
Value of	76i	342
Contact affinities of letters	77g(7)	386
Control elements for indicator encipherment	76g(4)	340
Conversion square, digital	28b†27	72
Conversion to monoalphabetic terms:		
Kryha machine systems	53h	194
Requirements for	12e	17
Wheatstone systems	51c(2), (3)	181
(See also "Reduction to monoalphabetic terms")		
Correct answers obtained in spite of errors	78f(6)†73; 81c†4	408, 416
Cribbing:		
Diagram for crib placement	18a(2)†12	31
Wheatstone systems	51c(2), (3)	180