Departamento de Matemáticas

"Generation of sequences for communications and cryptology"

A sequence is any ordered succession of numbers. Depending on the application, the required properties of the sequence vary. In cryptography, the sequences must be computationally indistinguishable from true random ones, while communications need orthogonally between the sequences. The aim of this talk is to give an overview of both approaches.
Pseudorandom Random Number Generators (PRNGs) that are initialized by a random seed, then a known algorithm produces a sequence with good statistical properties. The applications of these generators are many, just as a standalone application but also combined with physical processes to guarantee "randomness" in Hybrid random number generators (HRNGs). The presence of linear structures make it possible to generate sequences in a more efficient way, but also these results in a security vector attack because these relations can be computed quite efficiently.
Generation and simulation of families of sequences with good auto and cross correlation is required in wireless communications and other applications. Many constructions have been proposed that employ m-sequences as basic building blocks, such as the Gordon- Mills-Welch (GMW). The method of composition and substitution is useful to understand and construct generalized sequence generators.

Ana Isabel Gómez

Universidad Rey Juan Carlos, Madrid.

e-mail: ana.gomez.perez@urjc.es

Fecha: 18 de junio, a las 11:00 horas.
Lugar: Seminario de Matemáticas.
Enlace on line: https://meet.google.com/xtm-vckh-pto

Biography: Ana Isabel Gómez received a master degree in telecommunications engineering from the Universidad de Cantabria and, after working in the industry, completed her PhD in Science and Technology. Her research interests are oriented to applications of sequences in the area of cryptography, communications and radar. Apart from theoretical knowledge, she has hand-in experience in these areas from collaborations with companies in the field of Information Technologies and public research entities.
Now, she is an assistant professor in the department of Computer Science at Universidad Rey Juan Carlos in Madrid.