**Departamento de Matemáticas**

# Secuencias t-modificadas: una nueva clase de secuencias para uso criptográfico.

**Abstract:**

Los números aleatorios son un elemento clave en múltiples procesos de la vida digital. Estos se utilizan no sólo en aplicaciones con gran componente de aleatoriedad como puede ser el juego online, sino que también tienen múltiples aplicaciones en el mundo de la ciberseguridad.
En esa ocasión definiremos y analizaremos una familia de generadores de secuencia de uso criptográfico denominadas t-modificados.
Dicha familia incluye entre sus elementos al generador self-shrinking (SSG) y al generador modified self-shrinking (MSSG), los cuales poseen buenas propiedades criptográficas y son fáciles de implementar, como por ejemplo en sistemas de cifrado en flujo.

## Amparo Fúster

**Instituto de Tecnologías Físicas y de la Información**
**Consejo Superior de Investigaciones Científicas**

Fecha: 4 de marzo a las 13h
Lugar: Seminario de Matemáticas