

## OBJETIVO DEL CURSO

Este curso se enmarca dentro de la especialidad *Aplicaciones de las Matemáticas* del *Máster en Matemáticas y Aplicaciones de la Universidad Autónoma de Madrid*. El objetivo principal de este curso será el entendimiento en profundidad de las matemáticas que subyacen en algunos de los mas importantes sistemas criptográficos usados en la actualidad, centrándose en los de clave pública. Se mostrarán algunas aplicaciones de la criptografía en el mundo real.

Se hará uso de diversas técnicas provenientes de la Teoría de Números. Uno de ellas serán las curvas elípticas. De las que se aprenderán sus propiedades mas importantes así como su relevancia dentro de la criptografía moderna.

Se hará uso del software matemático libre **SAGE**.

---

## PROGRAMA

### 1. Introduccion a la Criptografía

- Criptografía clásica.
- Criptografía de clave privada vs. Criptografía de clave pública.

### 2. RSA

- Factorización.
- Tests de primalidad.
- Algunas aplicaciones: intercambio de claves, firmas digitales,...

### 3. Logaritmo discreto

- Diffie-Hellman.
- El Gamal.

### 4. Curvas elípticas y Criptografía.

- Ley de grupo en una curva elíptica.
  - Propiedades fundamentales de las curvas elípticas definidas sobre los racionales.
  - Propiedades fundamentales de las curvas elípticas definidas sobre cuerpos finitos.
  - Criotistemas basados en el logaritmo discreto en curvas elípticas.
- 

## PROFESORES

Enrique González Jiménez,  
enrique.gonzalez.jimenez@uam.es

Despacho C–XV–610  
<http://www.uam.es/enrique.gonzalez.jimenez>

---

## EVALUACIÓN

- **45 %:** Problemas y prácticas **SAGE**.
  - **45 %:** Trabajo y presentación final.
  - **10 %:** Participación en clase.
-

---

## BIBLIOGRAFÍA

- I. Blake, G. Seroussi, N. Smart. *Elliptic Curves and Cryptography*. Cambridge. University Press (1999)
- H. Cohen. *Handbook of elliptic and hyperelliptic curve cryptography*. Chapman & Hall/CRC (2006)
- D. Hankerson, A.J. Menezes, S. Vanstone. *Guide to Elliptic Curve Cryptography*. Springer (2004).
- J. Hoffstein, J. Pipher, J.H. Silverman. *An introduction to mathematical cryptography*. Springer (2008).
- N. Koblitz. *A course in Number Theory and Cryptography*, 2nd ed.. Springer-Verlag (1994).
- David R. Kohel. *Cryptography*. <http://echidna.maths.usyd.edu.au/~kohel/tch/Crypto/>
- J. Menezes, P. C. van Oorschot, S. A. Vanstone. *Handbook of applied cryptography*. CRC Press (1997). (Versión electrónica: <http://www.cacr.math.uwaterloo.ca/hac/>)
- D. R. Stinson. *Cryptography theory and practice*. Chapman & Hall/CRC (2006)

---

SAGE : <http://www.sagemath.org>