# TEORÍA DE CÓDIGOS Y CRIPTOGRAFÍA

**Curso 2010–11**

## OBJETIVO DEL CURSO

- Comprender el papel de las matemáticas en la transmisión segura y fiable de la información.
- Familiarizarse con algunos ejemplos notables de criptosistemas de clave simétrica. Saber cómo se usan, sus fortalezas y sus debilidades.
- Entender la diferencia entre criptografía de clave simétrica y criptografía de clave pública.
- Conocer algunas aplicaciones de la criptografía de clave pública, en particular las firmas digitales.
- Conocer el funcionamiento de RSA y de los criptosistemas basados en logaritmos discretos.
- Familiarizarse con los principales tests de primalidad y algoritmos de factorización.
- Conocer los fundamentos teóricos de los códigos detectores y correctores de errores.
- Trabajar con ejemplos usuales de códigos detectores (NIF, código de barras, ISBN, CCC, etc.).
- Familiarizarse con algunas familias de códigos correctores (Hamming, BCH).
- Saber utilizar los algoritmos de codificación/decodificación para detectar/corregir errores.

---

## PROGRAMA

### INTRODUCCIÓN:

Ideas generales. Códigos criptográficos y códigos detectores y correctores de errores.

### BLOQUE A: CRIPTOGRAFÍA.

A1: Criptosistemas clásicos. Cesar, Vigenère, matrices de cifra. Análisis de frecuencias e índice de coincidencia.

A2: Criptografía de clave pública. Una aplicación: las firmas digitales.

A3: Algoritmos de factorización y tests de primalidad. Introducción a la idea de complejidad.

A4: El criptosistema RSA.

A5: Otros criptosistemas de clave pública y más aplicaciones.

### BLOQUE B: TEORÍA DE CÓDIGOS.

B1: Códigos detectores y correctores de errores. Propiedades generales y estudio de tres ejemplos prácticos: El código de barras, el ISBN y el NIF.

B2: Códigos lineales.

B3: Algoritmos de codificación y decodificación para códigos lineales. Decodificación incompleta.

B4: Códigos de hamming. Relación con la geometría proyectiva.

B5: Códigos perfectos. Códigos de golay.

B6: Códigos BCH. Los códigos que se utilizan en un CD.

---

## BIBLIOGRAFÍA


- J. I. Hall. Notes on Coding Theory. `http://www.mth.msu.edu/~jhall/classes/classes.html`.
- R. Hill. A first course in coding theory. Oxford University Press, 1986.
- J. Hoffstein, J. Pipher, J.H. Silverman. *An introduction to mathematical cryptography*. Springer (2008).
- N. Koblitz. *A course in Number Theory and Criptography*, 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/`).
- N. Smart, Cryprography, an introduction. `http://www.cs.bris.ac.uk/~nigel/Crypto_Book/`.
- D. R. Stinson. *Cryptography theory and practice*. Chapman & Hall/CRC (2006).


## EVALUACIÓN

Examen Final Ordinario: 27 de Enero 2011 Examen Final Extraordinario: 8 de Septiembre 2011

Con carácter general, la nota será la que se obtenga en el examen final. Sin embargo, y como quedarán muchos temas abiertos, quien lo desee podrá realizar un trabajo adicional (teórico o de implementación informática) que, en caso de ser satisfactorio, servirá para subir la nota. Quienes estén interesados deberán indicárselo al profesor antes del 30 de noviembre, aunque el trabajo se podrá entregar hasta el día del examen. En ningún caso se asignará un trabajo después del examen.

## AULA, HORARIO, TUTORÍAS

Aula: 01.11.AU.205 Horario: 12:30–13-30, Lunes a Jueves

Tutorías: Se ruega pedir cita.

## PROFESOR


Enrique González Jiménez, Despacho 01.17.610

`enrique.gonzalez.jimenez@uam.es` `http://www.uam.es/enrique.gonzalez.jimenez`