TEORÍA DE CÓDIGOS Y CRIPTOGRAFÍA

Curso 2011–12

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: Introducción a la idea de complejidad.

A4: Algoritmos de factorización y tests de primalidad.

A5: El criptosistema RSA.

A6: 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.

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).
- D. 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/).
- R. A. Podestá. *Introducción a la teoría de códigos autocorrectores*. http://www.famaf.unc.edu.ar/series/pdf/pdfCMat/CMat35-3.pdf
- 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: 25 de enero 2012 Examen Final Extraordinario: 27 de junio 2012

Habrá dos examenes parciales voluntarios. El primero (25/11/2011) de ellos dedicado al Bloque A: Criptografía y el segundo (13/1/2013) al Bloque B: Teoría de Códigos.
Aquellos alumnos que no superen ambos parciales o quieran subir su calificación, podrán presentarse al examen final ordinario. La NOTA FINAL será la obtenida en el examen final o bien la media de los parciales, siempre y cuando hayan superado ambos parciales. Aquellos alumnos que habiendo aprobado ambos parciales se presenten al examen final obtendrán la NOTA FINAL igual a la obtenida en el examen final ordinario.

AULA, HORARIO, TUTORÍAS

Aula: 01.14.AU.403 Horario: 12:30–13-30, Lunes a Jueves
Tutorías: Solicitar cita.

PROFESOR

Enrique González Jiménez, Despacho 01.17.508
enrique.gonzalez.jimenez@uam.es http://www.uam.es/enrique.gonzalez.jimenez