Criptografía (itinerario Aplicado del Master)
Curso 2007-2008, 2º semestre.

Objetivos:

- Entender en profundidad las matemáticas que subyacen a los sistemas criptográficos más utilizados, tanto de clave pública como de clave privada.
- Conocer algunas aplicaciones de la criptografía.
- Aprender a programar protocolos criptográficos.

Programa:

Bloque 1: Consideraciones generales sobre Criptografía

1. Criptografía de clave privada frente a Criptografía de clave pública.
2. Algunos ejemplos de Criptosistemas de clave privada: Vigenère, la máquina Enigma.
3. Algunos ejemplos de Criptosistemas de clave pública: RSA, logaritmo discreto.
4. Algunas aplicaciones: intercambio de claves, firmas digitales, protocolos de conocimiento cero, funciones hash criptográficas.

Bloque 2: Curvas Elípticas y Criptografía

5. Qué es una curva elíptica. La ley de grupo.
6. Resultados fundamentales para CE sobre Q.
7. Resultados fundamentales para CE sobre cuerpos finitos.
8. Criptosistemas basados en el logaritmo discreto en CE.
9. Emparejamientos y criptografía.

Bloque3: Métodos avanzados de clave privada

10. Data Encription Standard (DES)
11. Advanced Encription Standard (AES).

Los Bloques 1 y 2 se complementarán con sesiones prácticas en el Laboratorio de Cálculo Numérico utilizando SAGE (se puede descargar gratuitamente para distintos sistemas operativos desde http://www.sagemath.com/)**.**

Referencias:

- 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).
- 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/
- S. Landau. Standing the Test of Time: The Data Encryption Standard. Notices of the AMS 47-3 (marzo 2000) y Communications Security for the Twenty-first Century: The Advanced Encryption Standard. Notices of the AMS 47-4 (abril 2000).
- 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)

Evaluación: Problemas y prácticas (50%), participación en clase (10%), examen o presentación final (40%).

Página web de la asignatura:

http://www.uam.es/enrique.gonzalez.jimenez/docencia/0708/cripto0708.html

Calendario previsto:

- 19 de febrero-13 de marzo (4 semanas): Bloque 1 e Intrioducción a SAGE.
- 25 de marzo-17 de abril (4 semanas): Bloque 2 y uso de SAGE para hacer criptografía usando curvas elípticas.
- 21-24 de abril (4 días), profesor invitado: **Roger Oyono**, Université de la Polynésie Française (Francia). Criptografía usando curvas de género >1, en particular curvas hiperélipticas.
- 28 de abril-4 de mayo (1 semana): descanso.
- 5-8 de mayo (4 días) , profesora invitada: **Tanja Lange**, Technische Universiteit Eindhoven (Holanda). Criptografía sobre curvas elípticas vs. Criptografía sobre curvas hiperelípticas.
- 13-29 de mayo (3 semanas): Bloque 3 [y remate de lo que quede pendiente del Bloque 2]
- 2-5 de junio (4 días), profesor invitado: **Steven Galbraith**, Royal Holloway University of London (Reino Unido). Emparejamientos y Criptografía; Criptografía basada en la identidad.

Horario previsto: Martes y jueves, de 14:30 a 16:00, salvo las semanas con profesores invitados en las que habrá clase de lunes a jueves. Cuando haya laboratorio habrá que alterar los horarios (los martes está ocupado).

Lugar: Habitualmente C-XV-320