Programa de Máster
"Matemáticas y aplicaciones"
Departamento de Matemáticas (UAM)
Año académico 2010-2011

Criptografía
Profesor: Fernando Chamizo Lorente

Objetivos del curso

Este curso introduce algunas técnicas matemáticas empleadas en la criptografía de clave pública. Se hace especial hincapié en la criptografía de curvas elípticas que está alcanzando un gran desarrollo y atención actualmente y que tiene un contenido matemático más profundo que el criptosistema RSA.

El temario está en la línea de anteriores ediciones del curso. En general se siguen los contenidos esenciales de los capítulos 1, 2, 3 y 5 de [**?**] y dentro de los temas complementarios habrá una incursión en el resto.

Las prácticas serán una parte fundamental del curso pero al estar dedicado a aspectos matemáticos su finalidad será entender y completar la base teórica más que diseñar aplicaciones reales o entender protocolos informáticos. Referente a los lenguajes de programación, algunas opciones son emplear C o Python dentro del paquete SAGE. Todo el *software* necesario será libre.

Se supone un conocimiento a nivel de licenciatura de teoría de números y de teoría de grupos. No obstante se repasarán los temas que se necesiten. En general son bienvenidos conocimientos de matemática discreta. Además para las prácticas se supone cierto gusto y habilidad programando.

Programa

1. Introducción histórica

1.1 Motivación y ejemplos

1.2 Repaso de teoría de grupos y teoría de números

1.3 Cuerpos finitos

1.4 Ejemplos sencillos de encriptación

2. El problema del logaritmo discreto

2.1 Enunciado y ejemplos

2.2 Ataques básicos

2.3 El intercambio de claves Diffie-Hellman

2.4 El criptosistema de ElGamal

3. El criptosistema RSA

3.1 Algoritmo, ejemplos y precauciones

3.2 Criterios de primalidad y factorización

3.3 Introducción a la criba de cuerpos de números

4. Criptografía de curvas elípticas

4.1 Curvas elípticas y ley de grupo

4.2 Factorización con curvas elípticas

4.3 Criptosistemas asociados al logaritmo discreto

5. Temas complementarios

5.1 Firmas digitales

5.2 El algoritmo DES

5.3 Criptosistemas *knapsacks*

5.4 Criptosistemas basados en retículos

Bibliografía

1. Ho-Pi-Si Hoffstein, J.; Pipher, J.; Silverman, J.H. An introduction to mathematical cryptography. Undergraduate Texts in Mathematics. Springer, New York, 2008.

2. Stein, W. Elementary number theory: primes, congruences, and secrets. A computational approach. Undergraduate Texts in Mathematics. Springer, New York, 2009.

3. Blake, I. F.; Seroussi, G.; Smart, N.P. Elliptic curves in cryptography. Reprint of the 1999 original. London Mathematical Society Lecture Note Series, 265. Cambridge University Press, Cambridge, 2000.

4. Koblitz, N. A course in number theory and cryptography. Second edition. Graduate Texts in Mathematics, 114. Springer-Verlag, New York, 1994.

5. Menezes, A.J.; van Oorschot, P.C.; Vanstone, S.A. Handbook of applied cryptography. With a foreword by Ronald L. Rivest. CRC Press Series on Discrete Mathematics and its Applications. CRC Press, Boca Raton, FL, 1997.

6. Buchmann, J. Introduction to cryptography. Second edition. Undergraduate Texts in Mathematics. Springer-Verlag, New York, 2004.