Asignatura: Criptografía
Código: 30076
Centro: Ciencias
Titulación: Máster en Matemáticas y aplicaciones
Nivel: Máster M2
Tipo: Optativa
Nº de créditos: 8

# ASIGNATURA / COURSE TITLE

Criptografía / Cryptography

## 1.1. Código / Course number

30076

## 1.2. Materia / Content area

Criptografía / Cryptography

## 1.3. Tipo / Course type

Formación optativa / Elective subject

## 1.4. Nivel / Course level

Máster M2 / Master M2

## 1.5. Curso / Year

2014/2015

## 1.6. Semestre / Semester

Segundo / Second (Spring semester)

## 1.7. Idioma / Language

Español e inglés. (El curso se podrá impartir en inglés siempre y cuando, al menos, un alumno internacional matriculado en la asignatura lo solicite). / Spanish and English. (The course can be taught in English if at least one officially registered international student requests so).

## 1.8. Requisitos previos / Prerequisites

Asumimos como prerequisito para este curso un conocimiento básico de teoría elemental de números y teoría de grupos. Será útil tener conocimientos básicos de curvas algebraicas (pero los resultados esenciales se recordarán durante el curso). Para los proyectos informáticos se asume que el estudiante tiene experiencia previa con ordenadores. Los proyectos usarán Sage.

We assume as a prerequisite for this course a basic proficiency in elementary number theory and group theory. Some knowledge of algebraic curves is useful (but key results will be recalled during the course). For the programming projects prior experience with computers is assumed. Projects will be handled using Sage.

## 1.9. Requisitos mínimos de asistencia a las sesiones presenciales / Minimum attendance requirement

75%

## 1.10. Datos del equipo docente / Faculty data

Docente(s) / Lecturer(s): Enrique González Jiménez
Departamento de / Department of: Mathematics
Facultad / Faculty: Science
Despacho - Módulo / Office – Module: 508– M17
Teléfono / Phone: +34 91 497 7641
Correo electrónico/Email: enrique.gonzalez.jimenez@uam.es
Página web/Website: http://www.uam.es/enrique.gonzalez.jimenez
Horario de atención al alumnado/Office hours: By appointment

## 1.11. Objetivos del curso / Course objectives

En este curso presentamos algunas de las técnicas matemáticas usadas en criptografía de clave pública. Estudiaremos los criptosistemas RSA, de ElGamal y los que utilizan curvas elípticas. Entre estos últimos se cuentan algunos de los más serios competidores al criptosistema RSA y son más profundos desde un punto de vista matemático.

In this course we present some of the mathematical techniques employed in public-key cryptography. We consider RSA, ElGamal and elliptic curve cryptosystems. This latter is one of the most serious competitors to RSA cryptosystem and deeper from the mathematical point of view.

## 1.12. Contenidos del programa / Course contents

1. **Introducción histórica.** Motivación y ejemplos. Teoría elemental de grupos y teoría elemental de números. Cuerpos finitos. Algoritmos de cifrado sencillos.
2. **El criptosistema RSA.** Algoritmo, ejemplos y precauciones. Tests de primalidad y algoritmos de factorización.
3. **Problema del Logaritmo Discreto.** Enunciado y ejemplos. Ataques básicos. Sistema de intercambio de claves de Diffie-Hellman. Criptosistema de

ElGamal. Ataques genéricos y específicos para un grupo para el Problema del Logaritmo Discreto

4. **Aplicaciones de curvas elípticas a la criptografía.** Curvas elípticas y la estructura de grupo. Versión elíptica del problema del logaritmo discreto. Emparejamientos y criptografía. Aplicaciones de curvas elípticas a factorización y test de primalidad.

1. **Historical introduction.** Motivation and examples. Elementary group theory and number theory. Finite fields. Simple encryption algorithms.
2. **The RSA cryptosystem.** Algorithm, examples and cautions. Primality tests and factorization algorithms.
3. **Discrete Logarithm Problem.** Statement and examples. Basic attacks. Diffie-Hellman key exchange. The ElGamal cryptosystem. Generic and group specific attacks for the Discrete Logarithm Problem
4. **Applications of elliptic curves to cryptography.** Elliptic curves and group law.The elliptic version of the discrete logarithm problem. Pairings and cryptography. Applications of elliptic curves to factorization and primality testing.

## 1.13. Referencias de consulta / Course bibliography


- 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.
- Cohen, H., Frey, F.; Handbook of elliptic and hyperelliptic curve cryptography. Chapman \& Hall/CRC, 2006.
- Hankerson, D., Menezes, A.J., Vanstone, S.; Guide to Elliptic Curve Cryptography. Springer, 2004.
- Hoffstein, J., Pipher, J., Silverman, J.H.; An introduction to mathematical cryptography. Springer, 2008.
- Koblitz, N.; A course in number theory and cryptography. Second edition. Graduate Texts in Mathematics, 114. Springer-Verlag, New York, 1994.
- Koblitz, N.; A Algebraic aspects of criptography, Springer-Verlag, New York, 1998.
- J. Menezes, P. C. van Oorschot, S. A. Vanstone. Handbook of applied cryptography, CRC Press, 1997. [http://www.cacr.math.uwaterloo.ca/hac/]
- Stein, W. Elementary number theory: primes, congruences, and secrets. A computational approach. Undergraduate Texts in Mathematics. Springer, New York, 2009.
- Stinson, D.R.;.Cryptography theory and practice. Chapman & Hall/CRC, 2006.

## 2. Métodos Docentes / Teaching methodology

Las clases combinarán contenido teórico y práctico. Intentaremos usar el ordenador. Sin embargo, dado que se trata de un curso orientado a los aspectos matemáticos de la criptografía, el propósito de los ejercicios de programación será entender los fundamentos teóricos más que intentar diseñar implementaciones eficientes.

The lectures will combine theoretical and practical contents. We shall try to use the computer. However, taking into account that the course is devoted to mathematical aspects of cryptography, the purpose of the programming exercises will be to understand the theoretical basis rather that to design actual efficient applications.

## 3. Tiempo de trabajo del estudiante / Student workload

| | | Nº de horas | |
|---|---|---|---|
| Presencial | Clases teóricas | 42h(21%) | 66h (33%) |
| | Clases prácticas | 4 h (2%) | |
| | Tutorías | 14 h (7%) | |
| | Seminarios y trabajos | 2 h (2%) | |
| | Examen final / proyecto | 2h (1%) | |
| No presencial | Elaboración de problemas | 40h(20%) | 134h (67%) |
| | Estudio semanal | 88h(44%) | |
| | Preparación del examen | 6h(3%) | |
| Carga total de horas de trabajo: 25 horas x 8 ECTS | | 200 h | |

## 4. Métodos de evaluación y porcentaje en la calificación final / Evaluation procedures and weight of components in the final grade

1) Examen final o proyecto: 50%.

2) Ejercicios y problemas para resolver con ordenador: 40%.

3) Ejercicios hechos en clase, participación: 10%

1) Final exam and/or final project: 50%.
2) Exercises and computer assignments: 40%.
3) In-class exercises, participation: 10%

**EVALUACIÓN EXTRAORDINARIA / Make up exam**:
Examen ante tribunal de Máster/ Examination by a committee.

## 5. Cronograma* / Course calendar

| Semana<br>Week | Contenido<br>Contents | Horas presenciales<br>Contact hours | Horas no presenciales<br>Independent study time |
|---|---|---|---|
| 1-2 | Historical introduction | 7 | 13 |
| 2-4 | The RSA cryptosystem | 10 | 19 |
| 4-6 | Discrete Logarithm problem | 12 | 22 |
| 6-8 | Attacks for the Discrete Logarithm Problem | 10 | 22 |
| 8-10 | Introduction to the arithmetic of elliptic curves | 9 | 19 |
| 11-12 | Elliptic curve cryptography | 10 | 20 |
| 13-14 | Applications of elliptic curves to factoring and primality testing | 8 | 19 |

*El cronograma es orientativo / This calendar is tentative.