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

ASIGNATURA / COURSE TITLE

Cryptography

1.1. Código / Course number

30076

1.2. Materia / Content area

Cryptography

1.3. Tipo / Course type

Elective subject.

1.4. Nivel / Course level

Master M2

1.5. Curso / Year

2011/2012

1.6. Semestre / Semester

2nd (Spring semester)

1.7. Número de créditos / Credit allotment

8 ECTS credits

1.8. Requisitos previos / Prerequisites

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. Key results will be recalled in the course. For the programming projects prior experience with computers is assumed. Projects will be handled using mostly Sage, but other computing languages are acceptable.

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

75%

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

1.10. Datos del equipo docente / Faculty data

Docente(s) / Lecturer(s): Adolfo Quirós Gracián
Departamento de / Department of: Mathematics
Facultad / Faculty: Science
Despacho - Módulo / Office – Module: 507 – M17
Teléfono / Phone: +34 91 497 4941
Correo electrónico/Email: adolfo.quiros@uam.es
Página web/Website: http://www.uam.es/adolfo.quiros
Horario de atención al alumnado/Office hours: By appointment

1.11. Objetivos del curso / Course objectives

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. **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. Introduction to the number field sieve.
3. **Discrete logarithm problem.** Statement and examples. Basic attacks. Diffie-Hellman key exchange. The ElGamal cryptosystem.
4. **Elliptic curve cryptography.** Elliptic curves and group law. Elliptic curves and factorization. The elliptic version of the discrete logarithm problem. Pairings and cryptography.
5. **Complementary topics.** Digital signatures. The DES and AES algorithms. Knapsack cryptosystems.

1.13. Referencias de consulta / Course bibliography

[1] 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.
[2] Koblitz, N. A course in number theory and cryptography. Second edition. Graduate Texts in Mathematics, 114. Springer-Verlag, New York, 1994.
[3] Koblitz, N. A Algebraic aspects of criptography, Springer-Verlag, New York, 1998
[4] J. Menezes, P. C. van Oorschot, S. A. Vanstone. Handbook of applied cryptography, CRC Press (1997). [http://www.cacr.math.uwaterloo.ca/hac/]
[5] Stein, W. Elementary number theory: primes, congruences, and secrets. A computational approach. Undergraduate Texts in Mathematics. Springer, New York, 2009.
[6] D. R. Stinson.Cryptography theory and practice. Chapman & Hall/CRC (2006)

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

2. Métodos Docentes / Teaching methodology

The lectures combine theoretical and practical aspect. 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. There will be programmed tutoring sessions.

3. Tiempo de trabajo del estudiante / Student workload

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

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

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 Week	Contenido Contents	Horas presenciales Contact hours	Horas no presenciales Independent study time
1-2	Historical introduction	6	12
2-5	Discrete logarithm problem	12	24
5-8	The RSA cryptosystem	12	24
8-12	Elliptic curve cryptography	16	32
12-14	Complementary topics	10	20
15-16	Evaluation	10	22

*This calendar is tentative.