Asignatura: Criptografía
Código: 32934
Centro: Ciencias
Titulación: Máster en Matemáticas y aplicaciones
Nivel: Máster M2
Tipo: Optativa
Nº de créditos: 6

ASIGNATURA / COURSE TITLE

Criptografía / Cryptography

1.1. Código / Course number

32934

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

2018/2019

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 preferentemente Sage (aunque el alumno podrá optar por otro lenguaje de programación que admita aritmética entera).

Asignatura: Criptografía
Código: 32934
Centro: Ciencias
Titulación: Máster en Matemáticas y aplicaciones
Nivel: Máster M2
Tipo: Optativa
Nº de créditos: 6

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 primarily Sage (but students can choose to use another programming language, provided it can handle integer arithmetic).

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): Yago Antolín Pichel
Departamento de / Department of: Mathematics
Facultad / Faculty: Science
Despacho - Módulo / Office – Module: 610– M17
Teléfono / Phone: +34 91 497 5610
Correo electrónico/Email: yago.antolin@uam.es
Página web/Website: https://sites.google.com/site/yagoanpi/
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. Estudiaremos problemas computacionales asociados a la teoría de grupos, y veremos propuestas de criptosistemas basados en estos problemas tomando como plataforma grupos no abelianos.

In this course we present some of the mathematical techniques employed in public-key cryptography. We consider RSA, ElGamal and elliptic curve cryptosystems. We will study computational problems associated to group theory, and we see how these problems led to cryptosystems over non-abelian groups.

1.12. Contenidos del programa / Course contents

1. **Introducción a la criptografía Moderna.** Motivación y ejemplos. Teoría elemental de grupos y teoría elemental de números. Cuerpos finitos. Teoría de la complejidad y algoritmos. Definición de criptosistema y definiciones de

Asignatura: Criptografía
Código: 32934
Centro: Ciencias
Titulación: Máster en Matemáticas y aplicaciones
Nivel: Máster M2
Tipo: Optativa
Nº de créditos: 6

seguridad. Factorización y RSA. Logaritmo discreto, Diffie-Hellmann y El Gamal. Firmas digitales.

2. **Curvas elípticas y 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.

3. **Grupos no conmutativos y criptografía.** Grupos finitamente generados. Presentaciones. Algunos problemas de decisio¤n
cla¤sicos. Algunos grupos populares: grupo de trenzas, grupos de Baumslag-Solitar, grupos de Thompson, grupos polici¤clcos.
Criptosistemas basados en problemas de decisio¤n.

1. **Introduction to Modern Criptography.** Motivation and examples. Elementary group theory and number theory. Finite fields. Complexity theory and algorithms. Definition of a cryptosystem and basics on security. Factorization and RSA. Discrete logarithm, Diffie-Hellmann and El Gamal. Digital signatures.
2. **Elliptic curves and 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.
3. **Group-based cryptography.** Finitely generated groups. Presentations and classic decision problems. Some popular groups: Braid groups, Baumslag-Solitar groups, Thompson groups, polyciclic groups. Criptosystems based on decision problems.

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.
- S. D. Galbraith. Mathematics of Public Key Cryptography, Cambridge University Press (2012).
- Gómez Pardo, J. L. Introduction to Cryptography with Maple. Springer, 2013.
- 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.
- J. Katz and Y. Lindell. Introduction to modern criptography, 2nd ed. , CRC Press (2014).

Asignatura: Criptografía
Código: 32934
Centro: Ciencias
Titulación: Máster en Matemáticas y aplicaciones
Nivel: Máster M2
Tipo: Optativa
Nº de créditos: 6

- 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/]
- A. G. Myasnikov, V. Shpilrain, and A. Ushakov, Group-based Cryptography. Advanced Courses in Mathematics – CRM Barcelona, Birkhauser Basel, 2008.
- 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	39 h (26%)	51 h (34%)
	Clases prácticas	3 h (2%)	
	Tutorías	6 h (4%)	
	Seminarios y trabajos	---	
	Examen final / proyecto	3 h (2%)	
No presencial	Elaboración de problemas	42 h (28%)	99 h (66%)
	Estudio semanal	49 h (33,3%)	
	Preparación del examen / proyecto	8 h (5,33%)	
Carga total de horas de trabajo: 25 horas x 6 ECTS		150 h	

Asignatura: Criptografía
Código: 32934
Centro: Ciencias
Titulación: Máster en Matemáticas y aplicaciones
Nivel: Máster M2
Tipo: Optativa
Nº de créditos: 6

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: 40%.

2) Ejercicios y problemas resueltos con ordenador (en su caso): 50%.

3) Ejercicios hechos en clase, participación: 10%

1) Final exam and/or final project: 40%.
2) Exercises and (possibly) computer assignments: 50%.
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
1-4	Introduction to Modern Criptography	12	25
5-8	Elliptic curves and cryptography	12	25
9-14	Group-based cryptography	15	40

*El cronograma es orientativo / This calendar is tentative.