Asignatura: Teoría de Códigos y Criptografía
Código: 16471
Centro: Facultad de Ciencias
Titulación: Grado en Matemáticas
Curso Académico: 2017-2018
Tipo: Optativa B
Nº. de Créditos: 6

1. ASIGNATURA / COURSE TITLE

TEORÍA DE CÓDIGOS Y CRIPTOGRAFÍA

1.1. Código / Course number

16471

1.2. Materia/ Content area

MATEMÁTICAS

1.3. Tipo /Course type

OPTATIVA B

1.4. Nivel / Course level

GRADO

1.5. Curso / Year

CUARTO

1.6. Semestre / Semester

PRIMERO

1.7. Idioma / Language

Español. Se emplea también Inglés en material docente / In addition to Spanish, English is also extensively used in teaching material

1.8. Requisitos previos / Prerequisites

El curso pretende ser "elemental". El requisito básico es tener confianza con las congruencias. Más concretamente, hay que conocer el contenido de "Conjuntos y Números" (divisibilidad y factorización; Algoritmo de Euclides; operaciones y polinomios con congruencias: el Pequeño Teorema de Fermat) y de "Algebra Lineal" (vectores y matrices sobre el cuerpo Z/p con p primo). También se utilizarán resultados básicos de Probabilidad. Pueden aparecer ocasionalmente

conceptos estudiados en otras asignaturas. Ocasionalmente se propondrán actividades con ordenador que podrán resolverse usando SAGE, MatLab, etc.

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

La asistencia a clase es muy recomendable. Pueden plantearse actividades de evaluación continua durante las horas de clase.

1.10. Datos del equipo docente / Faculty data

Coordinador:
Profª. Angélica Benito.
Departamento: Matemáticas
Facultad: Ciencias Módulo 17 Despacho 610
Teléfono: 91 497 3612
E-mail: angelica.benito@uam.es
http://www.uam.es/angelica.benito
Horario de Tutorías individuales: Se fijan a petición individual del alumno

El resto del profesorado implicado en la asignatura puede consultarse en la página web del título:

http://www.uam.es/ss/Satellite/Ciencias/es/1242671471248/listadoCombo/Profesorado.htm

1.11. Objetivos del curso / Course objectives

Se trata de aprender los conceptos básicos sobre códigos criptográficos, tanto de clave simétrica como de clave pública (que permiten, por ejemplo, comprar con seguridad por Internet) y sobre códigos detectores y correctores de errores (ejemplos: el NIF, el ISBN, los códigos de barras, los códigos de un CD). El curso se centrará en las ideas matemáticas subyacentes a estos códigos.

Resultados del aprendizaje

Los resultados de aprendizaje correspondientes a las asignaturas optativas del Grupo B (**Materias optativas de profundización con contenido matemático**) son:

R11.2-- Habrá completado su formación adecuándola al desarrollo de actividades profesionales, docentes y/o de investigación

1.12. Contenidos del programa / Course contents

1. Ideas generales. Códigos criptográficos y Códigos detectores y correctores de errores.
2. Criptosistemas clásicos: Cesar, Vigenère, matrices de cifra. Análisis de frecuéncias e índice de coincidencia.
3. Criptografía de clave pública. Una aplicación: las firmas digitales.
4. Algoritmos de factorización y tests de primalidad. Introducción a la idea de complejidad.
5. El criptosistema RSA.
6. Otros criptosistemas de clave pública y más aplicaciones.
7. Códigos detectores y correctores de errores. Propiedades generales y estudio de tres ejemplos prácticos: el código de barras, el ISBN y el NIF.
8. Códigos lineales.
9. Algoritmos de codificación y decodificación para códigos lineales. Decodificación incompleta.
10. Códigos de Hamming. Relación con la geometría proyectiva.
11. Códigos perfectos. Códigos de Golay.
12. Códigos BCH. Los códigos que se utilizan en un CD.

1.13. Referencias de consulta / Course bibliography

Referencias básicas:

- Hill, R.: A First Course in Coding Theory, Oxford University Press (1986).
- Koblitz, N: A course in Number Theory and Criptography, 2nd ed., Springer-Verlag (1994).

Otras referencias sobre Criptografía:

- F. L. Bauer: Decrypted Secrets, 2nd ed., Springer-Verlag (2000).
- Beutelspacher, A.: Cryptology, M. A. A. (1994).
- Pastor, J.- Sarasa, M.A.: Criptografía Digital. Prensas Universitarias de Zaragoza (1998).
- Stinson, D.R.: Cryptography, Theory and Practice, 3rd ed. CRC Press (2006).

Otras referencias sobre Códigos Correctores de Errores:

- Mac Williams - Sloane: The Theory of Error Correcting Codes, 10th imp., North-Holland (1998).

- Pless, V.: Introduction to the Theory of Error Correcting Codes, 3rd. edition, Wiley (1998).
- van Lint, J.H.: Introduction to Coding Theory, 3rd. edition, Springer (1999).
- Vanstone - van Oorschot: An Introduction to Error Correcting Codes with Applications, Kluwer (1989).

Buenas referencias disponibles on-line:

- Smart, N.: Cryptography, An Introduction [http://www.cs.bris.ac.uk/~nigel/Crypto_Book/]
- Menezes A. J. - van Oorschot P. C. - Vanstone, S.A.: Handbook of applied cryptography [http://cacr.uwaterloo.ca/hac/]
- Hall, J. I. : Notes on Coding Theory [http://www.mth.msu.edu/~jhall/classes/codenotes/coding-notes.html]

2. Métodos Docentes / Teaching methodology

El curso consta de las siguientes actividades: clases presenciales en el aula y resolución de problemas por parte de los alumnos. Durante las clases se desarrollará la teoría, se harán algunas presentaciones y se discutirán algunos (no todos) de los problemas en los que hayan trabajado los alumnos. Los problemas serán habitualmente "de lapiz y papel" pero en ocasiones pueden requerir el uso de sistemas informáticos.

3. Tiempo de trabajo del estudiante / Student workload

Cada semana habrá 3 horas de clase presencial y se espera que los alumnos dediquen sistemáticamente a la asignatura 5 horas de trabajo no presencial (un total de 8 horas semanales de trabajo), además del tiempo de estudio previo a las evaluaciones

Actividad	**Tiempo estimado en horas (ECTS)**
Clases	45 (1,8)
Estudio continuado y realización de actividades prácticas	75 (3)
Preparación para evaluaciones	25 (1)
Evaluaciones	5 (0,2)
TOTAL	**150 h (6 ECTS)**

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

La calificación final del curso se obtendrá combinando la evaluación final con la evaluación continuada.

El estudiante que haya participado en menos de un 30% de las actividades de evaluación y no se presente al examen final, será calificado en la convocatoria ordinaria como "No evaluado".

En su caso, la calificación correspondiente a la convocatoria extraordinaria será la nota obtenida en la prueba específica realizada en la fecha marcada por el calendario académico.

5. Cronograma* / Course calendar

Semanas	Contenido
1	Tema 1
2	Tema 2
3	Tema 3
4	Tema 4
5	Tema 4
6	Tema 5
7	Tema 5,6
8	Tema 7
9	Tema 8
10	Tema 9
11	Tema 9, 10
12	Tema 10
13	Tema 11
14	Tema 12

*Este cronograma tiene carácter orientativo.