ASIGNATURA CÓDIGOS Y CRIPTOGRAFÍA

Código	40209039
Titulación	GRADO EN MATEMÁTICAS
Módulo	MÓDULO XVI. GESTIÓN Y TRANSMISIÓN DE LA INFO ...
Materia	MATERIA XVI.2 CÓDIGOS Y CRIPTOGRAFÍA
Curso	3
Duración	SEGUNDO SEMESTRE
Tipo	OPTATIVA
Idioma	CASTELLANO
Ofertable en Lengua Extranjera	NO
Movilidad Nacional	SÍ
Movilidad Internacional	SÍ
Estudiante Visitante Nacional	SÍ
ECTS	6,00
Departamento	C101 - MATEMATICAS

REQUISITOS Y RECOMENDACIONES

Requisitos

Álgebra Lineal, Estructuras algebraicas.

Recomendaciones

Tener conocimientos básicos de Álgebra lineal, Combinatoria y Cuerpos finitos facilita la comprensión de esta asignatura. En cualquier caso, los resultados básicos necesarios para entender la materia pueden aprenderse en poco tiempo.

OFERTA EN LENGUA EXTRANJERA

No se oferta para Lengua Extranjera.

MOVILIDAD

- Movilidad Nacional (SICUE): Sí. Tipo de enseñanza: Presencial
- Movilidad Internacional: Sí. Tipo de enseñanza: Presencial
- Estudiante Visitante Nacional: Sí. Nº Plazas: 10. Tipo de enseñanza: Presencial

RESULTADO DEL APRENDIZAJE

Id.	Resultados
1	Conocer algunas familias de códigos importantes y sus aplicaciones.
2	Implementar algoritmos de codificación y decodificación (de algunos códigos autocorrectores) usando algún programa de cálculo simbólico.
3	Conocer algunos criptosistemas simétricos relevantes y conocer algunos criptosistemas de clave pública relevantes.
4	Implementar algoritmos de cifrado y descifrado (de algunos criptosistemas) usando algún programa de cálculo simbólico.

COMPETENCIAS

Tipo	Competencia
BÁSICA	Que los estudiantes hayan demostrado poseer y comprender conocimientos en un área de estudio que parte de la base de la educación secundaria general, y se suele encontrar a un nivel que, si bien se apoya en libros de texto avanzados, incluye también algunos aspectos que implican conocimientos procedentes de la vanguardia de su campo de estudio
BÁSICA	Que los estudiantes sepan aplicar sus conocimientos a su trabajo o vacación de una forma profesional y posean las competencias que suelen demostrarse por medio de la elaboración y defensa de argumentos y la resolución de problemas dentro de su área de estudio
BÁSICA	Que los estudiantes tengan la capacidad de reunir e interpretar datos relevantes (normalmente dentro de su área de estudio) para emitir juicios que incluyan una reflexión sobre temas relevantes de índole social, científica o ética
BÁSICA	Que los estudiantes puedan transmitir información, ideas, problemas y soluciones a un público tanto especializado como no especializado
BÁSICA	Que los estudiantes hayan desarrollado aquellas habilidades de aprendizaje necesarias para emprender estudios posteriores con un alto grado de autonomía
GENERAL	Utilizar herramientas de búsqueda de recursos bibliográficos.
GENERAL	Poder comunicarse en otra lengua de relevancia en el ámbito científico.
GENERAL	Comprobar o refutar razonadamente los argumentos de otras personas.
GENERAL	Utilizar con fluidez la informática a nivel de usuario.

Tipo	Competencia
ESPECÍFICA	Comprender y utilizar el lenguaje matemático. Adquirir la capacidad para enunciar proposiciones en distintos campos de las matemáticas, para construir demostraciones y para transmitir los conocimientos matemáticos adquiridos.
ESPECÍFICA	Conocer demostraciones rigurosas de algunos teoremas clásicos en distintas áreas de las matemáticas.
ESPECÍFICA	Asimilar la definición de un nuevo objeto matemático, en términos de otros ya conocidos y ser capaz de utilizar este objeto en diferentes contextos.
ESPECÍFICA	Saber abstraer las propiedades estructurales (de objetos matemáticos, de la realidad observada y de otros ámbitos) distinguiéndolas de aquellas puramente ocasionales y poder comprobarlas con demostraciones o refutarlas con contraejemplos, así como identificar errores en razonamientos incorrectos.
ESPECÍFICA	Resolver problemas matemáticos, planificando su resolución en función de las herramientas disponibles y de las restricciones de tiempo y recursos.
ESPECÍFICA	Proponer, analizar, validar e interpretar modelos de situaciones reales sencillas, utilizando las herramientas matemáticas más adecuadas a los fines que se persigan.
ESPECÍFICA	Utilizar aplicaciones informáticas de análisis estadístico, cálculo numérico y simbólico, visualización gráfica, optimización u otras para experimentar en matemáticas y resolver problemas.
ESPECÍFICA	Desarrollar programas que resuelvan problemas matemáticos utilizando para cada caso el entorno computacional adecuado.

CONTENIDOS

Contenido	Descripción
1. CÓDIGOS AUTOCORRECTORES. Parámetros. Decodificación. Códigos de Hamming. 2. BUENOS CÓDIGOS. Códigos de Golay. Códigos de Hadamard. Códigos de Reed-Muller. 3. CÓDIGOS CÍCLICOS. 4. INTRODUCCIÓN A LA CRIPTOGRAFÍA. Criptosistemas clásicos. 5. CRIPTOGRAFÍA DE CLAVE PRIVADA. Sistema DES. 6. CRIPTOGRAFÍA DE CLAVE PÚBLICA. Sistemas basados en factorización de enteros. Sistemas basados en el problema del logaritmo discreto. Firma digital.	

SISTEMA DE EVALUACIÓN

Procedimientos de evaluación

Tarea/Actividades	Medios, técnicas e instrumentos	Ponderación
Realización y exposición de trabajo	Medio: documento escrito y exposición. Técnica: evaluación del documento y exposición. Instrumento: valoración.	20 %
Pruebas parciales	Medio: examen escrito. Técnica: Corrección. Instrumento: Valoración.	80 %

Criterios de evaluación

El alumno puede elegir una de las 2 opciones siguientes para ser evaluado:
1. Con 2 pruebas parciales.

2. Con 2 pruebas parciales y una exposición.
En la opción 1 el valor de cada prueba es de 5 puntos cada una (sobre 10 puntos de la calificación global). En la opción 2 el valor de cada prueba es de 4 puntos cada una, y el valor de la exposición es de 2 puntos.

En caso de que se pueda realizar una prueba presencial en la fecha de examen fijada por la Facultad de Ciencias, el alumno podrá optar por ser evaluado sólo con esa prueba, y la calificación global se obtendrá en este caso sólo con la nota de esta prueba.

En cualquier caso, el alumno tendrá derecho a una prueba de evaluación global, en las dos convocatorias extraordinarias posteriores a la convocatoria ordinaria (la del cuatrimestre en el que se imparte). Esta modalidad de evaluación deberá ser solicitada en los plazos que el centro determine. Los criterios de evaluación y tipo de pruebas a realizar serán determinados por el equipo docente de la asignatura e informados con suficiente antelación a aquellos alumnos que la soliciten.

PROFESORADO

Profesorado	Categoría	Coordinador
LOPEZ JIMENEZ, BARTOLOME	PROFESOR TITULAR UNIVERSIDAD	Sí

ACTIVIDADES FORMATIVAS

Actividad	Horas	Detalle
03 Prácticas de informática	24	Prácticas de informática con el objetivo de implementar algoritmos.
08 Teórico-Práctica	36	Clases en las que se presenten materia teórica y ejemplos. Las presentaciones pueden ser a cargo del profesor o de los alumnos.
10 Actividades formativas no presenciales	78,00	Tiempo dedicado al estudio de la materia presentada en las clases, solución de ejercicios, realización de programas informáticos y preparación de la materia a exponer en las clases teórico-prácticas.
11 Actividades formativas de tutorías	5,00	Los alumnos dispondrán de la ayuda del profesor para la realización de sus tareas.
12 Actividades de evaluación	7,00	Pruebas parciales. Exposiciones. Examen final de la asignatura.

BIBLIOGRAFÍA

Bibliografía Básica

J.H. van Lint: Introduction to Coding Theory. Springer, 1999.
N. Smart: Criptography: An Introduction. Disponible en internet.
D. Stinson. Cryptography: Theory and Practice. CRC Press, 1995.

Bibliografía Específica

N. Koblitz. A course in Number Theory and Cryptography. Springer, 1994.
R. Hill. A first course in Coding Theory. Oxford University Press, 1986.

Bibliografía Ampliación

F.J. Macwilliams, N.J.A. Sloane: The Theory of Error-Correcting Codes. North-Holland, 1997.
W. Trappe, L. Washington: Introduction to Cryptography with Coding Theory. Pearson, 2006.