UNIVERSIDAD DE MURCIA

1. Identificación

1.1. De la asignatura

Curso Académico	2025/2026
Titulación	GRADO EN MATEMÁTICAS
Nombre de la asignatura	CÓDIGOS CORRECTORES Y CRIPTOGRAFÍA
Código	6102
Curso	CUARTO
Carácter	OPTATIVA
Número de grupos	1
Créditos ECTS	6.0
Estimación del volumen de trabajo	150.0
Organización temporal	1º Cuatrimestre
Idiomas en que se imparte	Inglés, Español

1.2. Del profesorado: Equipo docente

BERNAL BUITRAGO, JOSE JOAQUIN

Docente: **GRUPO 1**

Coordinación de los grupos: **GRUPO 1**

Coordinador de la asignatura

Categoría
PROFESOR PERMANENTE LABORAL

Área
ÁLGEBRA

Departamento
MATEMÁTICAS

Correo electrónico / Página web / Tutoría electrónica
josejoaquin.bernal@um.es Tutoría electrónica: **Sí**

Teléfono, horario y lugar de atención al alumnado

Duración:	Día:	Horario:	Lugar:
A	Lunes	13:00-15:00	(Sin Extensión), Facultad de Matemáticas y Aulario General B1.1.007

Observaciones:
No consta

Duración:	Día:	Horario:	Lugar:
A	Viernes	13:00-14:00	(Sin Extensión), Facultad de Matemáticas y Aulario General B1.1.007

Observaciones:
No consta

Duración:	Día:	Horario:	Lugar:
A	Jueves	13:00-14:00	(Sin Extensión), Facultad de Matemáticas y Aulario General B1.1.007

Observaciones:
No consta

Duración:	Día:	Horario:	Lugar:
A	Miércoles	13:00-14:00	(Sin Extensión), Facultad de Matemáticas y Aulario General B1.1.007

Observaciones:
No consta

Duración:	Día:	Horario:	Lugar:
A	Martes	13:00-14:00	(Sin Extensión), Facultad de Matemáticas y Aulario General B1.1.007

Observaciones:
No consta

2. Presentación

En esta asignatura se introducen las bases teóricas y las herramientas y resultados fundamentales de la Teoría de Códigos Correctores de Errores y la Criptografía con dos objetivos subyacentes:

- Facilitar la inserción laboral de los matemáticos en el sector de la informática y las telecomunicaciones
- Acceder al umbral de la investigación en un campo de gran actividad

3. Condiciones de acceso a la asignatura

3.1. Incompatibilidades

No constan

3.2. Requisitos

No constan

3.3. Recomendaciones

Conocimientos de álgebra lineal y álgebra abstracta al nivel del grado. Concretamente, se recomienda haber cursado previamente las asignaturas "Conjuntos y números", "Álgebra Lineal" y "Grupos y Anillos". También sería recomendable que el alumno hubiese cursado previamente, o la haga simultáneamente, la asignatura "Ecuaciones Algebraicas".

4. Competencias

4.1. Competencias básicas

- CB1: 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
- CB2: Que los estudiantes sepan aplicar sus conocimientos a su trabajo o vocación 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
- CB4: Que los estudiantes puedan transmitir información, ideas, problemas y soluciones a un público tanto especializado como no especializado
- CB5: Que los estudiantes hayan desarrollado aquellas habilidades de aprendizaje necesarias para emprender estudios posteriores con un alto grado de autonomía

4.2. Competencias de la titulación

- CG1: Ser capaz de expresarse correctamente en español en el ámbito de la Matemática.
- CG2: Comprender y expresarse en un idioma extranjero en el ámbito de la Matemática, particularmente en inglés.
- CG3: Ser capaz de gestionar la información y el conocimiento en el ámbito de la Matemática, incluyendo saber utilizar como usuario las herramientas básicas en TIC.
- CG4: Considerar la ética y la integridad intelectual como valores esenciales de la práctica profesional.
- CG6: Ser capaz de trabajar en equipo y relacionarse con otras personas del ámbito de la Matemática o cualquier otro ámbito.
- CG7: Desarrollar habilidades de iniciación a la investigación.
- CG8: Comprender y utilizar el lenguaje matemático. Adquirir la capacidad para enunciar proposiciones en distintos campos de la Matemática, para construir demostraciones y para transmitir los conocimientos matemáticos adquiridos.
- CG9: Conocer demostraciones rigurosas de algunos teoremas clásicos en distintas áreas de la Matemática.
- CG10: Asimilar la definición de un nuevo objeto matemático, en términos de otros ya conocidos, y ser capaz de utilizar este objeto en diferentes contextos.
- CG11: 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.
- CG12: Capacitar para el aprendizaje autónomo de nuevos conocimientos y técnicas.

- CE1: Resolver problemas de Matemáticas, mediante habilidades de cálculo básico y otras técnicas, planificando su resolución en función de las herramientas de que se disponga y de las restricciones de tiempo y recursos.
- CE2: Proponer, analizar, validar e interpretar modelos de situaciones reales sencillas, utilizando las herramientas matemáticas más adecuadas a los fines que se persigan.
- CE3: Utilizar aplicaciones informáticas de análisis estadístico, cálculo numérico y simbólico, visualización gráfica, optimización u otras para experimentar en Matemáticas y resolver problemas.
- CE4: Desarrollar programas que resuelvan problemas matemáticos utilizando para cada caso el entorno computacional adecuado.
- CE5: Utilizar herramientas de búsqueda de recursos bibliográficos.
- CE6: Comunicar, tanto por escrito como de forma oral, conocimientos, procedimientos, resultados e ideas matemáticas

4.3. Competencias transversales y de materia

- Conocer los problemas provenientes de la transmisión de datos
- Aprender a modelizar dichos problemas y conocer algunos métodos matemáticos de su tratamiento
- Conocer métodos de álgebra, teoría de los números y álgebra computacional para el tratamiento de dichos problemas
- Conocer las familias de códigos correctores más comunes (Hamming, BCH, Reed-Solomon, etc) y su tratamiento algebraico
- Conocer los métodos de encriptado más comunes (DES, AES, RSA, Logaritmo discreto, etc)
- Conocer las técnicas de criptoanálisis y algunos problemas de teoría de la complejidad asociados
- Conocer las bases matemáticas de los métodos de codificación y encriptado y saber resolver problemas asociados al tratamiento de la información

5. Contenidos

5.1. Teoría

Bloque 1: Códigos Correctores

Tema 1: Información y códigos
Transmisión de la información Fuentes de información Errores de transmisión

Tema 2: Generaliades sobre códigos
Conceptos básicos Distancia de Hamming Esquema de decodificación de Hamming Equivalencias y automorfismos de códigos Construcción de códigos a partir de otros

Tema 3: Códigos lineales
Matriz generadora Código dual Pesos y distancias Construcciones

Tema 4: Cotas a los parámetros. El problema fundamental de la Teoría de códigos.
El problema fundamental de la Teoría de códigos Cota de Hamming, cota de Singleton, códigos MDS

Tema 5: Códigos clásicos que son lineales
Códigos de Hamming, códigos simplex, códigos de Golay, códigos de Reed-Muller

Tema 6: Cuerpos finitos

Artimética de cuerpos finitos Existencia y unicidad Anillos de polinomios

Tema 7: Códigos cíclicos
Conceptos básicos Codificación y decodificación Cota BCH

Tema 8: Códigos clásicos que son cíclicos
Códigos de Hamming como códigos cíclicos Códigos BCH Códigos de Reed-Solomon

Bloque 2: Criptografía

Tema 9: Criptosistemas simétricos o de clave privada
Criptografía y criptoanálisis Criptosistemas de clave privada Seguridad perfecta DES y AES

Tema 10: Problemas y algoritmos. Complejidad.
Complejidad Tiempo de cálculo Función de dirección única

Tema 11: Criptosistemas asimétricos o de clave pública
Criptosistemas asimétricos RSA Criptosistemas basados en logaritmo discreto

Tema 12: Diseño de algoritmos y criptosistemas
Introducción al diseño de algoritmos relacionados con la estructura de ciertos criptosistemas

5.2. Prácticas

- **Práctica 1: Diseño de algoritmos con aplicaciones informáticas**

  Diseño de algoritmos en diferentes lenguajes (Python, GAP, .) relacionados con la estructura de ciertos criptosistemas

  Relacionado con:
  - Tema 12: Diseño de algoritmos y criptosistemas

6. Actividades Formativas

Actividad Formativa	Metodología	Horas	Presencialidad
AF1: Exposición teórica-práctica / Clase magistral de teoría-problemas		36.0	100.0
AF2: Tutoría ECTS o trabajos dirigidos		3.0	100.0
AF3: Resolución de problemas / Seminarios / Exposición y discusión de trabajos		6.0	100.0
AF4: Prácticas con ordenadores		15.0	100.0
AF5: Trabajo autónomo del estudiante		90.0	0.0
	Totales	150,00	

7. Horario de la asignatura

https://www.um.es/web/estudios/grados/matematicas/2025-26#horarios

8. Sistemas de Evaluación

Identificador	Denominación del instrumento de evaluación	Criterios de Valoración	Ponderación
SE1	Exámenes (escritos u orales)	En cada una de las convocatorias de exámenes las/los estudiantes deberán haber entregado en las fechas marcadas por el profesor un dossier, escrito a mano, con las soluciones a los problemas planteados en las hojas de problemas. Cada uno de las/los estudiantes podrá ser citado individualmente para responder a las preguntas sobre el trabajo realizado. Para la valoración del trabajo se tendrán en cuenta el planteamiento de las soluciones a los problemas propuestos, la correcta utilización de los conceptos y herramientas matemáticos utilizados, la corrección, rigor y claridad de la explicación de las soluciones y su interpretación.	63.0
SE2	Informes escritos, trabajos y proyectos	En cada una de las convocatorias de exámenes el profesor habilitará una Tarea en el Aula Virtual que consistirá en la resolución de problemas de carácter práctico mediante el diseño de los programas informáticos adecuados. Las/los estudiantes deberán entregar la lista de archivos correspondientes en dicha tarea dentro del plazo especificado por el profesor. Cada uno de las/los estudiantes podrá ser citado individualmente para responder a las preguntas sobre el trabajo realizado. Para la valoración del trabajo se tendrán en cuenta la correcta utilización del lenguaje de programación utilizado y la idoneidad de los programas diseñados para dar respuesta a los problemas planteados.	25.0
SE3	Presentación de trabajos	En el modelo de evaluación continua, exclusivo de la convocatoria de enero, en cada una de las hojas de ejercicios se incluirá uno o varios problemas adicionales que se podrán realizar de manera opcional. Las/los estudiantes entregarían estos ejercicios junto con los demás en el mismo plazo y forma. Caso de no realizar estos ejercicios el apartado SE1 pasaría a ponderarse con un 75 %. En el resto de convocatorias, el apartado SE1 pasaría a ponderarse con un 75 %.	12.0

9. Fechas de exámenes

https://www.um.es/web/estudios/grados/matematicas/2025-26#examenes

10. Resultados del Aprendizaje

- Conocer la aplicación de la matemática a la solución de problemas en la transmisión de datos
- Conocer algunas herramientas algebraicas específicas en el tratamiento de dichos problemas
- Conocer las familias de códigos correctores de errores clásicas
- Conocer técnicas de criptoanálisis y rudimentos de la teoría de la complejidad
- Conocer algunos métodos de encriptado clásicos

11. Bibliografía

Grupo: GRUPO 1

Bibliografía básica

- J. Munuera Gomez, Codificación de la información. Valladolid : Secretariado de Publicaciones e Intercambio Científico, Universidad de Valladolid, 1997. Manuales y textos universitarios. Ciencias ; 25. ISBN: 84-7762-764-9
- W. C. Huffman and V. Pless, Fundamentals of error-correcting codes, Cambridge University Press, 2003.
- José Joaquín Bernal. Apuntes de la asignatura. Estarán disponibles en el Aula Virtual
- Á. del Río, Introducción a la criptología

Bibliografía complementaria

- Koblitz, Neal (1948-) A course in number theory and cryptography.-- 2nd ed.-- New York : Springer, 1998.
- N. Koblitz, A course in Number Theory and Cryptography, Springer Graduate Texts in Mathematics, 1988. A Course in Number Theory and Cryptography (Graduate Texts in Mathematics)
- S. Roman, Coding and information theory. Springer. Graduate texts in mathematics 134 (1992)

12. Observaciones

EVALUACIÓN

- Modalidad de evaluación continua (exclusiva de la convocatoria de enero):

La nota del Bloque I se obtendrá como la media de las notas de las hojas de ejercicios correspondientes, siempre y cuando se hayan ido entregando dentro de los plazos fijados por el profesor y en todas ellas se haya obtenido al menos un 5. Para el cálculo de la nota de cada una de las hojas se tendrá en cuenta lo siguiente:

B = Nota sobre 10 de los ejercicios básicos; E= Nota sobre 10 de los ejercicios adicionales

N = Nota final de la hoja de ejercicios = máx(B, B·0'83+E·0'17)

Es decir, los ejercicios adicionales darán la oportunidad a los alumnos de mejorar su nota pero nunca le supondrán un perjuicio

La nota del Bloque II será la media entre la media de las notas de las hojas de ejercicios correspondientes, calculada cada una como se ha descrito arriba, y la nota de la Tarea de ejercicios prácticos, siempre y cuando se hayan ido entregando dentro de los plazos fijados.

Finalmente, la nota final del curso será la nota media de ambos Bloques, siempre y cuando se haya obtenido un 5 en cada uno de ellos.

- Modalidad de evaluación no continua y resto de convocatorias.

La nota se calcula como en el caso de evaluación continua con la salvedad de que no se tendrá en cuenta la entrega de los ejercicios adicionales; es decir, la nota sobre 10 de cada hoja se calcula únicamente con los ejercicios básicos.

Tanto en un caso como en otro, en cada convocatoria la/el estudiante resultará aprobado si la nota final del curso es al menos 5. En el caso de que la/el estudiante no entregue la totalidad de las hojas de ejercicios y tareas dentro del plazo fijado para la convocatoria en cuestión se considerará No Presentado.

OBJETIVOS DE DESARROLLO SOSTENIBLE (ODS)

- Esta asignatura se encuentra vinculada de forma directa con:

- Objetivo de Desarrollo Sostenible 4 "Educación de calidad", en particular con el 44 "Aumento de las competencias para acceder al empleo"

- Objetivo de Desarrollo Sostenible 9 "Industria, innovación e infraestructura", en particular con el 95 " Aumento de la investigación científica, capacidad tecnológica.26quot;

UTILIZACIÓN DE MEDIOS FRAUDULENTOS: Cuando proceda se aplicará el Artículo 22 del Reglamento de Evaluación de la UMU sobre conductas fraudulentas en las pruebas de evaluación

IDIOMASe considera como parte del material bibliográfico básico a ciertas referencias en inglés En el manejo de las herramientas informáticas necesarias el idioma a utilizar será el inglés

NECESIDADES EDUCATIVAS ESPECIALES

Aquellos estudiantes con discapacidad o necesidades educativas especiales podrán dirigirse al Servicio de Atención a la Diversidad y Voluntariado (ADYV - https://www.um.es/adyv) para recibir orientación sobre un mejor aprovechamiento de su proceso formativo y, en su caso, la adopción de medidas de equiparación y de mejora para la inclusión, en virtud de la Resolución Rectoral R-358/2016. El tratamiento de la información sobre este alumnado, en cumplimiento con la LOPD, es de estricta confidencialidad.

REGLAMENTO DE EVALUACIÓN DE ESTUDIANTES

El artículo 8.6 del Reglamento de Evaluación de Estudiantes (REVA) prevé que "salvo en el caso de actividades definidas como obligatorias en la guía docente, si el o la estudiante no puede seguir el proceso de evaluación continua por circunstancias sobrevenidas debidamente justificadas, tendrá derecho a realizar una prueba global".

Se recuerda asimismo que el artículo 22.1 del Reglamento de Evaluación de Estudiantes (REVA) estipula que "el o la estudiante que se valga de conductas fraudulentas, incluida la indebida atribución de identidad o autoría, o esté en posesión de medios o instrumentos que faciliten dichas conductas, obtendrá la calificación de cero en el procedimiento de evaluación y, en su caso, podrá ser objeto de sanción, previa apertura de expediente disciplinario".