Datos básicos de la asignatura

Titulación:	Grado en Matemáticas
Año plan de estudio:	2009
Curso implantación:	2009-10
Centro responsable:	Facultad de Matemáticas
Nombre asignatura:	Teoría de Códigos y Criptografía
Código asigantura:	1710029
Tipología:	OPTATIVA
Curso:	3
Periodo impartición:	Segundo cuatrimestre
Créditos ECTS:	6
Horas totales:	150
Área/s:	Algebra
Departamento/s:	Algebra

Coordinador de la asignatura

TORNERO SANCHEZ, JOSE MARIA

Profesorado

Profesorado de grupo principal
TORNERO SANCHEZ, JOSE MARIA

Profesorado de otros grupos
CASTAÑO DOMINGUEZ, ALBERTO
SOTO PRIETO, MANUEL JESUS

Objetivos y competencias

OBJETIVOS:

Conocer y manejar los principales resultados de teoría algebraica de números y criptografía.

Conocer y manejar los principales resultados de códigos correctores de errores.
COMPETENCIAS:

Competencias específicas:

E01. 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.

E02. Conocer demostraciones rigurosas de algunos teoremas clásicos en distintas áreas de las matemáticas.

E03. Asimilar la definición de un nuevo objeto matemático, en términos de otros ya conocidos, y ser capaz de utilizar este objeto en diferentes contextos.

E04. 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.

E05. Resolver problemas matemáticos, planificando su resolución en función de las herramientas disponibles y de las restricciones de tiempo y recursos.

E06. Proponer, analizar, validar e interpretar modelos de situaciones reales sencillas, utilizando las herramientas matemáticas más adecuadas a los fines que se persigan.

E07. Utilizar aplicaciones informáticas de análisis estadístico, cálculo numérico y simbólico, visualización gráfica, optimización u otras para experimentar en matemáticas y resolver problemas.

E08. Desarrollar programas que resuelvan problemas matemáticos utilizando para cada caso el entorno computacional adecuado.
Competencias genéricas:

G01. Poseer los conocimientos básicos y matemáticos de los distintos módulos que, partiendo de la base de la educación secundaria general, y apoyándose en libros de texto avanzados, se desarrollan en la propuesta de título de Grado en Matemáticas que se presenta.

G02. Saber aplicar los conocimientos básicos y matemáticos de cada módulo a su trabajo o vocación de una forma profesional y poseer las competencias que suelen demostrarse por medio de la elaboración y defensa de argumentos y la resolución de problemas dentro de las matemáticas y ámbitos en que se aplican directamente.

G03. Saber reunir e interpretar datos relevantes (normalmente de carácter matemático) para emitir juicios que incluyan una reflexión sobre temas relevantes de índole social, científica o ética.

G04. Poder transmitir información, ideas, problemas y sus soluciones, de forma escrita u oral, a un público tanto especializado como no especializado.

G05. Haber desarrollado aquellas habilidades de aprendizaje necesarias para emprender estudios posteriores con un alto grado de autonomía.

Contenidos o bloques temáticos

Teoría algebraica de números.

Códigos correctores de errores.

Criptografía.

Relación detallada y ordenación temporal de los contenidos

TEMA 1. Fundamentos

Semana 1: Grupos. Dominios y factorización. Cuerpos finitos (I)

Semana 2: Cuerpos finitos (II)

Semana 3: Teoría básica de la complejidad

TEMA 2. Códigos correctores de errores

Semana 4: Códigos lineales (I)

Semana 5: Códigos lineales (II)

Semana 6: Códigos cíclicos

Semana 7: Cotas

TEMA 3. Criptosistemas de clave privada

Semana 8: Cifrados históricos (I)

Semana 9: Cifrados históricos (II)

Semana 10: Cifrados de bloque. DES

TEMA 4. Criptosistemas de clave pública

Semana 11: Funciones trampilla. Protocolo Diffie-Hellman

Semana 12: Protocolos asimétricos: RSA, ElGamal, Rabin

Semana 13: Ataques a la factorización y al logaritmo discreto

Semana 14: Firmas digitales

Semana 15: Actividades de evaluación

REQUISITOS: Se deben haber cursado (e idealmente, aprobado) las asignaturas de Álgebra Básica, Álgebra Lineal y Geometría I y Estructuras Algebraicas. Otros conocimientos puntuales se desarrollan en el propio curso.

METODOLOGÍA: La asignatura consta de cuatro horas semanales: dos se dedican a clases expositivas de teoría, una a clases prácticas y una a laboratorio, aunque esta proporción puede variar en función de las necesidades de la asignatura. Se hará uso

intensivo de la plataforma de Enseñanza Virtual.

En las clases expositivas de teoría se adoptará una estrategia de clase invertida. El alumnado habrá preparado, previamente a la clase, la materia a tratar a través de indicaciones y material propuesto con la suficiente antelación. Este trabajo previo puede ser individual o colectivo. Al final de la clase el profesor expondrá las líneas básicas del trabajo a realizar la siguiente semana. Todos los materiales se encontrarán a disposición del alumnado en la plataforma de Enseñanza Virtual.

En las clases prácticas se resolverán dudas por parte del profesorado en primer lugar, para pasar a plantear al alumnado problemas o cuestiones que deben ser resueltos de manera individual. Esta actividad será evaluable de cara a la evaluación continua (ver Criterio de calificación). Los foros de la plataforma de Enseñanza Virtual se podrán utilizar como complemento a estas clases, bien para proponer cuestiones con antelación a la clase, como para presentar soluciones que hayan quedado pendientes.

En las horas de laboratorio se estudiará el programa de cálculo simbólico SAGE, haciendo énfasis en su aplicación a los objetivos de la asignatura. Este sistema es software libre, puede ser descargado gratuitamente e instalado o, si se prefiere, puede utilizarse online sin necesidad de descargar nada. Ambas opciones son adecuadas para cumplir los objetivos de la asignatura.

La metodología tendrá presente los siguientes escenarios y planes de contingencia:

* [Escenario 0 (presencialidad total)] La metodología se mantendrá con normalidad, con clases teóricas, de problemas y laboratorios presenciales.

* [Escenario A (presencialidad reducida)] Para una adaptación al escenario de presencialidad reducida, las clases teóricas, de problemas y laboratorios presenciales serán retransmitidos online de forma síncrona, durante el horario de clase, usando los medios que la Universidad ponga a disposición del profesorado para el alumnado no presencial. En este caso, el equipo docente podrá unificar grupos para una mejor gestión de recursos.

* [Escenario B (presencialidad suspendida)] Si se diera una suspensión absoluta de la presencialidad, o si los medios ténicos disponibles no fueran suficientes y adecuados al Escenario A, el equipo docente podrá unificar grupos para una mejor gestión de recursos, y se retransmitirán las clases online de forma síncrona o asíncrona, o bien se ofrecerán alternativas docentes tales como vídeos explicativos, problemas resueltos, material adicional o cualquier otra medida conducente a la docencia y el aprendizaje. En este caso se trazará un plan de estudios, con objetivos semanales, para que el alumnado pueda comprobar su progreso mediante autoevaluación. La plataforma preferente para este escenario será la Enseñanza Virtual.

Actividades formativas y horas lectivas

Actividad	Horas	Créditos
A Clases Teóricas	30	3
C Clases Prácticas en aula	15	1,5
G Prácticas de Informática	15	1,5

Idioma de impartición del grupo

ESPAÑOL

Sistemas y criterios de evaluación y calificación

El sistema de evaluación será detallado en el proyecto docente de la asignatura.

Metodología de enseñanza-aprendizaje

Horarios del grupo del proyecto docente

https://matematicas.us.es/index.php/informacion-academica/horarios

Calendario de exámenes

https://matematicas.us.es/index.php/informacion-academica/examenes

Tribunales específicos de evaluación y apelación

Presidente: LUIS NARVAEZ MACARRO
Vocal: ANTONIO ROJAS LEON
Secretario: FRANCISCO JAVIER CALDERON MORENO
Suplente 1: MANUEL JESUS GAGO VARGAS
Suplente 2: JUAN GONZALEZ-MENESES LOPEZ
Suplente 3: FERNANDO MURO JIMENEZ

Sistemas y criterios de evaluación y calificación del grupo

Criterio de calificación

Se pondrá a disposición del alumnado la posibilidad de someterse a evaluación continua. Esta tendrá en cuenta:

* Trabajo evaluable de laboratorio: dos prácticas de SAGE evaluables (20% de la nota final conjuntamente en todas las convocatorias).

* Trabajo evaluable de clases prácticas: siete prácticas evaluables (80% de la nota final).

Quienes que no aprueben por evaluación continua y quienes no deseen realizarla podrán optar por realizar únicamente el examen final (80%) y el trabajo evaluable de laboratorio (20%). Este último se deberá realizar en las horas dispuestas al efecto, independientemente de la modalidad de evaluación que se escoja. Esta estructura se mantendrá para todas las convocatorias.

Las fechas para todas las actividades de evaluación estarán disponibles en la Enseñanza Virtual. No será necesaria ninguna puntuación mínima para proceder a la evaluación.

La evaluación tendrá en cuenta los siguientes escenarios y planes de contingencias:

* [Escenario 0 (presencialidad total)] La evaluación continua tendrá lugar en horario de clase.

* [Escenario A (presencialidad reducida)] La evaluación se realizará de manera preferentemente presencial, en cuyo caso se llevará a cabo en horario de clase, teniendo en cuenta los turnos de asistencia establecidos. Podrá llevarse a cabo telemáticamente si las circunstancias así lo aconsejaran. En este caso, podrá contener una parte escrita y una parte oral. La parte oral tendría lugar a través de la plataforma de enseñanza virtual, de las aplicaciones corporativas de

la Universidad de Sevilla o de cualquier otra herramienta que pudiera facilitar el proceso. También se podrían usar estos u otros instrumentos en los exámenes escritos no presenciales con el fin de establecer mecanismos de garantía de la autoría de las pruebas. Todo se concretará con la mayor antelación posible en función de los recursos disponibles.

* [Escenario B (presencialidad suspendida)] La evaluación se realizará telemáticamente con las características descritas en el apartado anterior.

Bibliografía recomendada

Bibliografía Específica

Elementary number theory, cryptography and codes
Autores: M.W. Baldoni, C. Ciliberto, G.M. Piacentini Cattaneo
Edición:
Publicación: Springer-Verlag New York
ISBN: 978-3540691990
A first course in coding theory
Autores: R. Hill
Edición:
Publicación: Oxford University Press
ISBN: 978-0198538035
A course in number theory and cryptography
Autores: Neal Koblitz
Edición:
Publicación: Springer-Verlag New York
ISBN: 3-540-94293-9
Handbook of applied cryptography
Autores: Alfred J. Menezes, Paul C. van Oorschot, Acott A. Vanstone
Edición:
Publicación: CRC Press
ISBN: 0849385237
Codificación de la información
Autores: Juan Munuera Gómez, Juan Tena Ayuso
Edición:
Publicación: Universidad de Valladolid, Secretariado de Publicaciones e Intercambio Científico
ISBN: 84-7762-764-9
Cryptography: an introduction

Autores: Nigel Smart
Edición:
Publicación: McGraw-Hill
ISBN: 0077099877
Introduction to coding theory and algebraic geometry
Autores: Jacobus H. van Lint, Gerard van der Geer
Edición:
Publicación: Birkhäuser
ISBN: 3-7643-2230-6
Introduction to coding theory
Autores: J.H. van Lint
Edición:
Publicación: Springer-Verlag
ISBN: 3-540-54894-7

Información Adicional

Profesores evaluadores

ALBERTO CASTAÑO DOMINGUEZ
JOSE MARIA TORNERO SANCHEZ