Facultad de Ciencias

GUÍA DOCENTE DE LA ASIGNATURA

G116 - Álgebra Computacional

Doble Grado en Física y Matemáticas
Optativa. Curso 5

Grado en Matemáticas
Optativa. Curso 4

Curso Académico 2020-2021

1. DATOS IDENTIFICATIVOS

Título/s	Doble Grado en Física y Matemáticas Grado en Matemáticas			Tipología y Curso	Optativa. Curso 5 Optativa. Curso 4
Centro	Facultad de Ciencias				
Módulo / materia	MATERIA AMPLIACIÓN DE MATEMÁTICA COMPUTACIONAL MENCIÓN EN MATEMÁTICA PURA Y APLICADA				
Código y denominación	G116 - Álgebra Computacional				
Créditos ECTS	6	Cuatrimestre		Cuatrimestral (2)	
Web					
Idioma de impartición	Español	English friendly	No	Forma de impartición	Presencial

Departamento	DPTO. MATEMATICAS, ESTADISTICA Y COMPUTACION
Profesor responsable	DANIEL SADORNIL RENEDO
E-mail	daniel.sadornil@unican.es
Número despacho	Facultad de Ciencias. Planta: + 3. DESPACHO DANIEL SADORNIL RENEDO (3003D)
Otros profesores	MARIA DE UJUE ETAYO RODRIGUEZ

2. CONOCIMIENTOS PREVIOS

Las asignaturas de Estructuras Algebraicas y Teoría de Galois.

3. COMPETENCIAS GENÉRICAS Y ESPECÍFICAS DEL PLAN DE ESTUDIOS TRABAJADAS
Competencias Genéricas
(Autonomía) Aprender de manera autónoma nuevos conocimientos y técnicas.
(Buscar información) Utilizar herramientas de búsqueda de recursos bibliográficos y de Internet.
(Leer) Leer textos científicos escritos tanto en español como en inglés.
(Aplicar) Saber aplicar los conocimientos matemáticos 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 del área de las Matemáticas.
(Comunicar) Poder transmitir información, ideas, problemas y soluciones del ámbito matemático a un público tanto especializado como no especializado.
Competencias Específicas
(Conocer demostraciones) Conocer demostraciones rigurosas de algunos teoremas clásicos en distintas áreas de la Matemática.
(Modelizar) Proponer, analizar, validar e interpretar modelos de situaciones reales sencillas, utilizando las herramientas matemáticas más adecuadas a los fines que se persigan.
(Comprender) Comprender y utilizar el lenguaje matemático.
(Resolver) Resolver problemas de Matemáticas, mediante habilidades de cálculo básico y otros, planificando su resolución en función de las herramientas de que se disponga y de las restricciones de tiempo y recursos.
Competencias Básicas
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.
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.
Que los estudiantes hayan desarrollado aquellas habilidades de aprendizaje necesarias para emprender estudios posteriores con un alto grado de autonomía.

3.1 RESULTADOS DE APRENDIZAJE
- Conocer problemas abiertos y retos actuales en el área del álgebra.
- Aplicar algoritmos eficientes para decidir si un número es primo.
- Cifrar y descifrar datos usando diferentes métodos.
- Reconocer el uso de la criptografia en diversos protocolos.

4. OBJETIVOS
Aplicar los conocimientos de teoria de grupos y cuerpos a los tests de primalidad.
Mostrar una panorámica histórica de los sistemas de cifrado y su evolución.
Desarrollar el uso de la criptografia en los protocolos criptográficos usuales.

5. MODALIDADES ORGANIZATIVAS Y MÉTODOS DOCENTES	
ACTIVIDADES	HORAS DE LA ASIGNATURA
ACTIVIDADES PRESENCIALES	
HORAS DE CLASE (A)	
- Teoría (TE)	38
- Prácticas en Aula (PA)	22
- Prácticas de Laboratorio Experimental(PLE)	
- Prácticas de Laboratorio en Ordenador (PLO)	
- Prácticas Clínicas (CL)	
Subtotal horas de clase	60
ACTIVIDADES DE SEGUIMIENTO (B)	
- Tutorías (TU)	8
- Evaluación (EV)	7
Subtotal actividades de seguimiento	15
Total actividades presenciales (A+B)	75
ACTIVIDADES NO PRESENCIALES	
Trabajo en grupo (TG)	
Trabajo autónomo (TA)	75
Tutorías No Presenciales (TU-NP)	
Evaluación No Presencial (EV-NP)	
Total actividades no presenciales	75
HORAS TOTALES	150

6. ORGANIZACIÓN DOCENTE

	CONTENIDOS	TE	PA	PLE	PLO	CL	TU	EV	TG	TA	TU-NP	EV-NP	Semana
1	INTRODUCCION Grupos, Anillos y Cuerpos Finitos. Simbolo de Legendre y reciprocidad cuadrática. Nociones de complejidad computacional	10,00	6,00	0,00	0,00	0,00	0,00	0,00	0,00	15,00	0,00	0,00	1-3
2	TESTS DE PRIMALIDAD Congruencias y pseudoprimos. Lucas, Proth, Lehmer. Números de Fermat y de Mersenne. Test de primalidad APRCL y test AKS.	12,00	8,00	0,00	0,00	0,00	4,00	3,50	0,00	30,00	0,00	0,00	4-9
3	CRIPTOGRAFIA Criptografía de Clave Privada. Criptografía de Clave Pública. Factorización y RSA, logaritmo discreto. Protocolos criptográficos.	16,00	8,00	0,00	0,00	0,00	4,00	3,50	0,00	30,00	0,00	0,00	10-15
TOTAL DE HORAS		38,00	22,00	0,00	0,00	0,00	8,00	7,00	0,00	75,00	0,00	0,00	

Esta organización tiene carácter orientativo.

Ante la situación incierta de que las medidas de distanciamiento social establecidas por las autoridades sanitarias no permitan desarrollar alguna actividad docente de forma presencial en el aula para todos los estudiantes matriculados, se adoptará una modalidad mixta de docencia que combine esta docencia presencial en el aula con docencia a distancia. De la misma manera , la tutorización podrá ser sustituida por tutorización a distancia utilizando medios telemáticos.

TE	Horas de teoría
PA	Horas de prácticas en aula
PLE	Horas de prácticas de laboratorio experimental
PLO	Horas de prácticas de laboratorio en ordenador
CL	Horas de prácticas clínicas
TU	Horas de tutoría
EV	Horas de evaluación
TG	Horas de trabajo en grupo
TA	Horas de trabajo autónomo
TU-NP	Tutorías No Presenciales
EV-NP	Evaluación No Presencial

7. MÉTODOS DE LA EVALUACIÓN

Descripción	Tipología	Eval. Final	Recuper.	%
Resolución de Ejercicios	Otros	No	Sí	35,00

Calif. mínima	0,00
Duración	
Fecha realización	Durante el cuso
Condiciones recuperación	Mediante ejercicios adicionales en la convocatoria ordinaria o extraordinaria
Observaciones	A lo largo del curso se propocionará a los alumnos una serie de ejercicios para su resolución que serán expuestos en el aula.

Trabajo	Trabajo	No	Sí	30,00

Calif. mínima	0,00
Duración	
Fecha realización	ultima semana de docencia
Condiciones recuperación	
Observaciones	Los estudiantes realizarán un trabajo en grupo (2-3 personas) relacionado con algunpo de los tópicos tratados en la asignatura. Este se expondrá al profesor y al resto de compañeros en el aula.

Examen Final	Examen escrito	Sí	Sí	35,00

Calif. mínima	0,00
Duración	3 horas
Fecha realización	A determinar por la Faccultad
Condiciones recuperación	Enm la convocatoria Extraordinaria
Observaciones	Realización de cuestiones, ejercicios y problemas que versen sobre los tópicos tratados en la asignatura

TOTAL	100,00

Observaciones

En el examen final se habilitarán preguntas específicas para que los alumnos puedan recuperar o mejorar la nota de la resolución de ejercicios realizadas durante el curso.

En la convocatoria extraordinaria el alumno puede mantener la nota obtenida en el trabajo o realizar uno adicional.

En caso de que la evaluación no sea presencial, los diversos métodos de evaluación podrán realizarse de forma virtual.

Criterios de evaluación para estudiantes a tiempo parcial

Los alumnos a tiempo parcial realizarán un examen final con peso 100%.

8. BIBLIOGRAFÍA Y MATERIALES DIDÁCTICOS

BÁSICA

R. Crandall y C. Pomerance. Prime Numbers; A computacional Perspective. Springer 2005.

A. Fuster. et al. Técnicas Criptográficos de Protección de Datos, Ra-Ma. 2000.

Complementaria
D. Stinson. Cryptography : theory and practice. Chapman & Hall. 2006.
H. Riesel. Prime numbers and computer methods for factorization. Birkhauser. 1985.
A.J. Menezes, P. C. van Oorschot, S. A. Vanstone. Handbook of Applied Cryptography. CRC Press 1996. Disponible en http://cacr.uwaterloo.ca/hac/.

9. SOFTWARE

PROGRAMA / APLICACIÓN	CENTRO	PLANTA	SALA	HORARIO

10. COMPETENCIAS LINGÜÍSTICAS

☐ Comprensión escrita ☐ Comprensión oral
☐ Expresión escrita ☐ Expresión oral
☐ Asignatura íntegramente desarrollada en inglés

Observaciones