GUÍA DOCENTE ABREVIADA DE LA ASIGNATURA

G116 - Álgebra Computacional

Doble Grado en Física y Matemáticas
Grado en Matemáticas

Curso Académico 2023-2024

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	https://sites.google.com/view/ujuetayo/teaching				
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	

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 y algunos algoritmos de factorización de enteros.
- Cifrar y descifrar datos usando diferentes métodos. -Reconocer el uso de la criptografía en diversos protocolos

4. OBJETIVOS
Aplicar los conocimientos de teoria de grupos y cuerpos a los tests de primalidad y factorización
Mostrar una panorámica histórica de los sistemas de cifrado y su evolución.

6. ORGANIZACIÓN DOCENTE	
CONTENIDOS	
1	Introducción. Reciprocidad cuadrática. Nociones de complejidad computacional
2	Primalidad y Factorización de enteros.
3	Criptografía. Clave privada y clave pública. Protocolos.

7. MÉTODOS DE LA EVALUACIÓN

Descripción	Tipología	Eval. Final	Recuper.	%
Examen final	Examen escrito	Sí	Sí	50,00
Examen parcial	Examen escrito	No	Sí	50,00
TOTAL				100,00

Observaciones

El examen final se dividirá en dos partes: la parte correspondiente a la materia del examen parcial y el resto de la materia.

Los alumnos que tengan aprobado el examen parcial o hayan obtenido una nota superior a 4, solamente tendrán la obligación de examinarse en el examen final del resto de la materia.
Además, podrán repetir también la parte correspondiente al parcial si desean mejorar la nota. En este caso, para obtener la nota final, se calculará la media entre las dos partes, utilizando para ello la nota obtenida en el último examen.
Los alumnos que en el parcial hayan obtenido una nota inferior a 4 deben presentarse a las dos partes del examen final. Su calificación global será la media aritmética de las notas obtenidas en cada una de las dos partes del examen final.
La convocatoria extraordinaria tendrá las mismas características que la convocatoria ordinaria.

Criterios de evaluación para estudiantes a tiempo parcial

Las mismas condiciones que para el resto de los alumnos

8. BIBLIOGRAFÍA Y MATERIALES DIDÁCTICOS

BÁSICA

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

Von zur Gathen, J., y Gerhard, J. Modern Computer Algebra (3rd ed.). Cambridge University Press. 2013

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

Esta es la Guía Docente abreviada de la asignatura. Tienes también publicada en la Web la información más detallada de la asignatura en la Guía Docente Completa.