GUÍA DOCENTE ABREVIADA DE LA ASIGNATURA

G116 - Álgebra Computacional

Doble Grado en Física y Matemáticas
Grado en Matemáticas

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

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.

6. ORGANIZACIÓN DOCENTE

	CONTENIDOS
1	INTRODUCCION Grupos, Anillos y Cuerpos Finitos. Simbolo de Legendre y reciprocidad cuadrática. Nociones de complejidad computacional
2	TESTS DE PRIMALIDAD Congruencias y pseudoprimos. Lucas, Proth, Lehmer. Números de Fermat y de Mersenne. Test de primalidad APRCL y test AKS.
3	CRIPTOGRAFIA Criptografía de Clave Privada. Criptografía de Clave Pública. Factorización y RSA, logaritmo discreto. Protocolos criptográficos.

7. MÉTODOS DE LA EVALUACIÓN

Descripción	Tipología	Eval. Final	Recuper.	%
Resolución de Ejercicios	Otros	No	Sí	35,00
Trabajo	Trabajo	No	Sí	30,00
Examen Final	Examen escrito	Sí	Sí	35,00
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.

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.