GUÍA DOCENTE ABREVIADA DE LA ASIGNATURA

M1507 - Criptología

Máster Universitario en Matemáticas y Computación

Curso Académico 2021-2022

1. DATOS IDENTIFICATIVOS					
Título/s	Máster Universitario en Matemáticas y Computación			Tipología y Curso	Optativa. Curso 1
Centro	Facultad de Ciencias				
Módulo / materia	ÁLGEBRA Y GEOMETRÍA				
Código y denominación	M1507 - Criptología				
Créditos ECTS	3	Cuatrimestre		Cuatrimestral (1)	
Web					
Idioma de impartición	Español	English friendly	No	Forma de impartición	Presencial

Departamento	DPTO. MATEMATICA APLICADA Y CIENCIAS DE LA COMPUTACION
Profesor responsable	JAIME GUTIERREZ GUTIERREZ
E-mail	jaime.gutierrez@unican.es
Número despacho	E.T.S. de Ingenieros Industriales y de Telecomunicación. Planta: - 4. DESPACHO (S4041)
Otros profesores	DOMINGO GOMEZ PEREZ

3.1 RESULTADOS DE APRENDIZAJE

- El alumno ha adquirido la suficiente información y destreza para desarrollar las competencias.

4. OBJETIVOS

Entender los principios básicos de las técnicas criptográficas: el cifrado-descifrado tanto simétrico como asimétrico, tecnicas de criptoanalisis, las funciones hash criptográficas, firma digital, etc. Analizar (complejidad y programación) los algoritmos más importantes de estas técnicas. Conocer y comprender los estándares más aceptados.

6. ORGANIZACIÓN DOCENTE

	CONTENIDOS
1	TEMA 1. Sistemas criptográficos simétricos(DES, AES, cifrado en flujo, hash y blockchain y asimétricos (RSA, mochila, curvas elípticas,). TEMA 2. Protocolos criptográficos(funciones hash criptográficas, firma digital, intercambio de claves,....). TEMA 3. Criptoanálisis(retículas, sistemas de ecuaciones polinomiales, ...). TEMA 4. Complejidad y programación de los algoritmos más importantes en criptología.

7. MÉTODOS DE LA EVALUACIÓN

Descripción	Tipología	Eval. Final	Recuper.	%
Evaluación continua	Otros	Sí	Sí	50,00
Evaluación continua	Otros	No	No	50,00
TOTAL				100,00

Observaciones
Evaluación continua mediante solución de ejercicios/programas y realización de trabajos
Criterios de evaluación para estudiantes a tiempo parcial
Los alumnos matriculados a tiempo parcial deberán realizar un examen final en laboratorio.

8. BIBLIOGRAFÍA Y MATERIALES DIDÁCTICOS

BÁSICA

-Stinson, Douglas R. Cryptography, theory and practice. CRC Press Series on Discrete Mathematics and its Applications, 1996 .
-Jaime Gutierrez y Juan Tena. Protocolos Criptograficos y seguridad en redes. Servicio de publicaciones Universidad de Cantabria, 2003.
-D. Micciancio and S. Goldwasser. Complexity of Lattices Problems, The Kluwer International Series in Engineering and Computer Science, vol. 671, 2002.

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.