

GUÍA DOCENTE ABREVIADA DE LA ASIGNATURA

346 - Criptología

Máster Universitario en Matemáticas y Computación

Curso Académico 2025-2026

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	346 - Criptología				
Créditos ECTS	3	Cuatrimestre	Cuatrimestral (1)		
Web	https://cryptology.unican.es/				
Idioma de impartición	Español	English friendly	Sí	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					

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, técnicas de criptoanálisis, funciones hash criptográficas, blockchain, firma digital, etc. Analizar (complejidad y programación) los algoritmos más importantes de estas técnicas. Conocer y comprender los estándares más aceptados. Entender el papel de la criptología en la seguridad informática.

6. ORGANIZACIÓN DOCENTE	
CONTENIDOS	
1	<p>TEMA 1. Sistemas criptográficos simétricos(DES, AES, cifrado en flujo) y asimétricos (RSA, mochila, curvas elípticas).</p> <p>TEMA 2. Teoría de la Información. Complejidad y programación de los algoritmos más importantes en criptología. Criptología en seguridad informática.</p> <p>TEMA 3. Criptoanálisis(retículas, sistemas de ecuaciones polinomiales, ...).</p> <p>TEMA 4. Protocolos criptográficos y aplicaciones (funciones hash, blockchain, compartición de secretos, firma digital, intercambio de claves,...).</p> <p>TEMA 5. A collusion-resistant identity-based scheme for symmetric key generation</p> <p>TEMA 5. A collusion-resistant identity-based scheme for symmetric key generation</p>

7. MÉTODOS DE LA EVALUACIÓN				
Descripción	Tipología	Eval. Final	Recuper.	%
Controles de trabajo	Evaluación en laboratorio	No	Sí	50,00
Ejercicios clase	Evaluación en laboratorio	No	Sí	50,00
TOTAL				100,00
Observaciones				
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
<p>-Stinson, Douglas R. Cryptography, theory and practice. CRC Press Series on Discrete Mathematics and its Applications, 1996 .</p> <p>-Jaime Gutierrez y Juan Tena. Protocolos Criptograficos y seguridad en redes. Servicio de publicaciones Universidad de Cantabria, 2003.</p> <p>-D. Micciancio and S. Goldwasser. Complexity of Lattices Problems, The Kluwer International Series in Engineering and Computer Science, vol. 671, 2002.</p>

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.