

Facultad de Ciencias

## GUÍA DOCENTE DE LA ASIGNATURA

M1507 - Criptología

Máster Universitario en Matemáticas y Computación  
Optativa. Curso 1

Curso Académico 2019-2020

### 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

### 2. CONOCIMIENTOS PREVIOS

Algebra lineal  
Teoria de grupos, anillos y cuerpos  
Conocimientos de programación

### 3. COMPETENCIAS GENÉRICAS Y ESPECÍFICAS DEL PLAN DE ESTUDIOS TRABAJADAS

<b>Competencias Genéricas</b>
Conocimiento actualizado de las áreas más activas en ámbitos relacionados con Matemáticas, Computación o la interacción de ambas
<b>Competencias Específicas</b>
Conocer resultados avanzados y conocer y comprender problemas abiertos de Matemáticas y/o Computación para su iniciación a la investigación.
Conocer cómo modelizar matemáticamente situaciones prácticas provenientes de problemas de Ciencia, Ingeniería o Ciencias Sociales
Aplicar, analizar, diseñar y/o implementar algoritmos eficientes orientados a situaciones que admiten una modelización matemática.
<b>Competencias Básicas</b>
Poseer y comprender conocimientos que aporten una base u oportunidad de ser originales en el desarrollo y/o aplicación de ideas, a menudo en un contexto de investigación
Que los estudiantes sepan aplicar los conocimientos adquiridos y su capacidad de resolución de problemas en entornos nuevos o poco conocidos dentro de contextos más amplios (o multidisciplinares) relacionados con su área de estudio
Que los estudiantes sean capaces de integrar conocimientos y enfrentarse a la complejidad de formular juicios a partir de una información que, siendo incompleta o limitada, incluya reflexiones sobre las responsabilidades sociales y éticas vinculadas a la aplicación de sus conocimientos y juicios
<b>Competencias Transversales</b>
Que perfeccionen su competencia digital y, en general, sus habilidades para buscar, obtener, seleccionar, tratar, analizar y comunicar informaciones diversas, así como para transformarlas en conocimiento y ofrecerlo a la consideración de los demás.
Que cultiven su capacidad de aprendizaje autónomo, además de las competencias interpersonales relacionadas con el trabajo en equipo, la colaboración grupal en contextos social y culturalmente diversos, la capacidad crítica y autocrítica, y la auto-regulación emocional.
Exposición y presentación pública del trabajo mediante una comunicación efectiva.

#### 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, 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.

**5. MODALIDADES ORGANIZATIVAS Y MÉTODOS DOCENTES**

ACTIVIDADES	HORAS DE LA ASIGNATURA
<b>ACTIVIDADES PRESENCIALES</b>	
<b>HORAS DE CLASE (A)</b>	
- Teoría (TE)	20
- Prácticas en Aula (PA)	
- Prácticas de Laboratorio (PL)	10
- Horas Clínicas (CL)	
Subtotal horas de clase	30
<b>ACTIVIDADES DE SEGUIMIENTO (B)</b>	
- Tutorías (TU)	8
- Evaluación (EV)	7
Subtotal actividades de seguimiento	15
<b>Total actividades presenciales (A+B)</b>	<b>45</b>
<b>ACTIVIDADES NO PRESENCIALES</b>	
Trabajo en grupo (TG)	
Trabajo autónomo (TA)	30
Tutorías No Presenciales (TU-NP)	
Evaluación No Presencial (EV-NP)	
<b>Total actividades no presenciales</b>	<b>30</b>
<b>HORAS TOTALES</b>	<b>75</b>

## 6. ORGANIZACIÓN DOCENTE

CONTENIDOS		TE	PA	PL	CL	TU	EV	TG	TA	TU-NP	EV-NP	Semana
1	<p>TEMA 1. Sistemas criptográficos simétricos(DES, AES, cifrado en flujo, hash y blockchain y asimétricos (RSA, mochila, curvas elípticas, ).</p> <p>TEMA 2. Protocolos criptográficos( funciones hash criptográficas, firma digital, intercambio de claves,.....).</p> <p>TEMA 3. Criptoanálisis( retículas, sistemas de ecuaciones polinomiales, ...).</p> <p>TEMA 4. Complejidad y programación de los algoritmos más importantes en criptología.</p>	20,00	0,00	10,00	0,00	8,00	7,00	0,00	30,00	0,00	0,00	1-7
TOTAL DE HORAS		20,00	0,00	10,00	0,00	8,00	7,00	0,00	30,00	0,00	0,00	

Esta organización tiene carácter orientativo.

TE	Horas de teoría
PA	Horas de prácticas en aula
PL	Horas de prácticas de laboratorio
CL	Horas 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.	%
Evaluación continua	Trabajo	Sí	Sí	50,00
Calif. mínima	0,00			
Duración				
Fecha realización	A determinar			
Condiciones recuperación	Si la asignatura no se supera en las actividades de evaluación ordinarias realizadas durante los dos cuatrimestres se podrá acceder a la recuperación en septiembre. Los alumnos que se presenten a la recuperación no podrán optar a la calificación de MH.			
Observaciones				
Evaluación continua	Otros	No	No	50,00
Calif. mínima	0,00			
Duración				
Fecha realización	A lo largo del curso			
Condiciones recuperación				
Observaciones	Consistirá en la realización de ejercicios y programas durante las clases.			
<b>TOTAL</b>				<b>100,00</b>
<b>Observaciones</b>				
Evaluación continua mediante solución de ejercicios/programas y realización de trabajos				
Observaciones para alumnos 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.
Complementaria
-B. Schneider. Applied Cryptography. J. Wiley, 1994.
- Diversos artículos e informes científicos.
- T. Cormen, C. Leiserson, R. Rivest, C. Stein: "Introduction to Algorithms". MIT press.

## 9. SOFTWARE

PROGRAMA / APLICACIÓN	CENTRO	PLANTA	SALA	HORARIO
Sage	Industriales			
Diverso software criptográfico libre				

### 10. COMPETENCIAS LINGÜÍSTICAS

- |   |   |
|---|---|
| <input checked="" type="checkbox"/> Comprensión escrita                 | <input type="checkbox"/> Comprensión oral |
| <input type="checkbox"/> Expresión escrita                              | <input type="checkbox"/> Expresión oral   |
| <input type="checkbox"/> Asignatura íntegramente desarrollada en inglés |   |

**Observaciones**