

Facultad de Ciencias

GUÍA DOCENTE DE LA ASIGNATURA

M1713 - Criptología

Máster Universitario en Ingeniería Informática
Optativa. Curso 2

Curso Académico 2021-2022

1. DATOS IDENTIFICATIVOS

Título/s	Máster Universitario en Ingeniería Informática			Tipología v Curso	Optativa. Curso 2
Centro	Facultad de Ciencias				
Módulo / materia	ASIGNATURAS OPTATIVAS				
Código y denominación	M1713 - 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

Competencias Genéricas
Capacidad para la aplicación de los conocimientos adquiridos y de resolver problemas en entornos nuevos o poco conocidos dentro de contextos más amplios y multidisciplinares, siendo capaces de integrar estos conocimientos
Competencias Específicas
Capacidad para diseñar, desarrollar, gestionar y evaluar mecanismos de certificación y garantía de seguridad en el tratamiento y acceso a la información en un sistema de procesamiento local o distribuido
Competencias Básicas
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 comunicar sus conclusiones -y los conocimientos y razones últimas que las sustentan- a públicos especializados y no especializados de un modo claro y sin ambigüedades
Que los estudiantes posean las habilidades de aprendizaje que les permitan continuar estudiando de un modo que habrá de ser en gran medida autodirigido o autónomo
Competencias Transversales
Capacidad de análisis, síntesis y evaluación
Capacidad de organización y planificación
Capacidad de razonamiento crítico
Aprendizaje autónomo

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

6. ORGANIZACIÓN DOCENTE													
CONTENIDOS		TE	PA	PLE	PLO	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	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	0,00	10,00	0,00	8,00	7,00	0,00	30,00	0,00	0,00	

Esta organización tiene carácter orientativo.

Ante la situación incierta de que las medidas de distanciamiento social establecidas por las autoridades sanitarias no permitan desarrollar alguna actividad docente de forma presencial en el aula para todos los estudiantes matriculados, se adoptará una modalidad mixta de docencia que combine esta docencia presencial en el aula con docencia a distancia. De la misma manera, la tutorización podrá ser sustituida por tutorización a distancia utilizando medios telemáticos.

TE	Horas de teoría
PA	Horas de prácticas en aula
PLE	Horas de prácticas de laboratorio experimental
PLO	Horas de prácticas de laboratorio en ordenador
CL	Horas de prácticas 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	Otros	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.			
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.
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 checked="" type="checkbox"/> Expresión escrita | <input type="checkbox"/> Expresión oral |
| <input type="checkbox"/> Asignatura íntegramente desarrollada en inglés | |

Observaciones