Escuela Técnica Superior de Ingenieros Industriales y de Telecomunicación

GUÍA DOCENTE DE LA ASIGNATURA

G844 - Criptografía y Seguridad en Redes y Servicios

Grado en Ingeniería de Tecnologías de Telecomunicación
Optativa. Curso 4

Curso Académico 2021-2022

1. DATOS IDENTIFICATIVOS

Título/s	Grado en Ingeniería de Tecnologías de Telecomunicación			Tipología y Curso	Optativa. Curso 4
Centro	Escuela Técnica Superior de Ingenieros Industriales y de Telecomunicación				
Módulo / materia	MATERIA APLICACIONES Y SERVICIOS TELEMÁTICOS MENCIÓN EN TELEMÁTICA				
Código y denominación	G844 - Criptografía y Seguridad en Redes y Servicios				
Créditos ECTS	6	Cuatrimestre		Cuatrimestral (1)	
Web	https://www.tlmat.unican.es/index.php?l=es&p=teaching&s=subjects&ss=g_csrs&				
Idioma de impartición	Español	English friendly	Sí	Forma de impartición	Presencial

Departamento	DPTO. INGENIERIA DE COMUNICACIONES
Profesor responsable	LUIS MUÑOZ GUTIERREZ
E-mail	luis.munoz@unican.es
Número despacho	Edificio Ing. de Telecomunicación Prof. José Luis García García. Planta: - 2. DESPACHO (S202)
Otros profesores	JORGE LANZA CALDERON

2. CONOCIMIENTOS PREVIOS

La asignatura no presupone conocimientos previos específicos más allá de aquéllos relacionados con los protocolos y servicios para redes fijas y móviles.

3. COMPETENCIAS GENÉRICAS Y ESPECÍFICAS DEL PLAN DE ESTUDIOS TRABAJADAS
Competencias Genéricas
Capacidad de resolver problemas con iniciativa, toma de decisiones, creatividad, y de comunicar y transmitir conocimientos, habilidades y destrezas, comprendiendo la responsabilidad ética y profesional de la actividad del ingeniero técnico de telecomunicación.
Pensamiento lógico.
Creatividad.
Pensamiento crítico y reflexivo.
Uso de las TIC.
Búsqueda de información.
Comunicación verbal.
Comunicación escrita.
Competencias Específicas
Capacidad para aplicar las técnicas en que se basan las redes, servicios y aplicaciones telemáticas, tales como sistemas de gestión, señalización y conmutación, encaminamiento y enrutamiento, seguridad (protocolos criptográficos, tunelado, cortafuegos, mecanismos de cobro, de autenticación y de protección de contenidos), ingeniería de tráfico (teoría de grafos, teoría de colas y teletráfico) tarificación y fiabilidad y calidad de servicio, tanto en entornos fijos, móviles, personales, locales o a gran distancia, con diferentes anchos de banda, incluyendo telefonía y datos.
Capacidad de describir, programar, validar y optimizar protocolos e interfaces de comunicación en los diferentes niveles de una arquitectura de redes.

3.1 RESULTADOS DE APRENDIZAJE

- El alumno será capaz de conocer los conceptos, herramientas y técnicas que dan soporte a la criptografía y seguridad en redes de comunicaciones. Asimismo, deberá ser capaz de valorar la complejidad de los distintos esquemas criptográficos estudiados y sus implicaciones prácticas.

4. OBJETIVOS

El objetivo principal de la asignatura es abordar los conceptos y técnicas relativos a la confidencialidad, integridad y autenticidad de la transmisión y almacenamiento de la información. Para ello se presentan los fundamentos matemáticos de teoría de números que dan soporte a los esquemas de cifrado simétrico y asimétrico para posteriormente profundizar en el estudio de los correspondientes algoritmos.

5. MODALIDADES ORGANIZATIVAS Y MÉTODOS DOCENTES	
ACTIVIDADES	HORAS DE LA ASIGNATURA
ACTIVIDADES PRESENCIALES	
HORAS DE CLASE (A)	
- Teoría (TE)	38
- Prácticas en Aula (PA)	14
- Prácticas de Laboratorio Experimental(PLE)	8
- Prácticas de Laboratorio en Ordenador (PLO)	
- Prácticas Clínicas (CL)	
Subtotal horas de clase	60
ACTIVIDADES DE SEGUIMIENTO (B)	
- Tutorías (TU)	9
- Evaluación (EV)	6
Subtotal actividades de seguimiento	15
Total actividades presenciales (A+B)	75
ACTIVIDADES NO PRESENCIALES	
Trabajo en grupo (TG)	45
Trabajo autónomo (TA)	30
Tutorías No Presenciales (TU-NP)	
Evaluación No Presencial (EV-NP)	
Total actividades no presenciales	75
HORAS TOTALES	150

6. ORGANIZACIÓN DOCENTE

CONTENIDOS		TE	PA	PLE	PLO	CL	TU	EV	TG	TA	TU-NP	EV-NP	Semana
1	Introducción a la seguridad en redes. Terminología. Servicios de seguridad: Confidencialidad, autenticación, autorización y no repudio.	8,00	1,00	0,00	0,00	0,00	1,00	1,00	10,00	5,00	0,00	0,00	1-2
2	Cifrado de datos. Clasificación de los criptosistemas. Cifrado simétrico en bloque: DES, AES. Cifrado en flujo. LFSR. Aleatoriedad y período de las secuencias.	6,00	3,00	4,00	0,00	0,00	2,00	1,00	10,00	7,00	0,00	0,00	3-4
3	Criptografía y teoría de números. Números primos y relativamente primos. Conceptos básicos de aritmética modular. El Teorema de Fermat. El Teorema de Euler. El Algoritmo de Euclides: Cálculo del inverso multiplicativo; Teorema chino del resto.	8,00	4,00	0,00	0,00	0,00	2,00	2,00	10,00	8,00	0,00	0,00	5-7
4	Criptografía de clave pública. Introducción y principios generales de los criptosistemas de clave pública. Esquemas de funcionamiento de los criptosistemas de clave pública: Confidencialidad, autenticación, autenticación/confidencialidad. El esquema de Diffie-Hellman. El algoritmo RSA.	10,00	3,00	4,00	0,00	0,00	2,00	1,00	10,00	8,00	0,00	0,00	8-10
5	Autenticación. Introducción a los servicios de autenticación, autorización o control de acceso y firma digital. Funciones de hash. Funciones MAC. HMAC.	6,00	3,00	0,00	0,00	0,00	2,00	1,00	5,00	2,00	0,00	0,00	11-12
TOTAL DE HORAS		38,00	14,00	8,00	0,00	0,00	9,00	6,00	45,00	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	Examen escrito	No	Sí	40,00

Calif. mínima	0,00
Duración	1 hora por cada prueba de conocimientos realizada
Fecha realización	En el transcurso de la asignatura y coincidiendo con la finalización de los correspondientes temas.
Condiciones recuperación	En el examen final correspondiente a las convocatorias ordinaria y extraordinaria
Observaciones	

Examen final	Examen escrito	Sí	Sí	60,00

Calif. mínima	4,00
Duración	2 horas
Fecha realización	Al finalizar la asignatura en la fecha establecida por el centro al efecto.
Condiciones recuperación	En la convocatoria extraordinaria de septiembre
Observaciones	

TOTAL	100,00

Observaciones

En la evaluación de la asignatura se contempla la realización de un examen final cuya calificación, (CEF), está ponderada un 60% con la calificación procedente de la evaluación continua (CEC).
Se exige una nota en el examen final igual o superior a 4, para optar a hacer promedio con la calificación procedente de la evaluación continua. Así, la nota final de la asignatura se obtiene del máximo (CEF, CEF*0,60+CEC*0,40).
Los alumnos que opten por no realizar la evaluación continua o no asistan a clase serán evaluados en base a la calificación obtenida en el examen final.
Se prevé la evaluación a distancia de los ejercicios prácticos de laboratorio y pruebas escritas en el caso de que una nueva alerta sanitaria por COVID-19 haga imposible realizar la evaluación de forma presencial.

Criterios de evaluación para estudiantes a tiempo parcial

Los alumnos que opten por no realizar la evaluación continua o no asistan a clase serán evaluados en base a la calificación obtenida en el examen final.

8. BIBLIOGRAFÍA Y MATERIALES DIDÁCTICOS

BÁSICA

W. Stallings, "Cryptography and Network Security, Principles and Practices", Pearson International Edition, 2006. ISBN: 0-13-202322-9.
A. Menezes, "Handbook of Applied Cryptography", CRC, 1996. ISBN 0-8493-8523-7.

Complementaria

9. SOFTWARE

PROGRAMA / APLICACIÓN	CENTRO	PLANTA	SALA	HORARIO

10. COMPETENCIAS LINGÜÍSTICAS

☑ Comprensión escrita	☐ Comprensión oral
☐ Expresión escrita	☐ Expresión oral

☐ Asignatura íntegramente desarrollada en inglés

Observaciones