

GUÍA DOCENTE ABREVIADA DE LA ASIGNATURA

G844 - Criptografía y Seguridad en Redes y Servicios

Grado en Ingeniería de Tecnologías de Telecomunicación

Curso Académico 2021-2022

1. DATOS IDENTIFICATIVOS					
Título/s	Grado en Ingeniería de Tecnologías de Telecomunicación			Tipología v 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

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.

6. ORGANIZACIÓN DOCENTE

CONTENIDOS	
1	Introducción a la seguridad en redes. Terminología. Servicios de seguridad: Confidencialidad, autenticación, autorización y no repudio.
2	Cifrado de datos. Clasificación de los criptosistemas. Cifrado simétrico en bloque: DES, AES. Cifrado en flujo. LFSR. Aleatoriedad y período de las secuencias.
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.
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.
5	Autenticación. Introducción a los servicios de autenticación, autorización o control de acceso y firma digital. Funciones de hash. Funciones MAC. HMAC.

7. MÉTODOS DE LA EVALUACIÓN

Descripción	Tipología	Eval. Final	Recuper.	%
Evaluación continua	Examen escrito	No	Sí	40,00
Examen final	Examen escrito	Sí	Sí	60,00
TOTAL				100,00
Observaciones				
<p>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).</p> <p>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, $CEF*0,60+CEC*0,40$).</p> <p>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.</p> <p>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.</p>				
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.

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.