GUÍA DOCENTE ABREVIADA DE LA ASIGNATURA

G844 - Criptografía y Seguridad en Redes y Servicios

Grado en Ingeniería de Tecnologías de Telecomunicación

Curso Académico 2023-2024

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

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. Cifrado en flujo. Introducción al álgebra de grupos, anillos y cuerpos finitos. El algoritmo AES.
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.	%
Control de conocimientos -1	Examen escrito	No	Sí	30,00
Control de conocimientos-2	Examen escrito	No	Sí	30,00
Control de conocimientos-3	Examen escrito	No	Sí	30,00
Prácticas	Evaluación en laboratorio	No	No	10,00
TOTAL				100,00

Observaciones

Los alumnos que superen la evaluación continua, aprobando los tres controles de conocimientos, no precisarán realizar el examen final y tendrán como calificación el promedio de la calificación obtenida en la evaluación continua (CEC), entendida esta como el promedio ponderado de los tres controles de conocimientos y calificación de las prácticas. Podrán optar a subir la misma presentándose a la convocatoria ordinaria de modo que su calificación final, Calif_Final= Máximo (CEC, 0,60*CEC+0,40*CEF), siendo CEF la calificación de la convocatoria ordinaria.

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.