Guía docente
230713 - DPROT - Protección de los Datos

Última modificación: 15/06/2023

Unidad responsable: Escuela Técnica Superior de Ingeniería de Telecomunicación de Barcelona
Unidad que imparte: 749 - MAT - Departamento de Matemáticas.

Titulación: MÁSTER UNIVERSITARIO EN INGENIERÍA DE TELECOMUNICACIÓN (Plan 2013). (Asignatura optativa).
MÁSTER UNIVERSITARIO EN TECNOLOGÍAS AVANZADAS DE TELECOMUNICACIÓN (Plan 2019). (Asignatura optativa).
MÁSTER UNIVERSITARIO EN CIBERSEGURIDAD (Plan 2020). (Asignatura obligatoria).

Curso: 2023 **Créditos ECTS:** 5.0 **Idiomas:** Inglés

PROFESORADO

Profesorado responsable: Consultar aquí / See here: https://telecos.upc.edu/ca/estudis/curs-actual/professorat-responsables-coordinadors/responsables-assignatura

Otros: Consultar aquí / See here: https://telecos.upc.edu/ca/estudis/curs-actual/professorat-responsables-coordinadors/professorat-assignat-idioma

CAPACIDADES PREVIAS

Álgebra lineal y probabilidad, básicas.
Se recomienda un conocimiento básico de criptografía, a nivel introductorio.

METODOLOGÍAS DOCENTES

- Clases
- Trabajo individual
- Examen final

OBJETIVOS DE APRENDIZAJE DE LA ASIGNATURA

Entender las técnicas criptográficas necesarias utilizadas para proteger los datos durante su almacenamiento y transmisión, garantizando su confidencialidad, integridad y autenticidad.

HORAS TOTALES DE DEDICACIÓN DEL ESTUDIANTADO

Tipo	Horas	Porcentaje
Horas grupo pequeño	26,0	20.80
Horas aprendizaje autónomo	86,0	68.80
Horas grupo grande	13,0	10.40

Dedicación total: 125 h

CONTENIDOS

Introducción

Descripción:
Introducción a la criptografía desde el punto de vista de la protección de datos.

Dedicación: 9h 36m
Grupo pequeño/Laboratorio: 3h
Aprendizaje autónomo: 6h 36m

Clave simétrica

Descripción:
Cifrado de clave simétrica. Cifrados de flujo y de bloque. Modos de operación. Códigos de autenticación de mensages. Funciones de hash. Cifrado auténtico.

Dedicación: 19h 12m
Grupo pequeño/Laboratorio: 6h
Aprendizaje autónomo: 13h 12m

Clave pública

Descripción:
Intercambio de claves. Cifrado de clave pública. Ataque man-in-the-middle. Firmas digitales. Esquemas de identificación. Certificados de clave pública. Cryptografía basada en la identidad.

Dedicación: 29h
Grupo pequeño/Laboratorio: 9h
Aprendizaje autónomo: 20h

Modelos de seguridad

Descripción:
Definición de tareas computationales fáciles y difíciles. Nociones de seguridad para cifrado. Nociones de seguridad para firmas. El modelo del oráculo aleatorio. Reducciones y demostraciones de seguridad.

Dedicación: 19h 12m
Grupo pequeño/Laboratorio: 6h
Aprendizaje autónomo: 13h 12m

Conocimiento cero

Descripción:
Pruebas y argumentos de conocimiento cero. Conocimiento cero no interactivo. Aplicaciones.

Dedicación: 9h 36m
Grupo pequeño/Laboratorio: 3h
Aprendizaje autónomo: 6h 36m

Criptografía distribuida

Descripción:
Criptografía para múltiples usuarios. Compartición de secretos. Descifrado de umbral. Firma de umbral. Computación multiparte segura.

Dedicación: 19h 12m
Grupo pequeño/Laboratorio: 6h
Aprendizaje autónomo: 13h 12m

Casos prácticos

Descripción:
Estudio de protocolos criptográficos reales utilizados en algunos escenarios prácticos.

Dedicación: 19h 12m
Grupo pequeño/Laboratorio: 6h
Aprendizaje autónomo: 13h 12m

SISTEMA DE CALIFICACIÓN

examen final: 35%
entregas y trabajos de laboratorio: 40%
trabajo final: 25%

BIBLIOGRAFÍA

Básica:
- Delfs, Hans; Knebl, Helmut. Introduction to cryptography : principles and applications. 3rd ed. Berlin [etc.]: Springer, 2015. ISBN 9783662479735.

RECURSOS

Enlace web:
- http://toc.cryptobook.us/. A Graduate Course in Applied Cryptography (online book)