Guia docent
230713 - DPROT - Protecció de les Dades

Última modificació: 24/05/2024

Unitat responsable: Escola Tècnica Superior d'Enginyeria de Telecomunicació de Barcelona
Unitat que imparteix: 749 - MAT - Departament de Matemàtiques.

Titulació: MÀSTER UNIVERSITARI EN ENGINYERIA DE TELECOMUNICACIÓ (Pla 2013). (Assignatura optativa).
MÀSTER UNIVERSITARI EN TECNOLOGIES AVANÇADES DE TELECOMUNICACIÓ (Pla 2019). (Assignatura optativa).
MÀSTER UNIVERSITARI EN CIBERSEGURETAT (Pla 2020). (Assignatura obligatòria).

Curs: 2024 **Crèdits ECTS:** 5.0 **Idiomes:** Anglès

PROFESSORAT

Professorat responsable: JORGE LUIS VILLAR SANTOS

Altres: Primer quadrimestre:
JORGE LUIS VILLAR SANTOS - 11, 13

CAPACITATS PRÈVIES

Àlgebra lineal i probabilitat, bàsiques.
Es recomana un coneixement bàsic de criptografia, a nivell introductori.

METODOLOGIES DOCENTS

- Classes
- Treball individual
- Examen final

OBJECTIUS D'APRENENTATGE DE L'ASSIGNATURA

Entendre les tècniques criptogràfiques necessaries utilitzades per protegir les dades durant el seu emmagatzematge i la seva transmissió, garantint la seva confidencialitat, integritat i autenticitat.

HORES TOTALS DE DEDICACIÓ DE L'ESTUDIANTAT

Tipus	Hores	Percentatge
Hores grup petit	26,0	20.80
Hores aprenentatge autònom	86,0	68.80
Hores grup gran	13,0	10.40

Dedicació total: 125 h

CONTINGUTS

Introducció

Descripció:
Introducció a la criptografia des del punt de vista de la protecció de dades.

Dedicació: 9h 36m
Grup petit/Laboratori: 3h
Aprenentatge autònom: 6h 36m

Clau simètrica

Descripció:
Xifratge de clau simètrica. Xifratges de fluxe i de bloc. Modes d'operació. Codis d'autenticació de missatges. Funcions de hash. Xifratge autèntic.

Dedicació: 19h 12m
Grup petit/Laboratori: 6h
Aprenentatge autònom: 13h 12m

Clau pública

Descripció:
Intercanvi de claus. Xifratge de clau pública. Atac man-in-the-middle. Firmes digitals. Esquemes d'identificació. Certificats de clau pública. Criptografia basada en l'identitat.

Dedicació: 29h
Grup petit/Laboratori: 9h
Aprenentatge autònom: 20h

Models de seguretat

Descripció:
Definició de tasques computationals fàcils i difícils. Nocions de seguretat per a xifratge. Nocions de seguretat per a firmes. El model de l'oracle aleatori. Reduccions i demostracions de seguretat.

Dedicació: 19h 12m
Grup petit/Laboratori: 6h
Aprenentatge autònom: 13h 12m

Coneixement zero

Descripció:
Proves i arguments de coneixement zero. Coneixement zero no interactiu. Aplicacions.

Dedicació: 9h 36m
Grup petit/Laboratori: 3h
Aprenentatge autònom: 6h 36m

Criptografia distribuïda

Descripció:
Criptografia per a múltiples usuaris. Compartició de secrets. Desxifratge d'umbral. Firma d'umbral. Computació multipart segura.

Dedicació: 19h 12m
Grup petit/Laboratori: 6h
Aprenentatge autònom: 13h 12m

Casos pràctics

Descripció:
Estudi de protocols criptogràfics reals utilitzats en alguns escenaris pràctics.

Dedicació: 19h 12m
Grup petit/Laboratori: 6h
Aprenentatge autònom: 13h 12m

SISTEMA DE QUALIFICACIÓ

examen final: 35%
entregues i treballs pràctics: 40%
treball final: 25%

BIBLIOGRAFIA

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

RECURSOS

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