Guia docent
230300 - COMSECRET - Àlgebra Lineal, Codis Lineals i Esquemes de Compartició de Secrets

Última modificació: 29/04/2020

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

Titulació:
GRAU EN ENGINYERIA DE SISTEMES AUDIOVISUALS (Pla 2009). (Assignatura optativa).
GRAU EN ENGINYERIA DE SISTEMES ELECTRÒNICS (Pla 2009). (Assignatura optativa).
GRAU EN CIÈNCIES I TECNOLOGIES DE TELECOMUNICACIÓ (Pla 2010). (Assignatura optativa).
GRAU EN ENGINYERIA DE SISTEMES DE TELECOMUNICACIÓ (Pla 2010). (Assignatura optativa).
GRAU EN ENGINYERIA TELEMÀTICA (Pla 2010). (Assignatura optativa).
GRAU EN ENGINYERIA DE TECNOLOGIES I SERVEIS DE TELECOMUNICACIÓ (Pla 2015). (Assignatura optativa).
GRAU EN ENGINYERIA ELECTRÒNICA DE TELECOMUNICACIÓ (Pla 2018). (Assignatura optativa).

Curs: 2020 **Crèdits ECTS:** 2.0 **Idiomes:** Català

PROFESSORAT

Professorat responsable: Sáez Moreno, Germán

Altres: Fàbrega Canudas, Josep
Muñoz López, Francisco Javier
Sáez Moreno, Germán

CAPACITATS PRÈVIES

Conceptes i tècniques bàsiques d'àlgebra lineal.

REQUISITS

IMPORTANT: si s'ha cursat prèviament l'assignatura "Transmissió de dades" no s'hauria de cursar aquest seminari a posteriori.

METODOLOGIES DOCENTS

El seminari combina sessions de teoria i de problemes, i aplicació pràctica en sessions de laboratori.

OBJECTIUS D'APRENENTATGE DE L'ASSIGNATURA

L'objectiu del seminari és fer una breu introducció, fent servir mètodes elementals de l'àlgebra lineal, a alguns objectes i tècniques de l'enginyeria de telecomunicacions centrals en el disseny de sistemes de comunicacions fiables i segurs. Concretament, es presentaran les nocions més bàsiques sobre els codis binaris lineals correctors d'errors i els protocols criptogràfics de compartició de secrets.

HORES TOTALS DE DEDICACIÓ DE L'ESTUDIANTAT

Tipus	Hores	Percentatge
Hores grup gran	20,0	40.00
Hores aprenentatge autònom	30,0	60.00

Dedicació total: 50 h

CONTINGUTS

Introducció a l'aritmètica modular.

Descripció:
Introducció a l'aritmètica modular. Espais vectorials sobre el cos finit de dos elements.

Dedicació: 5h
Grup gran/Teoria: 5h

Introducció als esquemes de compartició de secrets.

Descripció:
Introducció als esquemes de compartició de secrets. Esquemes lineals vectorials sobre el cos finit de dos elements. Procès de distribució del secret i procès de reconstrucció. Seguretat de l'esquema. Conjunts autoritzats.

Dedicació: 5h
Grup gran/Teoria: 5h

Introducció als codis correctors d'errors.

Descripció:
Introducció als codis correctors d'errors. Codis lineals en espais vectorials sobre el cos finit de dos elements. Matriu generadora i matriu de control. Codificació i descodificació. Distància de Hamming. Detecció i correcció d'errors.

Dedicació: 5h
Grup gran/Teoria: 5h

Introducció a la criptografia.

Descripció:
Introducció a la criptografia. Història. Mètodes criptogràfics clàssics. Criptografia de clau pública. RSA. Signatura i autentificació.

Dedicació: 5h
Grup gran/Teoria: 5h

SISTEMA DE QUALIFICACIÓ

La nota s'obtindrà de la valoració d'activitats realitzades durant el curs (participació activa durant les sessions, entrega d'exercicis o realització d'activitats guiades). Si s'escau, la nota així obtinguda es podrà millorar amb un control al final del seminari.

BIBLIOGRAFIA

Bàsica:
- Biggs, N.L. Matemática discreta. Barcelona: Vicens-Vives, 1994. ISBN 8431633115.