

230152 - CSI - Codificació i Seguretat de la Informació

Unitat responsable: 230 - ETSETB - Escola Tècnica Superior d'Enginyeria de Telecomunicació de Barcelona
Unitat que imparteix: 744 - ENTEL - Departament d'Enginyeria Telemàtica
Curs: 2018
Titulació: GRAU EN ENGINYERIA TELEMÀTICA (Pla 2010). (Unitat docent Optativa)
GRAU EN CIÈNCIES I TECNOLOGIES DE TELECOMUNICACIÓ (Pla 2010). (Unitat docent Optativa)
GRAU EN ENGINYERIA DE TECNOLOGIES I SERVEIS DE TELECOMUNICACIÓ (Pla 2015). (Unitat docent Optativa)
Crèdits ECTS: 6 Idiomes docència: Castellà

Professorat

Responsable: Rico Novella, Francisco Jose

Altres: Forne Muñoz, Jorge

Metodologies docents

- Classes expositives
- Classes d'aplicació
- Treball en grup (no presencial)
- Treball individual (no presencial)
- Presentacions orals
- Proves de resposta llarga

Objectius d'aprenentatge de l'assignatura

- Aprenentatge de la teoria sobre la qual se sustenta la codificació de canal.
- Aprofundir en el coneixement dels principals codis de canal utilitzats.
- Aprenentatge de conceptes generals de seguretat i privacitat de la informació.
- Aprofundir en el coneixement dels principals protocols de seguretat usats a Internet.

Hores totals de dedicació de l'estudiantat

Dedicació total: 150h	Hores grup gran:	52h	34.67%
	Hores aprenentatge autònom:	98h	65.33%

230152 - CSI - Codificació i Seguretat de la Informació

Continguts

1. Teoria de la codificació de canal	Dedicació: 35h Grup gran/Teoria: 9h Grup mitjà/Pràctiques: 3h Aprenentatge autònom: 23h
Descripció: Codis lineals; Codis cíclics; Codis pràctics: BCH, Reed-Solomon.	
2. Codis convolucional i modulació codificada	Dedicació: 30h Grup gran/Teoria: 8h Grup mitjà/Pràctiques: 2h Aprenentatge autònom: 20h
Descripció: Codificació i descodificació de codis convolucional; Modulació codificada; Turbocódigos.	
3. Concatenació de codis. Anàlisi de prestacions	Dedicació: 10h Grup gran/Teoria: 3h Grup mitjà/Pràctiques: 1h Aprenentatge autònom: 6h
Descripció: Models de canal; Codificadors i entrelaçats intern i extern; Probabilitat residual d'error.	
4. Conceptes de Seguretat en xarxes	Dedicació: 10h Grup gran/Teoria: 4h Aprenentatge autònom: 6h
Descripció: Mecanismes i Serveis de Seguretat; Criptografia simètrica i de clau pública; signatura digital; Seguretat perimetral.	

230152 - CSI - Codificació i Seguretat de la Informació

5. Autenticació i Gestió Claus	Dedicació: 25h Grup gran/Teoria: 6h Grup mitjà/Pràctiques: 2h Aprenentatge autònom: 17h
Descripció: Protocols i mecanismes d'autenticació; Protocols de gestió de claus; Infraestructura de clau pública (PKI); Models de confiança.	
6. Protocols de Seguretat a Internet	Dedicació: 25h Grup gran/Teoria: 6h Grup mitjà/Pràctiques: 2h Aprenentatge autònom: 17h
Descripció: Seguretat IP i xarxes privades virtuals; Seguretat en correu electrònic, Seguretat en web.	
7. Privacitat	Dedicació: 15h Grup gran/Teoria: 4h Grup mitjà/Pràctiques: 2h Aprenentatge autònom: 9h
Descripció: Sistemes de comunicació anònims; microagregació estadística	

Planificació d'activitats

PRESENTACIONS ORALS
Descripció: Defensa oral del Treball d'intensificació que hagi escollit l'alumne.
EXAMEN DE RESPOSTES LLARGUES
Descripció: Examen final de l'assignatura.

230152 - CSI - Codificació i Seguretat de la Informació

Sistema de qualificació

La nota final de l'assignatura s'obtindrà a partir de la qualificació d'avaluació continuada (participació activa a classe i treballs proposats pel professor al llarg del curs) i l'examen final, segons el següent criteri:

Examen final: 60%

Treball en grup i presentació: 30%

Participació activa a classe: 10%

Bibliografia

Bàsica:

Stallings, W. *Cryptography and network security: principles and practice*. 6th ed. Boston: Prentice Hall, 2014. ISBN 9780273793359.

Rifà, J.; Huguet, L. *Comunicación digital: teoría matemática de la información, codificación algebraica, criptología*. Barcelona: Masson, 1991. ISBN 8431105763.

Complementària:

López García, C.; Fernández Veiga, M. *Teoría de la información y codificación*. 2a ed. Vigo: Universidad de Vigo, 2013. ISBN 9788484087328.

Altres recursos:

Informació addicional disponible a ATENEA.