Última modificació: 13-09-2017

34954 - CC - Codis i Criptografia

Unitat responsable: 200 - FME - Facultat de Matemàtiques i Estadística

Unitat que imparteix: 749 - MAT - Departament de Matemàtiques

Curs: 2017

Titulació: MÀSTER UNIVERSITARI EN MATEMÀTICA AVANÇADA I ENGINYERIA MATEMÀTICA (Pla 2010). (Unitat docent Optativa)

Crèdits ECTS: 7,5 Idiomes docència: Anglès

Professorat

Responsable: MARIA PAZ MORILLO BOSCH

Altres: Primer quadrimestre:
SIMEON MICHAEL BALL - A
JAVIER HERRANZ SOTOCA - A
MARIA PAZ MORILLO BOSCH - A

Capacitats prèvies

Descrits a la versió en anglès.

Requisits

Descrits a la versió en anglès.

Competències de la titulació a les quals contribueix l'assignatura

Específiques:

1. CE-1. RECERCA - Llegir i entendre un article matemàtic de nivell avançat. Conèixer els procediments d'investigació en matemàtiques, tant per a la producció de nous coneixements com per a la seva transmissió.
2. CE-3. CÀLCUL - Obtenir solucions (exactes o aproximades) per als models, en funció de les eines i recursos disponibles, incloent mitjans computacionals.
3. CE-4. ANÀLISIS CRÍTICA - Discutir la validesa, l'abast i la rellevància d'aquestes solucions i saber presentar i defensar les seves conclusions.

Transversals:

4. APRENENTATGE AUTÒNOM: Detectar mancances en el propi coneixement i superar-les mitjançant la reflexió crítica i l'elecció de la millor actuació per ampliar aquest coneixement.
5. COMUNICACIÓ EFICAÇ ORAL I ESCRITA: Comunicar-se de forma oral i escrita amb altres persones sobre els resultats de l'aprenentatge, de l'elaboració del pensament i de la presa de decisions; participar en debats sobre temes de la pròpia especialitat.
6. TERCERA LLENGUA: Conèixer una tercera llengua, que serà preferentment l'anglès, amb un nivell adequat de forma oral i per escrit i amb consonància amb les necessitats que tindran les titulades i els titulats en cada ensenyament.
7. TREBALL EN EQUIP: Ser capaç de treballar com a membre d'un equip, ja sigui com un membre més, o realitzant tasques de direcció amb la finalitat de contribuir a desenvolupar projectes amb pragmatisme i sentit de la responsabilitat, tot assumint compromisos considerant els recursos disponibles.
8. ÚS SOLVENT DELS RECURSOS D'INFORMACIÓ: Gestionar l'adquisició, l'estructuració, l'anàlisi i la visualització de dades i informació de l'àmbit d'especialitat i valorar de forma crítica els resultats d'aquesta gestió.

Última modificació: 13-09-2017

34954 - CC - Codis i Criptografia

Metodologies docents

Descrits a la versió en anglès.

Objectius d'aprenentatge de l'assignatura

Descrits a la versió en anglès.

Hores totals de dedicació de l'estudiantat

Dedicació total: 187h 30m	Hores grup gran:	60h	32.00%
	Hores aprenentatge autònom:	127h 30m	68.00%

Última modificació: 13-09-2017

34954 - CC - Codis i Criptografia

Continguts

Introduction

Dedicació: 6h 15m
Classes teòriques: 2h
Aprenentatge autònom: 4h 15m

Descripció:
Descritos en la versión en inglés.

Information and Entropy

Dedicació: 18h 45m
Classes teòriques: 6h
Aprenentatge autònom: 12h 45m

Descripció:
Descrits a la versió en anglès.

Source codes without memory

Dedicació: 12h 30m
Classes teòriques: 4h
Aprenentatge autònom: 8h 30m

Descripció:
Descrits a la versió en anglès.

Channel coding

Dedicació: 18h 45m
Classes teòriques: 6h
Aprenentatge autònom: 12h 45m

Descripció:
Descrits a la versió en anglès.

Block codes

Dedicació: 18h 45m
Classes teòriques: 6h
Aprenentatge autònom: 12h 45m

Descripció:
Descrits a la versió en anglès.

34954 - CC - Codis i Criptografia

Cyclic codes	Dedicació: 18h 45m Classes teòriques: 6h Aprenentatge autònom: 12h 45m
Descripció: Descrits a la versió en anglès.	

Introduction to modern cryptography	Dedicació: 15h 37m Classes teòriques: 5h Aprenentatge autònom: 10h 37m
Descripció: Descrits a la versió en anglès.	

Symmetric key cryptography	Dedicació: 15h 38m Classes teòriques: 5h Aprenentatge autònom: 10h 38m
Descripció: Descrits a la versió en anglès.	

Public key encryption	Dedicació: 15h 37m Classes teòriques: 5h Aprenentatge autònom: 10h 37m
Descripció: Descrits a la versió en anglès.	

Digital signatures	Dedicació: 15h 38m Classes teòriques: 5h Aprenentatge autònom: 10h 38m
Descripció: Descrits a la versió en anglès.	

Última modificació: 13-09-2017

34954 - CC - Codis i Criptografia

Proofs of knowledge and other cryptographic protocols	Dedicació: 15h 37m Classes teòriques: 5h Aprenentatge autònom: 10h 37m
Descripció: Descrits a la versió en anglès.	

Multiparty computation	Dedicació: 15h 38m Classes teòriques: 5h Aprenentatge autònom: 10h 38m
Descripció: Descrits a la versió en anglès.	

Sistema de qualificació

Descrits a la versió en anglès.

Normes de realització de les activitats

Descrits a la versió en anglès.

34954 - CC - Codis i Criptografia

Bibliografia

Bàsica:

Huffman, W. Cary; Pless, Vera. Fundamentals of error-correcting codes. Cambridge: Cambridge University Press, 2003. ISBN 0521782805.

Justesen, Jorn; Hoholdt, Tom. A Course in error-correcting codes. Zürich: European Mathematical Society, 2004. ISBN 3037190019.

Xambó Descamps, Sebastián. Block error-correcting codes : a computational primer. Berlin: Springer, 2003. ISBN 3540003959.

Delfs, Hans; Knebl, Helmut. Introduction to cryptography : principles and applications. 2nd ed. Berlin: Springer, 2007. ISBN 9783540492436.

Katz, Jonathan; Lindell, Yehuda. Introduction to modern cryptography : principles and protocols. Boca Raton: Chapman & Hall, 2008. ISBN 9781584885511.

Complementària:

Johnson, Sarah J. Iterative error correction : turbo, low-density parity-check and repeat-accumulate codes. Cambridge: Cambridge University Press, 2010. ISBN 9780521871488.

Welsh, Dominic. Codes and cryptography. Oxford: Oxford university Press, 1988. ISBN 0198532881.

Goldreich, Oded. Foundations of cryptography : basic tools. New York: Cambridge University Press, 2001. ISBN 0521791723.

Goldreich, Oded. Foundations of cryptography : basic applications. New York: Cambridge University Press, 2004. ISBN 9780521830843.