

Guia docent

34954 - CC - Codis i Criptografia

Última modificació: 11/04/2024

Unitat responsable: Facultat de Matemàtiques i Estadística
Unitat que imparteix: 749 - MAT - Departament de Matemàtiques.

Titulació: MÀSTER UNIVERSITARI EN MATEMÀTICA AVANÇADA I ENGINYERIA MATEMÀTICA (Pla 2010). (Assignatura optativa).

Curs: 2024 **Crèdits ECTS:** 7.5 **Idiomes:** Anglès

PROFESSORAT

Professorat responsable: SIMEON MICHAEL BALL MARKS

Altres: Segon quadrimestre:
SIMEON MICHAEL BALL MARKS - A
JAVIER HERRANZ SOTOCA - 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-2. MODELITZACIÓ - Formular, analitzar i validar models matemàtics de problemes pràctics, emprant les eines matemàtiques més adequades als objectius que es persegueixen.
3. CE-3. CÀLCUL - Obtenir solucions (exactes o aproximades) per als models, en funció de les eines i recursos disponibles, incloent mitjans computacionals.
4. CE-4. ANÀLISIS CRÍTICA - Discutir la validesa, l'abast i la rellevància d'aquestes solucions i saber presentar i defensar les seves conclusions.

Transversals:

5. APRENTATGE 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.
6. 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.
7. 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.
8. 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.
9. 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.

METODOLOGIES DOCENTS

Descrits a la versió en anglès.

OBJECTIUS D'APRENTATGE DE L'ASSIGNATURA

Descrits a la versió en anglès.

HORES TOTALS DE DEDICACIÓ DE L'ESTUDIANTAT

Tipus	Hores	Percentatge
Hores grup gran	60,0	32.00
Hores aprenentatge autònom	127,5	68.00

Dedicació total: 187.5 h

CONTINGUTS

Introduction

Descripció:

Descritos en la versión en inglés.

Dedicació: 6h 15m

Classes teòriques: 2h

Aprenentatge autònom: 4h 15m

Information and Entropy

Descripció:

Descrits a la versió en anglès.

Dedicació: 18h 45m

Classes teòriques: 6h

Aprenentatge autònom: 12h 45m

Source codes without memory

Descripció:

Descrits a la versió en anglès.

Dedicació: 12h 30m

Classes teòriques: 4h

Aprenentatge autònom: 8h 30m



Channel coding

Descripció:

Descrits a la versió en anglès.

Dedicació: 18h 45m

Classes teòriques: 6h

Aprenentatge autònom: 12h 45m

Block codes

Descripció:

Descrits a la versió en anglès.

Dedicació: 18h 45m

Classes teòriques: 6h

Aprenentatge autònom: 12h 45m

Cyclic codes

Descripció:

Descrits a la versió en anglès.

Dedicació: 18h 45m

Classes teòriques: 6h

Aprenentatge autònom: 12h 45m

Introduction to modern cryptography

Descripció:

Descrits a la versió en anglès.

Dedicació: 15h 37m

Classes teòriques: 5h

Aprenentatge autònom: 10h 37m

Symmetric key cryptography

Descripció:

Descrits a la versió en anglès.

Dedicació: 15h 38m

Classes teòriques: 5h

Aprenentatge autònom: 10h 38m

Public key encryption

Descripció:

Descrits a la versió en anglès.

Dedicació: 15h 37m

Classes teòriques: 5h

Aprenentatge autònom: 10h 37m

Digital signatures

Descripció:

Descrits a la versió en anglès.

Dedicació: 15h 38m

Classes teòriques: 5h

Aprenentatge autònom: 10h 38m

Proofs of knowledge and other cryptographic protocols

Descripció:

Descrits a la versió en anglès.

Dedicació: 15h 37m

Classes teòriques: 5h

Aprenentatge autònom: 10h 37m

Multiparty computation

Descripció:

Descrits a la versió en anglès.

Dedicació: 15h 38m

Classes teòriques: 5h

Aprenentatge autònom: 10h 38m

SISTEMA DE QUALIFICACIÓ

Descrits a la versió en anglès.

NORMES PER A LA REALITZACIÓ DE LES PROVES.

Descrits a la versió en anglès.

BIBLIOGRAFIA

Bàsica:

- 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.
- Ball, Simeon. A Course in algebraic error-correcting codes [en línia]. Birkhauser, 2020 [Consulta: 07/07/2023]. Disponible a: <https://ebookcentral-proquest-com.recursos.biblioteca.upc.edu/lib/upcatalunya-ebooks/detail.action?pq-origsite=primo&docID=6194949>. ISBN 9783030411534.
- Jones, Gareth A.; Jones, J. Mary. Information and coding theory. Springer, 2000. ISBN 9781447103615.

Complementària:

- Huffman, W. Cary; Pless, Vera. Fundamentals of error-correcting codes. Cambridge: Cambridge University Press, 2003. ISBN 0521782805.
- Justesen, Jorn; Høholdt, Tom. A Course in error-correcting codes. Zürich: European Mathematical Society, 2004. ISBN 3037190019.
- Welsh, Dominic. Codes and cryptography. Oxford: Oxford university Press, 1988. ISBN 0198532881.
- Xambó Descamps, Sebastián. Block error-correcting codes : a computational primer. Berlin: Springer, 2003. ISBN 3540003959.
- 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.