Guia docent
200245 - CRIPTOL - Criptologia

Última modificació: 19/04/2022

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

Titulació: GRAU EN MATEMÀTIQUES (Pla 2009). (Assignatura optativa).

Curs: 2022 **Crèdits ECTS:** 6.0 **Idiomes:** Anglès

PROFESSORAT

Professorat responsable: CARLES PADRO LAIMON

Altres: Primer quadrimestre:
CARLES PADRO LAIMON - M-A
JORGE LUIS VILLAR SANTOS - M-A

COMPETÈNCIES DE LA TITULACIÓ A LES QUALS CONTRIBUEIX L'ASSIGNATURA

Específiques:
GM-CE2. CE-2. Resoldre problemes de Matemàtiques, mitjançant habilitats de càlcul bàsic i d'altres, tot planificant-ne la resolució en funció de les eines de què es disposi i de les restriccions de temps i recursos.
GM-CE4. CE-4. Desenvolupar programes informàtics que resolguin problemes matemàtics, tot fent servir per a cada cas l'entorn computacional escaient.
GM-CE6. Tenir capacitat per a resoldre problemes d'àmbit acadèmic, tècnic, de les finances o social, mitjançant mètodes matemàtics.

Genèriques:
GM-CB5. Haver desenvolupat les habilitats d'aprenentatge que són necessàries per poder emprendre, amb un grau alt d'autonomia, estudis multidisciplinaris en disciplines científiques en què les Matemàtiques tenen un paper significatiu.
GM-CG1. CG-1. Comprendre i emprar el llenguatge matemàtic. Adquirir la capacitat d'enunciar propietats en diversos camps de la Matemàtica, de construir argumentacions, d'elaborar càlculs i de transmetre els coneixements matemàtics adquirits.
GM-CB4. CB-4. Ser capaç de transmetre conclusions, així com els coneixements i fonaments que les sustenten, tant a un públic especialitzat com al que no ho és, de manera clara i sense ambigüitats.
GM-CG2. CG-2. Conèixer demostracions rigoroses d'alguns teoremes clàssics en diferents àrees de la Matemàtica.
GM-CG3. CG-3. Assimilar la definició d'un nou objecte matemàtic en termes d'altres ja coneguts i ser capaç de fer servir aquest objecte en contextos diferents.
GM-CG4. CG-4. Saber abstreure les propietats estructurals (dels objectes matemàtics, de la realitat
observada i d'altres àmbits), distingint-les de les que només són ocasionals. Poder comprovar-les amb demostracions o refutar-les mitjançant contraexemples, així com identificar errors en els raonaments incorrectes.
GM-CG6. CG-6. Detectar deficiències en el propi coneixement i superar-les mitjançant la reflexió
crítica i l'elecció de la millor actuació per a ampliar aquest coneixement.

Transversals:
04 COE. 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.
07 AAT. 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.

METODOLOGIES DOCENTS

OBJECTIUS D'APRENENTATGE DE L'ASSIGNATURA

.

HORES TOTALS DE DEDICACIÓ DE L'ESTUDIANTAT

Tipus	Hores	Percentatge
Hores grup gran	30,0	20.00
Hores grup petit	30,0	20.00
Hores aprenentatge autònom	90,0	60.00

Dedicació total: 150 h

CONTINGUTS

Introducció

Descripció:
Criptologia, criptografia i criptanàlisi. Principis de Kerckhoffs. Teoria de Shannon. Sistemes criptogràfics antics.

Dedicació: 15h
Grup gran/Teoria: 3h
Grup petit/Laboratori: 3h
Aprenentatge autònom: 9h

Criptografia de clau simètrica

Descripció:
Xifrat simètric. Xifrats de bloc. Modes de xifrat encadenats. Propostes pràctiques. Xifrat en flux. Funcions de resum. Codis d'autentificació del missatge

Dedicació: 22h 30m
Grup gran/Teoria: 4h 30m
Grup petit/Laboratori: 4h 30m
Aprenentatge autònom: 13h 30m

Problemes computacionals per a la criptografia

Descripció:
Factorització de nombres enters. Logaritme discret. Corbes el·líptiques. Problema de la motxilla. Reticles

Dedicació: 22h 30m
Grup gran/Teoria: 4h 30m
Grup petit/Laboratori: 4h 30m
Aprenentatge autònom: 13h 30m

Criptografia de clau pública

Descripció:
Intercanvi de claus. Funcions unidireccionals. Xifrat de clau pública. Signatures digitals. Infrastructura de clau pública. Propostes pràctiques.

Dedicació: 22h 30m
Grup gran/Teoria: 4h 30m
Grup petit/Laboratori: 4h 30m
Aprenentatge autònom: 13h 30m

Models de seguretat

Descripció:
Seguretat demostrable. Models de seguretat per a esquemes de xifrat. Formalització de les demostracions de seguretat amb sequències de jocs. Models de seguretat per a signatures digitals

Dedicació: 22h 30m
Grup gran/Teoria: 4h 30m
Grup petit/Laboratori: 4h 30m
Aprenentatge autònom: 13h 30m

Altres primitives criptogràfiques

Descripció:
Esquemes de compromís. Transferència inconscient. Compartició de secrets. Proves de coneixement nul

Dedicació: 22h 30m
Grup gran/Teoria: 4h 30m
Grup petit/Laboratori: 4h 30m
Aprenentatge autònom: 13h 30m

Temes avançats

Descripció:
Computació multipart. Xifrat homomòrfic. Criptografia distribuïda. Criptografia quàntica. Criptografia post-quàntica

Dedicació: 22h 30m
Grup gran/Teoria: 4h 30m
Grup petit/Laboratori: 4h 30m
Aprenentatge autònom: 13h 30m

SISTEMA DE QUALIFICACIÓ

30% examen final, 40% treball final de curs amb presentació oral, 30% exercicis lliurats al llarg del curs

BIBLIOGRAFIA

Bàsica:
- Delfs, Hans; Knebl, Helmut. Introduction to cryptography : principles and applications [en línia]. Berlin: Springer, 2015Disponible a: https://ebookcentral-proquest-com.recursos.biblioteca.upc.edu/lib/upcatalunya-ebooks/detail.action?pq-origsite=primo&docID=6314866. ISBN 9783662479735.
- Hoffstein, Jeffrey; Pipher, Jill; Silverman, Joseph H. An introduction to mathematical cryptography [en línia]. New York: Springer, 2014Disponible a: https://link-springer-com.recursos.biblioteca.upc.edu/book/10.1007/978-0-387-77993-5. ISBN 9781493917105.
- Katz, Jonathan; Lindell, Yehuda. Introduction to modern cryptography [en línia]. Boca Raton: Taylor & Francis Group, 2017Disponible a: https://www-taylorfrancis-com.recursos.biblioteca.upc.edu/books/mono/10.1201/9781351133036/introduction-modern-cryptography-jonathan-katz-yehuda-lindell. ISBN 9781466570269.
- Galbraith, Steven D. Mathematics of public key cryptography [en línia]. Cambridge University Press, 2012 [Consulta: 13/07/2022]. Disponible a: https://www.cambridge.org/core/books/mathematics-of-public-key-cryptography/DDDFA3874A53C4E6846EB3AB06161E43. ISBN 9781107013926.
- Koblitz, Neal. A Course in number theory and cryptography. 2nd ed. New York: Springer-Verlag, cop. 1994. ISBN 0387942939.