Universitat de Lleida

GUIA DOCENT

EINES COMPUTACIONALS PER A LA RESOLUCIÓ DE PROBLEMES

Coordinació: PUJOLAS BOIX, JORDI

Any acadèmic 2021-22

EINES COMPUTACIONALS PER A LA RESOLUCIÓ D... 2021-22

Informació general de l'assignatura

<table>
<tr><td>Denominació</td><td>EINES COMPUTACIONALS PER A LA RESOLUCIÓ DE PROBLEMES</td></tr>
<tr><td>Codi</td><td>102042</td></tr>
<tr><td>Semestre d'impartició</td><td>1R Q(SEMESTRE) AVALUACIÓ CONTINUADA</td></tr>
<tr><td>Caràcter</td><td>
<table>
<tr><th>Grau/Màster</th><th>Curs</th><th>Caràcter</th><th>Modalitat</th></tr>
<tr><td>Grau en Enginyeria Informàtica</td><td>4</td><td>OPTATIVA</td><td>Presencial</td></tr>
<tr><td>Grau en Enginyeria Informàtica</td><td>4</td><td>OBLIGATÒRIA</td><td>Presencial</td></tr>
</table>
</td></tr>
<tr><td>Nombre de crèdits assignatura (ECTS)</td><td>6</td></tr>
<tr><td>Tipus d'activitat, crèdits i grups</td><td>
<table>
<tr><th>Tipus d'activitat</th><th>PRAULA</th><th>TEORIA</th></tr>
<tr><td>Nombre de crèdits</td><td>3</td><td>3</td></tr>
<tr><td>Nombre de grups</td><td>1</td><td>1</td></tr>
</table>
</td></tr>
<tr><td>Coordinació</td><td>PUJOLAS BOIX, JORDI</td></tr>
<tr><td>Departament/s</td><td>MATEMÀTICA</td></tr>
<tr><td>Distribució càrrega docent entre la classe presencial i el treball autònom de l'estudiant</td><td>150 hores de treball
60 hores de classe presencial
90 hores de treball autònom</td></tr>
<tr><td>Informació important sobre tractament de dades</td><td>Consulteu aquest enllaç per a més informació.</td></tr>
<tr><td>Idioma/es d'impartició</td><td>Inglés</td></tr>
</table>

EINES COMPUTACIONALS PER A LA RESOLUCIÓ D... 2021-22

Professor/a (s/es)	Adreça electrònica professor/a (s/es)	Crèdits impartits pel professorat	Horari de tutoria/lloc
MIRET BIOSCA, JOSE MARIA	josepmaria.miret@udl.cat	3	
PUJOLAS BOIX, JORDI	jordi.pujolas@udl.cat	3	

Informació complementària de l'assignatura

Requisits previs: Àlgebra, Estadística i Optimització, Programació 1.

Objectius acadèmics de l'assignatura

Els resultats d'aprenentatge que l'estudiant ha d'assolir en esta assignatura són:

- Solucionar sistemes d'equacions lineals amb diferents mètodes directes: Gauss, LU i QR.
- Determinar els valors i vectors propios d'una matriu quadrada.
- Solucionar sistemes d'equacions lineals amb mètodes iteratius i conèixer les seves condicions de convergència.
- Conèixer i utilitzar les transformacions geomètriques del pla més habituals per a desplaçar objectes.
- Determinar el polinomi interpolador d'un conjunt de punts del pla.
- Distribuir fragments d'una clau mitjançant l'esquema de compartició de secrets de Shamir.
- Conèixer i emprar adequadament algoritmes de factorització i tests de primalitat.
- Xifrar, desxifrar i signar digitalment amb el criptosistema RSA i el criptosistema d'ElGamal.
- Adquirir habilitats per a resoldre problemes computacionals amb el software matemàtic SAGE.

Competències

Competències específiques de la titulació.

- GII-C1. Capacitat per tenir un coneixement profund dels models de la computació i dels seus principis fonamentals, i saber-los aplicar per a interpretar, seleccionar, valorar, modelar, i crear nous conceptes, teories, usos i desenvolupaments tecnològics relacionats amb la informàtica.
- GII-C3. Capacitat per a evaluar la complexitat computacional d'un problema, conèixer estratègies algorítmiques que puguin portar a la seva resolució i recomenar, desenvolupar i implementar aquella que garanteixi el millor rendimient d'acord amb els requisits establerts.

Competències transversals de la titulació.

- EPS6. Capacitat d'anàlisi i síntesi.

Competències estratègiques de la UdL.

- CT2. Adquirir un domini significatiu d'una llengua extrangera, especialment de l' anglès.
- CT3. Adquirir capacitació en l'ús de les noves tecnologies i de las tecnologies de la informació i la comunicació.

Continguts fonamentals de l'assignatura

1. Cossos finits

    1. Aritmètica modular, nombres primers
    2. Construcció de cossos finits, representació dels elements

2. Criptografia

    1. Criptosistemes simètrics
    2. Criptosistemes de clau pública
    3. Problema del logaritme discret
    4. Criptosistema ElGamal
    5. Signatures digitals
    6. Criptografia amb corbes el.líptiques
    7. Criptografia homomòrfica

3. Blockchain

    1. Bitcoin
    2. Arbres de Merkle
    3. Transaccions i mineria

4. Àlgebra matricial

    1. Polinomi característic d'una matriu quadrada
    2. Valors i vectors propis
    3. Diagonalització de matrius quadrades

5. L'algorisme PageRank

    1. Matriu normalitzada d'enllaços
    2. Vector de Perron i mètode de la potència
    3. Aplicació a la cerca de pàgines web

6. Codis detectors i correctors d'errors

    1. Transmissió de la informació
    2. Codificació de la informació
    3. Codis correctors d'errors

Eixos metodològics de l'assignatura

Se combinan clases de teoría, clases de problemas y clases con el software de cálculo simbólico SAGE. Las clases de teoría aportan los conceptos básicos de la asignatura, incorporando ejemplos ilustrativos que facilitan la comprensión. En las clases de problemas se combinan la resolución conjunta en la pizarra con la resolución individual y en grupo de los estudiantes en el aula.

Pla de desenvolupament de l'assignatura

Setmana	Descripció	Activitat presencial	Treball autònom
1	Introducció. Sistemes d'equacions lineals.	Presentació de l'assignatura. 1.1, 1.2: Mètode de Gauss.	Estudiar la bibliografia i el pla de l'assignatura.
2	Sistemes d'equacions lineals.	1.3, 1.4: Descomposicions QR i LU.	Exercicis i resolució de problemes amb SAGE.

3	Sistemes d'equacions lineals.	1.5,1.6, 1.7: Mètodes iteratius.	L'algoritme Page Rank.
4	Transformacions geomètriques en el pla.	2.1: Transformacions bàsiques en el pla.	Exercicis i resolució de problemes amb SAGE.
5	Transformacions geomètriques en el pla.	2.2, 2.3: Formulació matricial i transformacions inverses.	Transformacions al pla en SAGE.
6	Interpolació polinòmica.	3.1, 3.2: Anells de polinomis. L'algoritme d'Euclides en anells de polinomis.	Exercicis i resolució de problemes amb SAGE.
7	Interpolació polinòmica.	3.3, 3.4: Interpolació. Interpolació de Lagrange. L'esquema de Shamir de compartició de secrets	Exercicis i resolució de problemes amb SAGE.
8	Aritmètica modular.	.4.1, 4.2: Anells de clases de residus, Cossos finits.	Exercicis i resolució de problemes amb SAGE.
9		**1er Examen Parcial**	Preparació examen.
10	Aritmètica modular.	4.3, 4.4: Primalitat i factorització.	Exercicis i resolució de problemes amb SAGE.
11	Introducció a la criptografia.	5.1,5.2: Nocions bàsiques de criptografia.	Exercicis i resolució de problemes amb SAGE.
12	Introducció a la criptografia.	5.3, 5.4: Factorització i RSA.	El criptosistema RSA amb SAGE.
13	Introducció a la criptografia.	5.5, 5.6: Logaritmes discrets i xifrat d'El Gamal.	El xifrat d'El Gamal amb SAGE.
14	Introducció a la criptografia.	5.7: Signatura Digital.	Exercicis i resolució de problemes amb SAGE.
15	Introducció a la criptografia.	5.8: Criptografia amb corbes el.líptiques.	Exercicis i resolució de problemes amb SAGE.
16		**2on Examen Parcial**	Preparació examen.
17		**2on Examen Parcial**	Preparació examen.
18		Exposicions orals.	Preparació de presentacions orals.
19		**Recuperació**	Preparació examen.

Sistema d'avaluació

Abr.	Activitat d'avaluació	Ponderació	Nota mínima	En grup	Obligatòria	Recuperable
C1	Pràctica de SAGE	10%	NO	NO	NO	NO
P1	1er Examen Parcial	40%	1.5	NO	SI	SI
C2	Presentació oral	10%	NO	SI (<=2)	NO	NO
P2	2on Examen Parcial	40%	1.5	NO	SI	SI

PCL	Participació a classe	0,5 punts	NO	NO	NO	NO
Els exàmens parcials, la pràctica de SAGE i la presentació oral són obligatoris.						
Nota Final = 0,1*C1 + 0,4*P1 + 0,1*C2 + 0,4*P2 + 0,05*PCL						

L'assignatura se supera si la nota final és igual a 5 o superior. La nota final és la suma ponderada dels exàmens parcials, la pràctica de SAGE, de la presentació oral i addicionalment d'un màxim de 0,5 punts de participació a classe i d'avaluació continuada. Els exàmens parcials són per escrit, tenen un pes del 40% sobre la nota final cadascun d'ells i tenen una nota mínima de 1,5 punts per a ser avaluables. Els exàmens parcials son obligatoris. Es poden obtenir fins a 0,5 punts addicionals per una participació activa a clase i per altres activitats d'avaluació continuada que seran degudament anunciats. L'examen de recuperació consta del 1er o del 2on parcial o de tots dos, a criteri de l'estudiant.

Bibliografia i recursos d'informació

Les matemàtiques de Google: l'algorisme PageRank. Butlletí SCM 26, no. 1, 2011, pp. 29-55.

H. Anton, Elementary Linear Algebra. Ed. John Wiley & Sons, 1994.

L. Childs, A Concrete Introduction to Higher Algebra. Ed. Springer, 1988.

R. Lidl, H. Niederreiter, Finite Fields, Ed. Cambridge University Press, 2003.

W. Stein, Elementary Number Theory: Primes, Congruences and Secrets. Ed. springer, 2009.Bit

Bitcoin: una moneda criptográfica. INTECO CERT. https://www.incibe-cert.es/sites/default/files/contenidos/estudios/doc/int_bitcoin.pdf