GUÍA DOCENTE

HERRAMIIENTAS COMPUTACIONALES PARA LA RESOLUCIÓN DE PROBLEMAS

Coordinación: PUJOLAS BOIX, JORDI

Año académico 2023-24

HERRAMIIENTAS COMPUTACIONALES PARA LA RESO... 2023-24

Información general de la asignatura

<table>
<tr><td>Denominación</td><td>HERRAMIIENTAS COMPUTACIONALES PARA LA RESOLUCIÓN DE PROBLEMAS</td></tr>
<tr><td>Código</td><td>102042</td></tr>
<tr><td>Semestre de impartición</td><td>1R Q(SEMESTRE) EVALUACIÓN CONTINUADA</td></tr>
<tr><td>Carácter</td><td>
<table>
<tr><th>Grado/Máster</th><th>Curso</th><th>Carácter</th><th>Modalidad</th></tr>
<tr><td>Grado en Ingeniería Informática</td><td>4</td><td>OBLIGATORIA</td><td>Presencial</td></tr>
<tr><td>Grado en Ingeniería Informática</td><td>4</td><td>OPTATIVA</td><td>Presencial</td></tr>
</table>
</td></tr>
<tr><td>Número de créditos de la asignatura (ECTS)</td><td>6</td></tr>
<tr><td>Tipo de actividad, créditos y grupos</td><td>
<table>
<tr><th>Tipo de actividad</th><th>PRAULA</th><th>TEORIA</th></tr>
<tr><td>Número de créditos</td><td>3</td><td>3</td></tr>
<tr><td>Número de grupos</td><td>1</td><td>1</td></tr>
</table>
</td></tr>
<tr><td>Coordinación</td><td>PUJOLAS BOIX, JORDI</td></tr>
<tr><td>Departamento/s</td><td>MATEMÁTICA</td></tr>
<tr><td>Distribución carga docente entre la clase presencial y el trabajo autónomo del estudiante</td><td>150 horas de trabajo
60 horas declase presencial
90 horas de trabajo autónomo</td></tr>
<tr><td>Información importante sobre tratamiento de datos</td><td>Consulte este enlace para obtener más información.</td></tr>
<tr><td>Idioma/es de impartición</td><td>Inglés</td></tr>
</table>

HERRAMIIENTAS COMPUTACIONALES PARA LA RESO... 2023-24

Profesor/a (es/as)	Dirección electrónica\nprofesor/a (es/as)	Créditos impartidos por el profesorado	Horario de tutoría/lugar
MIRET BIOSCA, JOSE MARIA	josepmaria.miret@udl.cat	3,6	
PUJOLAS BOIX, JORDI	jordi.pujolas@udl.cat	3,6	

Información complementaria de la asignatura

Requisitos previos: Álgebra, Estadística y Optimización, Programación 1.

Objetivos académicos de la asignatura

Los resultados de aprendizaje que el estudiante debe alcanzar en esta asignatura son:

- Comprender el funcionamiento de los cifrados de clave pública y clave privada.
- Cifrar, descifrar y firmar digitalmente con el criptosistema de ElGamal.
- Conocer los fundamentos de la tecnología Blockchain.
- Determinar los valores y vectores propios de una matriz cuadrada.
- Solucionar sistemas de ecuaciones lineales con métodos iterativos y conocer sus condiciones de convergencia.
- Conocer y utilizar adecuadamente algoritmos de factorización y tests de primalidad.
- Conocer los principios básicos de los códigos correctores de errores.
- Adquirir habilidades para resolver problemas computacionales con el software matemático SAGE.

Competencias

Competencias específicas de la titulación.

- GII-C1. Capacidad para tener un conocimiento profundo de los principios fundamentales y modelos de la computación y saberlos aplicar para interpretar, seleccionar, valorar, modelar, y crear nuevos conceptos, teorías, usos y desarrollos tecnológicos relacionados con la informática.
- GII-C3. Capacidad para evaluar la complejidad computacional de un problema, conocer estrategias algorítmicas que puedan conducir a su resolución y recomendar, desarrollar e implementar aquella que garantice el mejor rendimiento de acuerdo con los requisitos establecidos.

Competencias transversales de la titulación.

- EPS6. Capacidad de análisis y síntesis.

Competencias estratégicas de la UdL.

- CT2. Adquirir un dominio significativo de una lengua extranjera, especialmente del inglés.
- CT3. Adquirir capacitación en el uso de las nuevas tecnologías y de las tecnologías de la información y la comunicación.

Contenidos fundamentales de la asignatura

1. Cuerpos finitos
    1. Aritmética modular, números primos
    2. Construcción de cuerpos finitos, representación de los elementos
2. Criptografía
    1. Criptosistemas simétricos
    2. Criptosistemas de clave pública
    3. Problema del logaritmo discreto
    4. Criptosistema ElGamal
    5. Firmas digitales
    6. Criptografía con curvas elípticas
    7. Criptografía postcuántica
3. Blockchain
    1. Bitcoin
    2. Árboles de Merkle
    3. Transacciones y minería
4. Álgebra matricial
    1. Polinomio característico de una matriz cuadrada
    2. Valores y vectores propios
    3. Diagonalización de matrices cuadradas
5. El algoritmo PageRank
    1. Matriz normalizada de enlaces
    2. Vector de Perron y método de la potencia
    3. Aplicación a la búsqueda de sitios web
6. Códigos detectores y correctores de errores
    1. Transmisión de la información
    2. Codificación de la información
    3. Códigos correctores de errores

Ejes metodológicos de la asignatura

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.

Plan de desarrollo de la asignatura

Semana	Descripción	Actividad presencial	Trabajo autónomo
1	Introducción. Fundamentos matemáticos.	Presentación de la asignatura. 1.1: Aritmética modular y números primos.	Estudiar la bibliografía y el plan de la assignatura.
2	Fundamentos matemáticos.	1.2: Construcción de cuerpos finitos, representación de elementos.	Ejercicios y resolución de problemes con SAGE.
3	Criptografía.	2.1,2.2: Criptosistemas de clave pública y de clave compartida.	Ejercicios y resolución de problemes con SAGE.
4	Criptografía.	2.3,2.4: El problema del logaritmo discreto, el cifrado de ElGamal	Ejercicios y resolución de problemes con SAGE.

5	Criptografía.	2.5: Firma digital.	Ejercicios y resolución de problemes con SAGE.
6	Criptografía.	2.6: Curvas elípticas.	Ejercicios y resolución de problemes con SAGE.
7	Criptografía.	2.7: Criptografía pos-cuántica.	Ejercicios y resolución de problemes con SAGE.
8	Blockchain.	3.1,3.2,3.3: Bitcoin, árbol de Merkle, transacciones y minería.	Ejercicios y resolución de problemes con SAGE.
9		**1er Examen Parcial**	Preparación examen.
10	Álgebra matricial.	4.1, 4.2, 4.3: Polinomio característico, vectores y valores propios, diagonalització.	Ejercicios y resolución de problemes con SAGE.
11	Algorismo Page Rank	5.1,5.2, 5.3: Matriz normalitzada de enlaces, Vector de Perron y método de la potencia. Aplicación a la indexación de páginas web.	Ejercicios y resolución de problemes con SAGE.
12	Códigos detectores y correctores de errores	6.1,6.2: Transmisión y codificación de la información.	Ejercicios y resolución de problemes con SAGE.
13			
14	Códigos detectores y correctores de errores	6.3: Cóodigos lineales, síndrome.	Ejercicios y resolución de problemes con SAGE.
15		**Presentaciones Orales**	Preparación de la presentación.
16		**2on Examen Parcial**	Preparación examen.
17			
19		**Recuperación**	Preparación examen.

Sistema de evaluación

Abr.	Actividad de evaluación	Ponderación	Nota mínima	En grupo	Obligatoria	Recuperable
C1	Práctica de SAGE	10%	NO	NO	SI	NO
P1	1r Examen Parcial	40%	1.5	NO	SI	SI
C2	Presentación oral	10%	NO	SI (<=2)	SI	NO
P2	2o Examen Parcial	40%	1.5	NO	SI	SI
PCL	Participación en classe	0,5 puntos	NO	NO	NO	NO
Los exámenes parciales, la práctica de SAGE y la presentación oral son obligatorios.						

Nota Final = 0,1*C1 + 0,4*P1 + 0,1*C2 + 0,4*P2 + 0,05*PCL

La asignatura se supera si la nota final es igual a 5 o superior. La nota final es la suma ponderada de los exámenes parciales, la práctica de SAGE, de la presentación oral y adicionalmente de un máximo de 0,5 puntos de participación en classe y avaluación contínua. Los exámenes parciales son por escrito, tienen un peso del 40% sobre la nota final cada uno de ellos y tienen una nota mínima de 1,5 puntos para a ser evaluables. Los exámenes parciales, la práctica de SAGE y la presentación oral son obligatorios. Se pueden obtener hasta 0,5 puntos extras por una participación activa en clase y por otras actividades de evaluación contínua que serán debidamente anunciadas. El examen de recuperación consta del 1er o del 2o parcial o de ambos, a criterio del estudiante.

El estudiantado que cuente con el visto bueno para ser evaluado mediante evaluación alternativa (ver requisitos y procedimiento en la normativa de evaluación), seguirá el siguiente procedimiento de evaluación:

* Se evaluará el 100% de la nota en un examen único en la fecha que se fije para los exámenes de recuperación. Este examen constará de dos partes P1 y P2 (con una valoración de 5 puntos cada una). Para aprobar deberá sacar una nota global superior a 5 y una nota mínima por cada una de las partes de 2.5 puntos.
* Si el estudiante no supera esta evaluación única o no llega a la nota mínima en una de las partes, tendrá derecho a una recuperación del 100% de la nota en los mismos términos, en una fecha a acordar con el profesorado, y dentro del período anterior al cierre de actas de la asignatura.

Bibliografía y recursos de información

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.

M. Bellare, P. Rogaway, Introduction to Modern Cryptography, class notes, 2005.

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

A. Menezes, P. van Oorschot, S. Vanstone. Handbook of Applied Cryptography. CRC, Press, 1997.

C. Munuera, J. Tena. Codificación de la Información. Univ. Valladolid, 1997.