DEGREE CURRICULUM

COMPUTATIONAL TOOLS FOR PROBLEM SOLVING

Coordination: PUJOLAS BOIX, JORDI

Academic year 2023-24

COMPUTATIONAL TOOLS FOR PROBLEM SOLVING 2023-24

Subject's general information

<table>
<tr><td>Subject name</td><td>COMPUTATIONAL TOOLS FOR PROBLEM SOLVING</td></tr>
<tr><td>Code</td><td>102042</td></tr>
<tr><td>Semester</td><td>1st Q(SEMESTER) CONTINUED EVALUATION</td></tr>
<tr><td>Typology</td><td>
<table>
<tr><th>Degree</th><th>Course</th><th>Character</th><th>Modality</th></tr>
<tr><td>Bachelor's Degree in Computer Engineering</td><td>4</td><td>COMPULSORY</td><td>Attendance-based</td></tr>
<tr><td>Bachelor's Degree in Computer Engineering</td><td>4</td><td>OPTIONAL</td><td>Attendance-based</td></tr>
</table>
</td></tr>
<tr><td>Course number of credits (ECTS)</td><td>6</td></tr>
<tr><td>Type of activity, credits, and groups</td><td>
<table>
<tr><th>Activity type</th><th>PRAULA</th><th>TEORIA</th></tr>
<tr><td>Number of credits</td><td>3</td><td>3</td></tr>
<tr><td>Number of groups</td><td>1</td><td>1</td></tr>
</table>
</td></tr>
<tr><td>Coordination</td><td>PUJOLAS BOIX, JORDI</td></tr>
<tr><td>Department</td><td>MATHEMATICS</td></tr>
<tr><td>Teaching load distribution between lectures and independent student work</td><td>150 total hours of work
60 hours lecture attendance
90 hours student work</td></tr>
<tr><td>Important information on data processing</td><td>Consult this link for more information.</td></tr>
<tr><td>Language</td><td>English</td></tr>
<tr><td>Distribution of credits</td><td>Josep M. Miret Biosca 3
Jordi Pujolàs Boix 3</td></tr>
</table>

COMPUTATIONAL TOOLS FOR PROBLEM SOLVING 2023-24

Teaching staff	E-mail addresses	Credits taught by teacher	Office and hour of attention
MIRET BIOSCA, JOSE MARIA	josepmaria.miret@udl.cat	3,6	
PUJOLAS BOIX, JORDI	jordi.pujolas@udl.cat	3,6	

Subject's extra information

Requirements: Algebra, Statistics and Optimization, Introduction to Programming 1.

Learning objectives

The learning outcomes that the student must achieve in this subject are:

- To understand how public key and private key ciphers work.
- To encrypt, decrypt and digitally sign with ElGamal cryptosystem.
- To know the fundamentals of Blockchain technology.
- To determine the eigenvalues and vectors of a square matrix.
- To solve systems of linear equations with iterative methods and to know their convergence conditions.
- To know and properly use factorization algorithms and primality tests.
- To know the basic principles of error correcting codes.
- To acquire skills to solve computational problems with SAGE mathematical software.

Competences

Specific competences of the degree.

- GII-C1. Capacity to have a deep knowledge of the basic principles and models for computation and to know how to apply them in order to interpret, select, value, model, and create new concepts, theories, uses and technological developments related with the informatics.
- GII-C3. Capacity to evaluate the computational complexity of a problem, to know the algorithmic strategies that can drive to its solving and recommend, develop and implement the one which guarantee the best performance in accordance with the requirements.

Cross-disciplinary competences of the degree.

- EPS6. Capacity to work in situations with a lack of information and/or under pressure.

Strategic competences of the UdL.

- CT2. Mastering a foreign language, especially English.
- CT3. Training Experience in the use of the new technologies and the information and communication technologies.

COMPUTATIONAL TOOLS FOR PROBLEM SOLVING 2023-24

Subject contents

1. Finite Fields

1. Modular Arithmetic, Prime Numbers
2. Construction of Finite Fields, representation of elements

2. Criptography

1. Symmetric Cryptosystems
2. Public Key Cryptosystems
3. Discrete Logarithm Problem
4. ElGamal Cryptosystem
5. Digital Signatures
6. Elliptic Curve Cryptography
7. Postquantum Cryptography

3. Blockchain

1. Bitcoin
2. Merkle Trees
3. Transactions and mining

4. Matrix Àlgebra

1. Characteristic Polynomial of a square matrix
2. Eigenvalues and eigenvectors
3. Diagonalization of square matrices

5. PageRank Algorithm

1. Normalized link matrix
2. Perron Vector and the Power method
3. Web page search

6. Error detection and error correction codes

1. Information Transmission
2. Information Codification
3. Error correcting codes

Methodology

Theoretical and practical contents are mixed to combine basic aspects with illustrative examples and problem solving. Practical lectures include sessions with the open symbolic package SAGE.

Development plan

Week	Description	Activitat presencial	Autonomous work
1	Introduction. Math foundations.	Course introduction. 1.1: Modular arithmetic and prime numbers.	Study bibliography and course plan.
2	Math foundations.	1.2: Finite field construction and element representation.	Exercises and problem solving with SAGE.
3	Cryptography.	2.1,2.2: Public key and symmetric key cryptosystems.	Exercises and problem solving with SAGE.

4	Cryptography.	2.3,2.4: Discrete logarithm problem, El Gamal encryption.	Exercises and problem solving with SAGE.
5	Cryptography.	2.5: Digital signature.	Exercises and problem solving with SAGE.
6	Cryptography.	2.6: Elliptic curves.	Exercises and problem solving with SAGE.
7	Cryptography	2.7: Post quantum crypto.	Exercises and problem solving with SAGE.
8	Blockchain.	3.1,3.2,3.3: Bitcoin, Merkle trees, transactions and mining.	Exercises and problem solving with SAGE.
9		**1st Partial Exam**	Preparation for exam.
10	Matrix algebra.	4.1, 4.2, 4.3: Característic polynomial, eigenvalues, eigenvectors, diagonalitzation.	Exercises and problem solving with SAGE.
11	Page Rank Algorithm	5.1,5.2, 5.3: Normalitzed link matrix, Perron vector, power method, web page indexation.	Exercises and problem solving with SAGE.
12	Error correcting codes	6.1,6.2: Information codification and transmission.	Exercises and problem solving with SAGE.
13			
14	Error correcting codes	6.3: Linear codes, syndrome.	Exercises and problem solving with SAGE.
15		**Oral Presentations**	Preparació de la presentació.
16		**2nd Partial Exam**	Preparació examen.
17			
19		**2nd chance exam**	Preparació examen.

Evaluation

Abbr.	Marking Activity	Ponderation	Minimum Mark	Group	Compulsory	Mendable
C1	SAGE Test	10%	NO	NO	YES	NO
P1	1st Partial Exam	40%	1.5	NO	YES	YES
C2	Oral presentation	10%	NO	YES (<=2)	YES	NO
P2	2nd Partial Exam	40%	1.5	NO	YES	YES
PCL	Classroom participation	0.5 points	NO	NO	NO	NO
Both partial exams, the SAGE activity and the oral presentation are compulsory.						

Final Mark = 0.1*C1 + 0.4*P1 + 0.1*C2 + 0.4*P2 + 0.05*PCL

The course is passed if the final mark is 5 or higher. The final mark is a weighted sum of both partial exams, the SAGE coding exercise and the short oral presentation plus a maximum 0.5 points due to classroom participation. Each partial exam is a written exam and has a weight of 40% in the final mark, with a minimum mark of 1.5 required. Both partial exams, the SAGE test and the short oral presentation are compulsory. One or both written partial exams are eligible for second chance examination. An extra 0.5 points is obtainable for class participation.

Students who have been authorized to follow the alternative assessment (see requirements and procedure in the assessment regulations), will follow the following assessment procedure:

* Student will be assessed for 100% of the grade in a single exam on the date set for the additional exams.
* This exam will consist of two parts P1 and P2 (with an assessment of 5 points each). In order to pass, you will have to obtain an overall mark of more than 5 and a minimum mark for each of the parts of 2.5 points.
* If the student does not pass this unique assessment or does not reach the minimum mark in one of the parts, he will have the right to recover 100% of the mark under the same terms, on a date to be agreed with the teaching staff.

Bibliography

Les matemàtiques de Google: l'algorisme PageRank. Butllet\'{\i} 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.