ANX-PR/CL/001-01

LEARNING GUIDE

SUBJECT

615000520 - Information Coding

DEGREE PROGRAMME

61IW - Degree in Software Engineering

ACADEMIC YEAR & SEMESTER

2022/23 - Semester 1

Index

Learning guide

1. Description....1
2. Faculty....1
3. Prior knowledge recommended to take the subject....2
4. Skills and learning outcomes 2
5. Brief description of the subject and syllabus....4
6. Schedule....6
7. Activities and assessment criteria....9
8. Teaching resources....13

1. Description

1.1. Subject details

Name of the subject	615000520 - Information Coding
No of credits	6 ECTS
Type	Optional
Academic year ot the programme	Third year
Semester of tuition	Semester 5
Tuition period	September-January
Tuition languages	English
Degree programme	61IW - Degree in Software Engineering
Centre	61 - Escuela Tecnica Superior De Ingenieria De Sistemas Informaticos
Academic year	2022-23

2. Faculty

2.1. Faculty members with subject teaching role

Name and surname	Office/Room	Email	Tutoring hours *
Luis Miguel Pozo Coronado	2003	lm.pozo@upm.es	Not scheduled. Office hours will be published before the beginning of the term, both in moodle and on the bulletin boards

Ana Isabel Lias Quintero (Subject coordinator)		anaisabel.lias@upm.es	- -

* The tutoring schedule is indicative and subject to possible changes. Please check tutoring times with the faculty member in charge.

3. Prior knowledge recommended to take the subject

3.1. Recommended (passed) subjects

The subject - recommended (passed), are not defined.

3.2. Other recommended learning outcomes

- Understanding and writing simple mathematical proofs.

- Handling modular arithmetics and matrix calculus with ease.

4. Skills and learning outcomes *

4.1. Skills to be learned

CB1 - Ability to solve mathematical problems that may arise in engineering. Skill to apply knowledge about: algebra, differential and integral calculus and numerical methods; statistics and optimization

CB3 - Ability to understand and master the basic concepts of discrete, logical, algorithmic and computational complexity, and its application for the automatic processing of information through computer systems and their application to solve engineering problems.

CC1 - Ability to design, develop, select and evaluate computer applications and systems, ensuring its reliability, safety and quality, in accordance with ethical principles and current legislation and regulations.

CC6 - Knowledge and application of basic algorithmic procedures of computer technologies for designing solutions to problems, analyzing the suitability and complexity of the proposed algorithms

CC7 - Knowledge, design and efficient use of the types and structures of data most appropriate for solving a problem

CT1 - Analysis and synthesis: Breaking down information into smaller units, separating the essential components from the irrelevant ones and identifying the relationships between them. Synthesis: Combining information to build a whole from the previously analyzed entities.

CT12 - Use of information and communication technologies: Using information and communication technologies in the engineering communications' field.

CT2 - Problem solving: Identifying, analyzing and defining the significant elements that constitute a problem in order to effectively and judiciously solve it.

CT4 - Written communication: Relating effectively with other people through the clear expression of what one thinks, through writing and graphic supports.

4.2. Learning outcomes

RA296 - Applyig the main results of number theory to Cryptology, encrypting and decrypting with the RSA and ElGamal cryptosystems

RA297 - Adequately uses software to solve information coding problems, accurately describing the protocols used

RA291 - Uses the different types of information coding according to the objective pursued (correcting errors, encrypting information or compressing it)

RA295 - Determining the computational complexity of simple algorithms that involve elemental arithmetic operations

RA299 - Compresses files, using appropriate compression codes

RA290 - Knows and applies authentication protocols (digital signature) and key exchange based on public key cryptosystems

RA292 - Knows and applies deterministic and probabilistic primality tests

RA294 - Distinguish public key and private key cryptosystems. Encrypts and decrypts using translation cryptosystems, affine and matrix affine

RA298 - Encodes, detects and corrects errors using linear codes

RA293 - Solves open problems, considering several possible alternatives, evaluating them in a reasoned way and arguing their choice according to the criteria specified for their resolution. For the chosen alternative, identifies the information necessary for its solution, elaborates and develops an effective strategy to find it, and clearly presents the result and relevant conclusions

RA335 - Analyzes and applies the ElGamal algorithm for data encryption and decryption

RA334 - Analyzes and applies the RSA algorithm for data encryption and decryption.

5. Brief description of the subject and syllabus

5.1. Brief description of the subject

The subject of this course is the study of the different possibilities to encode the information numerically, depending on the intended goal: conciseness (data compression), integrity (error detection codes) or security (cryptography).

The general objectives are:

a) Understanding the different mathematical concepts and tools underlying the models under consideration; and

b) Implementing these models, with special attention to efficiency and security issues.

5.2. Syllabus

1. Introduction to Information Coding. Cryptology
    1.1. Trasmissión of Information
    1.2. Types of codes
    1.3. Cryptography and cryptosystems
    1.4. Private key cryptosystems
    1.5. Cryptanalysis
2. Computational complexity
    2.1. Problems and algorithms
    2.2. Complexity of elemental arithmetic operations

2.3. Classification of problems regarding its complexity

3. Number theory

3.1. The multiplicative group of integers mod n

3.2. Euler's totient function

3.3. Euler and Fermat Theorems

3.4. Order of an element. Primitive root

3.5. Discrete logarithm

4. Public key cryptosystems

4.1. Diffie- Hellman key exchange protocol

4.2. RSA cryptosystem

4.3. ElGamal cryptosystem

4.4. Digital signature

4.5. Other applications

5. Primality tests

5.1. Deterministic tests: Erathostenes' sieve and trial division

5.2. Probabilistic tests: Fermat, Miller and Miller-Rabin

6. Compression codes. Error-detection codes

6.1. Compression with variable-length codes: Huffman codification

6.1.1. Introduction to information theory

6.1.2. Huffman codification

6.1.3. Minimal variance Huffman codification

6.2. Error-detection with Cyclic redundancy codes

6.2.1. Linear codes

6.2.2. Polynomials. CRC

6. Schedule

6.1. Subject schedule*

Week	Classroom activities	Laboratory activities	Distant / On-line	Assessment activities
1	**Theory and/or exercises class. Introduction to the subject. Chapter 1** Duration: 02:00 Lecture	**Lab session: Introduction to maxima** Duration: 02:00 Laboratory assignments		
2	**Theory and/or exercises class. Chapter 1** Duration: 04:00 Lecture			
3	**Theory and/or exercises class. Chapter 1** Duration: 02:00 Lecture	**Lab session: Lab project 1** Duration: 02:00 Laboratory assignments		**Lab project 1 (RA297, RA295)** Group work Continuous assessment Not Presential Duration: 00:00 **Moodle test. (Non-recoverable test) Chapter 1 (RA291, RA294).** Online test Continuous assessment Not Presential Duration: 00:20
4	**Theory and/or exercises class. Chapter 2** Duration: 04:00 Lecture			
5	**Theory and/or exercises class. Chapter 2** Duration: 04:00 Lecture			**Moodle test. Chapter 2 Non-recoverable test (RA295)** Online test Continuous assessment Not Presential Duration: 00:20
6	**Theory and/or exercises class. Chapter 3** Duration: 04:00 Lecture			
7	**Theory and/or exercises class. Chapter 3** Duration: 04:00 Lecture			**Written test, chapters 1 and 2 (RA291, RA294, RA295 and RA293)** Written test Continuous assessment Presential Duration: 01:30
8		**Lab session: Lab project 2** Duration: 02:00 Laboratory assignments		**Moodle test. Chapter 3 Non-recoverable test (RA296).** Online test Continuous assessment Not Presential Duration: 00:20 **Lab project 2 (RA297, RA 296 and RA295)** Group work Continuous assessment Not Presential Duration: 00:00

9	**Theory and/or exercises class. Chapter 4** Duration: 04:00 Lecture			
10	**Theory and/or exercises class. Chapter 4** Duration: 02:00 Lecture	**Lab session: Lab project 3** Duration: 02:00 Laboratory assignments		**Moodle test. Chapter 4 Non-recoverable test (RA296 , RA290)** Online test Continuous assessment Not Presential Duration: 00:20 **Lab project 3 (RA297, RA296 and RA290)** Group work Continuous assessment Not Presential Duration: 00:00
11	**Theory and/or exercises class. Chapter 5** Duration: 04:00 Lecture		**Exercises Chapters 4 and 5.** Duration: 02:00 Problem-solving class	**Moodle test. Non-recoverable test Chapter 5 (RA292)** Online test Continuous assessment Not Presential Duration: 00:20
12	**Theory and/or exercises class. Chapter 6** Duration: 02:00 Lecture	**Lab session: Lab project 4** Duration: 02:00 Laboratory assignments		**Lab project 4 (RA297, RA292)** Group work Continuous assessment Not Presential Duration: 00:00
13				**Written test, chapters 3,4, and 5 (RA296, RA290, RA292 and RA293).** Written test Continuous assessment Presential Duration: 02:00
14	**Theory and/or exercises class. Chapter 6** Duration: 04:00 Lecture			
15	**Theory and/or exercises class. Chapter 6** Duration: 02:00 Lecture	**Lab session: Lab project 5** Duration: 02:00 Laboratory assignments		**Lab project 5 (RA297, RA299)** Group work Continuous assessment Not Presential Duration: 00:00 **Moodle test. Non-recoverable test Chapter 6 (RA291, RA298, RA299)** Online test Continuous assessment Not Presential Duration: 00:20
16				
				Lab test (RA296, RA290, RA292, RA297) Problem-solving test Continuous assessment Presential Duration: 01:00 **Written test, chapter 6 (RA291, RA298, RA299 and RA293)** Written test Continuous assessment Presential Duration: 01:00

17				**Final exam (RA290, RA291, RA292, RA293, RA294 RA295, RA296, RA297, RA298, RA299)** Written test Final examination Presential Duration: 03:00 **Autonomous study throughout the course (4 hours per week, average)** Other assessment Continuous assessment Not Presential Duration: 60:00 **Final lab project (Toolbox) (RA297)** Individual work Final examination Presential Duration: 01:00

Depending on the programme study plan, total values will be calculated according to the ECTS credit unit as 26/27 hours of student face-to-face contact and independent study time.

* The schedule is based on an a priori planning of the subject; it might be modified during the academic year, especially considering the COVID19 evolution.

7. Activities and assessment criteria

7.1. Assessment activities

7.1.1. Assessment

Week	Description	Modality	Type	Duration	Weight	Minimum grade	Evaluated skills
3	Lab project 1 (RA297, RA295)	Group work	No Presential	00:00	6%	/ 10	CC6 CT12 CB3 CC1 CC7 CB1
3	Moodle test. (Non-recoverable test) Chapter 1 (RA291, RA294).	Online test	No Presential	00:20	2%	7 / 10	CC6 CT1 CB3 CC1 CB1
5	Moodle test. Chapter 2 Non-recoverable test (RA295)	Online test	No Presential	00:20	2%	7 / 10	CC6 CT1 CB3 CC1 CC7 CB1
7	Written test, chapters 1 and 2 (RA291, RA294, RA295 and RA293)	Written test	Face-to-face	01:30	12%	/ 10	CC6 CT1 CT2 CB3 CC1 CC7 CT4 CB1
8	Moodle test. Chapter 3 Non-recoverable test (RA296).	Online test	No Presential	00:20	2%	7 / 10	CC6 CT1 CB3 CC1 CC7 CB1
8	Lab project 2 (RA297, RA 296 and RA295)	Group work	No Presential	00:00	6%	/ 10	CB3 CC1 CC7 CC6 CT2 CB1

10	Moodle test. Chapter 4 Non-recoverable test (RA296 , RA290)	Online test	No Presential	00:20	2%	7 / 10	CC6 CT1 CB3 CC1 CC7 CB1
10	Lab project 3 (RA297, RA296 and RA290)	Group work	No Presential	00:00	6%	/ 10	CT12 CB3 CC1 CC7 CC6 CB1
11	Moodle test. Non-recoverable test Chapter 5 (RA292)	Online test	No Presential	00:20	2%	7 / 10	CC6 CT1 CB3 CC1 CC7 CB1
12	Lab project 4 (RA297, RA292)	Group work	No Presential	00:00	6%	/ 10	CC6 CT12 CB3 CC1 CC7 CB1
13	Written test, chapters 3,4, and 5 (RA296, RA290, RA292 and RA293).	Written test	Face-to-face	02:00	20%	/ 10	CC6 CT1 CT2 CB3 CC1 CC7 CT4 CB1
15	Lab project 5 (RA297, RA299)	Group work	No Presential	00:00	6%	/ 10	CC6 CT12 CB3 CC1 CC7 CB1
15	Moodle test. Non-recoverable test Chapter 6 (RA291, RA298, RA299)	Online test	No Presential	00:20	%	7 / 10	CC6 CT1 CB3 CC1 CC7 CB1
17	Lab test (RA296, RA290, RA292, RA297)	Problem-solving test	Face-to-face	01:00	20%	/ 10	CC6 CT2 CT12 CB3 CC1 CC7 CB1

17	Written test, chapter 6 (RA291, RA298, RA299 and RA293)	Written test	Face-to-face	01:00	8%	/ 10	CC6 CT1 CT2 CB3 CC1 CC7 CT4 CB1
17	Autonomous study throughout the course (4 hours per week, average)	Other assessment	No Presential	60:00	%	/ 10	

7.1.2. Global examination

Week	Description	Modality	Type	Duration	Weight	Minimum grade	Evaluated skills
17	Final exam (RA290, RA291, RA292, RA293, RA294 RA295, RA296, RA297, RA298, RA299)	Written test	Face-to-face	03:00	70%	5 / 10	CC6 CT1 CT2 CB3 CC1 CC7 CT4 CB1
17	Final lab project (Toolbox) (RA297)	Individual work	Face-to-face	01:00	30%	/ 10	CC6 CT12 CB3 CC1 CC7 CB1

7.1.3. Referred (re-sit) examination

Description	Modality	Type	Duration	Weight	Minimum grade	Evaluated skills
Final exam (RA290, RA291, RA292, RA293, RA294 RA295, RA296, RA297, RA298, RA299)	Written test	Face-to-face	02:00	100%	5 / 10	CT1 CT2 CB3 CC1 CC7 CT4 CB1 CC6

Final lab project (Toolbox) (RA297)	Individual work	No Presential	00:00	%	/ 10	CT12 CB3 CC1 CC7 CB1 CC6

7.2. Assessment criteria

Continuous evaluation:

Online tests: One for each chapter; 10 multiple choice questions. If the result is at least 7/10, the test will add 2% to the final grade, **up to 10%** altogether.

Written tests: They take place out of lecture hours. The students must answer to questions regarding subject contents (including definitions, statements of theorems, exercises and problems). At least 70% of assessment will correspond to basic contents. Language precision and rigour in the results will be demanded.

Lab projects: 5 lab projects must be done along the term. Work will be done in pairs. The contribution of each project to the final grade will be 6%. Project assessment: Procedures, 50% (efficiency, clarity, documentation); solved problems, 40%; mathematical rigour, elegance, language precision, 10%.

Lab test: A validation test will take place in the lab, where some problems must be solved by using the functions programmed in the lab projects. This test will weigh a 20% of the total grade.

Final exam only, and july examination session

Students choosing the final exam option must apply for it before December 1st, using the tool in Moodle. Final exam will take place as scheduled by the school administration. The exam will have two parts: a written test regarding subject contents (including definitions, statements of theorems, exercises and problems), and a lab test where some problems must be solved by means of the functions listed in the lab projects (which each student must do in advence and bring to the exam). Each part will weigh 70% and 30% of the final grade, respectively. The function list and specifications will be published in Moodle. In addition, this exam can be used for updating the grade of any of the previous partials, using the proper weighting.

Addendum

Developing the UPM Evaluation Policy, subject teachers state that:

1. For a student to be examined on a date other than the scheduled exam, it must necessarily be verified the following circumstances:

(a) The reason the student is unable to attend the exam must be overselling and force majeure, legally established or sufficiently estimated by the Head of Studies. The concept of force majeure must be understood as the existence of an unpredictable external cause affecting the sufferer by preventing the fulfilment of an obligation.

(b) In these cases, in order for the test to take effect on a different date and time than the scheduled one, affected students must notify the coordinator, via email or telephone, no later than 48 hours and send the documents that prove the reason he/she were unable to attend. Otherwise, the test will not be re-tested.

2. If a copy is detected on any ongoing evaluation test, the students involved will have zero rating in the ordinary call. In addition, they will need to conduct a review defense in a oral procedure in the extraordinary call. In the event of a copy in the extraordinary examination, the facts will be reported to the Rector for the opening of a disciplinary file.

8. Teaching resources

8.1. Teaching resources for the subject

Name	Type	Notes
Buchmann, Johannes A: "Introduction to Cryptography". Second Edition. Springer-Verlag. 2004.	Bibliography	

Koblitz, Neal: "A Course in Number Theory and Cryptography". Second Edition. Springer-Verlag. 1994	Bibliography	
Lucena, Manuel José: "Criptografía y Seguridad en Computadores". 1999. wwwdi.ujaen.es/~mlucena	Web resource	
Munuera, Carlos; Tena, Juan: "Codificación de la Información". Universidad de Valladolid. 1997	Bibliography	
Ramió, Jorge: "Aplicaciones Criptográficas". Escuela Universitaria de Informática. U. Politécnica de Madrid. 1998	Bibliography	
Trappe, Wade; Washington, Lawrence C.: "Introduction to Crytography with Coding Theory". Prentice-Hall. 2002	Bibliography	
Rincón, Félix; García, Alfonsa; Martínez, Ángeles: "Cálculo científico con Maple". RA-MA. 1995	Bibliography	
Maxima handbook: http://maxima.sourceforge.net/docs/manual/es/maxima.html	Web resource	
UPM Moodle environment: http://moodle.upm.es/titulaciones/oficiales/	Web resource	Containing course info and additional resources
Lab resources: PCs	Equipment	
Software: Maxima, Maple	Equipment	