ANX-PR/CL/001-01

LEARNING GUIDE

SUBJECT

615000520 - Information Coding

DEGREE PROGRAMME

61IW - Grado En Ingenieria Del Software

ACADEMIC YEAR & SEMESTER

2020/21 - Semester 1

Index

Learning guide

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 - Grado en Ingenieria del Software
Centre	61 - Escuela Tecnica Superior De Ingenieria De Sistemas Informaticos
Academic year	2020-21

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	Sin horario. 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)	2005 / 6005	anaisabel.lias@upm.es	Sin horario. Office hours will be published before the beginning of the term, both in moodle and on the bulletin boards

* 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

- Logica Y Matematica Discreta

- Algebra

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 - Capacidad para la resolución de los problemas matemáticos que puedan plantarse en la ingeniería. Aptitud para aplicar los conocimientos sobre: algebra, cálculo diferencial e integral y métodos numéricos; estadística y optimización

CB3 - Capacidad para comprender y dominar los conceptos básicos de matemática discreta, lógica, algorítmica y complejidad computacional, y su aplicación para el tratamiento automático de la información por medio de sistemas computacionales y su aplicación para la resolución de problemas propios de la ingeniería.

CC1 - Capacidad para diseñar, desarrollar, seleccionar y evaluar aplicaciones y sistemas informáticos, asegurando

su fiabilidad, seguridad y calidad, conforme a principios éticos y a la legislación y normativa vigente.

CC6 - Conocimiento y aplicación de los procedimientos algorítmicos básicos de las tecnologías informáticas para diseñar soluciones a problemas, analizando la idoneidad y complejidad de los algoritmos propuestos

CC7 - Conocimiento, diseño y utilización de forma eficiente los tipos y estructuras de datos más adecuados a la resolución de un problema

CT1 - Análisis y síntesis: Descomponer la información en unidades más pequeñas separando los componentes fundamentales de los no relevantes e identificando las relaciones existentes entre ellos. Síntesis: Combinar información para construir un todo a partir de las entidades previamente analizadas.

CT12 - Uso de tecnologías de la información y las comunicaciones : Usar las tecnologías de la información y las comunicaciones en el ámbito de la ingeniería.

CT2 - Resolución de problemas: Identificar, analizar y definir los elementos significativos que constituyen un problema para resolverlo con criterio y de forma efectiva

CT4 - Comunicación escrita: Relacionarse eficazmente con otras personas a través de la expresión clara de lo que se piensa, mediante la escritura y los apoyos gráficos.

4.2. Learning outcomes

RA295 - Determina la complejidad computacional de algoritmos sencillos que involucren operaciones aritméticas elementales

RA297 - Utiliza adecuadamente software para la resolución de problemas de codificación de la información, describiendo con precisión los protocolos utilizados

RA291 - Utiliza los distintos tipos de codificación de la información según el objetivo perseguido (corregir errores, encriptar información o comprimirla)

RA299 - Comprime ficheros, usando códigos compresores adecuados

RA290 - Conoce y aplica protocolos de autenticación (firma digital) e intercambio de claves basados en criptosistemas de clave pública

RA292 - Conoce y aplica test de primalidad deterministas y probabilísticos

RA294 - Distingue criptosistemas de clave pública y clave privada. Cifra y descifra utilizando los criptosistemas de traslación, afín y matricial afín

RA298 - Codifica, detecta y corrige errores utilizando los códigos lineales

RA293 - Resuelve problemas abiertos, considerando varias alternativas posibles, valorándolas de forma razonada y argumentando su elección según los criterios especificados para su resolución. Para la alternativa elegida, identifica la información necesaria para su solución, elabora y desarrolla una estrategia eficaz para encontrarla, y presenta de forma clara el resultado y las conclusiones pertinentes

RA296 - Aplica los principales resultados de la teoría de números a la Criptología, cifrando y descifrando con los criptosistemas RSA y ElGamal

* The Learning Guides should reflect the Skills and Learning Outcomes in the same way as indicated in the Degree Verification Memory. For this reason, they have not been translated into English and appear in Spanish.

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:

- Understand the different mathematical concepts and tools underlying the models under consideration; and
- Implement these models, with special attention to efficiency and security issues.

5.2. Syllabus

1. Introduction to Information Coding. Cryptology
    1.1. Trasmission of Information
    1.2. Types of codes
    1.3. Compression with variable-length codes: Huffman codification
        1.3.1. Introduction to information theory
        1.3.2. Huffman codification
        1.3.3. Minimal variance Huffman codification
    1.4. Cryptography and cryptosystems
        1.4.1. Private key cryptosystems
        1.4.2. 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. Schedule

6.1. Subject schedule*

Week	Face-to-face classroom activities	Face-to-face 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		**Autonomous study** Group work Continuous assessment Not Presential Duration: 02:00
2	**Theory and/or exercises class. Chapter 1** Duration: 04:00 Lecture			**Autonomous study** Group work Continuous assessment Not Presential Duration: 02:00
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, RA299)** Group work Continuous assessment Not Presential Duration: 00:00 **Autonomous study** Group work Continuous assessment Not Presential Duration: 02:00 **Moodle test. Chapter 1A (RA291, RA299).** Online test Continuous assessment Not Presential Duration: 00:20
4	**Theory and/or exercises class. Chapter 1** Duration: 04:00 Lecture			**Moodle test. Chapter 1B (RA291, RA294).** Online test Continuous assessment Not Presential Duration: 00:20
5	**Theory and/or exercises class. Chapter 1** Duration: 02:00 Lecture	**Lab session: Lab project 2** Duration: 02:00 Laboratory assignments		**Lab project 2 (RA297, RA294)** Group work Continuous assessment Not Presential Duration: 00:00
6	**Theory and/or exercises class. Chapter 2** Duration: 04:00 Lecture			
7	**Theory and/or exercises class. Chapter 2** Duration: 04:00 Lecture			**Moodle test. Chapter 2 (RA295)** Online test Continuous assessment Not Presential Duration: 00:20

8	**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: 01:00
9	**Theory and/or exercises class. Chapter 3** 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		**Lab project 3 (RA297, RA 296 and RA295)** Group work Continuous assessment Not Presential Duration: 00:00 **Moodle test. Chapter 3 (RA296).** Online test Continuous assessment Not Presential Duration: 00:20
11	**Theory and/or exercises class. Chapter 4** Duration: 04:00 Lecture			**Moodle test. Chapter 4 (RA296 , RA290)** Online test Continuous assessment Not Presential Duration: 00:20
12	**Theory and/or exercises class. Chapter 5** Duration: 02:00 Lecture	**Lab session: Lab project 4** Duration: 02:00 Laboratory assignments		**Lab project 4 (RA297, RA296 and RA290)** Group work Continuous assessment Not Presential Duration: 00:00
13	**Theory and/or exercises class. Chapter 5** Duration: 04:00 Lecture			**Moodle test. Chapter 5 (RA292)** Online test Continuous assessment Not Presential Duration: 00:20
14	**Overall review. Introduction to CRC** Duration: 02:00 Additional activities	**Lab session: Lab project 5** Duration: 02:00 Laboratory assignments		**Lab project 5 (RA297, RA292)** Group work Continuous assessment Not Presential Duration: 00:00
15				**Written test, chapters 3,4, and 5 (RA296, RA290, RA292 and RA293).** Written test Continuous assessment Presential Duration: 01:00
16				
17				**Lab test (RA296, RA290, RA292, RA297)** Problem-solving test Continuous assessment Presential Duration: 01:00 **Final exam (RA290, RA291, RA292, RA293, RA294 RA295, RA296, RA297, RA298, RA299)** Written test Final examination Presential Duration: 03:00

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. Continuous assessment

Week	Description	Modality	Type	Duration	Weight	Minimum grade	Evaluated skills
1	Autonomous study	Group work	No Presential	02:00	0%	0 / 10	
2	Autonomous study	Group work	No Presential	02:00	0%	0 / 10	
3	Lab project 1 (RA297, RA299)	Group work	No Presential	00:00	6%	0 / 10	CB3 CC1 CC7 CB1 CC6 CT12
3	Autonomous study	Group work	No Presential	02:00	0%	0 / 10	
3	Moodle test. Chapter 1A (RA291, RA299).	Online test	No Presential	00:20	2%	7 / 10	CC6 CT1 CB3 CC1 CC7 CB1
4	Moodle test. Chapter 1B (RA291, RA294).	Online test	No Presential	00:20	2%	7 / 10	
5	Lab project 2 (RA297, RA294)	Group work	No Presential	00:00	6%	0 / 10	CC6 CT12 CB3 CC1 CC7 CB1
7	Moodle test. Chapter 2 (RA295)	Online test	No Presential	00:20	2%	7 / 10	CC6 CT1 CB3 CC1 CC7 CB1
8	Written test, chapters 1 and 2 (RA291, RA294, RA295 and RA293)	Written test	Face-to-face	01:00	16%	0 / 10	CC6 CT1 CT2 CB3 CC1 CC7 CT4 CB1

10	Lab project 3 (RA297, RA 296 and RA295)	Group work	No Presential	00:00	6%	0 / 10	CT2 CB3 CC1 CC7 CB1 CC6
10	Moodle test. Chapter 3 (RA296).	Online test	No Presential	00:20	2%	7 / 10	CC6 CT1 CB3 CC1 CC7 CB1
11	Moodle test. Chapter 4 (RA296 , RA290)	Online test	No Presential	00:20	2%	7 / 10	CT1 CB3 CC1 CC7 CB1 CC6
12	Lab project 4 (RA297, RA296 and RA290)	Group work	No Presential	00:00	6%	0 / 10	CC6 CT12 CB3 CC1 CC7 CB1
13	Moodle test. Chapter 5 (RA292)	Online test	No Presential	00:20	2%	7 / 10	CT1 CB3 CC1 CC7 CB1 CC6
14	Lab project 5 (RA297, RA292)	Group work	No Presential	00:00	6%	0 / 10	CB3 CC1 CC7 CB1 CC6 CT12
15	Written test, chapters 3,4, and 5 (RA296, RA290, RA292 and RA293).	Written test	Face-to-face	01:00	22%	/ 10	CC6 CT1 CT2 CB3 CC1 CC7 CT4 CB1
17	Lab test (RA296, RA290, RA292, RA297)	Problem-solving test	Face-to-face	01:00	20%	0 / 10	CC6 CT2 CT12 CB3 CC1 CC7 CB1

7.1.2. Final 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	100%	5 / 10	CC6 CT1 CT2 CT12 CB3 CC1 CC7 CT4 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	02:30	100%	5 / 10	CC6 CT1 CT2 CT12 CB3 CC1 CC7 CT4 CB1

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 November 24th, 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.

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	
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	Equipment	

9. Other information

9.1. Other information about the subject

En previsión de posibles recidivas de la epidemia de COVID, la presente guía contempla la impartición de la asignatura en formato bimodal: todas las actividades formativas planificadas inicialmente como actividades presenciales, en caso de ser necesario pasarán a desarrollarse a través de plataformas online. En caso de que esto ocurriera, se notificará en el moodle de la asignatura todas las acciones a realizar, el nuevo material (si procede), etc.