ANX-PR/CL/001-01

LEARNING GUIDE

SUBJECT

615000740 - Nformation Coding

DEGREE PROGRAMME

61TI - Grado En Tecnologias Para La Sociedad De La Informacion

ACADEMIC YEAR & SEMESTER

2021/22 - Semester 1

PR/CL/001
COORDINATION PROCESS OF
LEARNING ACTIVITIES

ANX-PR/CL/001-01
LEARNING GUIDE

E.T.S. de Ingenieria de
Sistemas Informaticos

Index

Learning guide

PR/CL/001
COORDINATION PROCESS OF
LEARNING ACTIVITIES

ANX-PR/CL/001-01
LEARNING GUIDE

E.T.S. de Ingenieria de
Sistemas Informaticos

1. Description

1.1. Subject details

Name of the subject	615000740 - Nformation 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	61TI - Grado en Tecnologias para la Sociedad de la Informacion
Centre	61 - Escuela Tecnica Superior De Ingenieria De Sistemas Informaticos
Academic year	2021-22

2. Faculty

2.1. Faculty members with subject teaching role

Name and surname	Office/Room	Email	Tutoring hours *
Luis Miguel Pozo Coronado	2004	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) | 2006 | anaisabel.lias@upm.es | Sin horario. Office hours will be published before the beginning of the term, both in moodle and on the bulletin board. |

* 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

CB01 - Que los estudiantes hayan demostrado poseer y comprender conocimientos en un área de estudio que parte de la base de la educación secundaria general, y se suele encontrar a un nivel que, si bien se apoya en libros de texto avanzados, incluye también algunos aspectos que implican conocimientos procedentes de la vanguardia de su campo de estudio

CB03 - Que los estudiantes tengan la capacidad de reunir e interpretar datos relevantes (normalmente dentro de su área de estudio) para emitir juicios que incluyan una reflexión sobre temas relevantes de índole social, científica o ética

CE07 - Capacidad para comprender, aplicar y gestionar la garantía y seguridad de los sistemas informáticos.

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.

OB09 - Capacidad para resolver problemas con iniciativa, toma de decisiones, autonomía y creatividad. Capacidad para saber comunicar y transmitir los conocimientos, habilidades y destrezas de la profesión de Ingeniero Técnico en Informática.

4.2. Learning outcomes

RA285 - Utiliza adecuadamente software para la resolución de problemas de codificación de la información, describiendo con precisión los protocolos utilizados

RA284 - Aplica los principales resultados de la teoría de números a la Criptología, cifrando y descifrando con los criptosistemas RSA y ElGamal

RA283 - Determina la complejidad computacional de algoritmos sencillos que involucren operaciones aritméticas elementales

RA282 - Distingue criptosistemas de clave pública y clave privada. Cifra y descifra utilizando los criptosistemas de traslación, afín y matricial afín

RA288 - Identifica y define eficazmente las metas, objetivos y prioridades de una tarea o proyecto a desempeñar estipulando las actividades, los plazos y los recursos requeridos y controlando los procesos establecidos

RA281 - 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

RA286 - Codifica, detecta y corrige errores utilizando los códigos lineales

RA287 - Comprime ficheros, usando códigos compresores adecuados

* 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:

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

PR/CL/001
COORDINATION PROCESS OF
LEARNING ACTIVITIES

ANX-PR/CL/001-01
LEARNING GUIDE

E.T.S. de Ingenieria de
Sistemas Informaticos

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

PR/CL/001
COORDINATION PROCESS OF
LEARNING ACTIVITIES

ANX-PR/CL/001-01
LEARNING GUIDE

E.T.S. de Ingenieria de Sistemas Informaticos

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** Other assessment Continuous assessment Not Presential Duration: 02:00
2	**Theory and/or exercises class. Chapter 1** Duration: 04:00 Lecture			**Autonomous study** Other assessment Continuous assessment Not Presential Duration: 03:00
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, RA295)** Group work Continuous assessment Not Presential Duration: 00:00 **Moodle test. Chapter 1 (RA291, RA294).** Online test Continuous assessment Not Presential Duration: 00:20 **Autonomous study** Other assessment Continuous assessment Not Presential Duration: 02:00
4	**Theory and/or exercises class. Chapter 2** Duration: 04:00 Lecture			**Autonomous study** Other assessment Continuous assessment Not Presential Duration: 02:00
5	**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 **Autonomous study** Other assessment Continuous assessment Not Presential Duration: 02:00

6	**Theory and/or exercises class. Chapter 3** Duration: 03:00 Lecture			**Written test, chapters 1 and 2 (RA291,** **RA294, RA295 and RA293)** Written test Continuous assessment Presential Duration: 01:30 **Autonomous study** Other assessment Continuous assessment Not Presential Duration: 04:00
7	**Theory and/or exercises class. Chapter 3** Duration: 04:00 Lecture			**Autonomous study** Other assessment Continuous assessment Not Presential Duration: 04:00
8	**Theory and/or exercises class. Chapters** **3 and 4** Duration: 02:00 Lecture	**Lab session: Lab project 2** Duration: 02:00 Laboratory assignments		**Moodle test. Chapter 3 (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 **Autonomous study** Other assessment Continuous assessment Not Presential Duration: 02:00
9	**Theory and/or exercises class. Chapter 4** Duration: 04:00 Lecture			**Autonomous study** Other assessment Continuous assessment Not Presential Duration: 04:00
10	**Theory and/or exercises class. Chapters** **4 and 5** Duration: 02:00 Lecture	**Lab session: Lab project 3** Duration: 02:00 Laboratory assignments		**Moodle test. Chapter 4 (RA296 , RA290)** Online test Continuous assessment Not Presential Duration: 00:20 **Autonomous study** Other assessment Continuous assessment Not Presential Duration: 02:00 **Lab project 3 (RA297, RA296 and RA290)** Group work Continuous assessment Not Presential Duration: 00:00

PR/CL/001
COORDINATION PROCESS OF
LEARNING ACTIVITIES

ANX-PR/CL/001-01
LEARNING GUIDE

E.T.S. de Ingenieria de
Sistemas Informaticos

11	**Theory and/or exercises class. Chapter 5** Duration: 04:00 Lecture			**Autonomous study** Other assessment Continuous assessment Not Presential Duration: 02:00
12	**Theory and/or exercises class. Chapters 5 and 6** Duration: 02:00 Lecture	**Lab session: Lab project 4** Duration: 02:00 Laboratory assignments		**Moodle test. Chapter 5 (RA292)** Online test Continuous assessment Not Presential Duration: 00:20 **Autonomous study** Other assessment Continuous assessment Not Presential Duration: 04:00 **Lab project 4 (RA297, RA292)** Group work Continuous assessment Not Presential Duration: 00:00
13	**Theory and/or exercises class. Chapter 6** Duration: 03:00 Lecture			**Autonomous study** Other assessment Continuous assessment Not Presential Duration: 04:00 **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: 02:00 Lecture	**Lab session: Lab project 5** Duration: 02:00 Laboratory assignments		**Autonomous study** Other assessment Continuous assessment Not Presential Duration: 02:00 **Lab project 5 (RA297, RA299)** Group work Continuous assessment Not Presential Duration: 00:00
15	**Theory and/or exercises class. Chapter 6** Duration: 04:00 Lecture			**Moodle test. Chapter 6 (RA291, RA298, RA299)** Online test Continuous assessment Not Presential Duration: 00:20 **Autonomous study** Other assessment Continuous assessment Not Presential Duration: 02:00

				Autonomous study
16				Other assessment
				Continuous assessment
				Not Presential
				Duration: 04:00
				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
				Other assessment
				Continuous assessment
				Not Presential
				Duration: 06:00
				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.

PR/CL/001
COORDINATION PROCESS OF
LEARNING ACTIVITIES

ANX-PR/CL/001-01
LEARNING GUIDE

E.T.S. de Ingenieria de
Sistemas Informaticos

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	Other assessment	No Presential	02:00	%	/ 10	
2	Autonomous study	Other assessment	No Presential	03:00	%	/ 10	
3	Lab project 1 (RA297, RA295)	Group work	No Presential	00:00	6%	/ 10	
3	Moodle test. Chapter 1 (RA291, RA294).	Online test	No Presential	00:20	2%	7 / 10	
3	Autonomous study	Other assessment	No Presential	02:00	%	/ 10	
4	Autonomous study	Other assessment	No Presential	02:00	%	/ 10	
5	Moodle test. Chapter 2 (RA295)	Online test	No Presential	00:20	2%	7 / 10	
5	Autonomous study	Other assessment	No Presential	02:00	%	/ 10	
6	Written test, chapters 1 and 2 (RA291, RA294, RA295 and RA293)	Written test	Face-to-face	01:30	12%	/ 10	OB09 CB03 CB01
6	Autonomous study	Other assessment	No Presential	04:00	%	/ 10	
7	Autonomous study	Other assessment	No Presential	04:00	%	/ 10	
8	Moodle test. Chapter 3 (RA296).	Online test	No Presential	00:20	2%	7 / 10	
8	Lab project 2 (RA297, RA 296 and RA295)	Group work	No Presential	00:00	6%	/ 10	
8	Autonomous study	Other assessment	No Presential	02:00	%	/ 10	
9	Autonomous study	Other assessment	No Presential	04:00	%	/ 10	
10	Moodle test. Chapter 4 (RA296 , RA290)	Online test	No Presential	00:20	2%	7 / 10	

PR/CL/001
COORDINATION PROCESS OF
LEARNING ACTIVITIES

ANX-PR/CL/001-01
LEARNING GUIDE

E.T.S. de Ingenieria de
Sistemas Informaticos

Week	Description	Modality	Type	Duration	Weight	Minimum grade	Evaluated skills
10	Autonomous study	Other assessment	No Presential	02:00	%	/ 10	
10	Lab project 3 (RA297, RA296 and RA290)	Group work	No Presential	00:00	6%	/ 10	
11	Autonomous study	Other assessment	No Presential	02:00	%	/ 10	
12	Autonomous study	Other assessment	No Presential	04:00	%	/ 10	
12	Moodle test. Chapter 5 (RA292)	Online test	No Presential	00:20	2%	7 / 10	
12	Lab project 4 (RA297, RA292)	Group work	No Presential	00:00	6%	/ 10	
13	Autonomous study	Other assessment	No Presential	04:00	%	/ 10	
13	Written test, chapters 3,4, and 5 (RA296, RA290, RA292 and RA293).	Written test	Face-to-face	02:00	20%	/ 10	OB09 CE07 CB03 CB01
14	Autonomous study	Other assessment	No Presential	02:00	%	/ 10	
14	Lab project 5 (RA297, RA299)	Group work	No Presential	00:00	6%	/ 10	CT12
15	Moodle test. Chapter 6 (RA291, RA298, RA299)	Online test	No Presential	00:20	%	7 / 10	
15	Autonomous study	Other assessment	No Presential	02:00	%	/ 10	
16	Autonomous study	Other assessment	No Presential	04:00	%	/ 10	
16	Lab test (RA296, RA290, RA292, RA297)	Problem-solving test	Face-to-face	01:00	20%	/ 10	CT12 CE07
16	Written test, chapter 6 (RA291, RA298, RA299 and RA293)	Written test	Face-to-face	01:00	8%	/ 10	
17	Autonomous study	Other assessment	No Presential	06:00	%	/ 10	

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	70%	5 / 10	CB03 CB01 OB09 CE07
17	Final lab project (Toolbox) (RA297)	Individual work	Face-to-face	01:00	30%	/ 10	CT12 CE07

7.1.3. Referred (re-sit) examination

PR/CL/001
COORDINATION PROCESS OF
LEARNING ACTIVITIES

ANX-PR/CL/001-01
LEARNING GUIDE

E.T.S. de Ingenieria de
Sistemas Informaticos

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	
Final lab project (Toolbox) (RA297)	Individual work	No Presential	00:00	%	/ 10	

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	

PR/CL/001
COORDINATION PROCESS OF
LEARNING ACTIVITIES

ANX-PR/CL/001-01
LEARNING GUIDE

E.T.S. de Ingenieria de
Sistemas Informaticos

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	