ANX-PR/CL/001-01

LEARNING GUIDE

SUBJECT

615000547 - Coding of information

DEGREE PROGRAMME

61SI - Grado En Sistemas De Informacion

ACADEMIC YEAR & SEMESTER

2018/19 - Semester 1

Index

Learning guide

1. Description

1.1. Subject details

Name of the subject	615000547 - Coding of information
No of credits	6 ECTS
Type	Optional
Academic year ot the programme	Fourth year
Semester of tuition	Semester 7
Tuition period	September-January
Tuition languages	English
Degree programme	61SI - Grado en sistemas de informacion
Centre	61 - Escuela Tecnica Superior de Ingenieria de Sistemas Informaticos
Academic year	2018-19

2. Faculty

2.1. Faculty members with subject teaching role

Name and surname	Office/Room	Email	Tutoring hours *
Luis Miguel Pozo Coronado (Subject coordinator)	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	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

El plan de estudios Grado en Sistemas de Informacion no tiene definidas asignaturas previas recomendadas para esta asignatura.

3.2. Other recommended learning outcomes

- Handling modular arithmetics and matrix calculus with ease.

- Understanding and writing simple mathematical proofs.

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

RA361 - Utiliza adecuadamente software para la resolución de problemas de codificación de la información, describiendo con precisión los protocolos utilizados

RA360 - Aplica los principales resultados de la teoría de números a la Criptología, cifrando y descifrando con los criptosistemas RSA y ElGamal

RA354 - Conoce y aplica protocolos de autenticación (firma digital) e intercambio de claves basados en criptosistemas de clave pública

RA362 - Codifica, detecta y corrige errores utilizando los códigos lineales

RA363 - Comprime ficheros, usando códigos compresores adecuados

RA355 - Utiliza los distintos tipos de codificación de la información según el objetivo perseguido (corregir errores, encriptar información o comprimirla)

RA358 - Distingue criptosistemas de clave pública y clave privada. Cifra y descifra utilizando los criptosistemas de traslación, afín y matricial afín

RA359 - Determina la complejidad computacional de algoritmos sencillos que involucren operaciones aritméticas

elementales

RA357 - 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

RA356 - Conoce y aplica test de primalidad deterministas y probabilísticos

* 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) Understand the different mathematical concepts and tools underlying the models under consideration; and b) Implement 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	Face-to-face classroom activities	Face-to-face laboratory activities	Other face-to-face activities	Assessment activities
1	**Introduction to the subject. Chapter 1** Duration: 02:00 Lecture	**Lab session. Introduction to Maxima.** Duration: 02:00 Laboratory assignments		
2	**Chapter 1.** Duration: 04:00 Lecture			
3	**Chapter 1** Duration: 02:00 Lecture	**Lab project 1** Duration: 02:00 Laboratory assignments		**Lab project 1 (RA 361, RA 359)** Group work Continuous assessment Duration: 00:00 **Moodle test, chapter 1 (RA 355, RA358)** Online test Continuous assessment Duration: 00:20
4	**Chapter 2** Duration: 04:00 Lecture			
5	**Chapter 2** Duration: 04:00 Lecture			**Moodle test, chapter 2 (RA359)** Online test Continuous assessment Duration: 00:20
6	**Chapter 3** Duration: 03:00 Lecture			**Written test, chapters 1 and 2 (RA355, RA358, RA359 and RA357)** Written test Continuous assessment Duration: 01:00
7	**Chapter 3** Duration: 04:00 Lecture			
8	**Chapters 3 and 4** Duration: 02:00 Lecture	**Lab project 2** Duration: 02:00 Laboratory assignments		**Lab project 2 (RA 361, RA 360)** Group work Continuous assessment Duration: 00:00 **Moodle test. Chapter 3 (RA360)** Online test Continuous assessment Duration: 00:20
9	**Chapter 4** Duration: 04:00 Lecture			

10	**Chapters 4 and 5** Duration: 02:00 Lecture	**Lab project 3** Duration: 02:00 Laboratory assignments		**Lab project 3 (RA 361, RA360, RA354)** Group work Continuous assessment Duration: 00:00 **Moodle test. Chapter 4 (RA360 , RA354)** Online test Continuous assessment Duration: 00:20
11	**Chapter 5** Duration: 04:00 Lecture			
12	**Chapters 5 and 6** Duration: 02:00 Lecture	**Lab project 4** Duration: 02:00 Laboratory assignments		**Lab project 4 (RA 361, RA 356)** Group work Continuous assessment Duration: 00:00 **Moodle test. Chapter 5 (RA356)** Online test Continuous assessment Duration: 00:20
13	**Chapter 6** Duration: 04:00 Lecture			**Written test, chapters 3,4, and 5 (RA360, RA354, RA356 and RA357)** Written test Continuous assessment Duration: 01:00
14	**Chapter 6** Duration: 02:00 Lecture	**Lab project 5** Duration: 02:00 Laboratory assignments		**Lab project 5 (RA 361, RA 363)** Group work Continuous assessment Duration: 00:00
15	**Chapter 6** Duration: 02:00 Lecture	**Lab project 6** Duration: 02:00 Laboratory assignments		**Lab project 6 (RA 361, RA 362)** Group work Continuous assessment Duration: 00:00
16	**Chapter 6** Duration: 02:00 Lecture			**Written test, chapter 6 (RA355, RA362, RA363 and RA357)** Written test Continuous assessment Duration: 01:00 **Final lab project (Toolbox) (RA361)** Individual work Continuous assessment Duration: 00:00 **Moodle test, chapter 6 (RA355, RA362, RA363)** Online test Continuous assessment Duration: 00:20 **Lab test (RA360, RA354, RA356, RA361)** Problem-solving test Continuous assessment Duration: 00:30

17				**Final exam (RA 354, 355, 356, 357, 358, 359, 360, 361, 362, 363)** Written test Final examination Duration: 02:00 **Final lab project (Toolbox) (RA361)** Individual work Final examination Duration: 00:00

The independent study hours are training activities during which students should spend time on individual study or individual assignments.

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 subject schedule is based on a previous theorical planning of the subject plan and might go to through experience some unexpected changes along throughout the academic year.

7. Activities and assessment criteria

7.1. Assessment activities

7.1.1. Continuous assessment

Week	Description	Modality	Type	Duration	Weight	Minimum grade	Evaluated skills
3	Lab project 1 (RA 361, RA 359)	Group work	No Presential	00:00	5%	/ 10	CB1 CC6 CT12 CC7 CB3 CC1
3	Moodle test, chapter 1 (RA 355, RA358)	Online test	No Presential	00:20	2%	7 / 10	CB1 CC6 CC7 CT1 CB3 CC1
5	Moodle test, chapter 2 (RA359)	Online test	No Presential	00:20	2%	7 / 10	CB1 CC6 CC7 CT1 CB3 CC1
6	Written test, chapters 1 and 2 (RA355, RA358, RA359 and RA357)	Written test	Face-to-face	01:00	12%	/ 10	CB1 CT4 CT2 CC6 CC7 CT1 CB3 CC1
8	Lab project 2 (RA 361, RA 360)	Group work	No Presential	00:00	5%	/ 10	CB1 CC6 CT12 CC7 CB3 CC1
8	Moodle test. Chapter 3 (RA360)	Online test	No Presential	00:20	2%	7 / 10	CB1 CC6 CC7 CT1 CB3 CC1

10	Lab project 3 (RA 361, RA360, RA354)	Group work	No Presential	00:00	5%	/ 10	CB1 CC6 CT12 CC7 CB3 CC1
10	Moodle test. Chapter 4 (RA360 , RA354)	Online test	No Presential	00:20	2%	7 / 10	CB1 CC6 CC7 CT1 CB3 CC1
12	Lab project 4 (RA 361, RA 356)	Group work	No Presential	00:00	5%	/ 10	CB1 CC6 CT12 CC7 CB3 CC1
12	Moodle test. Chapter 5 (RA356)	Online test	No Presential	00:20	2%	7 / 10	CC7 CT1 CB1 CC6 CB3 CC1
13	Written test, chapters 3,4, and 5 (RA360, RA354, RA356 and RA357)	Written test	Face-to-face	01:00	20%	/ 10	CB1 CT4 CT2 CC6 CC7 CT1 CB3 CC1
14	Lab project 5 (RA 361, RA 363)	Group work	No Presential	00:00	5%	/ 10	CB1 CC6 CT12 CC7 CB3 CC1
15	Lab project 6 (RA 361, RA 362)	Group work	No Presential	00:00	5%	/ 10	CB1 CC6 CT12 CC7 CB3 CC1
16	Written test, chapter 6 (RA355, RA362, RA363 and RA357)	Written test	Face-to-face	01:00	8%	/ 10	CB1 CT4 CT2 CC6 CC7 CT1 CB3 CC1

16	Final lab project (Toolbox) (RA361)	Individual work	No Presential	00:00	15%	/ 10	CB1 CT4 CC6 CT12 CC7 CB3 CC1
16	Moodle test, chapter 6 (RA355, RA362, RA363)	Online test	No Presential	00:20	2%	7 / 10	CB1 CC6 CC7 CT1 CB3 CC1
16	Lab test (RA360, RA354, RA356, RA361)	Problem-solving test	Face-to-face	00:30	5%	/ 10	CB1 CT2 CC6 CT12 CC7 CB3 CC1

7.1.2. Final examination

Week	Description	Modality	Type	Duration	Weight	Minimum grade	Evaluated skills
17	Final exam (RA 354, 355, 356, 357, 358, 359, 360, 361, 362, 363)	Written test	Face-to-face	02:00	100%	5 / 10	CB1 CT4 CT2 CC6 CC7 CT1 CB3 CC1
17	Final lab project (Toolbox) (RA361)	Individual work	No Presential	00:00	%	/ 10	CB1 CC6 CT12 CC7 CB3 CC1

7.1.3. Referred (re-sit) examination

Description	Modality	Type	Duration	Weight	Minimum grade	Evaluated skills
Final exam RA 354, 355, 356, 357, 358, 359, 360, 361, 362, 363)	Written test	Face-to-face	02:00	100%	5 / 10	CB1 CT4 CT2 CC6 CT12 CC7 CT1 CB3 CC1
Final lab project (Toolbox)(RA361)	Individual work	No Presential	00:00	%	/ 10	CB1 CC6 CT12 CC7 CB3 CC1

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 in normal 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: 6 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 5%. Project assessment: Procedures, 50% (efficiency, clarity, documentation); solved problems, 40%; mathematical rigour, elegance, language precision, 10%.

Final lab project (Toolbox): Every student must work individually on it. It consists of a library including all functions programmed along the term, and the corresponding help pages. A specification document will be published in Moodle, along with a list of all functions that must be included in the library. Students can send a draft version by the second week of november. The lecturer will send back a corrected version, along with suggestions for improvement.

The last week of lectures, a short validation test will take place in the lab, where some problems must be solved by using the toolbox functions. This test will weigh a 5% of the total grade.

Final version of the toolbox must be uploaded to Moodle before 22:00, December 22nd. Contribution to the final

grade is 15%. Assessment: Procedures 60%, Documentations and help pages 40%. Mathematical rigour, language precision, elegance in results presentation will be taken into account.

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 Toolbox (which each student must do in advence and bring to the exam). Each part will weigh 50% of the final grade. Toolbox specifications will be published in Moodle.

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, Maple	Equipment	