ANX-PR/CL/001-01
GUÍA DE APRENDIZAJE

ASIGNATURA

615001051 - Codificación De La Información

PLAN DE ESTUDIOS

61CI - Grado En Ingenieria De Computadores

CURSO ACADÉMICO Y SEMESTRE

2023/24 - Primer semestre

Índice

Guía de Aprendizaje

1. Datos descriptivos

1.1. Datos de la asignatura

Nombre de la asignatura	615001051 - Codificación de la Información
No de créditos	6 ECTS
Carácter	Optativa
Curso	Tercero curso
Semestre	Quinto semestre
Período de impartición	Septiembre-Enero
Idioma de impartición	Castellano
Titulación	61CI - Grado en Ingenieria de Computadores
Centro responsable de la titulación	61 - Escuela Tecnica Superior De Ingenieria De Sistemas Informaticos
Curso académico	2023-24

2. Profesorado

2.1. Profesorado implicado en la docencia

Nombre	Despacho	Correo electrónico	Horario de tutorías *
Ana Isabel Lias Quintero (Coordinador/a)		anaisabel.lias@upm.es	- -
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

* Las horas de tutoría son orientativas y pueden sufrir modificaciones. Se deberá confirmar los horarios de tutorías con el profesorado.

3. Conocimientos previos recomendados

3.1. Asignaturas previas que se recomienda haber cursado

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

3.2. Otros conocimientos previos recomendados para cursar la asignatura

- Handling modular arithmetics and matrix calculus with ease.

- Understanding and writing simple mathematical proofs.

4. Competencias y resultados de aprendizaje

4.1. Competencias

CB02 - Que los estudiantes sepan aplicar sus conocimientos a su trabajo o vocación de una forma profesional y posean las competencias que suelen demostrarse por medio de la elaboración y defensa de argumentos y la resolución de problemas dentro de su área de estudio

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.

4.2. Resultados del aprendizaje

RA410 - Aplica los principales resultados de la teoría de números a la Criptología, cifrando y descifrando con los criptosistemas RSA y ElGamal

RA411 - Utiliza adecuadamente software para la resolución de problemas de codificación de la información, describiendo con precisión los protocolos utilizados

RA409 - Determina la complejidad computacional de algoritmos sencillos que involucren operaciones aritméticas elementales

RA156 - Conoce y aplica métodos y algoritmos matemáticos que se usarán en las implementaciones criptográficas.

RA397 - Conoce y analiza la complejidad de un algoritmo

RA205 - Analiza y aplica el algoritmo RSA para la firma digital.

RA141 - Es capaz de trabajar como miembro de un equipo con la finalidad de contribuir a desarrollar proyectos con pragmatismo y sentido de la responsabilidad, asumiendo compromisos y teniendo en cuenta los recursos disponibles. Se desenvuelve de modo que logra generar confianza y credibilidad en un grupo de colaboradores, además del compromiso para el logro de la visión corporativa a través de negociaciones y motivaciones, y no de manera coercitiva e individualista.

RA413 - Comprime ficheros, usando códigos compresores adecuados

RA408 - Distingue criptosistemas de clave pública y clave privada. Cifra y descifra utilizando los criptosistemas de traslación, afín y matricial afín

5. Descripción de la asignatura y temario

5.1. Descripción de la asignatura

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. Temario de la asignatura

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. Cronograma

6.1. Cronograma de la asignatura *

Sem	Actividad en aula	Actividad en laboratorio	Tele-enseñanza	Actividades de evaluación
1	**Theory and/or exercises class. Introduction to the subject. Chapter 1** Duración: 02:00 LM: Actividad del tipo Lección Magistral	**Lab session: Introduction to Python** Duración: 02:00 PL: Actividad del tipo Prácticas de Laboratorio		
2	**Theory and/or exercises class. Chapter 1** Duración: 04:00 LM: Actividad del tipo Lección Magistral			
3	**Theory and/or exercises class. Chapter 1** Duración: 02:00 LM: Actividad del tipo Lección Magistral	**Lab session: Lab project 1** Duración: 02:00 PL: Actividad del tipo Prácticas de Laboratorio		**Lab project 1** TG: Técnica del tipo Trabajo en Grupo Evaluación continua No presencial Duración: 00:00 **Moodle test. (Non-recoverable test) Chapter 1** ET: Técnica del tipo Prueba Telemática Evaluación continua No presencial Duración: 00:20
4	**Theory and/or exercises class. Chapter 2** Duración: 06:00 LM: Actividad del tipo Lección Magistral			
5	**Theory and/or exercises class. Chapter 2** Duración: 02:00 PR: Actividad del tipo Clase de Problemas **Theory and/or exercises class. Chapter 3** Duración: 02:00 LM: Actividad del tipo Lección Magistral			**Moodle test. Chapter 2 Non-recoverable test** ET: Técnica del tipo Prueba Telemática Evaluación continua No presencial Duración: 00:20
6	**Theory and/or exercises class. Chapter 3** Duración: 04:00 LM: Actividad del tipo Lección Magistral			**Written test, chapters 1 and 2** EX: Técnica del tipo Examen Escrito Evaluación continua Presencial Duración: 02:00
7	**Theory and/or exercises class. Chapter 3** Duración: 02:00 LM: Actividad del tipo Lección Magistral **Theory and/or exercises class. Chapter 4** Duración: 02:00 LM: Actividad del tipo Lección Magistral			
8	**Theory and/or exercises class. Chapter 4** Duración: 02:00 LM: Actividad del tipo Lección Magistral	**Lab session: Lab project 2** Duración: 02:00 PL: Actividad del tipo Prácticas de Laboratorio		**Moodle test. Chapter 3 Non-recoverable test.** ET: Técnica del tipo Prueba Telemática Evaluación continua No presencial Duración: 00:20 **Lab project 2.**

				TG: Técnica del tipo Trabajo en Grupo Evaluación continua No presencial Duración: 00:00
9	**Theory and/or exercises class. Chapter 4** Duración: 02:00 LM: Actividad del tipo Lección Magistral			
10	**Theory and/or exercises class. Chapter 4** Duración: 01:00 LM: Actividad del tipo Lección Magistral **Theory and/or exercises class. Chapter 5** Duración: 03:00 LM: Actividad del tipo Lección Magistral			**Moodle test. Chapter 4 Non-recoverable test.** ET: Técnica del tipo Prueba Telemática Evaluación continua No presencial Duración: 00:20
11	**Theory and/or exercises class. Chapter 5** Duración: 02:00 LM: Actividad del tipo Lección Magistral	**Lab session: Lab project 3** Duración: 02:00 PL: Actividad del tipo Prácticas de Laboratorio		**Lab project 3.** TG: Técnica del tipo Trabajo en Grupo Evaluación continua No presencial Duración: 00:00
12	**Theory and/or exercises class. Chapter 5** Duración: 01:00 LM: Actividad del tipo Lección Magistral **Theory and/or exercises class. Chapter 6** Duración: 03:00 LM: Actividad del tipo Lección Magistral			**Moodle test. Non-recoverable test Chapter 5.** ET: Técnica del tipo Prueba Telemática Evaluación continua No presencial Duración: 00:20
13	**Theory and/or exercises class. Chapter 6** Duración: 02:00 LM: Actividad del tipo Lección Magistral	**Lab session: Lab project 4** Duración: 02:00 PL: Actividad del tipo Prácticas de Laboratorio		**Lab project 4.** TG: Técnica del tipo Trabajo en Grupo Evaluación continua No presencial Duración: 00:00 **Written test, chapters 3,4, and 5.** EX: Técnica del tipo Examen Escrito Evaluación continua Presencial Duración: 02:00
14	**Theory and/or exercises class. Chapter 6** Duración: 04:00 LM: Actividad del tipo Lección Magistral			
15	**Theory and/or exercises class. Chapter 6** Duración: 02:00 LM: Actividad del tipo Lección Magistral	**Lab session: Lab project 5** Duración: 02:00 PL: Actividad del tipo Prácticas de Laboratorio		**Moodle test. Non-recoverable test Chapter 6.** ET: Técnica del tipo Prueba Telemática Evaluación continua No presencial Duración: 00:20 **Lab project 5.** TG: Técnica del tipo Trabajo en Grupo Evaluación continua No presencial Duración: 00:00
16				
				Lab test. EP: Técnica del tipo Examen de Prácticas Evaluación continua Presencial Duración: 01:00 **Written test, chapter 6.** EX: Técnica del tipo Examen Escrito

17				Evaluación continua Presencial Duración: 01:00 **Final exam.** EX: Técnica del tipo Examen Escrito Evaluación sólo prueba final Presencial Duración: 03:00 **Autonomous study throughout the course (4 hours per week, average)** OT: Otras técnicas evaluativas Evaluación continua No presencial Duración: 60:00 **Final lab project (Toolbox).** TI: Técnica del tipo Trabajo Individual Evaluación sólo prueba final Presencial Duración: 01:00

Para el cálculo de los valores totales, se estima que por cada crédito ECTS el alumno dedicará dependiendo del plan de estudios, entre 26 y 27 horas de trabajo presencial y no presencial.

7. Actividades y criterios de evaluación

7.1. Actividades de evaluación de la asignatura

7.1.1. Evaluación (progresiva)

Sem.	Descripción	Modalidad	Tipo	Duración	Peso en la nota	Nota mínima	Competencias evaluadas
3	Lab project 1	TG: Técnica del tipo Trabajo en Grupo	No Presencial	00:00	6%	/ 10	
3	Moodle test. (Non-recoverable test) Chapter 1	ET: Técnica del tipo Prueba Telemática	No Presencial	00:20	2%	7 / 10	CB02
5	Moodle test. Chapter 2 Non-recoverable test	ET: Técnica del tipo Prueba Telemática	No Presencial	00:20	2%	7 / 10	CB02
6	Written test, chapters 1 and 2	EX: Técnica del tipo Examen Escrito	Presencial	02:00	12%	/ 10	CT12 CB02
8	Moodle test. Chapter 3 Non-recoverable test.	ET: Técnica del tipo Prueba Telemática	No Presencial	00:20	2%	7 / 10	CB02
8	Lab project 2.	TG: Técnica del tipo Trabajo en Grupo	No Presencial	00:00	6%	/ 10	CT12
10	Moodle test. Chapter 4 Non-recoverable test.	ET: Técnica del tipo Prueba Telemática	No Presencial	00:20	2%	7 / 10	CB02
11	Lab project 3.	TG: Técnica del tipo Trabajo en Grupo	No Presencial	00:00	6%	/ 10	CT12

12	Moodle test. Non-recoverable test Chapter 5.	ET: Técnica del tipo Prueba Telemática	No Presencial	00:20	2%	7 / 10	CB02
13	Lab project 4.	TG: Técnica del tipo Trabajo en Grupo	No Presencial	00:00	6%	/ 10	
13	Written test, chapters 3,4, and 5.	EX: Técnica del tipo Examen Escrito	Presencial	02:00	20%	/ 10	
15	Moodle test. Non-recoverable test Chapter 6.	ET: Técnica del tipo Prueba Telemática	No Presencial	00:20	%	7 / 10	CB02
15	Lab project 5.	TG: Técnica del tipo Trabajo en Grupo	No Presencial	00:00	6%	/ 10	CT12
17	Lab test.	EP: Técnica del tipo Examen de Prácticas	Presencial	01:00	20%	/ 10	CT12
17	Written test, chapter 6.	EX: Técnica del tipo Examen Escrito	Presencial	01:00	8%	/ 10	CB02
17	Autonomous study throughout the course (4 hours per week, average)	OT: Otras técnicas evaluativas	No Presencial	60:00	%	/ 10	

7.1.2. Prueba evaluación global

Sem	Descripción	Modalidad	Tipo	Duración	Peso en la nota	Nota mínima	Competencias evaluadas
17	Final exam.	EX: Técnica del tipo Examen Escrito	Presencial	03:00	70%	5 / 10	CT12 CB02
17	Final lab project (Toolbox).	TI: Técnica del tipo Trabajo Individual	Presencial	01:00	30%	/ 10	CT12 CB02

7.1.3. Evaluación convocatoria extraordinaria

Descripción	Modalidad	Tipo	Duración	Peso en la nota	Nota mínima	Competencias evaluadas
Final exam (RA290, RA291, RA292, RA293, RA294 RA295, RA296, RA297, RA298, RA299)	EX: Técnica del tipo Examen Escrito	Presencial	02:00	100%	5 / 10	
Final lab project (Toolbox) (RA297)	TI: Técnica del tipo Trabajo Individual	No Presencial	00:00	%	/ 10	

7.2. Criterios de evaluación

Progressive 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 (non-recoverable).
Written tests: They take place out of lecture hours, on Mondays, but the last one, that will be in January, the very same day that the final exam. 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 (non-recoverable). 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 global exam only, and july examination session

Final exam will take place as scheduled by the school administration. The exam, that includes the whole subject, 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 advance 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. Recursos didácticos

8.1. Recursos didácticos de la asignatura

Nombre	Tipo	Observaciones
Buchmann, Johannes A: "Introduction to Cryptography". Second Edition. Springer-Verlag. 2004.	Bibliografía	

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