ANX-PR/CL/001-01

GUÍA DE APRENDIZAJE

ASIGNATURA

Codificación de la información

PLAN DE ESTUDIOS

61CI , 61IW, 61SI, 61TI

CURSO ACADÉMICO Y SEMESTRE

2017-18 - Primer semestre

Índice

Guía de Aprendizaje

1. Datos descriptivos 1
2. Profesorado 1
3. Conocimientos previos recomendados 2
4. Competencias y resultados de aprendizaje 2
5. Descripción de la asignatura y temario 4
6. Cronograma 6
7. Actividades y criterios de evaluación.....8
8. Recursos didácticos 11

1. Datos descriptivos

1.1 Datos de la asignatura

Nombre de la Asignatura	615000532 - Codificacion de la informacion
Nº de Créditos	6 ECTS
Carácter	615000532
Curso	Tercero curso
Semestre	Quinto semestre
Período de impartición	Septiembre-Enero
Idioma de impartición	Inglés
Titulación	Todos los grados (61CI, 61IW, 61SI, 61TI)
Centro en el que se imparte	Escuela Técnica Superior de Ingeniería de Sistemas Informáticos
Curso Académico	2017-18

2. Profesorado

2.1 Profesorado implicado en la docencia

Nombre	Despacho	Correo electrónico	Horario de tutorías*
Luis Miguel Pozo Coronado (Coordinador/a)	2003	lm.pozo@upm.es	- -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

- Lógica y matemática discreta

- Algebra

3.2 Otros conocimientos previos recomendados para cursar la asignatura

- Understanding and writing simple mathematical proofs.

- Handling modular arithmetics and matrix calculus with ease.

4. Competencias y resultados de aprendizaje

4.1 Competencias que adquiere el estudiante al cursar la asignatura

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

CB04 - Que los estudiantes puedan transmitir información, ideas, problemas y soluciones a un público tanto especializado como no especializado

CE4 - Capacidad de diseñar e implementar software de sistema y de comunicaciones

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.

OB03 - Capacidad para diseñar, desarrollar, evaluar y asegurar la accesibilidad, ergonomía, usabilidad y seguridad de los sistemas, servicios y aplicaciones informáticas, así como de la información que gestionan.

OB08 - Conocimiento de las materias básicas y tecnológicas, que capaciten para el aprendizaje y desarrollo de nuevos métodos y tecnologías, así como las que les doten de una gran versatilidad para adaptarse a las nuevas situaciones.

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 Resultados del aprendizaje al cursar la asignatura

RA404 - Conoce y aplica protocolos de autenticación (firma digital) e intercambio de claves basados en criptosistemas de clave pública

RA405 - Utiliza los distintos tipos de codificación de la información según el objetivo perseguido (corregir errores, encriptar información o comprimirla)

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

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

RA407 - 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

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

RA406 - Conoce y aplica test de primalidad deterministas y probabilísticos

RA412 - Codifica, detecta y corrige errores utilizando los códigos lineales

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) 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 Temario de la asignatura

1. 1. Introduction to Information Coding
   - 1.1. Transmission of information
   - 1.2. Types of codes
   - 1.3. Huffman codes
   - 1.4. Linear codes
   - 1.5. Cyclic redundancy codes
2. Introduction to Cryptology
   - 2.1. Crytographt and cryptosystems
   - 2.2. Private key cryptosystems
   - 2.3. Cryptanalysis
3. Computational Complexity
   - 3.1. Problems and algorithms
   - 3.2. Complexity of elemental arithmetic operations
   - 3.3. Classification of problems regarding complexity
4. Number theory
   - 4.1. The multiplicative group of units mod n
   - 4.2. Euler's totient

4.3. Euler and Fermat theorems

4.4. Order of an element. Primitive roots mod n

4.5. Discrete logarithm

5. Public key cryptosystems

5.1. Diffie-Hellman key exchange protocol

5.2. RSA

5.3. El Gamal

5.4. Digital signature

5.5. Other applications of public key cryptography

6. Primality tests

6.1. Deterministic tests: Erathostenes sieve, trial division

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

6. Cronograma

6.1 Cronograma de la asignatura*

Semana	Actividad Presencial en Aula	Actividad Presencial en Laboratorio	Otra Actividad Presencial	Actividades de Evaluación
1	**Clase de teoría y ejercicios en aula** Duración: 02:00 LM: Actividad del tipo Lección Magistral			
2	**Clase de teoría y ejercicios en aula** Duración: 02:00 LM: Actividad del tipo Lección Magistral	**Clase de prácticas en laboratorio** Duración: 02:00 PL: Actividad del tipo Prácticas de Laboratorio		
3	**Clase de teoría y ejercicios en aula** Duración: 02:00 LM: Actividad del tipo Lección Magistral	**Clase de prácticas en laboratorio** Duración: 02:00 PL: Actividad del tipo Prácticas de Laboratorio		**Lab project 1** TG: Técnica del tipo Trabajo en GrupoEvaluación continua Duración: 00:00 **Moodle test** ET: Técnica del tipo Prueba TelemáticaEvaluación continua Duración: 00:20
4	**Clase de teoría y ejercicios en aula** Duración: 02:00 LM: Actividad del tipo Lección Magistral	**Clase de prácticas en laboratorio** Duración: 02:00 PL: Actividad del tipo Prácticas de Laboratorio		**Lab project 2** TG: Técnica del tipo Trabajo en GrupoEvaluación continua Duración: 00:00 **Written test, chapter 1** EX: Técnica del tipo Examen EscritoEvaluación continua Duración: 01:00
5	**Clase de teoría y ejercicios en aula** Duración: 02:00 LM: Actividad del tipo Lección Magistral	**Clase de prácticas en laboratorio** Duración: 02:00 PL: Actividad del tipo Prácticas de Laboratorio		
6	**Clase de teoría y ejercicios en aula** Duración: 04:00 LM: Actividad del tipo Lección Magistral			**Moodle test** ET: Técnica del tipo Prueba TelemáticaEvaluación continua Duración: 00:20
7	**Clase de teoría y ejercicios en aula** Duración: 02:00 LM: Actividad del tipo Lección Magistral	**Clase de prácticas en laboratorio** Duración: 02:00 PL: Actividad del tipo Prácticas de Laboratorio		**Lab project 3** TG: Técnica del tipo Trabajo en GrupoEvaluación continua Duración: 00:00
8	**Clase de teoría y ejercicios en aula** Duración: 04:00 LM: Actividad del tipo Lección Magistral			**Moodle test** ET: Técnica del tipo Prueba TelemáticaEvaluación continua Duración: 00:20
9	**Clase de teoría y ejercicios en aula** Duración: 04:00 LM: Actividad del tipo Lección Magistral			**Written test, chapters 2 and 3** EX: Técnica del tipo Examen EscritoEvaluación continua Duración: 01:00

10	**Clase de teoría y ejercicios en aula** Duración: 04:00 LM: Actividad del tipo Lección Magistral			
11	**Clase de teoría y ejercicios en aula** Duración: 04:00 LM: Actividad del tipo Lección Magistral			**Moodle test** ET: Técnica del tipo Prueba TelemáticaEvaluación continua Duración: 00:20
12	**Clase de teoría y ejercicios en aula** Duración: 02:00 LM: Actividad del tipo Lección Magistral	**Clase de prácticas en laboratorio** Duración: 02:00 PL: Actividad del tipo Prácticas de Laboratorio		
13	**Clase de teoría y ejercicios en aula** Duración: 04:00 LM: Actividad del tipo Lección Magistral			**Lab project 4** TG: Técnica del tipo Trabajo en GrupoEvaluación continua Duración: 00:00 **Moodle test** ET: Técnica del tipo Prueba TelemáticaEvaluación continua Duración: 00:20
14	**Clase de teoría y ejercicios en aula** Duración: 02:00 LM: Actividad del tipo Lección Magistral	**Clase de prácticas en laboratorio** Duración: 02:00 PL: Actividad del tipo Prácticas de Laboratorio		
15	**Clase de teoría y ejercicios en aula** Duración: 04:00 LM: Actividad del tipo Lección Magistral			
16	**Clase de teoría y ejercicios en aula** Duración: 02:00 LM: Actividad del tipo Lección Magistral			**Final lab project (Toolbox)** TI: Técnica del tipo Trabajo IndividualEvaluación continua Duración: 00:00 **Written test, chapters 4,5, and 6** EX: Técnica del tipo Examen EscritoEvaluación continua Duración: 01:00 **Moodle test** ET: Técnica del tipo Prueba TelemáticaEvaluación continua Duración: 00:20 **Lab test** EP: Técnica del tipo Examen de PrácticasEvaluación continua Duración: 00:30
17				**Final exam** EX: Técnica del tipo Examen EscritoEvaluación sólo prueba final Duración: 02:00 **Final lab project (Toolbox)** TI: Técnica del tipo Trabajo IndividualEvaluación sólo prueba final Duración: 00:00

* El cronograma sigue una planificación teórica de la asignatura y puede sufrir modificaciones durante el curso.

7. Actividades y criterios de evaluación

7.1 Actividades de evaluación de la asignatura

7.1.1 Evaluación continua

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	5%	/ 10	CE4 OB03 CT12 OB08
3	Moodle test	ET: Técnica del tipo Prueba Telemática	No Presencial	00:20	2%	7 / 10	OB03 OB08 CB03 CE4
4	Lab project 2	TG: Técnica del tipo Trabajo en Grupo	No Presencial	00:00	5%	/ 10	CE4 OB03 CT12 OB08
4	Written test, chapter 1	EX: Técnica del tipo Examen Escrito	Presencial	01:00	8%	/ 10	CE4 OB03 CB04 OB09 OB08 CB03
6	Moodle test	ET: Técnica del tipo Prueba Telemática	No Presencial	00:20	2%	7 / 10	CE4 OB03 OB08 CB03
7	Lab project 3	TG: Técnica del tipo Trabajo en Grupo	No Presencial	00:00	5%	/ 10	CE4 OB03 CT12 OB08
8	Moodle test	ET: Técnica del tipo Prueba Telemática	No Presencial	00:20	2%	7 / 10	OB03 OB08 CB03
9	Written test, chapters 2 and 3	EX: Técnica del tipo Examen Escrito	Presencial	01:00	12%	/ 10	OB09 OB08 CB03 OB03 CB04

11	Moodle test	ET: Técnica del tipo Prueba Telemática	No Presencial	00:20	2%	7 / 10	CE4 OB03 OB08 CB03
13	Lab project 4	TG: Técnica del tipo Trabajo en Grupo	No Presencial	00:00	5%	/ 10	CE4 OB03 CT12 OB08
13	Moodle test	ET: Técnica del tipo Prueba Telemática	No Presencial	00:20	2%	7 / 10	CE4 OB03 OB08 CB03
16	Final lab project (Toolbox)	TI: Técnica del tipo Trabajo Individual	No Presencial	00:00	25%	/ 10	CE4 OB03 CB04 CT12 OB08
16	Written test, chapters 4,5, and 6	EX: Técnica del tipo Examen Escrito	Presencial	01:00	20%	/ 10	CE4 OB03 CB04 OB09 OB08 CB03
16	Moodle test	ET: Técnica del tipo Prueba Telemática	No Presencial	00:20	2%	7 / 10	CE4 OB03 OB08 CB03
16	Lab test	EP: Técnica del tipo Examen de Prácticas	Presencial	00:30	5%	/ 10	CE4 OB03 CT12 OB09 OB08

7.1.2 Evaluación sólo prueba final

Sem.	Descripción	Modalidad	Tipo	Duración	Peso en la nota	Nota mínima	Competencias evaluadas
17	Final exam	EX: Técnica del tipo Examen Escrito	Presencial	02:00	100%	5 / 10	CE4 OB03 CB04 CT12 OB09 OB08 CB03
17	Final lab project (Toolbox)	TI: Técnica del tipo Trabajo Individual	No Presencial	00:00	%	/ 10	CE4 OB03 CT12 OB08

7.1.3 Evaluación convocatoria extraordinaria

Descripción	Modalidad	Tipo	Duración	Peso en la nota	Nota mínima	Competencias evaluadas
Final exam	EX: Técnica del tipo Examen Escrito	Presencial	02:00	100%	5 / 10	CE4 OB03 CB04 CT12 OB09 OB08 CB03
Final lab project (Toolbox)	TI: Técnica del tipo Trabajo Individual	No Presencial	00:00	%	/ 10	CE4 OB03 CT12 OB08

7.2 Criterios de Evaluación

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 (if all the six moodle tests are passed, only five of them will add to the final grade). The learning outcomes assessed in each test are: Chapter 1, RA405, RA412, RA413; Chapter 2, RA408; Chapter 3, RA409; Chapter 4, RA410; Chapter 5, RA410 , RA404.

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 precission and rigour in the results will be demanded. The learning outcomes assessed in each test are: Test 1, RA405, RA412, RA413 and RA407; Test 2, RA408, RA409 and RA407; test 3, RA410, RA404, RA406 and RA407.

Lab projects: 4 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 precission, 10%. All lab projects assess the learning outcome RA411. Additional learning outcomes assessed ine ach project are: Project 1, RA413; Project 2, RA412; Project 3, RA409; Project 4, RA410 y RA404.

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. The learning outcomes assessed are RA410, RA404, RA406, RA411.

Final version of the toolbox must be uploaded to Moodle before 22:00, December 22nd. Assesment: Procedures 60%, Documentations and help pages 40%. Mathjematical rigour, language precission, elegance in results presentation will be taken into account. Learning outcome assessed: RA411.

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. 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	