ANX-PR/CL/001-01

GUÍA DE APRENDIZAJE

ASIGNATURA

615000520 - Codificacion de la informacion

PLAN DE ESTUDIOS

61IW - Grado en Ingenieria del Software

CURSO ACADÉMICO Y SEMESTRE

2017-18 - Primer semestre

Índice

Guía de Aprendizaje

1. Datos descriptivos

1.1 Datos de la asignatura

Nombre de la Asignatura	615000520 - Codificacion de la informacion
Nº de Créditos	6 ECTS
Carácter	615000520
Curso	Tercero curso
Semestre	Quinto semestre
Período de impartición	Septiembre-Enero
Idioma de impartición	Inglés
Titulación	61IW - Grado en Ingenieria del Software
Centro en el que se imparte	Escuela Tecnica Superior de Ingenieria de Sistemas Informaticos
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

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

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

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 Resultados del aprendizaje al cursar la asignatura

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)

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

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

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. Introducción a la Codificación de la información
   1.1. Trasmisión de la Información.
   1.2. Tipos de Códigos.
   1.3. Códigos de Huffman.
   1.4. Códigos Lineales.
   1.5. Códigos de redundancia Cíclica
2. Introducción a la Criptología
   2.1. Criptografía y Criptosistemas
   2.2. Criptosistemas de clave secreta
   2.3. Criptoanálisis
3. Complejidad computacional
   3.1. Problemas, algoritmos.
   3.2. Complejidad de las operaciones aritméticas elementales
   3.3. Clasificación de problemas según su complejidad
4. Teoría de números
   4.1. El grupo multiplicativo de las unidades módulo n

4.2. Función ? de Euler

4.3. Teoremas de Euler y Fermat

4.4. Orden de un elemento. Raíz primitiva módulo n

4.5. Logaritmo discreto

5. Criptosistemas de clave pública

5.1. Protocolo de intercambio de claves de Diffie- Hellman

5.2. Criptosistema RSA

5.3. Criptosistema El Gamal

5.4. Firma digital

5.5. Otras aplicaciones de la criptografía de clave pública

6. Test de primalidad

6.1. Test deterministas: Criba de Eratóstenes y Divisiones sucesivas

6.2. Test probabilísticos: Test de Fermat, de Miller y de 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 **Moodle test** ET: Técnica del tipo Prueba TelemáticaEvaluación continua Duración: 00:20 **Written test, chapters 4,5, and 6** EX: Técnica del tipo Examen EscritoEvaluación continua Duración: 01:00 **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	CC7 CC6 CB3 CC1 CT12 CB1
3	Moodle test	ET: Técnica del tipo Prueba Telemática	No Presencial	00:20	2%	7 / 10	CC6 CB3 CC1 CB1 CC7 CT1
4	Lab project 2	TG: Técnica del tipo Trabajo en Grupo	No Presencial	00:00	5%	/ 10	CC7 CC6 CB3 CC1 CT12 CB1
4	Written test, chapter 1	EX: Técnica del tipo Examen Escrito	Presencial	01:00	8%	/ 10	CC7 CT1 CC6 CB3 CC1 CT2 CB1 CT4
6	Moodle test	ET: Técnica del tipo Prueba Telemática	No Presencial	00:20	2%	7 / 10	CC6 CB3 CC1 CB1 CC7 CT1
7	Lab project 3	TG: Técnica del tipo Trabajo en Grupo	No Presencial	00:00	5%	/ 10	CC7 CC6 CB3 CC1 CT2 CB1

8	Moodle test	ET: Técnica del tipo Prueba Telemática	No Presencial	00:20	2%	7 / 10	CC7 CT1 CC6 CB3 CC1 CB1
9	Written test, chapters 2 and 3	EX: Técnica del tipo Examen Escrito	Presencial	01:00	12%	/ 10	CC7 CT1 CC6 CB3 CC1 CT2 CB1 CT4
11	Moodle test	ET: Técnica del tipo Prueba Telemática	No Presencial	00:20	2%	7 / 10	CC7 CT1 CC6 CB3 CC1 CB1
13	Lab project 4	TG: Técnica del tipo Trabajo en Grupo	No Presencial	00:00	5%	/ 10	CC7 CC6 CB3 CC1 CT12 CB1
13	Moodle test	ET: Técnica del tipo Prueba Telemática	No Presencial	00:20	2%	7 / 10	CC7 CT1 CC6 CB3 CC1 CB1
16	Final lab project (Toolbox)	TI: Técnica del tipo Trabajo Individual	No Presencial	00:00	25%	/ 10	CC7 CC6 CB3 CC1 CT12 CB1 CT4
16	Moodle test	ET: Técnica del tipo Prueba Telemática	No Presencial	00:20	2%	7 / 10	CC7 CT1 CC6 CB3 CC1 CB1
16	Written test, chapters 4,5, and 6	EX: Técnica del tipo Examen Escrito	Presencial	01:00	20%	/ 10	CC7 CT1 CC6 CB3 CC1 CT2 CB1 CT4

16	Lab test	EP: Técnica del tipo Examen de Prácticas	Presencial	00:30	5%	/ 10	CC7 CC6 CB3 CC1 CT12 CT2 CB1

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	CC7 CT1 CC6 CB3 CC1 CT2 CB1 CT4
17	Final lab project (Toolbox)	TI: Técnica del tipo Trabajo Individual	No Presencial	00:00	%	/ 10	CC7 CC6 CB3 CC1 CT12 CB1

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	CC7 CT1 CC6 CB3 CC1 CT2 CB1 CT4
Final lab project (Toolbox)	TI: Técnica del tipo Trabajo Individual	No Presencial	00:00	%	/ 10	CC7 CC6 CB3 CC1 CT12 CB1

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. The learning outcomes assessed in each test are: Chapter 1, RA291, RA298, RA299; Chapter 2, RA294; Chapter 3, RA295; Chapter 4, RA296; Chapter 5, RA296 , RA290.
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. The learning outcomes assessed in each test are: Test 1, RA291, RA298, RA299 and RA293; Test 2, RA294, RA295 and RA293; test 3, RA296, RA290, RA292 and RA293.
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 precision, 10%. All lab projects assess the learning outcome RA297. Additional learning outcomes assessed in each project are: Project 1, RA299; Project 2, RA298; Project 3, RA295; Project 4, RA296 y RA290.
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 RA296, RA290, RA292, RA297.
Final version of the toolbox must be uploaded to Moodle before 22:00, December 22nd. Assessment: Procedures 60%, Documentations and help pages 40%. Mathematical rigour, language precision, elegance in results presentation will be taken into account. Learning outcome assessed: RA297.

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	