ANX-PR/CL/001-02

GUÍA DE APRENDIZAJE

ASIGNATURA

Codificacion de la informacion

CURSO ACADÉMICO - SEMESTRE

2015-16 - Primer semestre

Datos Descriptivos

Nombre de la Asignatura	Codificacion de la informacion
Titulación	61IF - Grado en Ingenieria del Software
Centro responsable de la titulación	E.T.S. de Ingenieria de Sistemas Informaticos
Semestre/s de impartición	Quinto semestre
Módulo	Modulo 4: materias optativas
Materia	Optativas
Carácter	Optativa
Código UPM	615000153
Nombre en inglés	Information Codes

Datos Generales

Créditos	6	**Curso**	3
Curso Académico	2015-16	**Período de impartición**	Septiembre-Enero
Idioma de impartición	Castellano	**Otros idiomas de impartición**	

Requisitos Previos Obligatorios

Asignaturas Superadas

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

Otros Requisitos

El plan de estudios Grado en Ingenieria del Software no tiene definidos otros requisitos para esta asignatura.

Conocimientos Previos

Asignaturas Previas Recomendadas

Algebra

Matematica discreta

Otros Conocimientos Previos Recomendados

Entender y hacer demostraciones matemáticas sencillas

Manejar con soltura la aritmética modular y el cálculo matricial

Competencias

E1. - Capacidad para desarrollar, mantener y evaluar servicios y sistemas software que satisfagan todos los requisitos del usuario y se comporten de forma fiable y eficiente, sean asequibles de desarrollar y mantener y cumplan normas de calidad, aplicando las teorías, principios, métodos y prácticas de la Ingeniería del Software.

G1. - Capacidad de análisis y síntesis

G3. - Comunicación oral y escrita

G5. - Uso de las tecnologías de la información y las comunicaciones

G6. - Resolución de problemas

G7. - Trabajo en equipo

I1 - 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

I19 - 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 i métodos numéricos; estadística y optimización

I21 - 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

I7 - Conocimiento, diseño y utilización de forma eficiente los tipos y estructuras de datos más adecuados a la resolución de un problema

Resultados de Aprendizaje

RA468 - Aplica los principales resultados de la teoría de números a la Criptología, cifrando y descifrando con los criptosistemas RSA y ElGamal.

RA469 - Utiliza adecuadamente software para la resolución de problemas de codificación de la información, describiendo con precisión los protocolos utilizados.

RA380 - Codifica, detecta y corrige errores utilizando los códigos lineales.

RA381 - Comprime ficheros, usando códigos compresores adecuados.

RA387 - Conoce y aplica protocolos de autenticación (firma digital) e intercambio de claves basados en criptosistemas de clave pública

RA379 - Utiliza los distintos tipos de codificación de la información según el objetivo perseguido (corregir errores, encriptar información o comprimirla)

RA388 - Conoce y aplica test de primalidad deterministas y probabilísticos

RA241 - 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.

RA466 - Distingue criptosistemas de clave pública y clave privada. Cifra y descifra utilizando los criptosistemas de traslación, afín y matricial afín.

RA467 - Determina la complejidad computacional de algoritmos sencillos que involucren operaciones aritméticas elementales.

Profesorado

Profesorado

Nombre	Despacho	e-mail	Tutorías
Pozo Coronado, Luis Miguel **(Coordinador/a)**	2003	lm.pozo@upm.es	El horario de tutorías se anunciará a principio del cuatrimestre en los tablones y en Moodle

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

Descripción de la Asignatura

En esta asignatura tratamos las distintas formas de codificar numéricamente la información en función del objetivo perseguido: concisión (códigos compresores), integridad (códigos detectores de errores) o seguridad (criptografía). Se explican los fundamentos matemáticos de los modelos utilizados y se implementan dichos modelos, atendiendo especialmente a criterios de eficiencia y seguridad.

Temario

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

Cronograma

Horas totales: 65 horas y 40 minutos

Horas presenciales: 64 horas (41%)

Peso total de actividades de evaluación continua: 100%

Peso total de actividades de evaluación sólo prueba final: 100%

Semana	Actividad Prensencial en Aula	Actividad Prensencial en Laboratorio	Otra Actividad Presencial	Actividades Evaluación
Semana 1	**Clase de teoría y ejercicios en aula** Duración: 02:00 LM: Actividad del tipo Lección Magistral			
Semana 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		
Semana 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		**Entrega de prácticas por parejas** Duración: 00:00 TG: Técnica del tipo Trabajo en Grupo Evaluación continua Actividad no presencial **Test de Moodle** Duración: 00:20 ET: Técnica del tipo Prueba Telemática Evaluación continua Actividad no presencial
Semana 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		**Entrega de prácticas por parejas** Duración: 00:00 TG: Técnica del tipo Trabajo en Grupo Evaluación continua Actividad no presencial **Examen T1** Duración: 01:00 EX: Técnica del tipo Examen Escrito Evaluación continua Actividad presencial
Semana 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		
Semana 6	**Clase de teoría y ejercicios en aula** Duración: 04:00 LM: Actividad del tipo Lección Magistral			**Test de Moodle** Duración: 00:20 ET: Técnica del tipo Prueba Telemática Evaluación continua Actividad no presencial
Semana 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		**Entrega de prácticas por parejas** Duración: 00:00 TG: Técnica del tipo Trabajo en Grupo Evaluación continua Actividad no presencial

Semana 8	**Clase de teoría y ejercicios en aula** Duración: 04:00 LM: Actividad del tipo Lección Magistral			**Test de Moodle** Duración: 00:20 ET: Técnica del tipo Prueba Telemática Evaluación continua Actividad no presencial
Semana 9	**Clase de teoría y ejercicios en aula** Duración: 04:00 LM: Actividad del tipo Lección Magistral			**Examen T2,T3** Duración: 01:00 EX: Técnica del tipo Examen Escrito Evaluación continua Actividad presencial
Semana 10	**Clase de teoría y ejercicios en aula** Duración: 04:00 LM: Actividad del tipo Lección Magistral			
Semana 11	**Clase de teoría y ejercicios en aula** Duración: 04:00 LM: Actividad del tipo Lección Magistral			**Test de Moodle** Duración: 00:20 ET: Técnica del tipo Prueba Telemática Evaluación continua Actividad no presencial
Semana 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		
Semana 13	**Clase de teoría y ejercicios en aula** Duración: 04:00 LM: Actividad del tipo Lección Magistral			**Entrega de prácticas por parejas** Duración: 00:00 TG: Técnica del tipo Trabajo en Grupo Evaluación continua Actividad no presencial **Test de Moodle** Duración: 00:20 ET: Técnica del tipo Prueba Telemática Evaluación continua Actividad no presencial
Semana 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		
Semana 15	**Clase de teoría y ejercicios en aula** Duración: 04:00 LM: Actividad del tipo Lección Magistral			

Semana 16	**Clase de teoría y ejercicios en aula** Duración: 02:00 LM: Actividad del tipo Lección Magistral			**Proyecto TOOLBOX** Duración: 00:00 TI: Técnica del tipo Trabajo Individual Evaluación continua Actividad no presencial **Examen T4,T5,T6** Duración: 01:00 EX: Técnica del tipo Examen Escrito Evaluación continua Actividad presencial **Examen de prácticas** Duración: 01:00 EP: Técnica del tipo Examen de Prácticas Evaluación continua Actividad presencial
Semana 17				**Examen Final** Duración: 02:00 EX: Técnica del tipo Examen Escrito Evaluación sólo prueba final Actividad presencial **Proyecto TOOLBOX** Duración: 00:00 TI: Técnica del tipo Trabajo Individual Evaluación sólo prueba final Actividad no presencial

Nota.- El cronograma sigue una planificación teórica de la asignatura que puede sufrir modificaciones durante el curso.

Nota 2.- Para poder calcular correctamente la dedicación de un alumno, la duración de las actividades que se repiten en el tiempo (por ejemplo, subgrupos de prácticas") únicamente se indican la primera vez que se definen.

Actividades de Evaluación

Semana	Descripción	Duración	Tipo evaluación	Técnica evaluativa	Presencial	Peso	Nota mínima	Competencias evaluadas
3	Entrega de prácticas por parejas	00:00	Evaluación continua	TG: Técnica del tipo Trabajo en Grupo	No	5%		I21, G3., I1, G7., G5., I7
3	Test de Moodle	00:20	Evaluación continua	ET: Técnica del tipo Prueba Telemática	No	2%	7 / 10	I19, I7, I21
4	Entrega de prácticas por parejas	00:00	Evaluación continua	TG: Técnica del tipo Trabajo en Grupo	No	5%		I21, G3., G5., G7., I1, I7
4	Examen T1	01:00	Evaluación continua	EX: Técnica del tipo Examen Escrito	Sí	8%		I19, G3., G6., G1., I21, I7
6	Test de Moodle	00:20	Evaluación continua	ET: Técnica del tipo Prueba Telemática	No	2%	7 / 10	I7, I21, I19
7	Entrega de prácticas por parejas	00:00	Evaluación continua	TG: Técnica del tipo Trabajo en Grupo	No	5%		I21, G3., G5., G7., I1, I7
8	Test de Moodle	00:20	Evaluación continua	ET: Técnica del tipo Prueba Telemática	No	2%	7 / 10	I7, I21, I19
9	Examen T2,T3	01:00	Evaluación continua	EX: Técnica del tipo Examen Escrito	Sí	12%		G6., I19, I21, G1., G3.
11	Test de Moodle	00:20	Evaluación continua	ET: Técnica del tipo Prueba Telemática	No	2%	7 / 10	I19, I21, I7
13	Entrega de prácticas por parejas	00:00	Evaluación continua	TG: Técnica del tipo Trabajo en Grupo	No	5%		I1, I21, G3., G7., G5., I7
13	Test de Moodle	00:20	Evaluación continua	ET: Técnica del tipo Prueba Telemática	No	2%	7 / 10	I7, I21, I19
16	Proyecto TOOLBOX	00:00	Evaluación continua	TI: Técnica del tipo Trabajo Individual	No	25%		I1, I21, G5., I7, E1., G3.
16	Examen T4,T5,T6	01:00	Evaluación continua	EX: Técnica del tipo Examen Escrito	Sí	20%		G1., G3., G6., I7, I19, I21, I1
16	Examen de prácticas	01:00	Evaluación continua	EP: Técnica del tipo Examen de Prácticas	Sí	5%		G3., G6., I21, G5., I7
17	Examen Final	02:00	Evaluación sólo prueba final	EX: Técnica del tipo Examen Escrito	Sí	100%		I19, G3., G6., I1, I21, G1., I7
17	Proyecto TOOLBOX	00:00	Evaluación sólo prueba final	TI: Técnica del tipo Trabajo Individual	No			E1., G3., G5., G7., I1, I7, I21

Criterios de Evaluación

PARA LA OPCIÓN DE EVALUACIÓN CONTINUA

Cuestionarios on line: Los estudiantes podrán realizar un cuestionario on-line, con diez preguntas sobre cada tema del curso. Cuando la calificación de dicho cuestionario sea igual o superior a 7 se sumará 0.2 a la nota final acumulada, hasta un máximo de un punto. Los resultados de aprendizaje evaluados en cada cuestionario son los siguientes: Tema 1, RA379, RA380,RA381; tema 2, RA466; tema 3, RA467; tema 4, RA468; Tema 5, RA468 y RA 387.

Pruebas escritas de evaluación continua: Se realizan en horario presencial y en ellas los estudiantes deben responder a

cuestiones teóricas y resolver ejercicios y problemas. En la calificación, al menos el 70% corresponderá a logros de objetivos básicos y se exigirá precisión en el lenguaje y rigor en la presentación de resultados. Los resultados de aprendizaje evaluados en cada prueba son: Prueba 1, RA379, RA380, RA381 y RA241; prueba 2, RA466, RA467 y RA241; prueba 3, RA468, RA387, RA388 y RA241.

Entrega de prácticas: Se deberán entregar resueltas 4 prácticas realizadas a lo largo del curso. Se realizarán por parejas y la contribución de cada una de ellas a la nota final es de 5%, para la evaluación continua.Valoración de cada práctica: Procedimientos definidos 50% (valorando eficiencia, claridad y documentación del código), resolución de los ejercicios 40%, rigor matemático, elegancia en la presentación de resultados y precisión en el lenguaje 10%. En todas las prácticas se evalúa el resultado de aprendizaje RA469. Los resultados de aprendizaje adicionales que son evaluados en cada práctica son: Práctica 2, RA381; práctica 3, RA380; práctica 5, RA467; práctica 7, RA468 y RA387.

Proyecto Toolbox-CI: Lo deben realizar todos los alumnos individualmente y consistirá en hacer una librería Maple, que incluya las funciones programadas a lo largo del curso y las páginas de ayuda correspondientes.Se publicará en Moodle un documento de especificaciones con la tabla de funciones que debe contener obligatoriamente la librería. A mediados de noviembre se entregará una primera versión del proyecto, que se devolverá corregida, con sugerencias de mejora.

La última semana lectiva cada estudiante realizará una pequeña prueba de validación consistente en el uso de las funciones de la propia librería CI, para resolver algún ejercicio o problema, que además se evaluará con un 5%. Los resultados de aprendizaje evaluados son RA468, RA387, RA388y RA469.

La versión definitiva de la librería (documentos CI.m y Ayuda.hdb) se subirán a Moodle antes de las 22 horas del día 22-12.Valoración: Procedimientos definidos 60%, construcción de la librería y páginas de ayuda 40%. Se tendrá en cuenta el rigor matemático, elegancia en la presentación de resultados y precisión en el lenguaje. Resultado de aprendizaje evaluado: RA469.

PARA LA ALTERNATIVA DE EVALUACIÓN MEDIANTE SÓLO PRUEBA FINAL Y LA CONVOCATORIA EXTRAORDINARIA

Los alumnos que elijan la opción de examen único deberán solicitarlo antes del día 21 de noviembre.El examen final se realizará en la fecha marcada por la Jefatura de estudios y tendrá dos partes: una prueba escrita relativa a los contenidos teóricos de la asignatura (definiciones, propiedades, ejercicios y problemas) y una práctica. El valor de cada una de estas dos partes es del 50% de la nota final. Para la parte práctica deberán traer y podrán usar la librería Maple Toolbox-CI construida

Recursos Didácticos

Descripción	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	
Rincón, Félix; García, Alfonsa; Martínez, Ángeles: "Cálculo científico con Maple". RA-MA. 1995	Bibliografía	
Trappe, Wade; Washington, Lawrence C.: "Introduction to Crytography with Coding Theory". Prentice-Hall. 2002	Bibliografía	
Entorno Moodle de la UPM: http://moodle.upm.es/titulaciones/oficiales/	Recursos web	Contiene información y material de apoyo
Instrumentación de laboratorio: Ordenadores personales	Equipamiento	
Aplicaciones software: Maple, Moodle	Equipamiento	