ANX-PR/CL/001-01

GUÍA DE APRENDIZAJE

ASIGNATURA

Teoria de codigos y criptografia

CURSO ACADÉMICO - SEMESTRE

2016-17 - Segundo semestre

Datos Descriptivos

Nombre de la Asignatura	Teoria de codigos y criptografia
Titulación	10MI - Grado en Matematicas e Informatica
Centro responsable de la titulación	Escuela Tecnica Superior de Ingenieros Informaticos
Semestre/s de impartición	Octavo semestre
Materias	Optatividad
Carácter	Optativa
Código UPM	105000146
Nombre en inglés	Coding theory and cryptography

Datos Generales

Créditos	6	**Curso**	4
Curso Académico	2016-17	**Período de impartición**	Febrero-Junio
Idioma de impartición	Castellano	**Otros idiomas de impartición**	

Requisitos Previos Obligatorios

Asignaturas Previas Requeridas

El plan de estudios Grado en Matematicas e Informatica no tiene definidas asignaturas previas superadas para esta asignatura.

Otros Requisitos

El plan de estudios Grado en Matematicas e Informatica no tiene definidos otros requisitos para esta asignatura.

Conocimientos Previos

Asignaturas Previas Recomendadas

El coordinador de la asignatura no ha definido asignaturas previas recomendadas.

Otros Conocimientos Previos Recomendados

Haber cursado el tercer curso del Grado en Matemáticas e Informática

Competencias

CE25 - Conocer los campos de aplicación de las matemáticas y la informática, y tener una apreciación de la necesidad de poseer unos conocimientos técnicos profundos en ciertas áreas de aplicación; apreciación del grado de esta necesidad en, por lo menos, una situación.

CE26 - Conocimiento de los tipos apropiados de soluciones, y comprensión de la complejidad de los problemas informáticos y la viabilidad de su solución.

CE37 - Combinar la teoría y la práctica para realizar tareas informáticas.

CE38 - Capacidad de realizar búsquedas bibliográficas y de utilizar bases de datos y otras fuentes de información.

CE39 - Conocimiento de tecnologías punteras relevantes y su aplicación.

CE43 - Capacidad para trabajar de forma efectiva como individuo, organizando y planificando su propio trabajo, de forma independiente o como miembro de un equipo.

CG01 - Capacidad de resolución de problemas aplicando conocimientos de matemáticas, ciencias e ingeniería.

CG02 - Capacidad para el aprendizaje autónomo y la actualización de conocimientos, y reconocimiento de su necesidad en las áreas de la matemática y la informática.

CG03 - Saber trabajar en situaciones carentes de información y bajo presión, teniendo nuevas ideas, siendo creativo.

CG04 - Capacidad de gestión de la información.

CG05 - Capacidad de abstracción, análisis y síntesis.

CG06 - Capacidad para trabajar dentro de un equipo, organizando, planificando, tomando decisiones, negociando y resolviendo conflictos, relacionándose, y criticando y haciendo autocrítica.

CG08 - Capacidad de comunicarse de forma efectiva con los compañeros, usuarios (potenciales) y el público en general acerca de cuestiones reales y problemas relacionados con la especialización elegida.

CG10 - Capacidad para usar las tecnologías de la información y la comunicación.

Resultados de Aprendizaje

RA120 - Dado un campo de aplicación de las matemáticas o de la informática, evaluar y diseñar la solución más apropiada para resolver alguno de sus problemas, exponiendo las dificultades técnicas y los limites de la aplicación.

RA121 - Dado un problema real elegir las herramientas matemáticas o la tecnología informática más apropiada para su solución y diseñar su desarrollo e integración, analizando la viabilidad de su solución.

RA122 - Desarrollar la solución matemática y algorítmica mas apropiada a un problema matemático o informático que requiera un tratamiento especialmente complejo, analizando y exponiendo su viabilidad.

RA123 - Conocer alguno de los campos situados en la frontera entre las matemáticas y la informática, que están en la base de nuevas tendencias y desarrollos.

Profesorado

Profesorado

Nombre	Despacho	e-mail	Tutorías
Sanchez Avila, Maria Del Carmen	A-305	carmen.sanchez.avila@upm.es	
Martin Garcia, Lorenzo Javier **(Coordinador/a)**	A-307	lorenzojavier.martin@upm.es	

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

Temario

1. Codificación de la información
   1.1. Códigos decodificables de manera única
   1.2. Códigos instantáneos y construcción
   1.3. Desigualdades de Kraft y McMillan
2. Códigos correctores de errores
   2.1. Distancia mínima
   2.2. Cotas de Hamming y Gilbert-Varshamov
   2.3. Matrices de Hadamard
3. Códigos lineales
   3.1. Descripción matricial
   3.2. Equivalencia entre códigos lineales
   3.3. Códigos Hamming
   3.4. Códigos de Golay
   3.5. Array standard y decodificación por síndrome
4. Códigos cíclicos y convolucionales
   4.1. Polinomio generador
   4.2. Códigos de BCH
   4.3. Implementación práctica de códigos convolucionales
   4.4. Decodificación mediante el algoritmo de Viterbi
5. Introducción a la Criptografía
   5.1. Antecedentes históricos
   5.2. Clasificación de los criptosistemas
   5.3. Criptoanálisis
   5.4. Aspectos legales
6. Criptografía de clave simétrica
   6.1. Principios
   6.2. Cifradores en bloque y cifradores en flujo
   6.3. Modos de operación
   6.4. Criptoanálisis

7. Criptografía de clave asimétrica

   7.1. Intercambio de clave de Diffie-Hellman

   7.2. Sistemas de cifrado de clave asimétrica

   7.3. Criptoanálisis

8. Funciones de autenticación

   8.1. Principios

   8.2. Funciones Hash

   8.3. Criptoanálisis

9. Firma digital y certificados

   9.1. Propiedades y principio

   9.2. Esquemas de firma digital

   9.3. Certificados digitales

Cronograma

Horas totales: 72 horas

Horas presenciales: 72 horas (46.2%)

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	**Tema 1: presentación de la teoría y ejercicios** Duración: 02:00 LM: Actividad del tipo Lección Magistral **Tema 1: presentación de la teoría y ejercicios** Duración: 02:00 PR: Actividad del tipo Clase de Problemas			
Semana 2	**Tema 1: presentación de la teoría y ejercicios** Duración: 02:00 LM: Actividad del tipo Lección Magistral **Tema 1: presentación de la teoría y ejercicios** Duración: 02:00 PR: Actividad del tipo Clase de Problemas			
Semana 3	**Tema 2: presentación de la teoría y ejercicios** Duración: 02:00 LM: Actividad del tipo Lección Magistral **Tema 2: presentación de la teoría y ejercicios** Duración: 02:00 PR: Actividad del tipo Clase de Problemas			
Semana 4	**Tema 2: presentación de la teoría y ejercicios** Duración: 02:00 LM: Actividad del tipo Lección Magistral **Tema 2: presentación de la teoría y ejercicios** Duración: 02:00 PR: Actividad del tipo Clase de Problemas			
Semana 5	**Tema 3: presentación de la teoría y ejercicios** Duración: 02:00 LM: Actividad del tipo Lección Magistral **Tema 3: presentación de la teoría y ejercicios** Duración: 02:00 PR: Actividad del tipo Clase de Problemas			

Semana 6	**Tema 3: presentación de la teoría y ejercicios** Duración: 02:00 LM: Actividad del tipo Lección Magistral **Tema 3: presentación de la teoría y ejercicios** Duración: 02:00 PR: Actividad del tipo Clase de Problemas			
Semana 7	**Tema 4: presentación de la teoría y ejercicios** Duración: 02:00 LM: Actividad del tipo Lección Magistral **Tema 4: presentación de la teoría y ejercicios** Duración: 02:00 PR: Actividad del tipo Clase de Problemas			
Semana 8	**Tema 4: presentación de la teoría y ejercicios** Duración: 01:00 LM: Actividad del tipo Lección Magistral **Tema 4: presentación de la teoría y ejercicios** Duración: 01:00 PR: Actividad del tipo Clase de Problemas			**Realización y entrega de un trabajo sobre codificación** Duración: 03:00 TG: Técnica del tipo Trabajo en Grupo Evaluación continua Actividad presencial **Examen** Duración: 03:00 OT: Otras técnicas evaluativas Evaluación continua Actividad presencial
Semana 9	**Tema 5: presentación de la teoría y ejercicios** Duración: 04:00 LM: Actividad del tipo Lección Magistral			
Semana 10	**Tema 6: presentación de la teoría y ejercicios** Duración: 02:00 LM: Actividad del tipo Lección Magistral **Tema 6: presentación de la teoría y ejercicios** Duración: 02:00 PR: Actividad del tipo Clase de Problemas			
Semana 11	**Tema 7: presentación de la teoría y ejercicios** Duración: 02:00 LM: Actividad del tipo Lección Magistral **Tema 7: presentación de la teoría y ejercicios** Duración: 02:00 PR: Actividad del tipo Clase de Problemas			

Semana 12	**Tema 7: presentación de la teoría y ejercicios** Duración: 02:00 LM: Actividad del tipo Lección Magistral **Tema 7: presentación de la teoría y ejercicios** Duración: 02:00 PR: Actividad del tipo Clase de Problemas			
Semana 13	**Tema 8: presentación de la teoría y ejercicios** Duración: 02:00 LM: Actividad del tipo Lección Magistral **Tema 8: presentación de la teoría y ejercicios** Duración: 02:00 PR: Actividad del tipo Clase de Problemas			
Semana 14	**Tema 9: presentación de la teoría y ejercicios** Duración: 02:00 LM: Actividad del tipo Lección Magistral **Tema 9: presentación de la teoría y ejercicios** Duración: 02:00 PR: Actividad del tipo Clase de Problemas			
Semana 15	**Repaso de los temas 5 al 9** Duración: 02:00 OT: Otras actividades formativas			**Realización y entrega de un trabajo sobre Criptografía** Duración: 03:00 TG: Técnica del tipo Trabajo en Grupo Evaluación continua Actividad presencial **Examen** Duración: 03:00 EX: Técnica del tipo Examen Escrito Evaluación continua Actividad presencial
Semana 16		**Sesión de prácticas de Codificación** Duración: 02:00 PL: Actividad del tipo Prácticas de Laboratorio **Sesión de prácticas de Criptografía** Duración: 02:00 PL: Actividad del tipo Prácticas de Laboratorio		
Semana 17				**Examen final** Duración: 02:00 EX: Técnica del tipo Examen Escrito Evaluación sólo prueba final Actividad 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
8	Realización y entrega de un trabajo sobre codificación	03:00	Evaluación continua	TG: Técnica del tipo Trabajo en Grupo	Sí	20%	4 / 10	CG01, CG02, CG04, CG05, CG06, CG08, CG10, CE25, CE26, CE37, CE38, CE39, CE43
8	Examen	03:00	Evaluación continua	OT: Otras técnicas evaluativas	Sí	30%	4 / 10	CG03, CG01, CG04, CG05, CE25, CE26, CE37, CE39, CE43
15	Realización y entrega de un trabajo sobre Criptografía	03:00	Evaluación continua	TG: Técnica del tipo Trabajo en Grupo	Sí	20%	4 / 10	CG01, CG02, CG04, CG05, CG06, CG08, CG10, CE25, CE26, CE37, CE38, CE39, CE43
15	Examen	03:00	Evaluación continua	EX: Técnica del tipo Examen Escrito	Sí	30%	4 / 10	CG03, CG01, CG04, CG05, CE25, CE26, CE37, CE39, CE43
17	Examen final	02:00	Evaluación sólo prueba final	EX: Técnica del tipo Examen Escrito	Sí	100%	5 / 10	CG03, CG01, CG02, CG04, CG05, CG06, CG08, CG10, CE25, CE26, CE37, CE38, CE39, CE43

Criterios de Evaluación

Convocatoria ordinaria

- Sistema general de evaluación continua: La asignatura puede considerarse dividida en dos partes independientes: Codificación y Criptografía. Cada parte se evaluará mediante un trabajo que puede aportar hasta un 20% de la nota final y un examen que puede aportar hasta un 30% de la nota final. El examen de la parte de Codificación consistirá en la realización de cuatro pruebas en la plataforma Moodle de la asignatura. El examen de la parte de Criptografía será presencial y escrito. La asignatura se considerará superada si se obtiene más de un 40% de la nota que aporta cada parte y más de un 50% de la nota total.
- Sistema de evaluación mediante sólo prueba final: El alumno que desee seguir el sistema de evaluación mediante sólo prueba final, deberá comunicarlo de la manera establecida. Este sistema de evaluación mediante sólo prueba final, consistirá en la realización de una prueba presencial que abarcará el temario completo de la asignatura. La asignatura se considerará superada si se obtiene más de un 50% de la nota total.

Convocatoria extraordinaria de julio

Seguirá el mismo esquema que la evaluación mediante sólo prueba final.

Recursos Didácticos

Descripción	Tipo	Observaciones
Página Moodle de la asignatura	Recursos web	Toda la información de la asignatura se gestionará mediante el recurso Moodle de la asignatura en Politécnica Virtual
G.A. Jones; M.Jones: Information and Coding theory. Springer-Verlag. Londres, 2000	Bibliografía	Libro recomendado para Codificación
S.Lin, D.J. Costello, Error Control Coding, Prentice-Hall, 2004	Bibliografía	Libro recomendado para Codificación
Alfred J. Menezes, Paul C. van Oorschot and Scott A. Vanstone, Handbook of Applied Cryptography, CRC Press, 2001. (http://cacr.uwaterloo.ca/hac/)	Bibliografía	Libro recomendado para Criptografía
D. Stinson, Cryptography. Theory and Practice, CRC Press, 1995	Bibliografía	Libro recomendado para Criptografía
Material elaborado por los profesores de la asignatura	Otros	Colección de problemas, apuntes, transparencias, etc. disponible en la plataforma Moodle de la asignatura

Otra Información

Codificación de algoritmos en Maple: En cada uno de los temas se explorarán y utilizarán las herramientas que proporciona Maple para realizar simulaciones.