Datos Descriptivos

ASIGNATURA:	**Teoría de códigos y Criptografía**
MATERIA:	**OPTATIVIDAD**
CRÉDITOS EUROPEOS:	**6**
CARÁCTER:	**Optativa**
TITULACIÓN:	**Grado en Matemáticas e Informática**
CURSO/SEMESTRE	**Curso 4º / Semestre 2º**
ESPECIALIDAD:	**No aplica**

CURSO ACADÉMICO	**2013/2014**		
PERIODO IMPARTICION	**Septiembre- Enero**	**Febrero - Junio**	
		X	
IDIOMA IMPARTICIÓN	**Sólo castellano**	**Sólo inglés**	**Ambos**
	X		

DEPARTAMENTO:	Matemática Aplicada a las TT.II., E.T.S.I. Telecomunicación

PROFESORADO		
NOMBRE Y APELLIDO (C = Coordinador)	**DTO-Centro**	**Correo electrónico**
Francisco Ballesteros Olmo	**DMA-ETSIT**	francisco.ballesteros@upm.es
Lorenzo Javier Martín García (C)	**DMA-ETSIT**	lorenzojavier.martin@upm.es
Carmen Sánchez Ávila	**DMA-ETSIT**	carmen.sanchez.avila@upm.es

CONOCIMIENTOS PREVIOS REQUERIDOS PARA PODER SEGUIR CON NORMALIDAD LA ASIGNATURA	
ASIGNATURAS SUPERADAS	**Haber completado tercer curso**
OTROS RESULTADOS DE APRENDIZAJE NECESARIOS	

Objetivos de Aprendizaje

COMPETENCIAS Y NIVEL ASIGNADAS A LA ASIGNATURA		
Código	**COMPETENCIA**	**NIVEL**
CE-25	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.	3
CE-26	Conocimiento de los tipos apropiados de soluciones, y comprensión de la complejidad de los problemas informáticos y la viabilidad de su solución.	3
CE-37	Combinar la teoría y la práctica para realizar tareas informáticas.	3
CE-38	Capacidad de realizar búsquedas bibliográficas y de utilizar bases de datos y otras fuentes de información.	3
CE-39	Conocimiento de tecnologías punteras relevantes y su aplicación.	3
CE-43	Capacidad para trabajar de forma efectiva como individuo, organizando y planificando su propio trabajo, de forma independiente o como miembro de un equipo.	3
CG-01	Capacidad de resolución de problemas aplicando conocimientos de matemáticas, ciencias e ingeniería.	3
CG-02	Capacidad para el aprendizaje autónomo y la actualización de conocimientos, y reconocimiento de su necesidad en las áreas de la matemática y la informática.	3
CG-03	Saber trabajar en situaciones carentes de información y bajo presión, teniendo nuevas ideas, siendo creativo.	3
CG-04	Capacidad de gestión de la información.	3
CG-05	Capacidad de abstracción, análisis y síntesis.	3
CG-06	Capacidad para trabajar dentro de un equipo, organizando, planificando, tomando decisiones, negociando y resolviendo conflictos, relacionándose, y criticando y haciendo autocrítica.	3
CG-08	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.	3
CG-10	Capacidad para usar las tecnologías de la información y la comunicación.	3

Código	RESULTADOS DE APRENDIZAJE DE LA ASIGNATURA
RA1.	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 límites de la aplicación.
RA2.	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.
RA3.	Desarrollar la solución matemática y algorítmica más apropiada a un problema matemático o informático que requiera un tratamiento especialmente complejo, analizando y exponiendo su viabilidad.
RA4.	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.

Contenidos y Actividades de Aprendizaje

CONTENIDOS ESPECÍFICOS (TEMARIO)		
TEMA / CAPITULO	**APARTADO**	**Indicadores Relacionados**
1. Codificación de la información	1.1. Códigos decodificables de manera única	I01
	1.2. Códigos instantáneos y construcción	I01
	1.3. Desigualdades de Kraft y McMillan	I01
2. Códigos correctores de errores	2.1. Distancia mínima	I01,I02
	2.2. Cotas de Hamming y Gilbert-Varshamov	I01, I02
	2.3. Matrices de Hadamard	I01, I02
3. Códigos lineales	3.1. Descripción matricial	I01, I02, I03
	3.2. Equivalencia entre códigos lineales	I02, I03
	3.3. Códigos Hamming	I03
	3.4. Códigos de Golay	I03
	3.5. Array standard y decodificación por síndrome	I02, I03
4. Códigos cíclicos y convolucionales	4.1. Polinomio generador	I02, I04
	4.2. Códigos de BCH	I04
	4.3. Implementación práctica de códigos convolucionales	I02, I05
	4.4.Decodificación mediante el algoritmo de Viterbi	I05
5. Introducción a la Criptografía	5.1 Antecedentes históricos	I06, I07
	5.2 Clasificación de los criptosistemas	I06, I07
	5.3 Criptoanálisis	I06, I07
6. Sistemas de clave privada	6.1 Principios	I08
	6.2 Cifradores en bloque: algoritmos	I08, I09
	6.3 Cifradores en flujo: algoritmos	I08, I09
7. Sistemas de clave pública	7.1 Intercambio de clave de Diffie-Hellman	I08
	7.2 Sistemas de cifrado de clave pública	I08, I09
	7.3 Funciones de autenticación	I08, I09, I10
	7.4 Firmas digitales	I08, I09, I10
8. Codificación de algoritmos en Maple	En cada uno de los temas se explorarán y utilizarán las herramientas que proporciona Maple para realizar simulaciones.	I03, I04, I05, I08, I09, I10

BREVE DESCRIPCIÓN DE LAS MODALIDADES ORGANIZATIVAS UTILIZADAS Y METODOS DE ENSEÑANZA EMPLEADOS	
Clases Teóricas	Método expositivo Lección magistral
Estudio y trabajo autónomo individual	Realizado por el alumno a partir de la documentación de la asignatura, incluye la implementación de algoritmos en un lenguaje de programación para efectuar simulaciones numéricas.
Clases prácticas	Método expositivo (directrices para realización de ejercicios). Realización individual de ejercicios bajo la supervisión del profesor. Resolución de ejercicios y de problemas y control de simulaciones numéricas.
Tutorías	Individuales y en grupo. Consultas a través de las páginas web de la asignatura (Moodle, etc.)
Estudio y trabajo en grupo	Realizado por los alumnos a partir de la documentación de la asignatura, incluye la implementación de algoritmos en un lenguaje de programación para efectuar simulaciones numéricas.
Prácticas individuales o en grupo	Realizadas en el aula sobre ejercicios propuestos, o fuera de ella a partir de la documentación de la asignatura.
Proyectos	Realizados para la evaluación de la asignatura

RECURSOS DIDÁCTICOS	
BIBLIOGRAFÍA	F.J MacWilliams, The theory of error-correcting codes, North Holland, 1977.
	L.C. Washington , Elliptic Curves: Number Theory and Cryptography, Chapman-Hall, 2003.
	G.A. Jones; M.Jones: Information and Coding theory. Springer-Verlag. Londres, 2000.
	S.Lin, D.J. Costello, Error Control Coding, Prentice-Hall, 2004.
	A. J. Menezes, P. C. van Oorschot and S. A. Vanstone, Handbook of Applied Cryptography (Discrete Mathematics and Its Applications), CRC Press, 1996.
	D. Hankerson, A. Menezes and S. Vanstone, Guide to Elliptic Curve Cryptography, Springer, 2003.
	Sheneier, Applied Cryptography: Protocols, Algorithms, and Source Code in C, John Wiley & Sons, 1996.
	R. Durán, L. Encinas, J. Muñoz, El Criptosistema RSA, Ra-Ma, 2005.
RECURSOS WEB	Página Moodle de la asignatura
	Otros

Cronograma de trabajo de la asignatura

Semana	Actividades Aula	Laboratorio	Trabajo Individual	Trabajo en Grupo	Actividades Evaluación	Otros
1 y 2	Tema 1: presentación de la teoría y ejercicios (8 horas).		Estudio y/o resolución de ejercicios (8 horas).	Resolución de ejercicios (3 horas)		
3 y 4	Tema 2: presentación de la teoría y ejercicios (8 horas).		Estudio y/o resolución de ejercicios (8 horas)	Resolución de ejercicios (4 horas)		
5 y 6	Tema 3: presentación de la teoría y ejercicios (8 horas).		Estudio y/o resolución de ejercicios (8 horas)	Resolución de ejercicios (4 horas)		
7	Tema 4: presentación de la teoría y ejercicios (4 horas).		Estudio y/o resolución de ejercicios (4 horas)	Resolución de ejercicios (2 horas)		
8	Tema 4: presentación de la teoría y ejercicios (2 horas). Examen presencial (2 horas)		Estudio y/o resolución de ejercicios (8 horas)	Resolución de ejercicios (4 horas)	Entrega de trabajo sobre Codificación Examen presencial	
9 y 10	Tema 5: presentación de la teoría y ejercicios (8 horas).		Estudio y/o resolución de ejercicios (8 horas).	Resolución de ejercicios (4 horas)		
11 y 12	Tema 6: presentación de la teoría y ejercicios (8 horas).		Estudio y/o resolución de ejercicios (8 horas)	Resolución de ejercicios (4 horas)		

Semana	Actividades Aula	Laboratorio	Trabajo Individual	Trabajo en Grupo	Actividades Evaluación	Otros
13 y 14	Tema 7: presentación de la teoría y ejercicios (8 horas).		Estudio y/o resolución de ejercicios (8 horas)	Resolución de ejercicios (3 horas)		
15	Repaso (2 horas). Examen presencial (2 horas)		Estudio y/o resolución de ejercicios (8 horas)	Resolución de ejercicios (4 horas)	Entrega de trabajo sobre Criptografía Examen presencial	

En total 160 horas: 60 presenciales y 100 de trabajo del alumno (68 individuales y 32 en grupo)

Sistema de evaluación de la asignatura

EVALUACION		
Ref	**INDICADOR DE LOGRO**	**Relacionado con RA:**
I.01	Conocer las características elementales de los procesos de codificación de la información.	RA4
I.02	Comprender el funcionamiento de los códigos detectores y correctores de errores.	RA4
I.03	Aplicar los mecanismos de detección-corrección en códigos lineales.	RA1, RA2, RA3
I.04	Generar códigos cíclicos.	RA1, RA2, RA3
I.05	Codificar y decodificar utilizando códigos convolucionales.	RA1, RA2, RA3
I.06	Conocer y comprender los fundamentos de la Criptografía y el Criptoanálisis	RA4
I.07	Conocer y comprender los principios básicos de las técnicas criptográficas más importantes.	RA4
I.08	Analizar los algoritmos y protocolos básicos de los criptosistemas de clave pública y clave privada más importantes y saber aplicarlos.	RA1, RA2, RA3
I.09	Conocer las aplicaciones más ilustrativas de los criptosistemas de clave pública y clave privada.	RA1, RA2, RA3
I.10	Comprender el funcionamiento de las firmas digitales y de los certificados.	RA1, RA2, RA3, RA4

EVALUACION SUMATIVA			
BREVE DESCRIPCION DE LAS ACTIVIDADES EVALUABLES	**MOMENTO**	**LUGAR**	**PESO EN LA CALIFICACIÓN**
Entrega de un trabajo sobre Codificación	Semana 8	Aula	20%
Realización de un examen presencial sobre Codificación	Semana 8	Aula	30%
Entrega de un trabajo sobre Criptografía	Semana 15	Aula	20%
Realización de un examen presencial sobre Criptografía.	Semana 15	Aula	30%

CRITERIOS DE CALIFICACIÓN

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 presencial que puede aportar hasta un 30% de la nota final.

  Los trabajos se entregarán al comienzo del examen presencial.

  La asignatura se considerará superada si se obtiene 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.