



DATOS IDENTIFICATIVOS

Teoría de códigos

Asignatura	Teoría de códigos			
Código	006G150V01971			
Titulación	Grado en Ingeniería Informática			
Descriptores	Creditos ECTS	Seleccione	Curso	Cuatrimstre
	6	OP	4	2c
Lengua	Castellano			
Impartición	Gallego			
Departamento	Informática			
Coordinador/a	Vilares Ferro, Manuel			
Profesorado	Vilares Ferro, Manuel			
Correo-e	vilares@uvigo.es			
Web	http://fatic.uvigo.es			
Descripción general	Teoría de Códigos es una asignatura optativa impartida en el segundo semestre del cuarto curso, en la que se pretende introducir a los alumnos en los conceptos básicos de la Teoría de Códigos. En el plan de estudios se establece como objetivos de aprendizaje que el alumno conozca y comprenda los fundamentos de la Teoría de la Información y Codificación, los códigos de detección y corrección más importantes, los aspectos básicos relativos a la comprensión de datos y textos, y, finalmente, una introducción a los sistemas criptográficos. No se usará inglés en clase, aunque algunas de las fuentes bibliográficas están en ese idioma.			

Competencias

Código	
A2	Que los estudiantes sepan aplicar sus conocimientos a su trabajo o vocación de una forma profesional y posean las competencias que suelen demostrarse por medio de la elaboración y defensa de argumentos y la resolución de problemas dentro de su área de estudio.
C4	Conocimientos básicos sobre el uso y programación de los ordenadores, sistemas operativos, bases de datos y programas informáticos con aplicación en ingeniería
C5	Conocimiento de la estructura, organización, funcionamiento e interconexión de los sistemas informáticos, los fundamentos de su programación, y su aplicación para la resolución de problemas propios de la ingeniería
C7	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
C13	Conocimiento, diseño y utilización de forma eficiente de los tipos y estructuras de datos más adecuados a la resolución de un problema
C28	Capacidad de identificar y analizar problemas y diseñar, desarrollar, implementar, verificar y documentar soluciones software sobre la base de un conocimiento adecuado de las teorías, modelos y técnicas actuales
C35	Capacidad para seleccionar, desplegar, integrar y gestionar sistemas de información que satisfagan las necesidades de la organización, con los criterios de coste y calidad identificados
C36	Capacidad de concebir sistemas, aplicaciones y servicios basados en tecnologías de red, incluyendo Internet, web, comercio electrónico, multimedia, servicios interactivos y computación móvil
D1	I1: Capacidad de análisis, síntesis y evaluación
D2	I2: Capacidad de organización y planificación
D8	I8: Resolución de problemas

Resultados de aprendizaje

Resultados previstos en la materia	Resultados de Formación y Aprendizaje		
RA1: Conocer y comprender los fundamentos de la Teoría de la Información y Codificación.	A2	C5	D1
		C7	D2
		C28	D8
		C35	
		C36	

RA2: Conocer y comprender los códigos correctores y detectores de errores más importantes.	A2	C4 C5 C7 C13 C28 C35 C36	D1 D2 D8
R3: Conocer y comprender los aspectos básicos relativos a la compresión de datos y de textos.	A2	C4 C5 C7 C13 C28 C35 C36	D1 D2 D8

Contenidos

Tema	
1.- Fundamentos de la teoría de la información.	1.1.- Distancia de Hamming. 1.2.- Detección y Corrección de errores. 1.3.- Códigos perfectos. 1.4.- Fiabilidad de un código.
2.- Códigos lineales.	2.1.- Generalidades: equivalencia, control de paridad, corrección de errores. 2.2.- Códigos de Hamming. 2.3.- Códigos de Reed-Muller. 2.3.- Códigos de Golay.
3.- Compresión de la información.	3.1.- Códigos de longitud variable. 3.2.- Códigos de Huffman.
4.- Criptografía.	4.1.- Criptografía de clave pública. 4.2.- Criptografía de clave secreta.

Planificación

	Horas en clase	Horas fuera de clase	Horas totales
Lección magistral	25.5	47.3571	72.8571
Prácticas de laboratorio	26.25	48.7501	75.0001
Examen de preguntas de desarrollo	2.1428	0	2.1428

*Los datos que aparecen en la tabla de planificación son de carácter orientativo, considerando la heterogeneidad de alumnado

Metodologías

	Descripción
Lección magistral	Exposición de los contenidos teóricos de la materia. Dado el carácter práctico de los contenidos propuestos, la exposición se complementará con ejemplos. El profesor podrá proponer ejemplos o ejercicios para su resolución por los alumnos, tanto dentro como fuera del aula.
Prácticas de laboratorio	En base a la materia teórica propuesta en clase, el profesor propondrá la implementación de casos prácticos simples por parte de los alumnos. Dichas prácticas se realizarán en grupos pequeños y tanto dentro como fuera de las horas de aula, y serán evaluadas como parte de la nota final, teniendo el alumno que entregar el código implementado y una pequeña memoria en donde se especificarán aquellos aspectos del funcionamiento de la práctica requeridos por el profesor.

Atención personalizada

Metodologías	Descripción
Prácticas de laboratorio	El profesor planteará las prácticas que deben realizarse, y, durante las horas en aula dedicadas a las prácticas de laboratorio, resolverá las dudas planteadas por los alumnos, supervisando el trabajo que estén realizando en ese momento.

Evaluación

Descripción	Calificación	Resultados de Formación y Aprendizaje
-------------	--------------	---------------------------------------

Prácticas de laboratorio	Los alumnos deberán realizar una defensa de las prácticas realizadas, consistente en una prueba de funcionamiento y en la contestación de las preguntas realizadas por el profesor, con el objetivo de comprobar lo aprendido por los alumnos durante la realización del trabajo. La calificación obtenida dependerá de la calidad del trabajo realizado y de la defensa realizada por los alumnos.	40	A2	C4 C5 C7 C13 C28 C35 C36	D1 D2 D8
Resultados de Aprendizaje: RA2, RA3					
Examen de preguntas de desarrollo	Al final del cuatrimestre se realizará una prueba escrita en donde se examinará a los alumnos sobre los conocimientos adquiridos en las clases teóricas.	60	A2	C5 C7 C28 C35 C36	D1 D2 D8
Resultados de Aprendizaje: RA1					

Otros comentarios sobre la Evaluación

CRITERIOS DE EVALUACIÓN PARA ASISTENTES 1ª EDICIÓN DE ACTAS

Para aprobar la asignatura será necesario obtener al menos el 50% de la nota máxima del examen teórico, que las prácticas sean presentados en el tiempo y plazo especificado por el profesor, y que la suma de las notas de teoría y prácticas alcance, al menos, el 50% de la nota máxima de la materia.

CRITERIOS DE EVALUACIÓN PARA NO ASISTENTES

Dado que el material preciso para la realización de las prácticas está disponible para todos los alumnos en formato electrónico, la evaluación para no asistentes será la misma que para asistentes.

CRITERIOS DE EVALUACIÓN PARA 2ª EDICIÓN DE ACTAS Y FIN DE CARRERA

La metodología de evaluación será la misma en todas las convocatorias, tanto para asistentes como para no asistentes.

PROCESO DE CALIFICACIÓN DE ACTAS

La nota de la asignatura será la suma de las notas de la prueba teórica y de prácticas, excepto en dos casos:

- Si alguna de las prácticas no es entregada y defendida en el plazo establecido por el profesor, la nota de la asignatura será un 0, independientemente de la nota obtenida en la teoría.
- Si la nota de la prueba teórica es menor que el 50% de la nota máxima de dicha prueba (3 puntos sobre 6), no se le sumará la calificación obtenida en las prácticas. La nota de la asignatura será sólo la nota de la prueba teórica.

De cumplirse ambos supuestos, a) y b), la nota será 0.

FECHAS DE EVALUACIÓN

El calendario de pruebas de evaluación aprobado oficialmente por la Junta de Centro de la ESEI está publicado en la página web <http://www.esei.uvigo.es>.

Fuentes de información

Bibliografía Básica

Hill, Raymond, **A First Course in Coding Theory**, 1ª Ed, Clarendon Press, 1986

Roman, Steven, **Introduction to Coding and Information Theory**, 1ª Ed, Springer, 1997

van Lint, J.H., **Introduction to Coding Theory**, 2ª Ed, Springer, 1998

Bibliografía Complementaria

Pretzel, Oliver, **Error-Correcting Codes and Finite Fields. Student Edition**, 1ª Ed, Oxford University Press, 1996

Adamek, Jiri, **Foundations of Coding**, 1ª Ed, Wiley, 1991

Stinson, Douglas R., **Cryptography: Theory and Practice**, 3ª Ed, Chapman and Hall, EEUU

O. Goldreich, **Foundations of Cryptography, Basic Applications**, 1ª Ed, Cambridge University Press, 2009

Menezes, Alfred J. y van Oorschot, Paul C. y Vanstone, Scott A., **Handbook of Applied Cryptography**, 1ª Ed, CRC Press, 1996

Bellare, Mihir y Rogaway, Phillip, **Introduction to Cryptography, Lecture Notes**

(<http://cseweb.ucsd.edu/~mihir/cse207/classnotes.html>), University of California San Diego, 2006

Recomendaciones

Asignaturas que se recomienda haber cursado previamente

Matemáticas: Álgebra lineal/O06G150V01101

Matemáticas: Análisis matemático/O06G150V01202

Matemáticas: Fundamentos matemáticos para la informática/O06G150V01103

Matemáticas: Estadística/O06G150V01301

Otros comentarios

Se recuerda a todo el alumnado la prohibición del uso de dispositivos móviles en ejercicios, prácticas y exámenes, en cumplimiento del artículo 13.2.d) del Estatuto del Estudiante Universitario, relativo a los deberes del estudiantado universitario, que establece el deber de "Abstenerse de la utilización o cooperación en procedimientos fraudulentos en las pruebas de evaluación, en los trabajos que se realicen o en documentos oficiales de la universidad."
