

DATOS IDENTIFICATIVOS				
Teoría de códigos				
Materia	Teoría de códigos			
Código	O06G150V01971			
Titulación	Grao en Enxeñaría Informática			
Descritores	Creditos ECTS	Sinale	Curso	Cuadrimestre
	6	OP	4	2c
Lingua de impartición	Castelán Galego			
Departamento	Informática			
Coordinador/a	Vilares Ferro, Manuel			
Profesorado	Vilares Ferro, Manuel			
Correo-e	vilares@uvigo.es			
Web	http://faitic.uvigo.es			
Descrición xeral	Teoría de Códigos é unha asignatura optativa impartida no segundo semestre del cuarto curso, na que preténdese introducir aos alumnos nos conceptos básicos da Teoría de Códigos. No plan de estudios establécense como obxectivos de aprendizaxe que o alumno coñeza e comprenda os fundamentos da Teoría da Información e Codificación, os códigos de detección e corrección máis importantes, os aspectos básicos relativos á comprensión de datos e textos, e, finalmente, unha introducción aos sistemas criptográficos. Non se usará inglés na clase, aínda que algunhas das fontes bibliográficas están nese idioma.			

Competencias	
Código	
A2	Que os estudantes saiban aplicar os seus coñecementos ó seu traballo ou vocación dunha forma profesional e posúan as competencias que adoitan demostrarse por medio da elaboración e defensa de argumentos e a resolución de problemas dentro da súa área de estudo.
C4	Coñecementos básicos sobre o uso e programación dos ordenadores, sistemas operativos, bases de datos e programas informáticos con aplicación na enxeñería
C5	Coñecemento da estrutura, organización, funcionamento e interconexión dos sistemas informáticos, os fundamentos da súa programación, e a súa aplicación para a resolución de problemas propios da enxeñería
C7	Capacidade para deseñar, desenvolver, seleccionar e avaliar aplicacións e sistemas informáticos, asegurando a súa fiabilidade, seguridade e calidade, conforme aos principios éticos e á lexislación e normativa vixente
C13	Coñecemento, deseño e utilización de forma eficiente dos tipos e estruturas de datos máis axeitados á resolución dun problema
C28	Capacidade de identificar e analizar problemas e deseñar, desenvolver, implementar, verificar e documentar solucións software sobre a base dun coñecemento axeitado das teorías, modelos e técnicas actuais
C35	Capacidade para seleccionar, despregar, integrar e xestionar sistemas de información que satisfagan as necesidades da organización, cos criterios de custo e calidade identificados
C36	Capacidade de concibir sistemas, aplicacións e servizos baseados en tecnoloxías de rede, incluíndo Internet, web, comercio electrónico, multimedia, servizos interactivos e computación móbil
D1	I1: Capacidade de análise, síntese e avaliación
D2	I2: Capacidade de organización e planificación
D8	I8: Resolución de problemas

Resultados de aprendizaxe			
Resultados previstos na materia	Resultados de Formación e Aprendizaxe		
RA1: Coñecer e comprender os fundamentos da Teoría da Información e Codificación.	A2	C5 C7 C28 C35 C36	D1 D2 D8

RA2: Coñecer e comprender os códigos correctores e detectores de erros máis importantes.	A2	C4 C5 C7 C13 C28 C35 C36	D1 D2 D8
RA3: Coñecer e comprender os aspectos básicos relativos á compresión de datos e de textos.	A2	C4 C5 C7 C13 C28 C35 C36	D1 D2 D8

Contidos	
Tema	
1.- Fundamentos da teoría da información.	1.1.- Distancia de Hamming. 1.2.- Detección y Corrección de erros. 1.3.- Códigos perfectos. 1.4.- Fiabilidade dun código.
2.- Códigos lineais.	2.1.- Xeralidades: equivalencia, control de paridade, corrección de erros. 2.2.- Códigos de Hamming. 2.3.- Códigos de Reed-Muller. 2.3.- Códigos de Golay.
3.- Compresión da información.	3.1.- Códigos de lonxitude variable. 3.2.- Códigos de Huffman.
4.- Criptografía	4.1.- Criptografía de clave pública. 4.2.- Criptografía de clave secreta.

Planificación			
	Horas na aula	Horas fóra da aula	Horas totais
Lección maxistral	20.5	41	61.5
Prácticas de laboratorio	29	36.25	65.25
Outros	2	19.25	21.25
Exame de preguntas de desenvolvemento	2	0	2

*Os datos que aparecen na táboa de planificación son de carácter orientador, considerando a heteroxeneidade do alumnado.

Metodoloxía docente	
	Descrición
Lección maxistral	Exposición dos contidos teóricos da materia. Dado o carácter práctico dos contidos propostos, a exposición complementarase con exemplos. O profesor poderá propoñer exemplos ou exercicios para a súa resolución polos alumnos, tanto dentro como fóra da aula.
Prácticas de laboratorio	En base á materia teórica proposta en clase, o profesor propondrá a implementación de casos prácticos simples por parte dos alumnos. Ditas prácticas se realizarán en grupos pequenos, tanto dentro como fóra das horas de aula, e serán avaliadas como parte da nota final, tendo o alumno que entregar o código implementado e unha pequena memoria en donde se especificarán aqueles aspectos do funcionamento da práctica requeridos polo profesor.
Outros	Actividades de recuperación realizadas polo alumnado que non supere a materia na primeira convocatoria.

Atención personalizada	
Metodoloxías	**Descrición**
Prácticas de laboratorio	O profesor plantexará as prácticas que deben realizarse, e, durante as horas en aula dedicadas ás prácticas de laboratorio, resolverá las dudas plantexadas polos alumnos, supervisando o traballo que estean realizando nese momento.

Avaliación			
	Descrición	Cualificación	Resultados de Formación e Aprendizaxe

Prácticas de laboratorio	Os alumnos deberán realizar unha defensa das prácticas realizadas, consistente nunha proba de funcionamiento e na contestación das preguntas realizadas polo profesor, co obxectivo de comprobar o aprendido polos alumnos durante a realización do traballo. A nota final dependerá da calidade do traballo realizado e da defensa realizada polos alumnos. Resultados de Aprendizaxe: RA2, RA3	40	A2	C4 C5 C7 C13 C28 C35 C36	D1 D2 D8
Exame de preguntas de desenvolvemento	Ao final do cuatrimestre se realizará unha proba escrita na se examinará aos alumnos sobre os coñecementos adquiridos nas clases teóricas. Resultados de Aprendizaxe: RA1	60	A2	C5 C7 C28 C35 C36	D1 D2 D8

Outros comentarios sobre a Avaliación

CRITERIOS DE AVALIACIÓN PARA ASISTENTES 1ª EDICIÓN DE ACTAS

Para aprobar a asignatura será necesario obter polo menos o 50% da nota máxima do examen teórico, que as prácticas sexan presentados no tempo e prazo especificado polo profesor, e que a suma das notas de teoría e prácticas alcance, como mínimo, o 50% da nota máxima da materia.

CRITERIOS DE AVALIACIÓN PARA NON ASISTENTES

Dado que o material preciso para a realización das prácticas está dispoñible para tódolos alumnos en formato electrónico, a avaliación para non asistentes será a mesma que para asistentes.

CRITERIOS DE AVALIACIÓN PARA 2ª EDICIÓN DE ACTAS E FIN DE CARREIRA

A metodoloxía de avaliación será a mesma en tódalas convocatorias, tanto para asistentes como para non asistentes.

PROCESO DE CALIFICACIÓN DE ACTAS

A nota da asignatura será a suma das notas da proba teórica e das prácticas, excepto en dous casos:

a) Se algunha das prácticas non é entregada e defendida no prazo establecido polo profesor, a nota da asignatura será un 0, independentemente da nota obtida na teoría.

b) Se a nota da proba teórica é menor que o 50% de nota máxima na devandita proba (3 puntos sobre 6), non se lle sumará a calificación obtida nas prácticas. A nota da asignatura será só a nota da proba teórica.

De cumprirse ambos supostos, a) e b), a nota será 0.

DATAS DE AVALIACIÓN

O calendario de probas de avaliación aprobado oficialmente pola Xunta de Centro da ESEI atópase publicado na páxina web http://www.esei.uvigo.es/index.php?id=29.

Bibliografía. Fontes 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

Recomendacións

Materias que se recomenda ter cursado previamente

Matemáticas: Álxebra lineal/O06G150V01101
Matemáticas: Análise matemática/O06G150V01202
Matemáticas: Fundamentos matemáticos para a informática/O06G150V01103
Matemáticas: Estatística/O06G150V01301

Outros comentarios

Lémbrase a todo o alumnado a prohibición do uso de dispositivos móbiles en exercicios, prácticas e exames, en cumprimento do artigo 13.2.d) do Estatuto do Estudante Universitario, relativo aos deberes do estudantado universitario, que establece o 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".