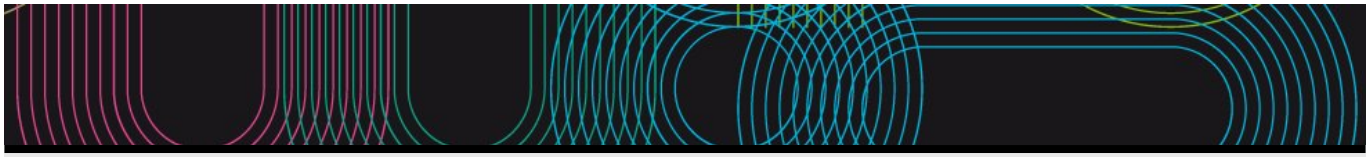

IDENTIFYING DATA

Codes Theory

Subject	Codes Theory			
Code	O06G151V01422			
Study programme	Grado en Ingeniería Informática			
Descriptors	ECTS Credits	Choose	Year	Quadmester
	6	Optional	4th	2nd
Teaching language	Spanish Galician			
Department				
Coordinator	Vilares Ferro, Manuel			
Lecturers	Vilares Ferro, Manuel			
E-mail	vilares@uvigo.es			
Web	http://moovi.uvigo.gal			
General description	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 Teoría de la Información y Codificación; los códigos de detección y corrección más importante; y los aspectos básicos relativos a la comprensión de datos y textos.			

Training and Learning Results

Code	
A2	Students will be able to apply their knowledge and skills in their professional practice or vocation and they will show they have the required expertise through the construction and discussion of arguments and the resolution of problems within the relevant area of study.
B9	Ability to solve problems by taking the initiative, making decisions and acting independently and creatively. Ability to communicate the knowledge contents, skills and abilities of the Computer Science Engineer profession.
C4	Essential knowledge of use and programming of computers, operating systems, data bases and computer programs with application in engineering.
C5	Knowledge of the structure, organization, functioning and interconnection of computing systems, the foundations of their programming, and their application to the resolution of specific problems in engineering.
C7	Ability to design, develop, choose and assess computer applications and systems to guarantee their reliability, safety and quality, according to ethical principles and existing legislation and regulations.
C13	Knowledge, design and efficient use of the most appropriate data structures and types for the resolution of a problem.
C28	Ability to identify and analyze problems and design, develop, implement, verify and document software solutions on the basis of sound knowledge of the theories, models and techniques available nowadays.
C35	Ability to select, design, implement, integrate and manage information systems that meet the needs of organizations, once the costs and quality criteria have been identified.
C37	Ability to understand, apply and manage the security and safety of computing systems.
D4	Analysis, synthesis and evaluation capacity
D5	Organizational and planning skills

Expected results from this subject

Expected results from this subject	Training and Learning Results			
New	A2	B9	C5 C7 C28 C35 C37	D4 D5

New	A2	B9	C4 C5 C7 C13 C28 C35 C37	D4 D5
New	A2	B9	C4 C5 C7 C13 C28 C35 C37	D4 D5

Contents	
Topic	
TEMA 1: Fundamentos de la teoría de la información	1.1.- Propiedades de Z. Orden algoritmo euclidiano. Principio del buen orden. Teorema fundamental de la aritmética. Congruencias. El anillo Z_n
TEMA 2: Codificación de la información en canales con ruído	2.1.- Códigos lineales 2.2.- Códigos Hamming 2.3.- Códigos de Golay
TEMA 3: Compresión de la información	3.1.- Códigos de descodificación única 3.2.- Codificación aritmética
(*)4.- Criptografía	(*)4.1.- Criptografía de clave pública. 4.2.- Criptografía de clave secreta.

Planning			
	Class hours	Hours outside the classroom	Total hours
Lecturing	22.5	45.5	68
Laboratory practical	27	53	80
Essay questions exam	2	0	2
*The information in the planning table is for guidance only and does not take into account the heterogeneity of the students.			

Methodologies	
	Description
Lecturing	
Laboratory practical	(*)En base á materia teórica proposta en clase, o profesor propondrá a implementación de casos prácticos 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. AVALIACIÓN CONTINUA Carácter: Obrigatorio Asistencia: obrigatoria para as sesións nas que se realicen actividades de avaliación. AVALIACIÓN GLOBAL Carácter: Obrigatorio

Personalized assistance	
Methodologies	**Description**
Laboratory practical	

Assessment						
	Description	Qualification	Training and Learning Results			
Laboratory practical	(*)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	B9	C4 C5 C7 C13 C28 C35 C37	D4 D5

Essay questions exam	(*)Realización de dúas probas escritas obrigatorias nas que se examinará aos alumnos sobre os coñecementos adquiridos nas clases teóricas. Resultados de Aprendizaxe: RA1	60	A2	B9	C5 C7 C28 C35 C37	D4 D5

Other comments on the Evaluation

Sources of information

Basic Bibliography

Hill, Raymond, **A First Course in Coding Theory**, 0-19-853803-0, 1ª Ed, Clarendon Press, 1986

Roman, Steven, **Introduction to Coding and Information Theory**, 0-387-94704-3, 1ª Ed, Springer, 1997

van Lint, J.H., **Introduction to Coding Theory**, 3-540-64133-5, 2ª Ed, Springer, 1998

Complementary Bibliography

Pretzel, Oliver, **Error-Correcting Codes and Finite Fields. Student Edition**, 0-19-269067-1, 1ª Ed, Oxford University Press, 1996

Adamek, Jiri, **Foundations of Coding**, 0471621870, 1ª Ed, Wiley, 1991

Stinson, Douglas R., **Cryptography: Theory and Practice**, 978-1-58488-508-5, 3ª Ed, Chapman and Hall, 2006

O. Goldreich, **Foundations of Cryptography, Basic Applications**, 978-1-58488-508-5, 1ª Ed, Cambridge University Press, 2009

Menezes, Alfred J. y van Oorschot, Paul C. y Vanstone, Scott A., **Handbook of Applied Cryptography**, 0-8493-8523-7, 1ª Ed, CRC Press, 1996

Recommendations