BASIC DETAILS:

Subject:	CRIPTOGRAFIA		
Id.:	30082		
Programme:	GRADUADO EN INGENIERÍA INFORMÁTICA. PLAN 2008 (BOE 15/12/2008)		
Module:	GESTION DE LA INFORMACION Y EL CONOCIMIENTO		
Subject type:	OPTATIVA		
Year:	4	**Teaching period:**	Primer Cuatrimestre
Credits:	3	**Total hours:**	75
Classroom activities:	36	**Individual study:**	39
Main teaching language:	Inglés	**Secondary teaching language:**	Inglés
Lecturer:	BALLARIN USIETO, PABLO (T)	**Email:**	pballarinu@usj.es

PRESENTATION:

This subject provides an introduction to the fundamental concepts, theory and application of cryptography, which a fundamental part of cybersecurity. Different cryptographic techniques and encryption algorithms will be studied and examined. The main goal is to analyse the practical application of modern cryptography.

PROFESSIONAL COMPETENCES ACQUIRED IN THE SUBJECT:

General programme competences	G02	Innovative capacity to propose and find new and efficient ways to undertake any task and/ or function within the professional environment - highly motivated by quality.
	G03	Capacity to work in multidisciplinary teams to achieve common objectives, placing group interests before personal ones.
	G10	Critical and analytical capacity when assessing information, data and courses of action.
	G12	Capacity to undertake professional activities with integrity, respecting social, organisational and ethical norms.
	G13	Capacity to use individual learning strategies aimed at continuous improvement in professional life and to begin further studies independently.
	G14	Capacity for abstraction to handle various complex knowledge models and apply them to examining and solving problems.
	G15	Capacity to structure reality by means of linking objects, situations and concepts through logical mathematical reasoning.
Specific programme competences	E01	Capacity to understand the engineering profession and commitment to serve society under the corresponding professional code of conduct.
	E02	Capacity to apply the intrinsic engineering principles based on mathematics and a combination of scientific disciplines.
	E03	Capacity to recognise the technical principles and apply the appropriate practical methods satisfactorily to analyse and solve engineering problems.
	E08	Capacity to communicate productively with clients, users and colleagues both orally and in writing, so as to pass on ideas, solve conflicts and achieve agreements.
	E10	Capacity to understand and assess the impact of technology on individuals, organisations, society and the environment, including ethical, legal and political factors, recognising and applying the pertinent standards and regulations.s éticos, legales y políticos, reconociendo y aplicando los estándares y regulaciones oportunos
	E12	Capacity to manage complexity through abstraction, modelling, 'best practices', patterns, standards and the use of the appropriate tools.
	E13	Capacity to identify, assess and use current and emerging technologies, considering how they apply in terms of individual or organisational needs.
	E17	Capacity to identify and analyse user needs with the intention of designing effective, usable IT solutions which can be incorporated into the user's operating environment.
Learning outcomes	R01	Evaluar las fortalezas y debilidades de seguridad de diferentes aplicaciones a través de distintos métodos criptográficos
	R02	Implementar un algoritmo criptográfico completo.
	R03	Entender los conceptos matemáticos sobre los que se apoyan los distintos métodos criptográficos
	R04	Distinguir y utilizar los conceptos principales de la criptografía.
	R05	Comparar las diferentes herramientas criptográficas

	R06	Conocer los diferentes problemas de seguridad de la sociedad de la información

PRE-REQUISITES:

SUBJECT PROGRAMME:

Subject contents:

1 - Cryptography as part of cybersecurity
1.1 - Cybersecurity concepts
1.2 - Vulnerabilities, threats and risks
1.3 - Cybersecurity protections
1.4 - Basic cybersecurity tools
2 - Introduction to cryptography
2.1 - Principles, terms and meanings
2.2 - Basic number theory
2.3 - Classical, symmetric and asymmetric encryption techniques and algorithms
2.4 - Cryptographic hash functions
2.5 - Cryptanalysis: decrypting the encrypted
3 - Symmetric encryption
3.1 - Purpose and operation
3.2 - Block and stream ciphers
3.3 - Substitution and permutation
3.4 - Triple DES (3DES)
3.5 - Advanced Encryption Standard (AES)
4 - Cryptographic hashing
4.1 - Purpose and operation
4.2 - Hash functions: cyclic redundancy checks, checksums, key cryptographic hash functions (MD5, SHA, ...)
5 - Asymmetric encryption
5.1 - Purpose and operation
5.2 - Diffie-Hellman key exchange
5.3 - RSA Public-Key encryption
5.4 - Key negotiation and distribution
5.5 - Message exchanges, authentication, non-repudiation
6 - Applications of cryptography
6.1 - Digital signatures, digital certificates, certification authorities and Public-Key Infrastructures (PKI)
6.2 - Cryptography in communication protocols: SSL/TLS, VPN, SSH
6.3 - Introduction to blockchain and cryptocurrencies

Subject planning could be modified due unforeseen circumstances (group performance, availability of resources, changes to academic calendar etc.) and should not, therefore, be considered to be definitive.

TEACHING AND LEARNING METHODOLOGIES AND ACTIVITIES:

Teaching and learning methodologies and activities applied:

This course will use the following methodologies in order to give the students the best opportunity to develop their competences: lectures, practical cases, exercises and cousework presentations.

Participation in class will be accounted in the final score.

All readings, practices and works will be announced using the Online University Platform (pdu.usj.es).

Student work load:

Teaching mode	Teaching methods	Estimated hours

Classroom activities	Master classes	10
	Practical work, exercises, problem-solving etc.	13
	Coursework presentations	2
	Workshops	7
	Assessment activities	4
Individual study	Tutorials	5
	Individual study	15
	Individual coursework preparation	15
	Other individual study activities	4
	Total hours:	75

ASSESSMENT SCHEME:

Calculation of final mark:

Written tests:	50	%
Individual coursework:	45	%
Participation:	5	%
TOTAL	100	%

*Las observaciones específicas sobre el sistema de evaluación serán comunicadas por escrito a los alumnos al inicio de la materia.

BIBLIOGRAPHY AND DOCUMENTATION:

Basic bibliography:

KATZ Jonathan and LINDELL Yehuda. Introduction to Modern Cryptography, 2nd Edition (Chapman & Hall/ CRC Cryptography and Network Security Series). CRC Press 2014.

Schneier, Bruce, Kohno, Tadayoshi, Ferguson, Niels & Bruce Schneier & Tadayoshi Kohno. Cryptography Engineering: Design Principles and Practical Applications. John Wiley & Sons, Inc, 2012

Recommended bibliography:

M. MARTIN, Keith. Everyday Cryptography, Fundamental Principles and Applications. Oxford, 2017

Alfred J. Menezes, Paul C. van Oorschot and Scott A. Vanstone. Handbook of applied cryptography. CRC Press, 2001

Recommended websites:

CrypTool 2 (CT2): programa de código abierto para Windows, con una interfaz de usuario a través de la cual se puede probar diferentes técnicas de cifrado.	https://www.cryptool.org
Daniel Miessler Cybersecurity Blog	https://danielmiessler.com/blog/
The hacker news	https://thehackernews.com/
Infosecurity Magazine	https://www.infosecurity-magazine.com/
Bruce Schneier web site	https://www.schneier.com/