

## SUBJECT TEACHING GUIDE

G844 - Cryptography and Security in Networks and Services

Degree in Telecommunication Technologies Engineering

Academic year 2019-2020

1. IDENTIFYING DATA					
Degree	Degree in Telecommunication Technologies Engineering			Type and Year	Optional. Year 4
Faculty	School of Industrial Engineering and Telecommunications				
Discipline	Subject Area: Telematic Applications and Services				
Course unit title and code	G844 - Cryptography and Security in Networks and Services				
Number of ECTS credits allocated	6	Term	Semester based (1)		
Web	<a href="https://www.tlmat.unican.es/index.php?l=es&amp;p=teaching&amp;s=subjects&amp;ss=g_csrs&amp;">https://www.tlmat.unican.es/index.php?l=es&amp;p=teaching&amp;s=subjects&amp;ss=g_csrs&amp;</a>				
Language of instruction	Spanish	English Friendly	Yes	Mode of delivery	Face-to-face

Department	DPTO. INGENIERIA DE COMUNICACIONES				
Name of lecturer	LUIS MUÑOZ GUTIERREZ				
E-mail	luis.munoz@unican.es				
Office	Edificio Ing. de Telecomunicación Prof. José Luis García García. Planta: - 2. DESPACHO (S202)				
Other lecturers	JORGE LANZA CALDERON				

### 3.1 LEARNING OUTCOMES

- The student will cope with the concepts, techniques and tools linked to both cryptography and network security. At the end, the student will be able to assess the complexity of the different algorithms and the corresponding practical implications.

### 4. OBJECTIVES

The main aim of this syllabus is present the main cryptographic algorithms used for preserving information in terms of confidentiality, integrity and authenticity.

6. COURSE ORGANIZATION	
CONTENTS	
1	Introduction to network security. Terminology. Confidentiality, authentication, authorization and non-repudiation.
2	Data ciphering. Cryptosystem classification. Symmetric ciphering: DES, AES. Stream ciphering. LFSR. Randomness and sequence period.
3	Cryptography and number theory. Prime numbers and co-primes. Basic concepts on modular arithmetic. The Fermat Theorem. The Euler Theorem. The Euclidean Algorithm. The multiplicative inverse. Chinese Remainder Theorem.
4	Public key cryptography. Introduction to the public key cryptosystems. Confidentiality and, authentication. The Diffie.Hellman approach. The RSA Algorithm.
5	Authentication. Digital signature. Hash funtions. MAC functions. HMAC.

7. ASSESSMENT METHODS AND CRITERIA				
Description	Type	Final Eval.	Reassessn	%
The subject will be evaluated through a final exam whose mark, FEM, will be weighted (60%) with the continuous evaluation, CEM. In the former, a mark higher than 4 points out of 10 is required to be considered for averaging both of them.	Written exam	No	Yes	40,00
The students not attending the lectures or deciding not to participate in the continuous evaluation will obtain the mark corresponding to the final exam.	Written exam	Yes	Yes	60,00
<b>TOTAL</b>				<b>100,00</b>
Observations				
The subject will be evaluated through a final exam whose mark, FEM, will be weighted (60%) with the continuous evaluation, CEM. In the former, a mark higher than 4 points out of 10 is required to be considered for averaging both of them.				
Observations for part-time students				
The students not attending the lectures or deciding not to participate in the continuous evaluation will obtain the mark corresponding to the final exam.				

8. BIBLIOGRAPHY AND TEACHING MATERIALS
BASIC
W. Stallings, "Cryptography and Network Security, Principles and Practices", Pearson International Edition, 2006. ISBN: 0-13-202322-9.
A. Menezes, "Handbook of Applied Cryptography", CRC, 1996. ISBN 0-8493-8523-7.