SUBJECT TEACHING GUIDE

G844 - Cryptography and Security in Networks and Services

Degree in Telecommunication Technologies Engineering

Academic year 2023-2024

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	https://www.tlmat.unican.es/index.php?l=es&p=teaching&s=subjects&ss=g_csrs&				
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 corresponsing 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. Stream ciphering. Introduction to groups, rings and finite fields algebra. The AES Algorithm. .
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	%
Partial exam-1	Written exam	No	Yes	30,00
Partial exam-2	Written exam	No	Yes	30,00
Partial exam-3	Written exam	No	Yes	30,00
There will be an exam related to the laboratory sessions. Its contribution to the continuous evaluation will be a 10%.	Laboratory evaluation	No	No	10,00
TOTAL				100,00

Observations

The students passing the three partial exams will pass the subject. However, if anyone wants to improve the mark, they can attend to the ordinary examination session. In this case the final mark will be the maximum of (FEM; FEM*0.60+CEM*0.40). FEM: Final Evaluation Mark/CEM: Continuous Evaluation Mark. The students not attending the lectures or deciding not to participate in the continuous evaluation will obtain the mark corresponding to the final exam.

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.