Course guide
230713 - DPROT - Data Protection

Last modified: 27/05/2025

Unit in charge: Barcelona School of Telecommunications Engineering
Teaching unit: 749 - MAT - Department of Mathematics.

Degree: MASTER'S DEGREE IN TELECOMMUNICATIONS ENGINEERING (Syllabus 2013). (Optional subject).
MASTER'S DEGREE IN ADVANCED TELECOMMUNICATION TECHNOLOGIES (Syllabus 2019). (Optional subject).
MASTER'S DEGREE IN CYBERSECURITY (Syllabus 2020). (Compulsory subject).

Academic year: 2025 **ECTS Credits:** 5.0 **Languages:** English

LECTURER

Coordinating lecturer: JORGE LUIS VILLAR SANTOS

Others: Primer quadrimestre:
JORGE LUIS VILLAR SANTOS - 11, 13

PRIOR SKILLS

Basic linear algebra and probability.
It is recommended a basic knowledge of cryptography, at an introductory level.

TEACHING METHODOLOGY

- Lectures
- Individual work
- Final Exam

LEARNING OBJECTIVES OF THE SUBJECT

Understanding the necessary cryptographic techniques used to protect data during storage and transmision, in order to guarantee its confidentiality, integrity and authentication.

STUDY LOAD

Type	Hours	Percentage
Hours small group	26,0	20.80
Self study	86,0	68.80
Hours large group	13,0	10.40

Total learning time: 125 h

CONTENTS

Introduction

Description:
Introduction to cryptography under the point of view of data protection.

Full-or-part-time: 9h 36m
Laboratory classes: 3h
Self study : 6h 36m

Symmetric key

Description:
Symmetric key encryption. Stream and block ciphers. Modes of operation. Message authentication codes. Hash functions. Authenticated encryption.

Full-or-part-time: 19h 12m
Laboratory classes: 6h
Self study : 13h 12m

Public key

Description:
Key Exchange. Public key encryption. Man-in-the-middle attacks. Digital signatures. Identification schemes. Public key certificates. Identity based cryptography.

Full-or-part-time: 29h
Laboratory classes: 9h
Self study : 20h

Security models

Description:
Definition of easy and hard computational tasks. Security notions for encryption. Security notions for signatures. The random oracle model. Reductions and security proofs.

Full-or-part-time: 19h 12m
Laboratory classes: 6h
Self study : 13h 12m

Zero-knowledge

Description:
Zero-knowledge proofs and arguments. Non-interactive zero-knowledge. Applications.

Full-or-part-time: 9h 36m
Laboratory classes: 3h
Self study : 6h 36m

Distributed cryptography

Description:
Cryptography for many users. Secret sharing. Threshold decryption. Threshold signatures. Secure multiparty computation.

Full-or-part-time: 19h 12m
Laboratory classes: 6h
Self study : 13h 12m

Case study

Description:
Study of real cryptographic protocols used in some practical scenarios.

Full-or-part-time: 19h 12m
Laboratory classes: 6h
Self study : 13h 12m

GRADING SYSTEM

Final exam: 40%
Assignments and lab. reports: 60%

BIBLIOGRAPHY

Basic:
- Delfs, Hans; Knebl, Helmut. Introduction to cryptography : principles and applications. 3rd ed. Berlin [etc.]: Springer, 2015. ISBN 9783662479735.

RESOURCES

Hyperlink:
- http://toc.cryptobook.us/. A Graduate Course in Applied Cryptography (online book)