Last update: 06-05-2019

230713 - DPROT - Data Protection

Coordinating unit: 230 - ETSETB - Barcelona School of Telecommunications Engineering

Teaching unit: 749 - MAT - Department of Mathematics

Academic year: 2019

Degree: MASTER'S DEGREE IN TELECOMMUNICATIONS ENGINEERING (Syllabus 2013). (Teaching unit Optional)
MASTER'S DEGREE IN ADVANCED TELECOMMUNICATION TECHNOLOGIES (Syllabus 2019). (Teaching unit Optional)

ECTS credits: 5 Teaching languages: English

Teaching staff

Coordinator: Jorge Villar

Others: Jorge Villar

Prior skills

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

Teaching methodology

- Lectures
- Individual work (distance)
- Oral presentations
- 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

Total learning time: 125h	Hours small group:	39h	31.20%
	Self study:	86h	68.80%

Last update: 06-05-2019

230713 - DPROT - Data Protection

Content

Introduction

Learning time: 9h 36m
Laboratory classes: 3h
Self study : 6h 36m

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

Symmetric key

Learning time: 19h 12m
Laboratory classes: 6h
Self study : 13h 12m

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

Public key

Learning time: 29h
Laboratory classes: 9h
Self study : 20h

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

Security models

Learning time: 19h 12m
Laboratory classes: 6h
Self study : 13h 12m

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

Last update: 06-05-2019

230713 - DPROT - Data Protection

Zero-knowledge	Learning time: 9h 36m Laboratory classes: 3h Self study : 6h 36m

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

Distributed cryptography	Learning time: 19h 12m Laboratory classes: 6h Self study : 13h 12m

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

Case study	Learning time: 19h 12m Laboratory classes: 6h Self study : 13h 12m

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

Qualification system

Final exam: 40%
Oral presentation: 20%
Assignments: 20%
Final report: 20%

Bibliography