Course guide
230713 - DPROT - Data Protection

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: 2022  ECTS Credits: 5.0  Languages: English

LECTURER

Coordinating lecturer: Consultar aquí / See here:
https://telecos.upc.edu/ca/estudis/curs-actual/professorat-responsables-coordinadors/responsables-assignatura

Others: Consultar aquí / See here:
https://telecos.upc.edu/ca/estudis/curs-actual/professorat-responsables-coordinadors/professorat-assignat-idioma

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 transmission, in order to guarantee its confidentiality, integrity and authentication.

STUDY LOAD

<table>
<thead>
<tr>
<th>Type</th>
<th>Hours</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hours small group</td>
<td>39,0</td>
<td>31.20</td>
</tr>
<tr>
<td>Self study</td>
<td>86,0</td>
<td>68.80</td>
</tr>
</tbody>
</table>

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:**

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

## Public key

**Description:**

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

## Security models

**Description:**

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

## Zero-knowledge

**Description:**

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

Description:

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: 35%
Oral presentation: 15%
Assignments and lab. reports: 30%
Final report: 20%

BIBLIOGRAPHY

Basic:

RESOURCES

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