### 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 transmission, 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% |
## Introduction

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

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

## Symmetric key

**Description:**  

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

## Public key

**Description:**  

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

## Security models

**Description:**  

**Learning time:** 19h 12m  
Laboratory classes: 6h  
Self study: 13h 12m
### Zero-knowledge

<table>
<thead>
<tr>
<th>Description:</th>
<th>Learning time: 9h 36m</th>
</tr>
</thead>
</table>
| Zero-knowledge proofs and arguments. Non-interactive zero-knowledge. Applications. | Laboratory classes: 3h  
Self study: 6h 36m |

### Distributed cryptography

<table>
<thead>
<tr>
<th>Description:</th>
<th>Learning time: 19h 12m</th>
</tr>
</thead>
</table>
| Cryptography for many users. Secret sharing. Threshold decryption. Threshold signatures. Secure multiparty computation. | Laboratory classes: 6h  
Self study: 13h 12m |

### Case study

<table>
<thead>
<tr>
<th>Description:</th>
<th>Learning time: 19h 12m</th>
</tr>
</thead>
</table>
| Study of real cryptographic protocols used in some practical scenarios. | Laboratory classes: 6h  
Self study: 13h 12m |

### Qualification system

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

### Bibliography