## Course guides

**230300 - COMSECRET - Linear Algebra, Linear Codes and Secret-Sharing Schemes**

<table>
<thead>
<tr>
<th>Unit in charge:</th>
<th>Barcelona School of Telecommunications Engineering</th>
</tr>
</thead>
<tbody>
<tr>
<td>Teaching unit:</td>
<td>749 - MAT - Department of Mathematics.</td>
</tr>
</tbody>
</table>

**Degree:**
- BACHELOR'S DEGREE IN AUDIOVISUAL SYSTEMS ENGINEERING (Syllabus 2009). (Optional subject).
- BACHELOR'S DEGREE IN ELECTRONIC SYSTEMS ENGINEERING (Syllabus 2009). (Optional subject).
- BACHELOR'S DEGREE IN TELECOMMUNICATIONS SCIENCE AND TECHNOLOGY (Syllabus 2010). (Optional subject).
- BACHELOR'S DEGREE IN TELECOMMUNICATIONS SYSTEMS ENGINEERING (Syllabus 2010). (Optional subject).
- BACHELOR'S DEGREE IN NETWORK ENGINEERING (Syllabus 2010). (Optional subject).
- BACHELOR'S DEGREE IN TELECOMMUNICATIONS TECHNOLOGIES AND SERVICES ENGINEERING (Syllabus 2015). (Optional subject).
- BACHELOR'S DEGREE IN ELECTRONIC ENGINEERING AND TELECOMMUNICATION (Syllabus 2018). (Optional subject).

**Academic year:** 2020  
**ECTS Credits:** 2.0  
**Languages:** Catalan

### LECTURER

- **Coordinating lecturer:** Sáez Moreno, Germán
- **Others:**  
  - Fàbrega Canudas, Josep  
  - Muñoz López, Francisco Javier  
  - Sáez Moreno, Germán

### PRIOR SKILLS

Basic concepts and tools from linear algebra.

### REQUIREMENTS

IMPORTANT: if you have taken previously "Data transmission" subject, then this seminar don't should be taken (after the subject "Data transmission").

### TEACHING METHODOLOGY

Class hours combine both theoretical and practical sessions. A practical laboratory session is also included.

### LEARNING OBJECTIVES OF THE SUBJECT

The aim of the seminar is to provide, by using methods from elementary linear algebra, a brief introduction to some objects and techniques of telecommunications engineering which are central in the design of secure and reliable communications systems. Specifically, we present some basic notions on binary linear error correcting codes and cryptographic protocols for secret sharing schemes.
STUDY LOAD

<table>
<thead>
<tr>
<th>Type</th>
<th>Hours</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hours large group</td>
<td>20.0</td>
<td>40.00</td>
</tr>
<tr>
<td>Self study</td>
<td>30.0</td>
<td>60.00</td>
</tr>
</tbody>
</table>

Total learning time: 50 h

CONTENTS

**Introduction to modular arithmetic.**

**Description:**
Introduction to modular arithmetic. Vector space over the finite field of two elements.

**Full-or-part-time:** 5h
Theory classes: 5h

**Introduction to secret sharing schemes.**

**Description:**
Introduction to secret sharing schemes. Linear vectorial schemes over the finite field of two elements. Secret distribution and reconstruction process. Security of the scheme. Authorized subsets of participants.

**Full-or-part-time:** 5h
Theory classes: 5h

**Introduction to error correcting codes.**

**Description:**

**Full-or-part-time:** 5h
Theory classes: 5h

**Introduction to cryptography.**

**Description:**

**Full-or-part-time:** 5h
Theory classes: 5h

GRADING SYSTEM
BIBLIOGRAPHY

Basic: