Course guide
230152 - CSI - Information Security and Coding

Unit in charge: Barcelona School of Telecommunications Engineering
Teaching unit: 744 - ENTEL - Department of Network Engineering.

Degree: 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: 2023 ECTS Credits: 6.0 Languages: Spanish

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

TEACHING METHODOLOGY
- Lectures
- Application lectures
- Teamwork
- Individual work
- Presentations
- Written exams

LEARNING OBJECTIVES OF THE SUBJECT

The subject is divided into two parts that are taught in parallel, but in a coordinated way, since the knowledge offered in each part is reused in the other.

The first part is focused on cryptography as an information encoding tool, and has the following learning objectives:
- Learning the mathematical foundations used in modern cryptography.
- Learning about the most commonly used public key cryptographic systems
- Description of other mechanisms used in cryptography
- Description of the use of cryptography beyond encryption and digital signature.

The second part of the subject focuses on different aspects of information security and privacy, with the following learning objectives:
- Learning of general concepts of information security and privacy.
- Knowing the main mechanisms of authentication and key management.
- Deepening the knowledge of the main security protocols used on the Internet.
- Introducing the main data anonymization algorithms and the associated privacy guarantees
- Introducing anonymous communication systems
STUDY LOAD

<table>
<thead>
<tr>
<th>Type</th>
<th>Hours</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Self study</td>
<td>98,0</td>
<td>65.33</td>
</tr>
<tr>
<td>Hours large group</td>
<td>52,0</td>
<td>34.67</td>
</tr>
</tbody>
</table>

Total learning time: 150 h

CONTENTS

PARTE I. CRYPTOGRAPHY

Description:
1. Number Theory in Cryptography (Theory 8 hrs, Independent learning 13 hrs). Knowledge of number theory necessary to understand modern cryptographic systems.
3. Other types of cryptography (Theory 2 hrs, Autonomous learning 6 hrs). Elliptic Curve Cryptography and Quantum Cryptography are presented
4. Other applications of Cryptography (Theory 4 hrs, Self-directed learning 9 hrs). Other uses of cryptography such as toss-up over the phone, secret sharing, primality testing, etc. are presented.

Full-or-part-time: 75h
Theory classes: 26h
Self study : 49h

PARTE II. INFORMATION SECURITY AND PRIVACY

Description:
1. Network Security Concepts
2. Authentication and Key Management
3. Internet Security Protocols
4. Introduction to data privacy
5. Anonymization of databases
6. Privacy in personalized information systems
7. Differential privacy
8. Anonymous communication systems

Full-or-part-time: 75h
Theory classes: 26h
Self study : 49h

GRADING SYSTEM

The grade will be obtained from the continuous assessment, including active participation in class, as well as tests, oral presentations and class projects. If the student do not pass the continuous assessment, she/he can attend to a final exam.
BIBLIOGRAPHY

Basic:

Complementary:

RESOURCES

Other resources:
Additional information available on ATENEA