Course guide
34954 - CC - Codes and Cryptography

Unit in charge: School of Mathematics and Statistics
Teaching unit: 749 - MAT - Department of Mathematics.

Degree: MASTER'S DEGREE IN ADVANCED MATHEMATICS AND MATHEMATICAL ENGINEERING (Syllabus 2010).
(Optional subject).

Academic year: 2023 ECTS Credits: 7.5 Languages: English

LECTURER
Coordinating lecturer: SIMEON MICHAEL BALL MARKS
Others: Segon quadrimestre: SIMEON MICHAEL BALL MARKS - A
JAVIER HERRANZ SOTOCA - A

PRIOR SKILLS
Basic probability, basic number theory and linear algebra

REQUIREMENTS
Undergraduate mathematics

DEGREE COMPETENCES TO WHICH THE SUBJECT CONTRIBUTES

Specific:
1. RESEARCH. Read and understand advanced mathematical papers. Use mathematical research techniques to produce and transmit new results.
2. MODELLING. Formulate, analyse and validate mathematical models of practical problems by using the appropriate mathematical tools.
3. CALCULUS. Obtain (exact or approximate) solutions for these models with the available resources, including computational means.
4. CRITICAL ASSESSMENT. Discuss the validity, scope and relevance of these solutions; present results and defend conclusions.

Transversal:
5. SELF-DIRECTED LEARNING. Detecting gaps in one's knowledge and overcoming them through critical self-appraisal. Choosing the best path for broadening one's knowledge.
6. EFFICIENT ORAL AND WRITTEN COMMUNICATION. Communicating verbally and in writing about learning outcomes, thought-building and decision-making. Taking part in debates about issues related to the own field of specialization.
7. THIRD LANGUAGE. Learning a third language, preferably English, to a degree of oral and written fluency that fits in with the future needs of the graduates of each course.
8. TEAMWORK. Being able to work as a team player, either as a member or as a leader. Contributing to projects pragmatically and responsibly, by reaching commitments in accordance to the resources that are available.
9. EFFECTIVE USE OF INFORMATION RESOURCES. Managing the acquisition, structure, analysis and display of information from the own field of specialization. Taking a critical stance with regard to the results obtained.

TEACHING METHODOLOGY
The course is divided in two parts: codes and cryptography. Each part consists of 26 h of ordinary classes, including theory and problem sessions.
LEARNING OBJECTIVES OF THE SUBJECT

This course aims to give a solid understanding of the uses of mathematics in Information technologies and modern communications. The course focuses on the reliable and efficient transmission and storage of the information. Both the mathematical foundations and the description of the most important cryptographic protocols and coding systems are given in the course.

STUDY LOAD

<table>
<thead>
<tr>
<th>Type</th>
<th>Hours</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hours large group</td>
<td>60,0</td>
<td>32.00</td>
</tr>
<tr>
<td>Self study</td>
<td>127,5</td>
<td>68.00</td>
</tr>
</tbody>
</table>

Total learning time: 187.5 h

CONTENTS

Introduction

Description:
The problem of communication. Information theory, Coding theory and Cryptographic theory

Full-or-part-time: 6h 15m
Theory classes: 2h
Self study : 4h 15m

Information and Entropy

Description:
Uncertainty or information. Entropy. Mutual information

Full-or-part-time: 18h 45m
Theory classes: 6h
Self study : 12h 45m

Source codes without memory

Description:

Full-or-part-time: 12h 30m
Theory classes: 4h
Self study : 8h 30m

Channel coding

Description:
Discrete channels without memory. Symmetric channels. Shannon's theorem.

Full-or-part-time: 18h 45m
Theory classes: 6h
Self study : 12h 45m
<table>
<thead>
<tr>
<th>Topic</th>
<th>Description</th>
<th>Full-or-part-time: 18h 45m</th>
<th>Theory classes: 6h</th>
<th>Self study : 12h 45m</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Block codes</strong></td>
<td>Hamming's distance. Detection and correction of errors. Bounds. Linear codes.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Cyclic codes</strong></td>
<td>Cyclic codes. Generator and control matrices. Factorization of $x^n-1$. Roots of a cyclic code. BCH codes. Primitive Reed-Solomon codes. Meggit's decoder.</td>
<td>18h 45m</td>
<td>6h</td>
<td>12h 45m</td>
</tr>
<tr>
<td><strong>Introduction to modern cryptography</strong></td>
<td>The setting: secure storage and symmetric key encryption. Turing machines and complexity classes. Security definitions. Adversarial models. Reductionist security proofs.</td>
<td>15h 37m</td>
<td>5h</td>
<td>10h 37m</td>
</tr>
<tr>
<td><strong>Symmetric key cryptography</strong></td>
<td>Symmetric key encryption. Pseudorandom generators. Block ciphers. Message authentication codes.</td>
<td>15h 38m</td>
<td>5h</td>
<td>10h 38m</td>
</tr>
<tr>
<td><strong>Public key encryption</strong></td>
<td>Definitions and security notions. One way functions. Probabilistic encryption. Main constructions. Homomorphic encryption. Chosen ciphertext security.</td>
<td>15h 37m</td>
<td>5h</td>
<td>10h 37m</td>
</tr>
</tbody>
</table>
Digital signatures

Description:
Security definitions. RSA and Schnorr signatures.

Full-or-part-time: 15h 38m
Theory classes: 5h
Self study: 10h 38m

Proofs of knowledge and other cryptographic protocols

Description:
Ring signatures. Distributed signatures. Identity and attribute based protocols.

Full-or-part-time: 15h 37m
Theory classes: 5h
Self study: 10h 37m

Multiparty computation

Description:
Secret sharing schemes. Unconditionally and computationally secure multiparty computation.

Full-or-part-time: 15h 38m
Theory classes: 5h
Self study: 10h 38m

GRADING SYSTEM

Exam of coding part (50%) and exam of crypto part (50%). If the average is less than 5 out of 10, there is a chance to pass the subject in a final exam.

EXAMINATION RULES.

All the subjects are important. To pass the course it is required to fulfill all the items.

BIBLIOGRAPHY

Basic:

Complementary: