34954 - CC - Codes and Cryptography

Coordinating unit: 200 - FME - School of Mathematics and Statistics
Teaching unit: 749 - MAT - Department of Mathematics
Academic year: 2018
Degree: MASTER'S DEGREE IN ADVANCED MATHEMATICS AND MATHEMATICAL ENGINEERING (Syllabus 2010). (Teaching unit Optional)
ECTS credits: 7,5  Teaching languages: English

Teaching staff
Coordinator: SIMEON MICHAEL BALL
Others: Primer quadrimestre:
SIMEON MICHAEL BALL - 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. CALCULUS. Obtain (exact or approximate) solutions for these models with the available resources, including computational means.
3. CRITICAL ASSESSMENT. Discuss the validity, scope and relevance of these solutions; present results and defend conclusions.

Transversal:
4. 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.
5. 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.
6. 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.
7. 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.
8. 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.
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>Total learning time: 187h 30m</th>
<th>Hours large group: 60h</th>
<th>32.00%</th>
</tr>
</thead>
<tbody>
<tr>
<td>Self study:</td>
<td>127h 30m</td>
<td>68.00%</td>
</tr>
</tbody>
</table>
## Content

<table>
<thead>
<tr>
<th>Category</th>
<th>Learning Time</th>
<th>Description</th>
</tr>
</thead>
</table>
| **Introduction**                  | **6h 15m**    | Theory classes: 2h  
Self study: 4h 15m  

Description:  
The problem of communication. Information theory, Coding theory and Cryptographic theory |
| **Information and Entropy**       | **18h 45m**   | Theory classes: 6h  
Self study: 12h 45m  

Description:  
Uncertainty or information. Entropy. Mutual information |
| **Source codes without memory**   | **12h 30m**   | Theory classes: 4h  
Self study: 8h 30m  

Description:  
| **Channel coding**                | **18h 45m**   | Theory classes: 6h  
Self study: 12h 45m  

Description:  
Discrete channels without memory. Symmetric channels. Shannon's theorem. |
| **Block codes**                   | **18h 45m**   | Theory classes: 6h  
Self study: 12h 45m  

Description:  
<table>
<thead>
<tr>
<th>Cyclic codes</th>
<th>Learning time: 18h 45m</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Theory classes: 6h</td>
</tr>
<tr>
<td></td>
<td>Self study : 12h 45m</td>
</tr>
</tbody>
</table>

Description:

<table>
<thead>
<tr>
<th>Introduction to modern cryptography</th>
<th>Learning time: 15h 37m</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Theory classes: 5h</td>
</tr>
<tr>
<td></td>
<td>Self study : 10h 37m</td>
</tr>
</tbody>
</table>

Description:

<table>
<thead>
<tr>
<th>Symmetric key cryptography</th>
<th>Learning time: 15h 38m</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Theory classes: 5h</td>
</tr>
<tr>
<td></td>
<td>Self study : 10h 38m</td>
</tr>
</tbody>
</table>

Description:

<table>
<thead>
<tr>
<th>Public key encryption</th>
<th>Learning time: 15h 37m</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Theory classes: 5h</td>
</tr>
<tr>
<td></td>
<td>Self study : 10h 37m</td>
</tr>
</tbody>
</table>

Description:

<table>
<thead>
<tr>
<th>Digital signatures</th>
<th>Learning time: 15h 38m</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Theory classes: 5h</td>
</tr>
<tr>
<td></td>
<td>Self study : 10h 38m</td>
</tr>
</tbody>
</table>

Description:
Security definitions. RSA and Schnorr signatures.
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.

**Qualification 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.

**Regulations for carrying out activities**

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

<table>
<thead>
<tr>
<th>Proofs of knowledge and other cryptographic protocols</th>
<th>Learning time: 15h 37m</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Theory classes: 5h</td>
</tr>
<tr>
<td></td>
<td>Self study : 10h 37m</td>
</tr>
</tbody>
</table>

**Description:**

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

<table>
<thead>
<tr>
<th>Multiparty computation</th>
<th>Learning time: 15h 38m</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Theory classes: 5h</td>
</tr>
<tr>
<td></td>
<td>Self study : 10h 38m</td>
</tr>
</tbody>
</table>

**Description:**

Secret sharing schemes. Unconditionally and computationally secure multiparty computation.
### Bibliography

#### Basic:


#### Complementary:


