200245 - CRIPTOL - Cryptology

Coordinating unit: 200 - FME - School of Mathematics and Statistics
Teaching unit: 749 - MAT - Department of Mathematics
Academic year: 2018
Degree: BACHELOR'S DEGREE IN MATHEMATICS (Syllabus 2009). (Teaching unit Optional)
ECTS credits: 6
Teaching languages: Catalan, Spanish, English

Teaching staff

Coordinator: CARLES PADRO LAIMON
Others: Primer quadrimestre: CARLES PADRO LAIMON - A

Degree competences to which the subject contributes

Specific:
GM-CE2. CE-2. Solve problems in Mathematics, through basic calculation skills, taking in account tools availability and the constraints of time and resources.
GM-CE4. CE-4. Have the ability to use computational tools as an aid to mathematical processes.
GM-CE6. Ability to solve problems from academic, technical, financial and social fields through mathematical methods.

Generic:
GM-CB5. To have developed those learning skills necessary to undertake further interdisciplinary studies with a high degree of autonomy in scientific disciplines in which Mathematics have a significant role.
GM-CG1. CG-1. Show knowledge and proficiency in the use of mathematical language.
GM-CB4. CB-4. Have the ability to communicate their conclusions, and the knowledge and rationale underpinning these to specialist and non-specialist audiences clearly and unambiguously.
GM-CG2. CG-2. Construct rigorous proofs of some classical theorems in a variety of fields of Mathematics.
GM-CG3. CG-3. Have the ability to define new mathematical objects in terms of others already know and ability to use these objects in different contexts.
GM-CG4. CG-4. Translate into mathematical terms problems stated in non-mathematical language, and take advantage of this translation to solve them.
GM-CG6. CG-6 Detect deficiencies in their own knowledge and pass them through critical reflection and choice of the best action to extend this knowledge.

Transversal:
04 COE. 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.
07 AAT. 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.
Learning objectives of the subject

Study load

<table>
<thead>
<tr>
<th>Total learning time: 150h</th>
<th>Hours large group: 30h</th>
<th>20.00%</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Hours medium group: 0h</td>
<td>0.00%</td>
</tr>
<tr>
<td></td>
<td>Hours small group: 30h</td>
<td>20.00%</td>
</tr>
<tr>
<td></td>
<td>Guided activities: 0h</td>
<td>0.00%</td>
</tr>
<tr>
<td></td>
<td>Self study: 90h</td>
<td>60.00%</td>
</tr>
</tbody>
</table>
# Content

<table>
<thead>
<tr>
<th>Introduction</th>
<th>Learning time: 15h</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Theory classes: 3h</td>
</tr>
<tr>
<td></td>
<td>Laboratory classes: 3h</td>
</tr>
<tr>
<td></td>
<td>Self study: 9h</td>
</tr>
</tbody>
</table>

**Description:**

<table>
<thead>
<tr>
<th>Symmetric Key Cryptography</th>
<th>Learning time: 22h 30m</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Theory classes: 4h 30m</td>
</tr>
<tr>
<td></td>
<td>Laboratory classes: 4h 30m</td>
</tr>
<tr>
<td></td>
<td>Self study: 13h 30m</td>
</tr>
</tbody>
</table>

**Description:**

<table>
<thead>
<tr>
<th>Computational Problems for Cryptography</th>
<th>Learning time: 22h 30m</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Theory classes: 4h 30m</td>
</tr>
<tr>
<td></td>
<td>Laboratory classes: 4h 30m</td>
</tr>
<tr>
<td></td>
<td>Self study: 13h 30m</td>
</tr>
</tbody>
</table>

**Description:**

<table>
<thead>
<tr>
<th>Public Key Cryptography</th>
<th>Learning time: 22h 30m</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Theory classes: 4h 30m</td>
</tr>
<tr>
<td></td>
<td>Laboratory classes: 4h 30m</td>
</tr>
<tr>
<td></td>
<td>Self study: 13h 30m</td>
</tr>
</tbody>
</table>

**Description:**
# Security Models

**Learning time:** 22h 30m  
Theory classes: 4h 30m  
Laboratory classes: 4h 30m  
Self study: 13h 30m  

**Description:**  

---

# Other Cryptographic Primitives

**Learning time:** 22h 30m  
Theory classes: 4h 30m  
Laboratory classes: 4h 30m  
Self study: 13h 30m  

**Description:**  

---

# Advanced Topics

**Learning time:** 22h 30m  
Theory classes: 4h 30m  
Laboratory classes: 4h 30m  
Self study: 13h 30m  

**Description:**  

---

# Qualification system

30% final exam, 40% final report and oral presentation, 30% deliverables

---

# Bibliography

**Basic:**