270131 - C - Cryptography

Coordinating unit: 270 - FIB - Barcelona School of Informatics
Teaching unit: 749 - MAT - Department of Mathematics
Academic year: 2019
Degree: BACHELOR'S DEGREE IN INFORMATICS ENGINEERING (Syllabus 2010). (Teaching unit Optional)
ECTS credits: 6
Teaching languages: Catalan, Spanish

Teaching staff

Coordinator: - Fernando Martínez Sáez (fernando.martinez@upc.edu)
Others: - Anna Rio Doval (ana.rio@upc.edu)
- Jose Luis Ruiz Muñoz (jose.luis.ruiz@upc.edu)

Degree competences to which the subject contributes

Specific:
CEC4.2. To demonstrate comprehension, to apply and manage the guarantee and security of computer systems.
CTI2.3. To demonstrate comprehension, apply and manage the reliability and security of the computer systems (CEI C6).
CTI3.1. To conceive systems, applications and services based on network technologies, taking into account Internet, web, electronic commerce, multimedia, interactive services and ubiquitous computation.
CTI2.2A. To interpret, select and value concepts, theories, uses and technological developments related to computer science and its application derived from the needed fundamentals of mathematics, statistics and physics. Capacity to solve the mathematical problems presented in engineering. Talent to apply the knowledge about: algebra, differential and integral calculus and numeric methods; statistics and optimization.
CTI2.2C. To use properly theories, procedures and tools in the professional development of the informatics engineering in all its fields (specification, design, implementation, deployment and products evaluation) demonstrating the comprehension of the adopted compromises in the design decisions.

Generical:
G3. THIRD LANGUAGE: to know the English language in a correct oral and written level, and accordingly to the needs of the graduates in Informatics Engineering. Capacity to work in a multidisciplinary group and in a multi-language environment and to communicate, orally and in a written way, knowledge, procedures, results and ideas related to the technical informatics engineer profession.
G9. PROPER THINKING HABITS: capacity of critical, logical and mathematical reasoning. Capacity to solve problems in her study area. Abstraction capacity: capacity to create and use models that reflect real situations. Capacity to design and perform simple experiments and analyse and interpret its results. Analysis, synthesis and evaluation capacity.

Teaching methodology

Lectures in which the contents of the subject will be exposed. Lab classes where students solve real situations that can be found in practice.

Learning objectives of the subject

1. Distinguish between cryptosystems that can be safe and those that are snake oil.
2. Distinguish between public-key and secret-key cryptosystems
3. To understand the main ideas of secret-key cryptosystems.
4. To understand the main ideas of public-key cryptosystems.
5.
To understand the idea of digital signature and their role nowadays in internet.

### Study load

| Total learning time: 156h | Hours large group: 30h 19.23% | Hours medium group: 0h 0.00% | Hours small group: 30h 19.23% | Guided activities: 6h 3.85% | Self study: 90h 57.69% |
# Content

## Basic concepts

**Degree competences to which the content contributes:**

**Description:**
- Cryptology, Cryptography, and Cryptanalysis.
- Classic cryptography and modern cryptography.
- Basic techniques: encryption-decryption and signature.
- Private key cryptography and public key cryptography.
- The mathematical bases of cryptography.

## Modern secret key techniques

**Degree competences to which the content contributes:**

**Description:**
- Block encryption, Stream ciphers.
- Data Encryption Standard: Description, History, Standardisation, Cryptanalysis.
- Advanced Encryption Standard: Description, Standardisation.
- Operation modes for block-encrypted systems.

## Public key encryption

**Degree competences to which the content contributes:**

**Description:**
- Multi-precision arithmetic operations. Euclidean algorithms.
- Congruences, multiplication group, modular arithmetic, modular exponential, Chinese Remainder Theorem.
- Calculation of square roots.
- Prime numbers, probabilistic criteria of primeness, random generation of prime numbers.
- Factorising integers, current state of the problem.
- The discrete algorithm problem: variants over Finite Fields and elliptic curves.
- RSA cryptosystem (Rivest, Shamir, Adleman).
- ElGamal cryptosystem.
- Diffie-Hellman key exchange.

## Digital signatures

**Degree competences to which the content contributes:**

**Description:**
- Digital signatures: RSA, DSA and ECDSA
- PKI: digital certificates X509, CRL and OCSP.

## Cryptographic protocols and standards
### Degree competences to which the content contributes:

**Description:**
- Encryption and decryption transformations. Mixed private key - public key techniques.
- Identification schemes and protocols.
- SSL.
- Micro-payments.
- Shared secrets.
- Electronic voting.
- Watermarks.
- SMIME.
- PKCS...

### New trends in Cryptography

**Degree competences to which the content contributes:**

**Description:**
- Lattice-Based Public-Key Cryptography.
- Hyperelliptic curve cryptography.
- Quantum Cryptography.
### Planning of activities

<table>
<thead>
<tr>
<th>Section</th>
<th>Hours</th>
<th>Theory classes:</th>
<th>Practical classes:</th>
<th>Laboratory classes:</th>
<th>Guided activities:</th>
<th>Self study:</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Introduction</strong></td>
<td>6h</td>
<td>2h</td>
<td>0h</td>
<td>2h</td>
<td>0h</td>
<td>2h</td>
</tr>
<tr>
<td><strong>Secret-key cryptography</strong></td>
<td>22h</td>
<td>6h</td>
<td>0h</td>
<td>4h</td>
<td>0h</td>
<td>12h</td>
</tr>
<tr>
<td><strong>Secret-cryptography test</strong></td>
<td>1h</td>
<td></td>
<td></td>
<td></td>
<td>1h</td>
<td>0h</td>
</tr>
<tr>
<td><strong>Public-key cryptography</strong></td>
<td>50h</td>
<td>12h</td>
<td>0h</td>
<td>8h</td>
<td>0h</td>
<td>30h</td>
</tr>
<tr>
<td><strong>Digital signature</strong></td>
<td>8h</td>
<td>4h</td>
<td>0h</td>
<td>0h</td>
<td>0h</td>
<td>4h</td>
</tr>
</tbody>
</table>

**Specific objectives:**

1. 2
2. 3
1. 2, 3
1. 2, 4
1. 2, 3
1. 2, 3
1. 2, 3
1. 2, 3
1. 2, 3
### 270131 - C - Cryptography

<table>
<thead>
<tr>
<th>Specific objectives:</th>
<th>Hours: 19h</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Theory classes: 3h</td>
</tr>
<tr>
<td></td>
<td>Practical classes: 0h</td>
</tr>
<tr>
<td></td>
<td>Laboratory classes: 0h</td>
</tr>
<tr>
<td></td>
<td>Guided activities: 0h</td>
</tr>
<tr>
<td></td>
<td>Self study: 16h</td>
</tr>
</tbody>
</table>

### Protocols and cryptographic standars

<table>
<thead>
<tr>
<th>Specific objectives:</th>
<th>Hours: 1h</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Guided activities: 1h</td>
</tr>
<tr>
<td></td>
<td>Self study: 0h</td>
</tr>
</tbody>
</table>

### public-key test

<table>
<thead>
<tr>
<th>Specific objectives:</th>
<th>Hours: 5h</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Theory classes: 1h</td>
</tr>
<tr>
<td></td>
<td>Practical classes: 0h</td>
</tr>
<tr>
<td></td>
<td>Laboratory classes: 0h</td>
</tr>
<tr>
<td></td>
<td>Guided activities: 0h</td>
</tr>
<tr>
<td></td>
<td>Self study: 4h</td>
</tr>
</tbody>
</table>

### New trends in cryptography

<table>
<thead>
<tr>
<th>Specific objectives:</th>
<th>Hours: 4h</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Theory classes: 0h</td>
</tr>
<tr>
<td></td>
<td>Practical classes: 0h</td>
</tr>
<tr>
<td></td>
<td>Laboratory classes: 1h</td>
</tr>
<tr>
<td></td>
<td>Guided activities: 2h</td>
</tr>
<tr>
<td></td>
<td>Self study: 1h</td>
</tr>
</tbody>
</table>

### eDNI

| Specific objectives:                  | Hours: | |
|---------------------------------------|--------| |
|                                       | Theory classes: | |
|                                       | Practical classes: | |
|                                       | Laboratory classes: | |
|                                       | Guided activities: | |
|                                       | Self study: | |
### secure email

**Specific objectives:**
1, 2, 3, 4, 5

<table>
<thead>
<tr>
<th>Hours</th>
</tr>
</thead>
<tbody>
<tr>
<td>5h</td>
</tr>
</tbody>
</table>

**Theory classes:** 0h  
**Practical classes:** 0h  
**Laboratory classes:** 2h  
**Guided activities:** 2h  
**Self study:** 1h

### Cryptographic hash functions

**Specific objectives:**
5

<table>
<thead>
<tr>
<th>Hours</th>
</tr>
</thead>
<tbody>
<tr>
<td>3h</td>
</tr>
</tbody>
</table>

**Theory classes:** 0h  
**Practical classes:** 0h  
**Laboratory classes:** 1h  
**Guided activities:** 0h  
**Self study:** 2h

### AES

**Specific objectives:**
1, 2, 3

<table>
<thead>
<tr>
<th>Hours</th>
</tr>
</thead>
<tbody>
<tr>
<td>11h</td>
</tr>
</tbody>
</table>

**Theory classes:** 0h  
**Practical classes:** 0h  
**Laboratory classes:** 5h  
**Guided activities:** 0h  
**Self study:** 6h

### Key distribution and digital signatures

**Specific objectives:**
2, 3, 4, 5

<table>
<thead>
<tr>
<th>Hours</th>
</tr>
</thead>
<tbody>
<tr>
<td>10h</td>
</tr>
</tbody>
</table>

**Theory classes:** 0h  
**Practical classes:** 0h  
**Laboratory classes:** 4h  
**Guided activities:** 0h  
**Self study:** 6h
### Cryptographic system

| Hours | Theory classes: 0h  
|       | Practical classes: 0h  
|       | Laboratory classes: 1h  
|       | Guided activities: 0h  
|       | Self study: 0h  |

**Specific objectives:**
2, 3, 4, 5

### Openssl/ TLS

| Hours | Theory classes: 0h  
|       | Practical classes: 0h  
|       | Laboratory classes: 2h  
|       | Guided activities: 2h  
|       | Self study: 6h  |

**Specific objectives:**
3, 4, 5

### Qualification system

There will be two tests in which the total content corresponding to Secret Key Cryptography has a weight of 20% of the final grade and the total content corresponding to Public Key Cryptography has a weight of 40% of the final grade. These two tests may be replaced by a final examination.

The other 40% of the grade will correspond to the laboratory.
Bibliography

Basic:


Complementary: