270131 - C - Cryptography

Coordinating unit: 270 - FIB - Barcelona School of Informatics
Teaching unit: 749 - MAT - Department of Mathematics
Academic year: 2018
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)

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

<table>
<thead>
<tr>
<th>Total learning time: 156h</th>
<th>Hours large group: 30h</th>
<th>19.23%</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>19.23%</td>
</tr>
<tr>
<td></td>
<td>Guided activities: 6h</td>
<td>3.85%</td>
</tr>
<tr>
<td></td>
<td>Self study: 90h</td>
<td>57.69%</td>
</tr>
</tbody>
</table>
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
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

| Introduction | Hours: 6h  
Theory classes: 2h  
Practical classes: 0h  
Laboratory classes: 2h  
Guided activities: 0h  
Self study: 2h |
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Specific objectives:</td>
<td>1, 2</td>
</tr>
</tbody>
</table>

| secret-key cryptography | Hours: 22h  
Theory classes: 6h  
Practical classes: 0h  
Laboratory classes: 4h  
Guided activities: 0h  
Self study: 12h |
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Specific objectives:</td>
<td>1, 2, 3</td>
</tr>
</tbody>
</table>

| Secret-cryptography test | Hours: 1h  
Guided activities: 1h  
Self study: 0h |
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Specific objectives:</td>
<td>1, 2, 3</td>
</tr>
</tbody>
</table>

| public-key cryptography | Hours: 50h  
Theory classes: 12h  
Practical classes: 0h  
Laboratory classes: 8h  
Guided activities: 0h  
Self study: 30h |
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Specific objectives:</td>
<td>1, 2, 4</td>
</tr>
</tbody>
</table>

| Digital signature | Hours: 8h  
Theory classes: 4h  
Practical classes: 0h  
Laboratory classes: 0h  
Guided activities: 0h  
Self study: 4h |
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>
### Specific objectives:

<table>
<thead>
<tr>
<th>Protocols and cryptographic standards</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>

<table>
<thead>
<tr>
<th>public-key test</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>

<table>
<thead>
<tr>
<th>New trends in cryptography</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>

<table>
<thead>
<tr>
<th>eDNI</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>

### Specific objectives:

<table>
<thead>
<tr>
<th>Protocols and cryptographic standards</th>
</tr>
</thead>
<tbody>
<tr>
<td>1, 2, 4, 5</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>public-key test</th>
</tr>
</thead>
<tbody>
<tr>
<td>1, 2, 4, 5</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>New trends in cryptography</th>
</tr>
</thead>
<tbody>
<tr>
<td>1, 2</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>eDNI</th>
</tr>
</thead>
<tbody>
<tr>
<td>2, 5</td>
</tr>
</tbody>
</table>
# 270131 - C - Cryptography

## secure email

**Hours:** 5h  
Theory classes: 0h  
Practical classes: 0h  
Laboratory classes: 2h  
Guided activities: 2h  
Self study: 1h

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

## Cryptographic hash functions

**Hours:** 3h  
Theory classes: 0h  
Practical classes: 0h  
Laboratory classes: 1h  
Guided activities: 0h  
Self study: 2h

**Specific objectives:**  
5

## AES

**Hours:** 11h  
Theory classes: 0h  
Practical classes: 0h  
Laboratory classes: 5h  
Guided activities: 0h  
Self study: 6h

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

## Key distribution and digital signatures

**Hours:** 10h  
Theory classes: 0h  
Practical classes: 0h  
Laboratory classes: 4h  
Guided activities: 0h  
Self study: 6h

**Specific objectives:**  
2, 3, 4, 5
### Cryptographic system

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

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

### Openssl/TLS

**Hours:** 10h  
- Theory classes: 0h  
- Practical classes: 0h  
- Laboratory classes: 2h  
- Guided activities: 2h  
- Self study: 6h

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

### Qualification system

20 % Secret-key test.  
40 % Public-key test.  
40 % Lab.
270131 - C - Cryptography

Bibliography

Basic:


Complementary:


