



*Unitat d'Innovació Docent  
en Educació Superior*

## MODULES TEACHING HANDBOOK

### GENERAL DATA ABOUT THE MODULE

<b>Name of Module</b>	Information, Coding and Security III: Security			
<b>Code</b>	40707			
<b>Course and</b>	First and second semestrer			
<b>Timetable</b>	Monday from 9h to 13h; thursday from 15h to 18h			
<b>ECTS credits</b>	10			
<b>Type of Module</b>	Compulsory (Common in the Master)			
<b>Requirements for the Module</b>	There are no requirements.			
<b>Teaching Language</b>	Catalan, Spanish, English.			
<b>Professor in charge</b>	Dr. Jordi Herrera Joancomartí			
<b>Department in charge</b>	Enginyeria de la Informació i de les Comunicacions (dEIC)			
<b>TEACHERS</b>				
<b>Professor</b>	<b>Depart.</b>	<b>Office</b>	<b>e-mail</b>	<b>Tutorship</b>
Helena Rifà	dEIC	QC-2014	hrifa@deic.uab.cat	To be scheduled
Ramon Martí	dEIC	QC-2009	rmati@deic.uab.cat	To be scheduled
Josep Rifà	dEIC	QC-2027	jrifa@deic.uab.cat	To be scheduled
Sergi Robles	dEIC	QC-2017	srobles@deic.uab.cat	To be scheduled

**SPECIFIC DATA ABOUT THE MODULE**

<p><b>Formative Goals of the Module</b></p>	<p>The objective of this module consists of providing an introduction to information processing, emphasizing the mathematical theory of information and its treatment, the data compression and/or images coding, the encoding for error correction, techniques and cryptographic encoding for the security of the information, applications to communications networks, and the design of applications.</p> <p>After completeness of the module, the student will be able of:</p> <ol style="list-style-type: none"> <li>1. To formulate methods for the compression of the information, image coding, and the codification for error correction.</li> <li>2. To decide what is the type of codification depending on the structure of the channel.</li> <li>3. To analyze and to evaluate the implementation requirements of security algorithms.</li> <li>4. To establish policies of security in the scope of system control.</li> <li>5. To plan and to develop research projects with contents included in the data processing field.</li> </ol>	
	<p><b>Specific Competences of the Module</b></p>	<p><b>Competence</b></p>
<p><b>1. Knowledge:</b></p>		<ul style="list-style-type: none"> <li>• Computer networks.</li> <li>• Cryptography.</li> <li>• Security.</li> </ul>
<p><b>2. Expertise</b></p>		<ul style="list-style-type: none"> <li>• To work in different but related research areas.</li> <li>• Communicative capacity.</li> <li>• Capacity to find solutions.</li> <li>• Resolution of specific tasks.</li> <li>• Analysis and design of a practical process.</li> <li>• Implementation of processes.</li> </ul>
<p><b>3. Attitude</b></p>		<ul style="list-style-type: none"> <li>• Ethical sense.</li> <li>• Quality commitment.</li> <li>• Planning capacity.</li> </ul>

**Structure and  
Contents of the  
Module**

1. Network attacks
  - Attacks and prevention mechanisms at network level
  - Attacks and prevention mechanisms at transport level
  - Attacks and prevention mechanisms at application level
2. Cryptographic basics
  - Private and public key cryptosystems
  - Trust models
  - PKI
  - Long-term signatures
  - e-invoice
3. Advanced networks
  - Introduction to advanced networks and mobile IP
  - Ad-hoc Networks
  - Distributed hash tables and Service Discovery
  - Wireless sensor networks. RFID.
  - Distributed applications
  - Agents
4. Security for advanced networks
  - Access control
  - Single Sign On protocols for web services
  - Federation models
  - Security in ad-hoc networks
  - Security in cognitive radio networks
5. Advanced cryptography
  - Elliptic Cryptography. Curves and rational points.
  - Elliptic curves geometry. Elliptic curves on finite fields.
  - Cryptography based on elliptic curves. The problem of elliptic logarithm. The assignment of messages to points. Interleaved curves. Cryptographic protocols based on EC.

<p><b>Teaching Methodology</b></p>	<p>The methodology applied to the student work will combine the attended lectures, the laboratories, the independent work of the student, the presentation of working papers throughout the course, and the oral and public dissertation about a specific subject previously approved.</p> <p>Distribution of the tasks:</p> <p>Attended activities: 30%</p> <p>Guided learning activities (outside classroom): 40%</p> <p>Learning self-activities (outside classroom): 30% presented/displayed.</p>
<p><b>Evaluation</b></p>	<p>The final evaluation will take into account the portfolio delivered by the students, the attendance and participation in class, and the oral presentation.</p> <ol style="list-style-type: none"> <li>1. Attendance and active participation are compulsory. At least an 80% of the lectures shall be attended. Absences might be compensated with a home-work after agreement with the teacher. Mark: 20%.</li> <li>2. Class activities will be proposed. Some home-works will be compulsory, others will be optional. Mark: 30%.</li> <li>3. Oral presentation of a particular subject. Presentation in English is strongly advised. Mark: 40%.</li> </ol>
<p><b>Bibliography</b></p>	<p><b>References:</b></p> <ul style="list-style-type: none"> <li>• Bruce Schneier, Applied Cryptography, (2nd edition), Wiley, 1995.</li> <li>• M.A. Sarasa López J.P. Franco. Criptografía Digital: Fundamentos y Aplicaciones. Prensas Universitarias de Zaragoza, 1998.</li> <li>• Neal Koblitz. A Course in Number Theory and Cryptography. Springer-Verlag, New York, 1987.</li> <li>• Neal Koblitz. Algebraic Aspects of Cryptography. Springer-Verlag, Berlin, 1998.</li> <li>• Alfred Menezes Neal Koblitz and Scott Vanstone. The state of elliptic curve cryptography. Designs, Codes and Cryptography, 19, 173-193, 2000.</li> </ul>