Program	61IW – Bachelor of Science in Software Engineering 61CI – Bachelor of Science in Computer Engineering 61SI – Bachelor of Science in Information Systems 61TI – Bachelor of Science in Information Society Technologies

Course number and name	
Number	615000355, 615000307, 615000244, 615000721
Name	Information Security
Semester	S4 [(February-June)]

Credits and contact hours	
ECTS Credits	3
Contact hours	30

Coordinator's name	Giannicola Scarpa (g.scarpa@upm.es)

Specific course information

Description of course content

The subject of this course is the study public-key cryptography. We start from the generic definition of a public-key scheme and the different tasks one can achieve within such schemes. Then, we detail algorithms and their underlying mathematical foundations for the tasks of secure key exchange, encryption, and digital signatures. We also cover the concept of hash functions and some common implementations.

We finish with the broader concepts of Certificates, Certification Authorities, and the ISO standards for Information Security Management Systems. These topics are also explored in practice with the aid of didactical software and the industry standard OpenSSL.

The general objectives are: a) To understand the different mathematical concepts and tools underlying the models under consideration; and b) To practice with the integration of encryption and data security tools in a software production environment.

List of topics to be covered

1. Public-key or asymmetric cryptography
    - 1.1. Introduction
    - 1.2. Advantages and disadvantages of public-key crypto
    - 1.3. Diffie-Hellman key exchange
    - 1.4. Extended Euclidean algorithm
    - 1.5. Fast Modular Exponentiation algorithm
2. Principle of RSA
    - 2.1. Principles
    - 2.2. Parameters and key generation
    - 2.3. Encryption and decryption

2.4. Block coding
3. Security aspects of the keys and field elements in RSA
3.1. Alternative private keys
3.2. Alternative public keys
3.3. Non-cipherable inputs
4. Attacks to RSA
4.1. Factoring large numbers
4.2. Cyclic encryption attack
4.3. Birthday attacks
4.4. Side-channel attacks
5. Elgamal's algorithm
5.1. Principles
5.2. Parameters and key generation
5.3. Encryption and decryption
5.4. Block coding
6. Hash functions
6.1. Properties of hash functions.
6.2. MD5, SHA-1 and SHA-2
6.3. SHA-3
6.4. Birthday attacks
7. Digital signature algorithms
7.1. Signature with RSA
7.2. The DSA algorithm
8. Digital Certificates
8.1. Mechanisms of authentication in public-key cryptography
8.2. Digital Certificates
8.3. Certification Authorities
8.4. The X.509 standard
9. Information Security Management Systems
9.1. Introduction to data security policies
9.2. Implementing an ISM system
9.3. Maintenance of an ISM system

Prerequisites or co-requisites

None.

Course category in the program

__X_ **R (required)**	___ **E (elective)** *(elective courses may not be offered every year)*

Specific goals for the course

Specific outcomes of instruction

- RA418 – Understand the DSA algorithm
- RA184 – Understand and apply mathematical algorithm for cryptography
- RA415 – Analysis and application of RSA to encrypt and decrypt data
- RA419 – Understand and analyze hash functions: MD5, SHA-1 y SHA2
- RA420 – Analyze and apply Elgamal's algorithm to encrypt and decrypt
- RA148 – Work as a member of a group in order to develop projects assuming responsibilities, committing towards the goal and plan the use of the available resources. Avoid individualistic behavior in favor of a collaborative effort.

- RA251 – Understand the public key schemes for information exchange (RSA, D-H)
- RA257 – Know the properties and vulnerabilities of RSA keys and the common attacks to the system
- RA252 – Compare symmetric and asymmetric schemes and choose the adequate solution to different requirements
- RA255 – Understand authentication methods, such as digital certificates
- RA254 – Use RSA for digital signatures
- RA78 – Develop information security management systems according to international standards and applicable laws.

Further reading and supplementary materials
– William Stallings. Cryptography and Network Security: Principles and Practice (Pearson). – Bruce Schneier. Applied Cryptography: Protocols, Algorithms, and Source Code in C (Wiley).

Teaching methodology			
_X_ **lectures**	__ **problem solving sessions**	__ **collaborative actions**	_X_ **laboratory sessions**
Other:			