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	615000520, 615000532, 615000740, 615000547
Name	Information Coding
Semester	S7 [(September-January)]

Credits and contact hours	
ECTS Credits	6
Contact hours	60

Coordinator's name	Lias Quintero, Ana Isabel (anaisabel.lias@upm.es)

Specific course information

Description of course content

The subject of this course is the study of the different possibilities to encode the information numerically, depending on the intended goal: conciseness (data compression), integrity (error detection codes) or security (cryptography). The general objectives are: a) To understand the different mathematical concepts and tools underlying the models under consideration; and b) To implement these models, with special attention to efficiency and security issues.

List of topics to be covered

1. Introduction to Information Coding. Cryptology
    - 1.1. Trasmission of Information
    - 1.2. Types of codes
    - 1.3. Compression with variable-length codes: Huffman codification
    - 1.3.1. Introduction to information theory
    - 1.3.2. Huffman codification
    - 1.3.3. Minimal variance Huffman codification
    - 1.4 Error detection codes
    - 1.4.1 Cyclic Redundancy Codes (CRC).
    - 1.5. Cryptography and cryptosystems
    - 1.5.1. Private key cryptosystems
    - 1.5.2. Cryptanalysis
2. Computational complexity
    - 2.1. Problems and algorithms
    - 2.2. Complexity of elemental arithmetic operations

2.3. Classification of problems regarding its complexity

3. Number theory
   - 3.1. The multiplicative group of integers mod n
   - 3.2. Euler's totient function
   - 3.3. Euler and Fermat Theorems
   - 3.4. Order of an element. Primitive root
   - 3.5. Discrete logarithm

4. Public key cryptosystems
   - 4.1. Diffie- Hellman key exchange protocol
   - 4.2. RSA cryptosystem
   - 4.3. ElGamal cryptosystem
   - 4.4. Digital signature
   - 4.5. Other applications

5. Primality tests
   - 5.1. Deterministic tests: Erathostenes' sieve and trial division
   - 5.2. Probabilistic tests: Fermat, Miller and Miller-Rabin

Prerequisites or co-requisites

None.

Course category in the program

__ R (required)	**_X_ E (elective)** *(elective courses may not be offered every year)*

Specific goals for the course

Specific outcomes of instruction

- RA295 - Be able to determine the computational complexity of simple algorithms involving elementary arithmetic operations
- RA297 - Be able to use software properly to solve information coding problems, accurately describing the protocols used
- RA291 - Be able to use different information coding types depending on the goal (error correction, information encryption or information compression)
- RA299 - Be able to compress files using the right compressor codes
- RA290 - Know and apply authentication protocols (digital signature) and key exchange protocols based on public key cryptosystems.
- RA292 - Know and apply deterministic and probabilistic primality tests
- RA294 - Know the difference between public and private key cryptosystems and be able to encrypt and decrypt using translation, affine and affine matrix cryptosystems
- RA298 - Be able to use linear codes for error encoding, detection and correction
- RA293 - Be able to solve open problems, assessing several possible alternatives and arguing for the selected option according to the specified problem-solving criteria. Be able to identify, and design and develop an effective strategy to locate, the information required for the chosen option, and clearly report the result and respective findings.
- RA296 - Be able to apply key results in number theory to cryptology, using the RSA and El-Gamal cryptosystems for encryption and decryption.

Further reading and supplementary materials
– Buchmann, Johannes A: "Introduction to Cryptography". Second Edition. Springer-Verlag. 2004. – Koblitz, Neal: "A Course in Number Theory and Cryptography". Second Edition. Springer-Verlag. 1994 – Trappe, Wade; Washington, Lawrence C.: "Introduction to Crytography with Coding Theory". Prentice-Hall.

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