Cryptography

Academic Year: (2022 / 2023) **Review date: 20-05-2022**

Department assigned to the subject: Computer Science and Engineering Department

Coordinating teacher: GONZALEZ-TABLAS FERRERES, ANA ISABEL

Type: Compulsory ECTS Credits : 6.0

Year : 2 Semester : 1

REQUIREMENTS (SUBJECTS THAT ARE ASSUMED TO BE KNOWN)

Programming (1 course, semester 1)
Discrete Mathematics (1 course, semester 2)
Programming Techniques (1 course, semester 2)

DESCRIPTION OF CONTENTS: PROGRAMME

1.- Introduction to cryptography.
2.- Mathematical foundations of cryptography.
3.- Classic cryptography.
4.- Fundamental cryptography concepts.
5.- Symmetric encryption.
6.- Key distribution and asymmetric encryption.
7.- Hash functions, MAC and authenticated encryption.
8.- Digital signatures schemes.
9.- Public key infrastructure.
10.- User authentication.

LEARNING ACTIVITIES AND METHODOLOGY

LEARNING ACTIVITIES AND METHODOLOGY

THEORETICAL-PRACTICAL CLASSES. [44 hours with 100% classroom instruction, 1.67 ECTS]
Knowledge and concepts students must acquire. Student receive course notes and will have basic reference texts to facilitate following the classes and carrying out follow up work. Students partake in exercises to resolve practical problems and participate in workshops and evaluation tests, all geared towards acquiring the necessary capabilities.

TUTORING SESSIONS. [4 hours of tutoring with 100% on-site attendance, 0.15 ECTS]
Individualized attendance (individual tutoring) or in-group (group tutoring) for students with a teacher.

STUDENT INDIVIDUAL WORK OR GROUP WORK [98 hours with 0 % on-site, 3.72 ECTS]

WORKSHOPS AND LABORATORY SESSIONS [8 hours with 100% on site, 0.3 ECTS]

FINAL EXAM. [4 hours with 100% on site, 0.15 ECTS]
Global assessment of knowledge, skills and capacities acquired throughout the course.

METHODOLOGIES

THEORY CLASS. Classroom presentations by the teacher with IT and audiovisual support in which the subject's main concepts are developed, while providing material and bibliography to complement student learning.

PRACTICAL CLASS. Resolution of practical cases and problem, posed by the teacher, and carried out individually or in a group.

TUTORING SESSIONS. Individualized attendance (individual tutoring sessions) or in-group (group tutoring sessions) for students with a teacher as tutor.

LABORATORY PRACTICAL SESSIONS. Applied/experimental learning/teaching in workshops and laboratories under the tutor's supervision.

ASSESSMENT SYSTEM

EVALUATION SYSTEMS

SE1 - FINAL EXAM. [30 %]
Global assessment of knowledge, skills and capacities acquired throughout the course.

SE2 - CONTINUOUS EVALUATION. [70 %]
Assesses papers, projects, class presentations, debates, exercises, internships and workshops throughout the course.

To pass the course, it is required to get a grade equal or greater to the 40% in the final exam.

% end-of-term-examination:	30
% of continuous assessment (assigments, laboratory, practicals…):	70

BASIC BIBLIOGRAPHY

- Jean-Philippe Aumasson Serious Cryptography: A Practical Introduction to Modern Encryption , Random House LCC US .
- W. STALLINGS CRYPTOGRAPHY AND NETWORK SECURITY. (5ª EDICIÓN), PRENTICE HALL.