Cryptography and computer security

Academic Year: (2021 / 2022) **Review date: 20/07/2021 12:18:48**

Department assigned to the subject: Computer Science and Engineering Department

Coordinating teacher: FUENTES GARCIA ROMERO DE TEJADA, JOSE MARIA

Type: Compulsory ECTS Credits : 6.0

Year : 3 Semester : 1

REQUIREMENTS (SUBJECTS THAT ARE ASSUMED TO BE KNOWN)

Programming (Course 1 / Semester 1)
Discrete Mathematics (Course 1 / Semester 2)
Statistics (Course 2 / Semester 1)
Software development (Course 2 / Semester 2)

OBJECTIVES

The objectives of this course are for the student to recognize the current importance of cryptography and its related technologies, their weaknesses and threats. Likewise, the student must know the principles, methods and means of security systems.
Regarding learning outcomes:
- R1. Knowledge and understanding: Have basic knowledge and understanding of the scientific and technological foundations of computer engineering, as well as specific knowledge of computer science, computer engineering and information systems.
- R2 Engineering Analysis: Be able to identify Computer Engineering problems, recognize their specifications, establish different resolution methods and select the most appropriate for their solution, taking into account the applicable social, human health, environment, and commercial limitations at stake.
- R3 Engineering Design: Being able to carry out engineering designs according to their level of knowledge and understanding. These designs must meet the required specifications and must be done collaborating with other engineers and graduates. Designing encompasses devices, processes, methods and objects, and specifications that are broader than strictly technical, including social awareness, health and safety, and environmental and business considerations.
In relation to basic and general competences, this subject addresses:
- CB1: That students have demonstrated to possess and understand knowledge in an area of study that starts from the base of general secondary education, and is usually found at a level that, although it is supported by advanced textbooks, also includes some aspects that involve knowledge from the forefront of the field of study.
- CGB3: Ability to understand and master the basic concepts of discrete mathematics, logic, algorithmic and computational complexity, and its application to solve engineering problems.
- CGO3 - Ability to design, develop, assess and ensure the accessibility, ergonomics, usability and security of computer systems, services and applications, as well as the information they manage.
Regarding the specific ones:
- CECRI1 - Ability to design, develop, choose and assess computer applications and systems, ensuring their reliability, safety and quality, in accordance with ethical principles and current legislation and regulations.

DESCRIPTION OF CONTENTS: PROGRAMME

1. Fundamentals of computer security
2. Mathematical foundations of cryptography
3. Cryptographic mechanisms and protocols
4. Authentication and Public Key Infrastructures

5. Legal aspects

LEARNING ACTIVITIES AND METHODOLOGY

¿ THEORETICAL-PRACTICAL CLASSES. 1.75 ECTS with 100% attendance. Knowledge that students must acquire. They will receive class notes in electronic form and will have basic reference texts to facilitate the follow-up of the classes and the development of the subsequent work. Exercises, practical problems will be solved by the student and workshops and evaluation tests will be carried out to acquire the necessary skills.
¿ TUTORING. 0.25 ECTS with 100% attendance. Individualized assistance (individual tutorials) or in groups (collective tutorials) to students given by the teacher.
¿ STUDENT INDIVIDUAL OR GROUP WORK. 3.75 ECTS with 0% face-to-face.
¿ WORKSHOPS AND LABORATORIES. 0.25 ECTS with 100% attendance.

Methodology:
¿ MASTER CLASS. Lectures in the teacher's class with the support of computer and audiovisual media, in which the main concepts of the subject are developed and materials and bibliography are provided to complement the students' learning.
¿ PRACTICES. Resolution of practical cases, problems, etc. raised by the teacher individually or in a group.
¿ TUTORING. Individualized assistance (individual tutorials) or in groups (collective tutorials) to students by the teacher. For subjects of 6 credits, 4 hours will be dedicated with 100% attendance.
¿ LABORATORY PRACTICES. Applied / experimental teaching to workshops and laboratories under the supervision of a tutor.

ASSESSMENT SYSTEM

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

SE1. FINAL EXAM. In which the knowledge, skills and abilities acquired throughout the course will be assessed globally. The evaluation percentage varies for each subject in a range between 30% and 60%.

SE2. CONTINUOUS ASSESSMENT. In it, the assignments throughout the course will be graded. The assessment percentage varies for each subject in a range between 40 and 70% of the final grade. It may be required to obtain a minimum performance in the final exam.

In particular:
1. ORDINARY SITTING
1.1. CONTINUOUS ASSESSMENT
The evaluation will be based on the following criteria:
- Resolution of a practical case throughout the course (compulsory): 50%
- Partial exam (compulsory): 20%
- Final exam (compulsory): 30%
Attendance and active participation in class may be considered to obtain additional marks.

To pass the course, two conditions must be met:
- Obtain a grade equal to or greater than 4 out of 10 points in the final exam.
- Achieve, as the sum of all the parts, at least 5 points out of 10.

1.2. NON-CONTINUOUS ASSESSMENT
This alternative applies if any of the proposed assignments or exams is not delivered.
The evaluation will be based on the following criteria:
- Final exam: 60%
The final exam will include specific tests, questions or parts to verify the knowledge that must have been acquired by carrying out the proposed continuous assessment tasks.
To pass the course you must satisfy:
- Achieve at least 5.0 points out of 10.

EXTRAORDINARY SITTING
2.1. IF THE STUDENT FOLLOWED CONTINUOUS ASSESSMENT IN THE ORDINARY SITTING
The evaluation will be based on the following criteria:
- The grade obtained in the continuous evaluation in relation to the works is kept (70%)
- Final exam (mandatory): 30%

To pass the course, two conditions must be met:

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

- Obtain a grade equal to or greater than 4 out of 10 points in the final exam.
- Achieve, as the sum of all the parts, at least 5 points out of 10.

2.2. NON-CONTINUOUS ASSESSMENT

This alternative applies if any of the proposed works were not delivered.

The evaluation will be based on the following criteria:

- Final exam: 100 %

The final exam will include specific tests, questions or parts to verify the knowledge that must have been acquired by carrying out the proposed continuous assessment tasks.

To pass the course you must satisfy:

- Achieve at least 5.0 points out of 10.

BASIC BIBLIOGRAPHY

- A.I. González-Tablas Ferreres y P. Martín González Problem Book 2010-2015. Final Exam problem collection. Cryptography and Computer Security., CopyRed, 2016

- C. Paar Understanding Cryptography: A Textbook for Students and Practitioners, Springer-Verlag, 2014

- J. PASTOR; M.A. SARASA; J.L. SALAZAR CRIPTOGRAFÍA DIGITAL. FUNDAMENTOS Y APLICACIONES. (2ª EDICIÓN), PRENSAS UNIVERSITARIAS DE ZARAGOZA.

- 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.