Cryptographic techniques and protocols

Academic Year: (2021 / 2022) **Review date: 09-06-2021**

Department assigned to the subject:

Coordinating teacher: CAMARA NUÑEZ, MARIA CARMEN

Type: Electives ECTS Credits : 3.0

Year : 1 Semester : 1

OBJECTIVES

The students will acquire the capabilities of usage, analysis and design in the following knowledge areas:

1) Analysis and design of cryptographic protocols.

2) Knowledge and skills to use the classic and modern cryptanalysis techniques.

3) Analysis and design of cryptographic primitives.

4) Hardware basics for the design of cryptographic primitives and algorithms.

DESCRIPTION OF CONTENTS: PROGRAMME

Block 1. Introduction
a. Introduction to cybersecurity.

Block 2. Protocols
a. Standard cryptographic protocols
b. Ultra-light cryptographic protocols

Block 3. Cryptanalysis
a. Cryptanalysis of cryptographic protocols

Block 4. Cybersecurity in devices with limited capabilities
a. Vulnerabilities
b. Attacks
c. Countermeasures

LEARNING ACTIVITIES AND METHODOLOGY

Activities:

1) Theoretical and practical sessions

2) Tutoring

3) Individual work

4) Teamwork

ASSESSMENT SYSTEM

The assessment may be continuous assessment or non-continuous assessment:

1. Ordinary sitting - continuous assessment:

A. End of term examination (50% of the final mark)
-A minimum grade of 4.0 is mandatory to pass the subject

B. Practical cases (50% of the final mark)

2. Ordinary sitting - non-continuous assessment:
A. End of term examination (100% of the final mark)
- A maximum grade of 6.0 may be achieved (i.e. 100% = 6.0)
- At least 5.0 marks must be achieved to pass the subject.
- The exam contains specific parts regarding the competencies that have been addressed in the assignments.

3. Extraordinary sitting
In the extraordinary sitting, the following rules apply:

a. If the student followed the continuous assessment method, the exam will have the same relative weight as in the ordinary sitting. The mark of the continuous evaluation is kept.

b. Otherwise, students will have an exam counting for 100% of the final mark. This exam may contain questions related to the proposed assignments. Assignments cannot be re-delivered in this sitting.

% end-of-term-examination:	50
% of continuous assessment (assigments, laboratory, practicals…):	50

BASIC BIBLIOGRAPHY

- Alfred J. Menezes, Paul C. van Oorschot and Scott A. Vanstone Handbook of Applied Cryptography, CRC Press.

- Christopher Swenson Modern Cryptanalysis: Techniques for Advanced Code Breaking, ohn Wiley & Sons Ltd .

- Colin Boyd and Anish Mathuria Protocols for Authentication and Key Establishment , Springer .

- Dr Sandeep Kumar Sood Authentication Protocols: CRYPTANALYSIS OF PASSWORD BASED AUTHENTICATION AND KEY AGREEMENT PROTOCOLS, LAP LAMBERT Academic Publishing.
- Mark Stamp and Richard M. Low Applied Cryptanalysis: Breaking Ciphers in the Real World, Wiley-Blackwell.

- Pedro Peris-Lopez Lightweight Cryptography in Radio Frequency Identification Systems. Analysis and Design of Protocols and Cryptographic Primitives. , Verlag Dr. Muller (VDM), 2010