Cryptographic techniques and protocols

Academic Year: (2019 / 2020) **Review date: 02-05-2019**

Department assigned to the subject:

Coordinating teacher: PERIS LOPEZ, PEDRO

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

1. Protocols
   1.1 Standard cryptographic protocols.
   1.2 Lightweight cryptographic protocols.

2. Cryptographic primitives
   2.1 Standard cryptographic primitives.
   2.2 Modern cryptographic primitives.

3. Cryptanalysis
   3.1 Cryptanalysis of cryptographic protocols.
   3.2 Cryptanalysis of cryptographic primitives.

4. Hardware implementations
   4.1 Hardware design of cryptographic protocols.
   4.2 Hardware design of cryptographic primitives

LEARNING ACTIVITIES AND METHODOLOGY

Activities:

1) Theoretical and practical sessions

2) Tutoring

3) Individual work

4) Teamwork

ASSESSMENT SYSTEM

The students are grading by a research project about one of the topics reviewed in the course. The students have to show their results in a public presentation.

In detail, the assessment will be done in the following way:

- Report and programming code(s): 85%.
- Oral presentation and explanations: 15%.

Alternatively, the grade of the course could be made through an exam with practical exercises (100% of the grade).

% end-of-term-examination:	100
% of continuous assessment (assigments, laboratory, practicals…):	0

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.