Cryptography and computer security

Academic Year: (2019 / 2020) **Review date: 23-04-2020**

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 : 2

REQUIREMENTS (SUBJECTS THAT ARE ASSUMED TO BE KNOWN)

Programming
Statistics
Discrete Mathematics

OBJECTIVES

The objectives of this course are to make the student aware of the current importance of computer security and to show the vulnerabilities and threats the technology involved faces. Thus, the student will learn the principles and methods used by security systems. In order to achieve these goals, the student must acquire specific knowledge, capacities and attitudes.

Regarding knowledge, at the end of the course the student will be able to:
- Know mathematical fundaments of cryptography and cryptanalysis, especially those related to number theory.
- Master cryptosystems and main encryption algorithms.
- Master digital signature schemes based on public key cryptography.
- Understand the key management problem and main proposed solutions.
- Understand the principles of security measures, focusing on cryptographic systems and protocols, their methods and means.
- Know main authentication systems; acknowledge their advantages and disadvantages
- Distinguish the different security objectives

The capacities the student will acquire can be divided in specific and generic:

Specific capacities:
- Solve number theory problems related to cryptography (P.O.: a)
- Acknowledge the advantages and disadvantages of secret and public key cryptographic systems. (P.O.: a, c)
- Encrypt and decrypt in different environments, identifying possible attacks. (P.O.: a, c)
- Sign and verify in different environments, identifying possible attacks. (P.O.: a, c)
- Design and implementation of the appropriate security mechanisms (mainly cryptographic) for specific information systems (P.O.: a, c, e)
- Apply appropriate authentication mechanisms to different information systems (P.O.: a, c, e)

General capacities:
- Search relevant information to solve a particular problem (P.O.: a, b)
- Solve particular problems with multidisciplinary knowledge (P.O.: a, c, e, g)
- Analyze specific systems to identify vulnerabilities and threats (P.O.: a, b)

Regarding attitudes, the student will be encouraged to:
- Adopt a critical view of the security provided by a particular system (P.O.: i)
- Distrust the purported security of information systems and cryptographic protocols deployed in them. (P.O.: i)

Regarding basic capacities detailed in the third article of the RD 1393/2007 modified by the RD 861/2010, this subject considers capacity CB1.

Regarding capacities specified in section 5 of Annex II of Resolución del 8 de junio de 2009, by the Secretaría General de Universidades (BOE of August 4th of 2009), this subject considers capacity CGB3.

DESCRIPTION OF CONTENTS: PROGRAMME

1. Mathematical background
1.1. Number theory
1.2. Modular arithmetic
1.3. Computation of multiplicative inverses
1.4. Discrete logarithm
1.5. Galois fields
2. Cryptography
2.1. Introduction
2.2. Classic encryption methods and cryptanalysis
2.3. Symmetric cryptosystems.
2.4. Hash functions and MAC
2.5. Asymmetric cryptosystems.
2.6. Key generation and distribution.
2.7. Digital signature.
2.8. Public Key Infrastructure
3. User authentication
4. Introduction to information security
4.1. Threats and vulnerabilities
4.2. Security measures and mechanisms

LEARNING ACTIVITIES AND METHODOLOGY

The teaching methodology includes:

(1) Lectures (2,5 ECTS). Teachers will present the theoretic concepts. It is expected that students participate actively in the lectures. Basic documentation (lecture notes, bibliography, and complementary documentation) will be accessible to students through the web-based learning platform. Students have to read and study the basic documentation (student work). (P.O.: a, c, g, i)
(2) Problem solving (2 ECTS). Students, guided by teachers, will solve a set of representative problems during problem sessions in order to apply the theoretic concepts. Students will solve additional problems outside the regular problem sessions (student work). (P.O.: a, c, g, i)
(3) Laboratory assignments (1,5 ECTS). Students will learn main defensive practical cryptographic tools. Instructions will be published in advance. Students will attend laboratory sessions where teachers will support students in the development of the laboratory assignment. Students will complete the laboratory assignments outside the regular laboratory sessions (student work). (P.O.: a, b, c, e, g, i)

ASSESSMENT SYSTEM

Assessment will consider:
1) Hand in of laboratory assignment results and tests: 30% (P.O.: a, b, c, e, g, i)
The grade will be calculated as the sum of the grades of all lab assessment activities.
2) Exams regarding theory and problems: 70% (P.O.: a, c, g, i)
2.1) Mid-term exam: 30% (during the course)
2.2) Final exam (mandatory). Theory questions and problems: 40%. A minimum grade will be required in the final exam to pass the course.

CONTINUOUS ASSESSMENT ALGORITHM:

TOTAL_GRADE = LAB_GRADE + EX_GRADE + FINAL_EX_GRADE;

IF FINAL_EX_GRADE<2 THEN
--IF TOTAL_GRADE>5 THEN
----TOTAL_GRADE=4,5
--END_IF
END_IF

Additional optional activities may be offered, that will not be taken into account for assignment of MATRÍCULAS DE HONOR, although they will be taken into account for the student final grade.

% end-of-term-examination:	40
% of continuous assessment (assigments, laboratory, practicals…):	60

BASIC BIBLIOGRAPHY

- A. MENEZES HANDBOOK OF APPLIED CRYPTOGRAPHY, CRC PRESS.

- A.I. González-Tablas Ferreres y P. Martín González Problem Book 2010-2015. Final Exam problem collection. Cryptography and Computer Security., CopyRed, 2016
- J. PASTOR; M.A. SARASA; J.L. SALAZAR CRIPTOGRAFÍA DIGITAL. FUNDAMENTOS Y APLICACIONES. (2ª EDICIÓN), PRENSAS UNIVERSITARIAS DE ZARAGOZA.
- W. STALLINGS CRYPTOGRAPHY AND NETWORK SECURITY. (5ª EDICIÓN), PRENTICE HALL.