Cryptography and computer security

Academic Year: (2020 / 2021) **Review date: 10/07/2020 22:19:05**

Department assigned to the subject: Computer Science and Engineering Department

Coordinating teacher: GONZALEZ-TABLAS FERRERES, ANA ISABEL

Type: Compulsory ECTS Credits : 6.0

Year : 3 Semester : 1

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

AF1.THEORETICAL-PRACTICAL CLASSES. Knowledge and concepts students must acquire. Student receive course notes and will have basic reference texts to facilitatefollowing the classes and carrying out follow up work.Students partake in exercises to resolve practical problems and participatein workshops and an evaluation tests, all geared towards acquiring the necessary capabilities.Subjects with 6 ECTS are44 hours as a general rule/ 100% classroom instruction
AF2.TUTORING SESSIONS. Individualized attendance (individual tutoring) or in-group (group tutoring) for students with a teacher.Subjects with 6 credits have 4 hours of tutoring/ 100% on- site attendance.
AF3.STUDENT INDIVIDUAL WORK OR GROUP WORK.Subjects with 6 credits have 98 hours/0% on-site.
AF8.WORKSHOPS AND LABORATORY SESSIONS. Subjects with 3 credits have 4 hours with 100% on-site instruction. Subjects with 6 credits have 8 hours/100% on-site instruction.
MD1.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.
MD2.PRACTICAL CLASS. Resolution of practical cases and problem, posed by the teacher, and carried out individually or in a group.
MD3.TUTORING SESSIONS. Individualized attendance (individual tutoring sessions) or in-group (group tutoring sessions) for students with teacher as tutor. Subjects with 6 credits have 4 hours of tutoring/100% on-site.
MD6.LABORATORY PRACTICAL SESSIONS. Applied/experimental learning/teaching in workshops and laboratories under the tutor's supervision.

ASSESSMENT SYSTEM

% end-of-term-examination/test:	20
% of continuous assessment (assigments, laboratory, practicals…):	80

SE1.FINAL EXAM. Global assessment of knowledge, skills and capacities acquired throughout the course.The percentage of the evaluation varies for each subject between 60% and 0%.
SE2.CONTINUOUS EVALUATION. Assesses papers, projects, class presentations, debates, exercises, internships and workshops throughout the course.The percentage of the evaluation varies for each subject between 40% and 100% of the final grade.
A minimum grade might be required at the final exam.

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

- 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.