Techniques of information hiding

Academic Year: (2023 / 2024) **Review date: 15-09-2023**

Department assigned to the subject: Telematic Engineering Department

Coordinating teacher: MUÑOZ MERINO, PEDRO JOSE

Type: Compulsory ECTS Credits : 6.0

Year : 3 Semester : 1

REQUIREMENTS (SUBJECTS THAT ARE ASSUMED TO BE KNOWN)

Mathematics, Statistics and Computer Science from Module I (basic training), and Statistics from Module III (foundations of engineering).

OBJECTIVES

OBJECTIVES

Know the basic fundations of cryptography and steganography, as well as the technologies that allow their treatment, their weaknesses and the threats they face. In order to achieve these objectives, the student must acquire a range of knowledge, skills and attitudes as detailed below.

KNOWLEDGE

At the end of the course, the student should be able to:
- Know the classic cryptographic systems and the reasons for their insecurity.
- Know the steganography
- Know the mathematical foundations of modern cryptography, as well as the techniques to analyze their security based on cryptanalysis.
- Master the main cryptosystems and the current encryption algorithms.
- Know the signature and verification systems based on public key

CAPACITIES

As regards capacities, they can be broken down into specific and generic (skills).
Concerning specific skills, the learner will be able to
- Solve problems of number theory in its application to cryptography. (P.O.: a)
- Recognize the advantages, disadvantages and uses of secret and public-key systems. (P.O.: a, c)
- Sign and verify in different environments, detecting possible attacks (P.O.: a, c)

As for the general capacities or skills, during the course they will be worked on:
- The ability to find and select relevant information to solve a specific problem. (P.O.: a, b)
- The ability to apply multidisciplinary knowledge to the resolution of a given problem. (P.O.: a, c, e, g)
- The ability to investigate a particular cryptosystem or steganosystem in a given environment and find its vulnerabilities and threats. (P.O.: a, b)

As far as attitudes are concerned, the student after taking the course should have
- A critical attitude towards the security offered by particular encryption or information concealment system, in a given environment and given risks. (P.O.: i)
- A suspicious attitude towards the security supposed by the information hiding systems implemented in the systems. (P.O.: i)

DESCRIPTION OF CONTENTS: PROGRAMME

1. Introduction to Security in Communication Systems and Information Security Concepts
 1.1. Introduction to security in communication systems
 1.2. Different types of attacks in communication systems
 1.3. Information Security Goals
 1.4. Vulnerabilities, Risks, and Attacks
 1.5. Security Measures and Mechanisms
 1.6. Cryptologia
 1.7. Secure Channels

2. Mathematical and Information Theoretic Foundations
 2.1. Number Systems

2.2. Logic Operations with Binary Variables
2.3. Information Theory
2.4. Modular Arithmetic

3. Classic Ciphers
3.1. Monoalphabetic Ciphers
3.2. Polyalphabetic Ciphers
3.3. Polygraphic Ciphers
3.4. Transposition Ciphers
3.5. Rotor Machines

4. Symmetric Ciphers: Stream Ciphers
4.1. Perfect Secrecy: The Vernam Cipher (OTP)
4.2. Pseudorandom Sequence Generators
4.3. Linear Generators: LFSRs
4.4. The A5/1 Cipher
4.5. The RC4 Cipher

5. Symmetric Ciphers: Block Ciphers
5.1. Feistel Networks
5.2. Sustitution-Permutation Networks
5.3. The AES Cipher
5.4. Operation Modes

6. Hash Functions and MAC
6.1. Cryptographic Hash Functions
6.2. The Merkle-Daamgard Construction
6.3. Block Cipher-based Constructions
6.4. The SHA Family
6.5. Message Authentication Codes (MAC)

7. Asymmetric Ciphers
7.1. Diffie-Hellman Key Exchange Protocol
7.2. Assymetric Encryption and Signing Algorithms
7.3. RSA
7.4. Other Public-key Cryptosystems

8. Steganographic algorithms. Types, uses and weaknesses

LEARNING ACTIVITIES AND METHODOLOGY

Teaching methodology includes:

(1) Lectures. The lecturer will present the concepts that students must acquire. The student is expected to actively participate during lectures.

(2) Problems The student, guided by the lecturer during problem-solving lectures, will solve exercises that serve to apply acquired concepts. Students will solve additional problems during their study time (student work).

(3) Laboratories using the computer. The student will learn the use of cryptographic tools. Instructions on how to solve the lab questions will be published. There will be sessions in which a lecturer will give support to students to complete the lab sessions. Students are expected to complete all required tasks in their study time (student work).

ASSESSMENT SYSTEM

The grading system includes continuous assessment of the student's work (tests assessing skils, theoretical, and practical concepts, and also laboratory tasks) and a final assessment through a written exam that will assess the concepts, skills, and abilities acquired throughout the module.

Grading will be done according to the following criteria:

1. Written exams containing both theory and problems: 70% of the final mark, consisting of:
   1.1. Continuous assessment exam: 10% of the final mark. This will take place approximately by mid-term.
   1.2. Final written exam: 60% of the final mark. To pass the module, the student must get a minimum grade of 4 out of 10 in this exam.

2. Partial exam about practical assignments: 30% of the final mark

In the extraordinary exam, the student will choose between:
a) A final written exam accounting for 100% of the final grade. This exam consists of theory, problems, and practical material covered in the lab sessions; or
b) A final written exam accounting for 60% of the final grade. This exam consists of theory and problems. The remaining 40% comes from the grade obtained during the term in the continuous assessment exam (10%) and practical assignments (30%).

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

BASIC BIBLIOGRAPHY

- Alfred J. Menezes, Paul C. van Oorschot and Scott A. Vanstone Handbook of Applied Cryptography, CRC Press, 1996
- Juan Tapiador, Pedro Peris López Criptografía y Ocultación de la Información, Centro Universitario de la Guardia Civil, 2015

BASIC ELECTRONIC RESOURCES

- Alfred J. Menezes, Paul C. van Oorschot and Scott A. Vanstone . Handbook of Applied Cryptography: http://cacr.uwaterloo.ca/hac/