

Academic Year: ( 2024 / 2025 )

Review date: 17-01-2025

Department assigned to the subject: Telematic Engineering Department

Coordinating teacher: MUÑOZ ORGANERO, MARIO

Type: Compulsory ECTS Credits : 6.0

Year : 4 Semester : 1

**REQUIREMENTS (SUBJECTS THAT ARE ASSUMED TO BE KNOWN)**

Basic communication and network protocols concepts. In particular, it is recommended to have passed the following subjects:

- Communications networks and services
- Telematic Applications

A basic knowledge of probability and algebraic structures is also needed, so knowledge of the following subjects if recommended:

- Statistics

**LEARNING OUTCOMES**

CB1: Students have demonstrated possession and understanding of knowledge in an area of study that builds on the foundation of general secondary education, and is usually at a level that, while relying on advanced textbooks, also includes some aspects that involve knowledge from the cutting edge of their field of study

CB2: Students are able to apply their knowledge to their work or vocation in a professional manner and possess the competences usually demonstrated through the development and defence of arguments and problem solving within their field of study.

CG1: Ability to write, develop and sign projects in the area of telecommunications engineering aimed at the design, development and utilization of telecommunications and electronic networks, services and applications, in accordance with the competences acquired in the degree program, as set out in Section 5 of OM CIN 352/2009.

ECRT1: Ability to learn and acquire autonomously the requisite new knowledge for the design, development and utilization of telecommunication systems and services.

ECRT12: Knowledge and use of the concepts of network architecture, protocols and communications interfaces.

ECRT13: Ability to differentiate the concepts of network access and transport, circuit switching and packet switching networks, fixed and mobile networks as well as systems and applications of distributed networks, voice services, audio, data, video and interactive services and multimedia.

ECRT14: Knowledge of methods of network and routing interconnection as well as the fundamentals of network planning and sizing based on traffic parameters.

ETEGITT5: Capacity to apply techniques on which telematics networks, services and applications are based. These include systems for management, signaling and switching, routing, security (cryptographic protocols, tunneling, firewalls, payment authentication mechanisms, and content protection), traffic engineering (graph theory, queuing theory and tele-traffic), tariffication and service reliability and quality, in fixed, mobile, personal, local or long distance environments, with different bandwidths, including by telephone and data.

ETEGITT6: Ability to design network architectures and telematics services.

ETEGITT9: Ability to create, codify, manage, disseminate and distribute multimedia content, in accordance with criteria of usability, accessibility of audiovisual services, diffusion and interactivity.

RA1: Knowledge and understanding of the general fundamentals of engineering, scientific and mathematical principles, as well as those of their branch or specialty, including some knowledge at the

forefront of their field.

RA3: Design. Graduates will have the ability to make engineering designs according to their level of knowledge and understanding, working as a team. Design encompasses devices, processes, methods and objects, and specifications that are broader than strictly technical, including social awareness, health and safety, environmental and commercial considerations

RA4: Research. Graduates will be able to use appropriate methods to carry out detailed research and studies of technical aspects, commensurate with their level of knowledge. The research involves bibliographic searches, design and execution of experiments, interpretation of data, selection of the best proposal and computer simulation. May require consultation of databases, standards and security procedures.

RA5: Applications. Graduates will have the ability to apply their knowledge and understanding to solve problems, conduct research, and design engineering devices or processes. These skills include knowledge, use and limitations of materials, computer models, process engineering, equipment, practical work, technical literature and information sources. They must be aware of all the implications of engineering practice: ethical, environmental, commercial and industrial.

RA6: Generic competences. Graduates will have the generic skills necessary for engineering practice, and which are widely applicable. First, to work effectively, both individually and as a team, as well as to communicate effectively. In addition, demonstrate awareness of the responsibility of engineering practice, social and environmental impact, and commitment to professional ethics, responsibility and standards of engineering practice. They must also have knowledge of business and project management practices, as well as risk management and control, and understand their limitations. Finally, have the capacity for continuous learning.

## OBJECTIVES

Summary: To have the knowledge, to be able to analyze and design and know how to apply to the resolution of specific problems, the main cryptographic techniques, as well as their applications to security systems in telematic networks and services. Students should familiarize themselves with symmetric and asymmetric encryption techniques, hash functions, cryptographic checksums, digital signatures and certificates, authentication protocols and their combined applications.

Detail in terms of knowledge:

- Know the generic environment of the cryptosystem together with the different agents that make it up.
- Know the evolution of the different classic security mechanisms as a basis for modern security mechanisms.
- Know the conventional encryption techniques (symmetric encryption) as well as the current encryption standard (AES) and the previous standard (DES).
- Know the main modes of operation used in symmetric encryption.
- To know the mathematical bases of the main mechanisms of public key encryption. Understand the RSA algorithm in depth.
- Know the different hash techniques and their use in conjunction with public key algorithms to create digital signatures and digital certificates (PKI).
- Know the different techniques of distribution of session keys, both based on public key and based on secret code.
- Know the joint use of the different mechanisms by studying different security protocols (IPSec, SSL, etc.)

Detail in terms of analysis, design and resolution of problems:

- Ability to use the cryptosystem definition as a framework for comparing different security mechanisms to analyze communication systems and networks.
- Ability to use the acquired criteria to evaluate the security of a given protocol.
- Ability to analyze and know how to choose with criteria the most appropriate security algorithm in each circumstance and according to certain requirements.
- Ability to define a security protocol for the resolution of a given scenario and providing security services.
- Ability to use security tools that allow to apply the different mechanisms studied.
- Be able to solve in couple a series of cryptographic challenges such as breaking passwords, determine from encrypted messages how to encrypt and certain parameters of the algorithms as well as generate certificates and digitally sign information.
- Be able to understand recommendations about cryptographic standards.
- Basic capabilities of cryptanalyzing systems

## DESCRIPTION OF CONTENTS: PROGRAMME

This is a basic and introductory subject to communication security covering the main technologies in order to create network security services and secure information transfer channels.

The programme is divided into 4 parts:

1. Introduction to security.
  - 1.1. What is Security?
  - 1.2 Security Mechanisms.
  - 1.3 Security Services.
  - 1.4 Information Theory.
2. Symmetric Cryptography.
  - 2.1 Classical cryptography algorithms.
  - 2.2 Symmetric Encryption algorithms.
  - 2.3 DES. TDES. AES.
  - 2.4 Modes of operation.
  - 2.5 Key distribution mechanisms.
3. Asymmetric Cryptography
  - 3.1 Asymmetric cryptography algorithms.
  - 3.2 Digital Signatures.
  - 3.3 Digital Certificates (identity and attribute certificates).
- 4 Applications.
  - 4.1 IPsec (Network level Security)
  - 4.2 SSL/TLS (Security on TCP connections)

## LEARNING ACTIVITIES AND METHODOLOGY

The learning activities and methodology include:

- Theoretical lectures, problem solving classes in small groups, student presentations, individual tutoring and personal work of the student, including study, tests and exams; oriented to the acquisition of theoretical knowledge.
- Laboratory practices and classes of problems in small groups, individual tutoring and personal work of the student, including study, tests and exams; oriented to the acquisition of practical skills related to the program of each subject.

## ASSESSMENT SYSTEM

<b>% end-of-term-examination:</b>	55
<b>% of continuous assessment (assignments, laboratory, practicals...):</b>	45

The evaluation system has been improved to value all the effort made by the student.

The evaluation system includes the continuous evaluation of the student's work (assignments, laboratory practice reports, class participation and assessment tests of theoretical and practical skills and knowledge) and the final evaluation through a final written exam in which the It will globally evaluate the knowledge, skills and abilities acquired throughout the course.

Specific:

- Continuous evaluation (40%):
  - + Delivery of 4 laboratories carried out in pairs on the different aspects of the subject (30%)
  - + 1 continuous assessment exam (10%) that will facilitate the study of the partial contents of the subject and aim to motivate the completion of class exercises
- Final exam (60%)

## BASIC BIBLIOGRAPHY

- A. J. Menezes, P. C. van Oorschot, and S. A. Vanstone Handbook of Applied Cryptography, CRC Press, August 2001
- Mike Speciner; Radia Perlman; Charlie Kaufman Network Security: Private Communication in a Public World, Prentice Hall, 2002
- William Stallings Cryptography and network security . Principles and Practice, Pearson Education M.U.A., 2014

#### ADDITIONAL BIBLIOGRAPHY

- Martti Lehto, Pekka Neittaanmäki Cyber Security Power and Technology, Springer, 2018
- Xiaodong Lin, Ali Ghorbani, Kui Ren, Sencun Zhu Security and Privacy in Communication Networks: SecureComm 2017 International Workshops, ATCS and SePriIoT, Niagara Falls, ON, Canada, October 22, 23, 24, 25, ... and Telecommunications Engineering, Springer, 2018

#### BASIC ELECTRONIC RESOURCES

- John Black . Network Security: <https://www.youtube.com/watch?v=E03gh1huvW4>