Syllabus
2025 - 2026

TECHNICAL SHEET OF THE SUBJECT

Data of the subject	
Subject name	Cryptography, Digital signature and Blockchain
Subject code	DTC-MCS-512
Mainprogram	Master in Cybersecurity
Involved programs	Máster Universitario en Ingeniería de Telecomunicación y Máster en Ciberseguridad [First year] Máster en Ciberseguridad [First year]
Level	Master
Quarter	Semestral
Credits	6,0 ECTS
Type	Optativa
Department	Department of Telematics and Computer Sciencies
Coordinator	Rafael Palacios Hielscher

Teacher Information	
Teacher	
Name	Luis Hernández Encinas
Department	Department of Telematics and Computer Sciencies
EMail	lhernandez@icai.comillas.edu
Teacher	
Name	Raúl Olivar Merchante
Department	Department of Telematics and Computer Sciencies
EMail	rolivar@icai.comillas.edu
Teacher	
Name	Alonso Alfredo Rodríguez Rodríguez
Department	Department of Telematics and Computer Sciencies
EMail	aarodriguez@icai.comillas.edu
Teacher	
Name	Luis Hernández Álvarez
Department	Department of Telematics and Computer Sciencies
EMail	lhalvarez@comillas.edu

SPECIFIC DATA OF THE SUBJECT

Contextualization of the subject

Prerequisites

There are no prerequisites for this course

Competencies - Objectives

Learning outcomes

The course is aimed at training students in the theoretical concepts of cryptography and its practical use in the world of IT through the use of digital signature and blockchain chains.

From the cryptographic point of view it will be presented the historical facts (classical, medieval encryption systems and encryption machines used throughout the twentieth century) and the elementary concepts that define the current cryptology (security, confidentiality, integrity, availability, identification, etc.). The basic fundamentals and mathematical problems that are the basis of the security of modern cryptology will be explained. Once these fundamentals have been learned, the key exchange/agreement protocols (DH and ECDH), the symmetric (TDES and AES) and asymmetric (RSA and ECC) cryptosystems will be studied in depth, as well as the main ones cryptographic protocols that guarantee the authentication of the participants in a communication (RSA, DSA, ECDSA) and the integrity of the information exchanged (SHA-1, SHA-2, etc.).

As a first practical element of cryptography, its use in **digital signature** systems will be presented, including the bases that support the whole system, from certificates to Certification Authorities and Trusted Service Providers. The legal principles underpinning the entire model, the different types of signatures from functional and technical points of view, and their benefits for business processes and digital transformation will be reviewed. Tests will be developed with an open system (openSSL) and with a cloud signature system certified according to EU Regulation 910/2014 eIDAS. From the security and website point of view, the use of protocols such as SSL/TLS will be presented as elements to guarantee confidence in navigation and transactions.

In chapters relating to **BlockChain** the students will be looking at how conventional Blokchain networks operate. First of all, the functioning of the most popular public networks will be discussed and will go further into studying the Bitcoin and Ethereum networks. The main and most popular attacks regarding these networks will be analysed. We'll have a look at which are the main objectives and we'll go into which are the situations that make the network more vulnerable. Semi-Permissioned networks, their advantages and possible applications, will be studied. We will also go deeper into private networks, discussing common tools we can find when starting an ad-hoc development. To consolidate all the knowledge, practices will be carried out in which the student must use the knowledge acquired in theory lessons.

THEMATIC BLOCKS AND CONTENTS

Contents - Thematic Blocks

Cryptography

Introduction to Cryptography

- Basic concepts
- Historical milestones
- Cryptography and Cryptanalysis

Random Number Generators

- Entropy
- Golomb postulates

- TRNG
- PRNG

Symmetric cryptosystems

- Stream cyphers
- Block cyphers

Mathematical foundations for cryptography

- Algorithms
- Computational complexity
- Modular arithmetic
- Algebraic structures
- Computationally difficult problems
- Elliptic curves

Hash functions

Key-agreement protocols (DH)

Asymmetric cryptosystems

- RSA
- ElGamal
- ECC

Public Key Infrastructure

- Digital signatures (RSA, ECC, DSA, ECDSA, etc.)
- Digital certificates

Software: Cryptool

Digital Signature

Digital certificates y PKI

- Review of the fundamentals of security and cryptography
- Certificate Basics
- Certification Authorities Basics
- PKI and Certification Service Providers

Formats and types of signatures

- Review of concepts
- Electronic signature. Technical Formats
- Electronic signature. Requirements for an electronic signature

- Electronic signature. Types of signature from a functional perspective
- Electronic signature. Types of Signatures from a Legal Perspective
- Electronic signature. Basic examples of signature types

Signature examples

- Introduction to OpenSSL
- Use of hash functions
- Use of symmetric encryption
- CA keys and certificate issuance
- Validation and use of our CA certificate
- ASN.1 structures
- Issuing keys and requesting an user's certificate
- User's certificate issuance from the CA
- Creation of a user PCKS#12 from keys and cert
- Signature of binary files and signature with Acrobat

Regulatory environment

- A little bit of history...
- What is eIDAS?
- The main actors... QTSP (Qualified Trusted Service Providers)
- The digital signature
- Signature devices and environments certifications
- The one to come

Electronic signature as a process transformation agent

- The digital signature as an element of transformation
- A real case... signing employment contracts
- Proposed solution, functional definition of the new model
- Demo/Practice on a real environment

Web trust

- Internet Security and SSL Certificates
- Needs to get the system up and running
- Roots of trust and navigators
- Types of certificates and safety levels
- And what for our website?
- Managing certificates as a key element of business

Introduction to Blockchain networks

- History
- What blockchain is
- Different types of blockchain networks

Bitcoin network

- Operation
- Nodes
- Algorithm
- Wallets

Ethereum network

- Operation
- Algorithms
- EVM

Attacks and security flaws

- Concepts
- Attacks

Semi-Permissioned networks

- Concepts
- Networks

Permissioned networks

- Concepts
- Networks
- Tools

Blockchain use cases

TEACHING METHODOLOGY

General methodological aspects of the subject

- Classroom lessons
- Laboratory practices

EVALUATION AND CRITERIA

Ratings

Grading system:

- Cryptography (42%). Exam.
- Digital Signature (33%). Exam.
- Blockchain (25%): Exam (16.25%) + Labs (8.75%)

BIBLIOGRAPHY AND RESOURCES