Guía docente
330712 - ACR - Criptografía Avanzada

Última modificación: 28/04/2025

Unidad responsable: Escuela Politécnica Superior de Ingeniería de Manresa
Unidad que imparte: 750 - EMIT - Departamento de Ingeniería Minera, Industrial y TIC.

Titulación: MÁSTER UNIVERSITARIO EN APRENDIZAJE AUTOMÁTICO Y CIBERSEGURIDAD PARA SISTEMAS CONECTADOS A INTERNET (Plan 2024). (Asignatura optativa).

Curso: 2025 **Créditos ECTS:** 3.0 **Idiomas:** Inglés

PROFESORADO

Profesorado responsable: Battagliola Michele

Otros:

METODOLOGÍAS DOCENTES

OBJETIVOS DE APRENDIZAJE DE LA ASIGNATURA

CONTENIDOS

(CAST) TOPIC 1: Basic algebra introduction

Dedicación: 6h
Grupo grande/Teoría: 2h
Aprendizaje autónomo: 4h

(CAST) TOPIC 2: Introduction to provable security

Dedicación: 6h
Grupo grande/Teoría: 2h
Aprendizaje autónomo: 4h

(CAST) TOPIC 3: Encryption Scheme

Dedicación: 16h
Grupo grande/Teoría: 4h
Grupo pequeño/Laboratorio: 2h
Aprendizaje autónomo: 10h

(CAST) TOPIC 4: Digital Signatures and Zero Knowledge Proofs

Dedicación: 17h
Grupo grande/Teoría: 6h
Grupo pequeño/Laboratorio: 2h
Aprendizaje autónomo: 9h

(CAST) TOPIC 5: Multi-Party Computation and Threshold Protocols

Dedicación: 11h 30m
Grupo grande/Teoría: 4h 30m
Aprendizaje autónomo: 7h

(CAST) TOPIC 6: Evoting

Dedicación: 7h
Grupo grande/Teoría: 3h
Aprendizaje autónomo: 4h

(CAST) TOPIC 7: Post quantum cryptography

Dedicación: 11h 30m
Grupo grande/Teoría: 4h 30m
Aprendizaje autónomo: 7h

ACTIVIDADES

(CAST) LECTURES

Dedicación: 26h
Grupo grande/Teoría: 26h

(CAST) LABORATORY WORK

Dedicación: 4h
Grupo pequeño/Laboratorio: 4h

(CAST) INDEPENDENT STUDY

Dedicación: 41h
Aprendizaje autónomo: 41h

(CAST) EXAM

Dedicación: 4h
Aprendizaje autónomo: 4h

SISTEMA DE CALIFICACIÓN

BIBLIOGRAFÍA

Básica:
- Boneh, Dan ; Shoup, Victor. A Graduate course in applied cryptography [en línea]. 2023 [Consulta: 08/10/2024]. Disponible a: https://toc.cryptobook.us/book.pdf.
- Selection of scientific papers indicated during the lectures.