Ana I. González-Tablas Ferreres
José María de Fuentes García-Romero de Tejada
Lorena González Manzano
Pablo Martín González
UNIVERSIDAD CARLOS III DE MADRID |

PRESENTACIÓN BLOQUE 1

El primer bloque del curso introduce la disciplina de criptografía y sus fundamentos, en cuatro temas.

- En el Tema 1 los alumnos aprenderán los undamentos matemáticos de la criptografía, aprendiendo las operaciones básicas de la aritmética modular en grupos finitos de enteros y polinomios con coeficientes binarios.

- En el Tema 2 se introducen los conceptos básicos de la criptografía incluyendo qué es un criptosistema y cuáles son sus características principales, así como la seguridad de los algoritmos criptográficos se fundamenta en el criptoanálisis de éstos.

- En el Tema 3 se explica cómo la teoría de la información fundamenta la criptografía moderna a través de los conceptos de entropía y entropía condicionada, así como otros conceptos intrísecamente ligados a la criptografía y su seguridad, como la aleatoriedad y la complejidad algorítmica.

- Por último, en el Tema 4 se estudian los principales algoritmos de criptografía clásica y su criptoanálisis, pues permite ilustrar con mayor facilidad los conceptos y técnicas utilizados en la criptografía moderna.

Material asociado

Como material asociado a este tema se incluye el material de teoría y una colección de ejercicios propuestos con su solución sobre los aspectos tratados en el tema. Además se ofrecen un conjunto de pruebas de respuesta objetiva, con soluciones, que permiten a los alumnos verificar su grado de aprendizaje en este módulo.