

Contenidos

Tema 1. Fundamentos matemáticos y criptografía clásica

Conceptos básicos

Aritmética modular

Criptografía clásica

Tema 2. Algoritmos de criptografía simétrica

Cifradores de bloque

Cifradores de flujo

Funciones resumen

Tema 3. Algoritmos de criptografía asimétrica

Cifradores asimétricos

Certificados y firmas digitales

Tema 4. Protocolos de intercambio de claves

Gestión de claves simétricas

Protocolos de comunicación

Tema 5. Criptoanálisis y ataques criptográficos

Conceptos básicos

Ataques a los operadores criptográficos

Ataques a los protocolos criptográficos