Criptografía

Contenidos/descriptores:

I. Conceptos básicos:
Confidencialidad.
Criptoanálisis y tipos de ataques.
Criptografía simétrica y asimétrica.
Funciones resumen y firma digital.
II. Algoritmos básicos:
Tests de primalidad.
Algoritmos de factorización.
Logaritmos discretos.
Curvas elípticas sobre cuerpos finitos.
III. Protocolos:
Pruebas de conocimiento cero.
Esquemas de uso compartido de secretos.
Firmas ciegas, acreditación e identificación.
Voto electrónico.
E-comercio, moneda electrónica.