



13020 CRIPTOGRAFÍA (OPTATIVA)

2º SEMESTRE. 6 créditos (3 teóricos + 3 prácticos)
PROFESOR/ES: D. José M.ª Muñoz Pomas
D. Francisco José Plaza Martín

PROGRAMA

1. Aritmética. Aritmética Modular. Teorema chino de los restos. Números primos. Cuerpos finitos. Complejidad computacional. Factorización. 2. Criptosistemas de clave privada. Cifrados de sustitución, trasposición, afines y en flujo. 3. Criptografía de clave pública. Logaritmo discreto. Cifrados RSA, Diffie-Hellman, Massey-Omura. 4. Protocolos criptográficos. Funciones hash. Protocolos de firma digital, conocimiento cero, etc.

BIBLIOGRAFÍA

JOHANNES BUCHMANN: "Introduction to cryptography". Undergraduate texts in mathematics, Springer.
NEAL KOBLITZ: "A Course in Number Theory and Cryptography". Graduate Texts in Mathematics, 114, Springer.
AMPARO GUSTER SABATER: "Técnicas criptográficas de protección de datos". Madrid: Ra-ma, cop. 2004.
D. WELLSCH: "Codes and Cryptography". Oxford Univ. Press, New York, 1988.

OBJETIVOS

El objetivo de este curso es dar al alumno un conocimiento básico de los principales métodos de encriptación de uso en la actualidad. Se pondrá especial énfasis en sus aplicaciones prácticas así como en la implementación de los sistemas y protocolos.

EVALUACIÓN

Evaluación continuada durante el curso y trabajo al final del mismo.