



Departamento de
Matemática Aplicada I

Criptografía

Optativa de 5° curso de Ingeniería Informática

Segundo cuatrimestre

Curso 2004/2005

Programa

● Introducción

La historia de los secretos. Algunos usos de la Criptografía. Trasposición y sustitución. Algunos criptosistemas de sustitución. Seguridad. Distintos tipos de ataque. El oponente. Confusión y difusión. Criptoanálisis. Secreto perfecto.

● Cifrado polialfabético clásico

Criptosistema de Vigenère. Criptoanálisis. Criptoanálisis del criptosistema de Vigenère. XOR simple. Criptoanálisis. Otros criptosistemas.

● Cifrado simétrico

Criptosistemas de clave secreta (simétricos) Blowfish. El criptosistema AES.

● Aritmética modular

Inversos en \mathbb{Z}_n . Función de Euler. Primer teorema de Fermat. Teorema Chino del Resto. Función de Euler y factorización. Números grandes.

● Cifrado de clave pública

La idea fundamental de los criptosistemas de clave pública. Funciones de un solo sentido. Diferencias con los sistemas clásicos. Autenticación. Intercambio de claves. Método de Diffie-Hellman.

● Criptosistema RSA

El criptosistema RSA. Implementación. Primalidad. Seudoprimos. Números de Carmichael. Test de Solovay-Strassen y de Miller-Rabin. La implementación de RSA en la práctica. Exponenciación modular. Seguridad de RSA: primeros métodos de factorización de números grandes.

Autenticación y firmas digitales

Los problemas de autenticación. Funciones de autenticación. Códigos de autenticación de mensajes. Funciones resumen simples. Seguridad de las funciones resumen. Firmas digitales.

● Criptosistema de ElGamal

Criptosistema de ElGamal. El logaritmo discreto. Algoritmos de Polling-Hellman y de Shanks. El método del cálculo del índice. Seguridad del criptosistema de ElGamal.

Prácticas: Algoritmos de solución del problema del logaritmo discreto: implementación y pruebas. cifrado y descifrado con el criptosistema de ElGamal. Criptoanálisis de casos concretos del criptosistema de ElGamal.

● Criptosistema de Merkle-Hellman

Criptosistema de Merkle-Hellman: el problema de la mochila. Algoritmo para sucesiones supercrecientes. Implementación del criptosistema de Merkle-Hellman. Seguridad. Criptoanálisis de Lenstra-Shamir. Otros criptosistemas basados en el problema de la mochila.

● Sobres digitales

Concepto de sobre digital. PGP. Seguridad de PGP. Otros criptosistemas.

Bibliografía

- William Stallings: *Cryptography and network security. Principles and Practice*. Prentice hall, 1999.
- Stinson, Douglas R: *Cryptography. Theory and Practice*. CRC Press. 1995.
- Schneier, Bruce: *Applied cryptography*. John Wiley & Sons 1996.
- Konheim, Alan: *Cryptography: A primer*. John Wiley & Sons 1981.
- Joseph Silverman: *A Friendly Introduction to Number Theory*. Prentice Hall 1996.
- Charles Kaufman, Radia Perlman, Michael Speciner: *Network Security: Private Communication in a Public World*. Prentice Hall 1995.
- Ramanujachary Kumanduri, Cristina Romero: *Number Theory with Computer Applications*. Prentice Hall 1998.

Metodología

Consulte la [Página de material](#) para el curso actual.

Evaluación

Para superar la asignatura los alumnos podrán optar por las siguientes modalidades (no excluyentes):

Prácticas

Dado el carácter eminentemente aplicado de esta asignatura todas las clases tendrán una orientación práctica.

Profesores

- **Álvarez Solano, Víctor** ⓘ
Grupo 2 (teoría y prácticas).
- **Armario Sampalo, José Andrés** ⓘ
Grupo 2 (teoría y prácticas).
- **Valeiras Reina, Gerardo** ⓘ
Grupo 1 (teoría y prácticas).

Tutorías

Los horarios de tutoría y asistencia al alumnado se publicarán en el Departamento.

