Departamento de Matemática Aplicada I

Criptografía

Optativa de 5° curso de Ingeniería Informática

Segundo cuatrimestre

Curso 2002/2003

Programa

Introducción

Algunos usos de la Criptografía. Conceptos generales sobre criptosistemas. Seguridad. Distintos tipos de ataque. Características del oponente. Criptoanálisis.

Teoría elemental de números: algunos criptosistemas simples.

Divisibilidad y el algoritmo de Euclides. Números primos. La aritmética de las congruencias. Criptosistema por desplazamiento. Criptoanálisis. Clave afín. Índice de coincidencia. Criptoanálisis de la clave afín. Criptosistemas de permutación y sustitución. Criptoanálisis.

Prácticas: cifrado y descifrado con el criptosistema afín. Intercambio de mensajes cifrados con el criptosistema afín. Criptoanálisis de mensajes cifrados con el criptosistema afín. Obtención de la clave a partir del mensaje cifrado. cifrado y descifrado con criptosistemas de sustitución. Intercambio de mensajes cifrados por sustitución. Criptoanálisis de mensajes cifrados por sustitución. Obtención de la clave a partir del mensaje cifrado.

Otros criptosistemas clásicos

Criptosistema de Vigenère. Criptoanálisis. XOR simple Criptosistema de Hill. Diferentes ataques al criptosistema de Hill. Criptosistemas en flujo. Criptosistemas producto.

Prácticas: cifrado y descifrado con el criptosistema de Vigenère. Intercambio de mensajes cifrados con Vigenère. Criptoanálisis de mensajes cifrados con Vigenère. Obtención de la clave a partir del mensaje cifrado. cifrado y descifrado con XOR simple y comparación con Vigenère. Criptoanálisis. Cifrado y descifrado con el criptosistema de Hill.

Uso de los algoritmos criptográficos

cifrado de canales de comunicación. cifrado de datos para almacenamiento. cifrado por hardware y por software. Compresión y cifrado. Los criptosistemas clásicos en este contexto.

Teoría de la Información. Complejidad

Secreto perfecto. Seguridad. Entropía e incertidumbre. Propiedades. Ratio de un lenguaje. Confusión y difusión. Complejidad de problemas.

Aritmética modular

Inversos en en Z_n. Función de Euler. Primer teorema de Fermat. Teorema Chino del Resto. Función de Euler y factorización. Números grandes.

Prácticas: Cálculo de inversos en Z Implementación de un algoritmo para el Teorema Chino del Resto. Cálculo efectivo de la función de Euler. Primeros algoritmos de factorización.

Criptosistemas de clave pública

La idea fundamental de los criptosistemas de clave pública. Funciones de un solo sentido. Diferencias con los sistemas clásicos. Autentificación. 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.

Prácticas: Uso práctico de los test de primalidad para la obtención de primos aleatorios grandes. Generación de claves RSA. Pruebas de factorización de números grandes. cifrado y descifrado con el criptosistema RSA. Intercambio de mensajes RSA con claves inseguras. Criptoanálisis. Intercambio de mensajes RSA con claves seguras.

Autentificación y firmas digitales

Los problemas de autentificación. Funciones de autentificación. Códigos de autentificación 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.

Prácticas: cifrado y descifrado con el criptosistema de Merkle-Hellman. Criptoanálisis del criptosistema de Merkle-Hellman con claves inseguras. Criptoanálisis de Shamir: casos prácticos.

Algunos criptosistemas de clave privada y mixtos

Criptosistema IDEA. PGP. Seguridad de PGP. Otros criptosistemas

Prácticas: cifrado y descifrado con el criptosistema IDEA. Intercambio de mensajes cifrados con IDEA. Generación de claves PGP. cifrado y descifrado con PGP. Intercambio de mensajes cifrados con PGP.

Bibliografía

- **William Stallings**: ***Criptography and network security. Principles and Practice.*** Prentice hall, 1999.
- **Stinson, Douglas R**: ***Criptography. Theory and Practice.*** CRC Press. 1995.
- **Schneier, Bruce**: ***Applied criptography.*** John Wiley & Sons 1996.
- **Konheim, Alan**: ***Criptography: 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

Apuntes

El Departamento no tiene publicados apuntes de esta asignatura. Deberán usarse las notas de clase y la bibliografía.

Evaluación

Los alumnos pueden optar por realizar un trabajo de desarrollo práctico del algunos temas relacionados con los contenidos de la asignatura o realizar un examen en la fecha fijada por el centro. Este examen consistirá en varios ejercicios de carácter teórico práctico. Los trabajos propuestos y la forma de su adjudicación se determinarán al comienzo de las clases.

Prácticas

Dado el carácter eminentemente aplicado de esta asignatura todas las clases tendrán una orientación práctica y siempre que sea posible se impartirán en el laboratorio.

Se utilizarán programas diseñados especialmente para estas prácticas. Los alumnos que lo deseen podrán obtener una copia del programa de instalación en Cripto MiniLab.

Profesores

- **Martín García, Elena**
  Grupo 1.
- **Valeiras Reina, Gerardo**

Tutorías

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