UNIVERSIDAD DE SEVILLA
Dpto. Matemática Aplicada I

Criptografía

Optativa de 5° curso

Curso 2000/2001 2° Cuatrimestre

INGENIERO EN INFORMÁTICA

Introducción

El increible desarrollo reciente de las capacidades de computación de los sistemas informáticos y el auge de las comunicaciones electrónicas, ha vuelto a poner en el centro del interés los temas relacionados con la confidencialidad y la seguridad.

Los orígenes de la escritura secreta pueden remontarse casi a los orígenes de la historia. Por otra parte los avances en matemáticas, en temas abstractos y *aparentemente sin aplicación,* aplicados a la moderna criptografía, han permitido el desarrollo de técnicas criptográficas que sin necesidad de grandes sistemas, permiten un nivel de seguridad impensable sólo hace unos años.

El objetivo de esta asignatura es el desarrollo de las principales técnicas criptográficas actuales, poniendo especial énfasis en sus aspectos prácticos. De hecho se intentará que la mayoría de las clases se impartan en un laboratorio donde los alumnos podrán experimentar con programas de ordenador diseñados especialmente.

Se abordan en primer lugar los criptosistemas clásicos, estudiando su debilidad y experimentando con programas capaces de romper fácilmente estos códigos. A continuación se centra el estudio en la moderna criptografía de clave pública, recorriendo los principales sistemas y estudiando sus distintos niveles de seguridad, así como su aplicación en distintos contextos relacionados con la informática y las comunicaciones.

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.

- Clave afín. Índice de coincidencia. Criptoanálisis de la clave afín.
- Criptosistemas de permutación y sustitución. Criptoanálisis.
- *Prácticas:*
    - Codificación y descodificación con el criptosistema afín.
    - Intercambio de mensajes codificados con el criptosistema afín.
    - Criptoanálisis de mensajes codificados con el criptosistema afín. Obtención de la clave a partir del mensaje codificado.
    - Codificación y descodificación con criptosistemas de sustitución.
    - Intercambio de mensajes codificados por sustitución.
    - Criptoanálisis de mensajes codificados por sustitución. Obtención de la clave a partir del mensaje codificado.

Otros criptosistemas clásicos

- Criptosistema de Vigenère. Criptoanálisis.
- XOR simple
- Criptosistema de Hill. Diferentes ataques al criptosistema de Hill. .
- Criptosistemas en flujo.
- Criptosistemas producto.
- *Prácticas:*
    - Codificación y descodificación con el criptosistema de Vigenère.
    - Intercambio de mensajes codificados con Vigenère.
    - Criptoanálisis de mensajes codificados con Vigenère. Obtención de la clave a partir del mensaje codificado.
    - Codificación y descodificación con XOR simple y comparación con Vigenère. Criptoanálisis.
    - Codificación y descodificación con el criptosistema de Hill.

Uso de los algoritmos criptográficos

- Codificación de canales de comunicación.
- Codificación de datos para almacenamiento.
- Codificación por hardware y por software.
- Compresión y codificación.
- 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_n mediante distintos algoritmos.
  - 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.
  - Codificación y descodificación 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.
  - Codificación y descodificación 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:*
  - Codificación y descodificación 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:*
  - Codificación y descodificación con el criptosistema IDEA.
  - Intercambio de mensajes codificados con IDEA.
  - Generación de claves PGP.
  - Codificación y descodificación con PGP.
  - Intercambio de mensajes codificados con PGP.

BIBLIOGRAFIA

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.