♦2.2.29. CRIPTOGRAFÍA (5º) (Ingeniero en Informática)

PROFESORADO

Profesor coordinador de la asignatura: D. Gerardo Valeiras Reina
- Consúltese Plan de Organización Docente

PROGRAMACIÓN DE LA ASIGNATURA

La asignatura *Criptografía* se imparte como optativa en el segundo cuatrimestre de 5º curso de Ingeniería informática con 4 horas semanales de clases que incluyen las prácticas.

Introducción
El increíble 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

Teoría elemental de números
Divisibilidad y el algoritmo de Euclides. Números primos.
Congruencias. Primer teorema de Fermat. Teorema Chino del Resto.
Función de Euler y factorización. Números grandes.

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

Algunos criptosistemas simples
Conceptos generales sobre criptosistemas.
Criptoanálisis. Distintos tipos de ataque. Seguridad.
Criptosistema por desplazamiento. 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.
Criptosistema de Hill. Diferentes ataques al criptosistema de Hill.
XOR simple.
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 el criptosistema de Hill.
Intercambio de mensajes codificados con Hill.
Criptoanálisis de mensajes codificados con Hill.
Codificación y descodificación con XOR simple y comparación con Vigenère. Criptoanálisis.

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.

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.

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.

Horario
La asignatura se impartirá semanalmente durante el segundo cuatrimestre los lunes de 12:30 a 14:30 y los miércoles de 10:30 a 12:30. Dado el carácter práctico y aplicado del curso, se intentará que se imparta en un laboratorio, para que los asistentes puedan experimentar con los algoritmos y programas del curso.

Profesores
Gerardo Valeiras Reina
Departamento de Matemática Aplicada I
Universidad de Sevilla
geval@cica.es
http://euler.fie.us.es/geval