CC51K SEGURIDAD DE DATOS Y FIRMAS DIGITALES
10 UD

Semestre 2000/1 Prof. Roberto Opazo

1. Requisitos

CC30A Algoritmos y Estructuras de Datos.
CC30B Fundamentos de Ciencias de la Computación.

2. Objetivos

El objetivo central del curso es entregar a los alumnos una base teórica y práctica que les permita analizar, diseñar e implementar sistemas seguros en un entorno abierto.

Al final del curso, los alumnos deberán comprender los principales conceptos y técnicas presentes en la seguridad de sistemas, así como los métodos más eficaces para evitar posibles ataques o violaciones de seguridad.

Los alumnos deberán desarrollar un conocimiento adecuado del estado del arte de la criptografía moderna y sus aplicaciones para garantizar privacidad y autenticidad de la información digital.

3. Contenidos Específicos

3.1 Palabras clave

Autenticación, Autenticidad, Certificado, Confusión, DES, DSA, DSS, Encriptamiento, Estampas de Tiempo, Difusión, Dispositivo Biométrico, Firma Digital, Hash, IDEA, Integridad, IP, IPSec, MIME, PGP, Privacidad, RC2, RC4, RC5, RC6, RSA, SET, S/MIME, S-DES, SSL.

3.2 Estructura del Curso

El curso está planificado considerando 10 UD, que equivalen a 10 horas de trabajo semanal, en las cuales se incluyen 2 módulos de cátedra (1,5 horas c/u), un módulo para clase auxiliar o trabajo conjunto en laboratorio (1,5 horas) y 5,5 horas de estudio o trabajo personal.

El semestre dura 15 semanas, por lo que se dispone de 30 módulos de cátedra, los que se dividen en 19 clases del profesor, 4 charlas de expositores invitados, 3 controles, un examen y 1 módulo de holgura para adaptar el plan a algún tipo de imprevisto.

El contenido del curso está separado en las siguientes secciones:

3.2.1 Motivación (2 Clases)

Historia de la criptografía, desde los Egipcios hasta Internet, incluyendo la definición de las 2 guerras mundiales, gracias a los exitosos ataques de análisis criptográfico de los aliados.

3.2.2 Criptografía Simétrica (7 Clases)

Definiciones y algoritmos convencionales de encriptamiento, basados en una clave compartida por el emisor y receptor del mensaje.

Se estudiarán sistemas basados en sustitución y permutación, tanto en el ámbito de caracteres, como de bloques de texto. Algunos métodos específicos a estudiar son "Encriptador de Cesar", "Encriptador por Sustitución", "Encriptador de Playfair", "Encriptador de Hill", "Encriptador por Permutación" y "Rotores". Todos estos métodos son relevantes por las técnicas de ataque que pueden ser utilizadas en cada uno de ellos, más que por su uso práctico.

Además, se estudiarán técnicas modernas de criptografía simétrica, tales como DES (Data Encryption Standard), su versión académica S-DES (Simplified DES) y su análisis criptográfico diferencial y lineal.

Al final de la sección se analizará la vigencia de este estándar y sus alternativas, como Triple DES, IDEA y sus posibles reemplazantes, como MARS, RC6 y Twofish, entre otros.

3.2.3 Criptografía Asimétrica (7 Clases)

Definiciones y algoritmos usados en un esquema de llaves públicas y privadas.

Se estudiará el uso de estas técnicas para proveer privacidad y autenticidad en los mensajes. Se realizará un estudio detallado de los métodos estándares actuales (tales como RSA) para implementar privacidad (encriptamiento) y autenticidad (firmas digitales), incluyendo gran parte de la teoría de números en que se basan dichas técnicas (números primos y aritmética modular entre otros).

También se estudiarán algunos aspectos prácticos para la implementación de este tipo de modelos, como distribución de llaves privadas.

3.2.4 Cable a Tierra (2 Clases, 3 Charlas)

Se revisará el uso práctico de los conceptos aprendidos, su utilización actual a escala mundial y algunas experiencias en Chile.

Se estudiarán aspectos legales relevantes para la implementación de firmas digitales, revisando el estado de la normativa en Estados Unidos y la Comunidad Europea. En este contexto, será de particular interés el estudio del uso de firmas digitales en la administración pública chilena y el proyecto de ley de firmas digitales presentado en el congreso chileno.

Otros usos prácticos de los métodos criptográficos a revisar son las redes privadas virtuales (VPN) y tarjetas inteligentes.

También se estudiarán algunas tecnologías complementarias en la definición de un sistema seguro, como lectores de características biológicas de los usuarios.

3.2.5 Seguridad en Internet (3 Clases, 1 Charla)

Implantación de modelos de seguridad en empresas conectadas a Internet. Revisión del modelo de seguridad en UNIX y NT, análisis de mecanismos de protección, tales como router y firewall.

Alcances para la utilización del correo electrónico en forma segura (PGP, S/MIME), instalación de un certificado X.509 y habilitación de SSL, S/MIME, SET, entre otros.

3.3 Charlas de Expositores Invitados

Para apoyar los aspectos contenidos en el plan del curso, se realizarán las siguientes charlas:

- "Aspectos Legales de las Firmas Digitales": Será dictada por un abogado experto en derecho informático. Sección "Cable a Tierra".
- "Firmas Digitales en la Administración Pública": Será dictada por un asesor de la administración pública, que haya participado en el proceso estatal. "Sección Cable a Tierra".

· "Dispositivos Biométricos": Charla demostrativa de un vendedor de dispositivos biométricos. Será dictada por un representante de una empresa privada, que comercialice alguno de los dispositivos más utilizados a escala mundial. Sección "Cable a Tierra".

· "Firewall": Charla demostrativa de un Firewall comercial. Será dictada por un representante de una empresa privada, que comercialice alguno de los productos de firewall más utilizados a escala mundial. Sección "Seguridad en Internet".

4. Esquema de Evaluación

El curso tendrá 3 controles, 3 tareas y un examen. La nota final será obtenida según los siguientes porcentajes:

Promedio de Controles:	50%
Promedio de Tareas:	30%
Examen:	20%

5. Bibliografía

- "Handbook of Applied Cryptography", Menezes, van Oorschot & Vanstone, 1997, CRC Press.
  ISBN 0849385237

- "Cryptography, Theory & Practice", D. Stinson, 1995, CRC Press.
  ISBN 0849385210

- "Cryptography and Network Security: Principles and Practice", W. Stallings 1998, Prentice Hall.
  ISBN 0138690170

- "Applied Cryptography: Protocols, Algorithms, and Source Code in C, second edition", B. Schneier, 1995, John Wiley & Sons.
  ISBN 0471128457

- "The Codebreakers; The Comprehensive History of Secret Communication from Ancient Times to the Internet" David Kahn, 1996.
  ISBN: 0684831309