UNIVERSIDAD DIEGO PORTALES
Facultad de Ingeniería
Escuela de Ingeniería Informática

PROGRAMA DE ESTUDIOS 2004

ASIGNATURA	:	**SEGURIDAD DE DATOS**
Código	:	INF2021
Pre-requisito	:	Redes de Datos II
Requisito de	:	Sistemas de Telecomunicación
Nº sesiones semanales	:	2 de Cátedra 1 de Ayudantía o Laboratorio

I OBJETIVOS GENERALES

Conocer, comprender y aplicar los principales conceptos y técnicas utilizadas para proteger la información. Específicamente:

- Introducir al alumno en los fundamentos matemáticos y las técnicas utilizadas para la protección de la información en sistemas informáticos.
- Dotar al alumno de los conocimientos necesarios para comprender y aplicar métodos y algoritmos criptográficos clásicos y modernos.
- Proporcionar los conocimientos necesarios para aplicar técnicas criptográficas adecuadas en criptosistemas de clave pública, criptosistemas de clave privada y cifradores de flujo.
- Introducir los conceptos de protocolos, esquemas de seguridad, métodos de autenticación y gestión de claves.
- Introducir al alumno en la problemática de la protección y seguridad de la información en medios electrónicos de intercambio de información, correo electrónico, páginas Web, etc.
- Introducir a los alumnos en las tecnologías que existen para proteger la privacidad y la integridad de datos y a los sistemas de autenticación.

II OBJETIVOS ESPECÍFICOS

Al finalizar el curso el alumno deberá ser capaz de:

- Conocer cómo se aplican estas tecnologías en aplicaciones de comercio electrónico y de mensajería.
- Entender el rol de las Entidades Certificadoras, el uso de los certificados digitales y conocer qué establece la Ley de Firma Electrónica en Chile.

III CONTENIDOS

1. INTRODUCCIÓN

Conceptos fundamentales sobre la Seguridad Informática. Confidencialidad, integridad y disponibilidad de la información. Amenazas y métodos de defensa. Terminología, componentes y tipos de criptosistemas.

2. FUNDAMENTOS TEORICOS

Introducción a la teoría de los números. Introducción a la teoría de la complejidad de los algoritmos.

3. CRIPTOGRAFIA CLASICA

Introducción a los criptosistemas clásicos. Métodos de cifra monográmica por sustitución Métodos de cifra monográmica por transposición. Métodos de cifra poligrámica.

4. CRIPTOSISTEMAS DE CLAVE PRIVADA

Generalidades sobre sistema de clave secreta. Algoritmos de Encriptación Simétrica (DES, 3DES, AES). Otros cifrados de bloque.

5. CRIPTOSISTEMAS DE CIFRADO EN FLUJO

El cifrado con clave continua. Postulados de Golomb para secuencias cifrantes. Estructuras generadoras de secuencias cifrantes. Cifrados en flujo con registros de desplazamiento.

6. CRIPTOSISTEMAS DE CLAVE PÚBLICA

Introducción a la cifra con clave pública. Protocolo de Diffie y Hellman para el intercambio de claves. Cifradores de mochila de Merkle-Hellman. Cifradores exponenciales con algoritmos RSA y El Gamal.

7. FUNCIONES DE AUTENTICACION

El problema de la integridad y autenticación. Autenticación de mensajes con sistemas simétricos y asimétricos. Firma digital con los algoritmos RSA y El Gamal. Funciones hash para firma digital: MD5 y SHA. Ley de Firma Electrónica en Chile.

8. SEGURIDAD EN INTERNET

El programa PGP, Pretty Good Privacy. Seguridad del correo con navegadores estándar. El problema de la certificación y de las entidades certificadoras. Introducción a los cortafuegos.

9. PROTOCOLOS CRIPTOGRAFICOS

Transferencia inconsciente o trascordada. El lanzamiento de la moneda, la firma de contratos, el correo certificado, el descubrimiento parcial de secretos, póker mental, canal subliminal y transferencia con conocimiento nulo.

Jerarquía Digital PDH. Sistema europeo E1 y americano T1. Jerarquía Digital SDH. Sistema SONET.

IV METODOLOGÍA

Se evaluará mediante varios controles periódicos más dos pruebas Solemnes y un examen final escrito en la hora y día que establezca la Dirección de la Escuela.

Se contemplan 2 sesiones de teoría semanales con clases expositivas con apoyo de material audiovisual, software de aplicación, talleres interactivos, trabajos de investigación y análisis, exposición y defensa de casos.

Realización de 2 pruebas solemnes, controles parciales o tareas y un examen.

Evaluación de la asignatura

- La nota de presentación a examen (NP) estará compuesta de 60% nota de Solemne más 40% promedio de tareas/laboratorios.
- La nota final de la asignatura (NF) tendrá una ponderación de 70% nota final de cátedra y 30% de examen.
- Para aprobar el curso debe tenerse que NF $\geq$ 4.0 y para presentarse a Examen NP $\geq$ 3.5

V BIBLIOGRAFÍA

- Bruce Schneier; *Applied Cryptography: Protocols, Algorithms, and Source Code in C*. 2nd Edition, John Wiley & Sons, 1996.

Bibliografía complementaria

- Ruixi Yuan, W. Timothy Strayer; *Virtual Private Networks, Technologies and Solutions*. Addison-Wesley, 2001.
- Ramió Aguirre, Jorge; *Aplicaciones Criptográficas*. Dpto. de Publicaciones de la EUI-UPM; edición julio 1999.