udp FACULTAD DE INGENIERÍA

Facultad de Ingeniería
Escuela de Informática y Telecomunicaciones

PROGRAMA DE ASIGNATURA
Criptografía y seguridad en redes

I. Identificación

Código	: CIT-2105
Créditos	: 6
Duración	: Semestral
Ubicación en plan de estudio	: Semestre 8
Requisitos	: Sistemas Operativos (CIT-2003)
Sesiones Semanales	: 2 cátedras, 1 ayudantía o laboratorio.

II. Objetivos Generales y Específicos

El objetivo general del curso corresponde a conocer, comprender y aplicar los principales conceptos y técnicas utilizadas para proteger la información, a partir de los fundamentos matemáticos y las técnicas para la protección de la información en sistemas informáticos y en redes de datos.

En este contexto, al finalizar el curso el alumno será capaz de:

- Comprender y aplicar métodos y algoritmos criptográficos clásicos y modernos.
- Aplicar técnicas criptográficas adecuadas en criptosistemas de clave pública, criptosistemas de clave privada y cifradores de flujo.
- Manejar conceptos de protocolos, esquemas de seguridad, métodos de autenticación y gestión de claves en sistemas informáticos y redes de datos.
- Diseñar medidas de protección y seguridad de la información en medios electrónicos de intercambio de información, correo electrónico, páginas Web, etc.

III. Descripción de Contenidos

1. Introducción: Conceptos fundamentales, confidencialidad, integridad y disponibilidad de la información, amenazas y métodos de defensa, terminología, componentes y tipos de criptosistemas, ISO/IEC 27001.
2. Criptografía clásica: Introducción a los criptosistemas clásicos, métodos de cifra monográmica por sustitución, métodos de cifra monográmica por transposición, métodos de cifra poligrámica.
3. **Criptosistemas de clave privada**: Generalidades sobre sistema de clave

secreta, algoritmos de Encriptación Simétrica (DES, 3DES, AES), otros cifrados de bloque y flujo.

4. **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.
5. **Funciones de autenticación**: 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.
6. **Seguridad en redes**: 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 y detección de intrusos.
7. **Protocolos criptográficos**: Implementación de protocolos seguros en servicios, análisis de protocolos criptográficos mediante wireshark.

IV. Importancia del curso en el plan de estudios

Para un futuro Ingeniero Civil en Informática y Telecomunicaciones resulta esencial el poder identificar eventuales fallas de seguridad existentes en los sistemas informáticos o en las redes de datos empresariales. Así también, este ingeniero debe proveer soluciones tecnológicamente factibles y eficientes para asegurar la confidencialidad de la información y la invulnerabilidad de las redes. En este contexto, este curso entrega las herramientas necesarias para desarrollar de manera apropiada estas tareas.

Así, este curso contribuye al cumplimiento del perfil de egreso a través del desarrollo del siguiente conjunto de objetivos de aprendizaje (vistos como una serie de conocimientos, habilidades, actitudes y valores):

- Modelar el comportamiento de sistemas, empleando lenguaje matemático, conceptos de física, lenguaje computacional y simulación, entre otros métodos.
- Elaborar y adaptar diseños en el campo de las Tecnologías de la Información y de las Comunicaciones, que permitan satisfacer necesidades detectadas mediante el diagnóstico y la modelación.
- Planificar, analizar y diseñar sistemas informáticos y de telecomunicaciones con una visión de negocio.
- Contribuir al mejoramiento de la calidad de los procesos de producción de software y/o de diseño de sistemas de telecomunicaciones.
- Comunicar ideas en forma oral y escrita
- Capacidad de pensar en forma analítica y racional
- Habilidad de procesar datos generados experimentalmente
- Capacidad de abstracción y modelación
- Habilidad de identificar, formular y resolver problemas complejos de forma

autónoma, con enfoque sistémico
- Capacidad de integrar conocimientos
- Capacidad de trabajar en equipos disciplinarios o multidisciplinarios
- Capacidad de aprender en forma autónoma y continua
- Capacidad de adaptarse a nuevas situaciones
- Capacidad de actuar con iniciativa y tomar decisiones
- Capacidad de crítica y autocrítica.
- Motivación al logro y a la calidad
- Ética profesional acorde con los valores de la Universidad

V. Metodología

Se contemplan dos clases semanales de cátedra, mezclando –a lo largo del semestre- sesiones de carácter expositivo (basadas en presentaciones electrónicas, con apoyo adicional de pizarrón, y/o contenido audiovisual) con sesiones de trabajo en aula donde se realizarán talleres interactivos y/o análisis/defensa de casos. Esto será complementado con lectura de textos y material adicional, para la realización de tareas, laboratorios o trabajos de investigación, permitiendo desarrollar habilidades relacionadas con el autoaprendizaje continuo.

Se fomentará la evaluación del conocimiento adquirido, el nivel de comprensión, la capacidad de análisis, síntesis, y aplicación. Esto será medido a través de controles periódicos más dos pruebas solemnes, la ejecución de un proyecto de auditoria de seguridad que combine componentes de software y redes, junto a un examen final escrito en la hora y día que establezca la Dirección de la Escuela.

Se fomentará también el desarrollo de habilidades relacionadas con la expresión oral y escrita, así como de trabajo grupal y procesamiento de datos medidos, a partir de la realización de presentaciones orales, prácticas de laboratorio (con sus respectivos informes) y trabajos de investigación. Esto se evaluará mediante presentaciones orales y en la evaluación de informes escritos (laboratorios, tareas, trabajos).

VI. Evaluación

Se realizarán controles parciales, trabajos, prácticas de laboratorio, dos pruebas solemnes y un examen final.

Las experiencias de laboratorio serán evaluadas mediante un control y el informe correspondiente. Para aprobar la asignatura el alumno DEBE haber aprobado las experiencias de laboratorio y el proyecto de auditoría (nota promedio de igual o superior a 4.0), donde la asistencia al 100% de las experiencias es una condición necesaria, pero no suficiente. En caso contrario, el alumno reprobará la asignatura con nota final igual al mínimo entre el promedio de sus experiencias de laboratorio o del proyecto de auditoría y 3.9.

Nota de Presentación = (20% Solemne 1 + 20% Solemne 2 + 20% Notas Parciales + 10%

udp FACULTAD DE INGENIERÍA

Proyecto Auditoría)/0.7

Nota Final= 70% Nota de Presentación + 30% Examen.

Podrán eximirse aquellos alumnos cuya nota de presentación sea superior a 5.0, que hayan rendido todas sus evaluaciones.

VII. Bibliografía básica de referencia

Bibliografía obligatoria

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

Bibliografía complementaria

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

PAUTAS ETICAS BASICAS

El plagio es el uso de las ideas o trabajo de otra persona sin el adecuado consentimiento. El plagio puede ser intencional o no. El plagio intencional es el claro intento de hacer pasar el trabajo o ideas ajenas como el suyo propio para su beneficio. El plagio no intencional puede ocurrir si Ud. no conoce el mecanismo adecuado de referenciar la fuente de sus ideas e información. Si no está seguro de los métodos aceptados para referenciar, debería consultar con su profesor, tutor o personal de biblioteca.

El plagio comprobado es una actitud que puede resultar en severas sanciones disciplinarias y/o en la exclusión de la Universidad (Artículo 44, Reglamento del Estudiante de Pregrado).

Elaborado por: Luciano Ahumada, Diego Dujovne, Nicolás Boettcher.
Fecha revisión: Enero 2016.
Fecha vigencia: Marzo 2016.