Facultad de Ingeniería y Ciencias
Escuela de Informática y Telecomunicaciones

PROGRAMA DE ASIGNATURA
Criptografía y seguridad en redes

I. Identificación

- Nombre : Criptografía y Seguridad en redes
- Código : CIT-2113
- Créditos : 6
- Duración : Semestral
- Ubicación en plan de estudio: Semestre 8
- Requisitos : CIT-2108 Taller de redes y servicios
- Sesiones semanales : 2 cátedras, 1 ayudantía, 1 laboratorio

II. Descripción del curso

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.

III. Resultados de aprendizaje

Al finalizar el curso el alumno será capaz de:

1. Diseñar medidas de protección y seguridad de la información en medios electrónicos de intercambio de información, para aplicarlos en servicios tales como correo electrónico y páginas Web, evaluando su performance.
2. Evaluar el desempeño y limitantes de protocolos, esquemas de seguridad, métodos de autenticación y gestión de claves en sistemas informáticos y redes de datos, para diseñar sistemas integrales de seguridad de datos.
3. Aplicar técnicas criptográficas adecuadas en criptosistemas de clave pública, criptosistemas de clave privada y cifradores de flujo, para así estimar métricas comparadas de funcionamiento en términos de robustez y uso de recursos.
4. Aplicar métodos y algoritmos criptográficos clásicos y modernos, para evaluar la performance comparada mediante mediciones o simulación grupal de sistemas de encriptación de datos, documentando así el desempeño de los algoritmos bajo análisis.

IV. Unidades Temáticas

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.

V. Metodología

Se contemplan clases, combinando –a lo largo del semestre- 2 sesiones de carácter expositivo (basadas en presentaciones electrónicas, con apoyo adicional de pizarrón, y/o contenido audiovisual) con 2 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 realizará un mínimo de 4 laboratorios, talleres interactivos o defensa de casos.

Se fomentará la evaluación del conocimiento adquirido, el nivel de comprensión, la capacidad de análisis, síntesis, y aplicación. Esto será medido a través de trabajos 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 trabajos, prácticas de laboratorio, dos pruebas solemnes y un examen final.

Las experiencias de laboratorio serán evaluadas mediante informes. 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% Proyecto Auditoría)/0.7

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

Podrán eximirse aquellos alumnos cuya nota de presentación sea igual o superior a 5.0, que hayan rendido todas sus evaluaciones de acuerdo al item “nota de presentación” definido más arriba.

VII. Bibliografía Básica

1. Bruce Schneier; Applied Cryptography: Protocols, Algorithms, and Source Code in C. 2nd Edition, John Wiley & Sons, 2015.
2. Cristof Paar, Jan Pelzl; Understanding Cryptography: A Textbook for Students and

Practitioners, 1st Ed., Springer, 2010.
3. Hans Delfs, Helmut Knebl; Introduction to Cryptography: Principles and Applications (Information Security and Cryptography), 3rd Ed., Springer, 2015

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).

Así también, el trato entre estudiantes de la universidad está regido por distintos reglamentos, aplicándose (entre ellos) lo establecido en el Reglamento del estudiante de pregrado, y en la política de género. Más información en www.genero.udp.cl y https://www.udp.cl/universidad/reglamentos/.

Elaborado por: Nicolás Boettcher.

Fecha revisión: 9 de Septiembre de 2019
Fecha vigencia: Marzo de 2020