

**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**

Resulta esencial el poder identificar eventuales fallas de seguridad existentes en los sistemas informáticos o en las redes de datos empresariales. Así también, se debe poder 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/la estudiante 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

monográfica por sustitución, métodos de cifra monográfica por transposición, métodos de cifra poligráfica.

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.
7. **Protocolos criptográficos:** Implementación de protocolos seguros en servicios, análisis de protocolos criptográficos mediante Wireshark.
8. **Brechas de Seguridad:** Se presentarán configuraciones vulnerables relacionadas a implementaciones de servicios web, y sus contramedidas. Asimismo se introducirán ataques informáticos relacionados a brechas en sistemas de cifrados de llave simétrica y asimétrica, como también en sistemas de autenticación.

## 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 1 sesión de trabajo en laboratorio donde se realizarán talleres interactivos. 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 5 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, evaluaciones al finalizar cada campo de conocimiento más dos pruebas solemnes, , 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). Esto se evaluará mediante presentaciones orales y en la evaluación de informes escritos (laboratorios, tareas, trabajos).

## VI. Evaluación

Se realizarán prácticos de laboratorio, evaluaciones de campo de conocimiento, dos pruebas solemnes y un examen final.

Las experiencias de laboratorio serán evaluadas mediante informes. Para aprobar la

asignatura se **debe** haber aprobado las experiencias de laboratorio (nota promedio igual o superior a 4.0), donde la asistencia al 100% de las experiencias es una condición necesaria, pero no suficiente. En caso contrario, reprobará la asignatura con nota final igual al promedio de sus experiencias de laboratorio

Nota de Presentación = (25% Solemne 1 + 25% Solemne 2 + 20% Notas Parciales + 30% laboratorios)

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

Podrá eximirse el/la estudiante cuya nota de presentación sea igual o superior a 5.0, que haya rendido todas sus evaluaciones de acuerdo al ítem “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 Pezl; Understanding Cryptography: A Textbook for Students and Practitioners, 1<sup>st</sup> Ed., Springer, 2010.
3. Hans Delfs, Helmut Knebl; Introduction to Cryptography: Principles and Applications (Information Security and Cryptography), 3<sup>rd</sup> Ed., Springer, 2015

### **PAUTAS ETICAS BASICAS**

*El aula es un espacio donde los intercambios buscan generar un clima que potencie el aprendizaje, basado en el respeto y el buen trato. Las diferencias, tanto entre estudiantes, como entre estudiante y docentes, deben abordarse desde este marco de respeto.*

*La universidad cuenta con dos reglamentos importantes de conocer:*

- *Reglamento de Convivencia*
- *Normativa de Prevención y Sanción de Acciones de Discriminación, Violencia Sexual y/o de Género.*

*Puedes consultar los reglamentos aquí: <https://www.udp.cl/universidad/reglamentos-y-politicas/>*

*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*

Elaborado por: Nicolás Boettcher.

Fecha revisión: 9 de Septiembre de 2019

Fecha vigencia: Marzo de 2020