Universidad de Santiago de Chile
Facultad de Ciencia
Departamento de Matemática y Ciencia de la Computación.

LICENCIATURA EN CIENCIA DE LA COMPUTACIÓN
PROGRAMA DE ASIGNATURA

Electivo I

INTRODUCCIÓN A LA CRIPTOGRAFÍA

Autor: Beatriz Ontiveros

Nivel VII- TEL: 4-2-0

I. Objetivos

El propósito de este curso es desarrollar las competencias básicas para introducir al alumno en las técnicas matemáticas y computacionales empleadas en criptografía. Así como brindar facilidad en los manejos esenciales a los desarrollos criptográficos. En particular en lo que concierne a aritmética modular, estructuras algebraicas, a los modelos de computación elementales, estimaciones de complejidad, y nociones sobre problemas tratables e intratables.

Al finalizar el curso el alumno será capaz de:

- Razonar matemáticamente acerca de la seguridad algoritmos criptográficos tanto del tipo simétrico como del tipo asimétrico.
- Modelar y analizar formalmente algoritmos criptográficos basados en cifradores de bloque, funciones de Hash y primitivas basadas en teoría de números.
- Diseñar y evaluar soluciones criptográficas para problemas prácticos (confidencialidad, autentificación) presentes en redes de computadores.

II. Contenidos

Unidad I: Base Matemática para la Criptografía, Teoría de Números

- Números enteros. Divisibilidad. Algoritmo de división. Congruencias. Máximo común divisor y mínimo común múltiplo. Ecuaciones diofánticas y ecuaciones de congruencia. Primos. Teorema fundamental de la aritmética. Pequeño teorema de Fermat. Teorema Chino del Resto.

- Polinomios. Divisibilidad. Algoritmo de división. Irreducibilidad. Anillos cociente.
- Estructuras Algebraicas. Cuerpos. Anillos cocientes, ejemplos. Grupos, grupos cíclicos, grupos finitos. Cuerpos, cuerpos finitos $GF\left(2^m\right)$.

Unidad II: Criptografía Clásica.

- Conceptos Básicos: objetivo de seguridad (privacidad, autentificación), adversarios.
- Criptografía Convencional (cifrados de sustitución y variantes, ataques)
- Algoritmos Clásicos.
- Algoritmos Modernos.
- Confidencialidad.

Unidad III: Criptografía Simétrica

- Criptosistemas simétricos o de clave privada.
- Técnicas de cifrado en bloque.
- Técnicas de cifrado en flujo.
- Implementación.

Unidad IV: Criptografía Asimétrica.

- Algoritmos asimétricos o de Clave Pública.
- Algoritmo de Diffie-Hellman.
- Funciones Hash.
- Algoritmos Criptográficos basados en el problema de la Factorización.
- Algoritmos Criptográficos basados en el Problema del Logaritmo Discreto.
- Firmas Digitales y Protocolos de Autentificación.
- Implementación.

III. Metodología

En las clases se dará un conocimiento básico del tema el cual se complementará con el desarrollo en la parte práctica. Se trabajará principalmente sobre los ejemplos concretos y la metodología por casos.
Para el desarrollo de este curso el alumno contará con una plataforma de formación on-line y enseñanza virtual a la cual accederá, previa autentificación de sus datos personales, en la

página web de la Profesora. En dicha plataforma encontrará material didáctico, como así también el software necesario para la realización de actividades prácticas.

Las estrategias utilizadas para el logro de los objetivos incluyen los procedimientos y actividades siguientes:

- Presentación y análisis del tema.
- Discusiones sobre el tema.
- Ejercicios de aplicación donde se diseñen, modelen y evalúen diferentes algoritmos.
- Evaluación del tema mediante pruebas escritas.

IV. Evaluación

La evaluación se basa en dos pruebas específicas programadas (PEP) y un proyecto. El proyecto es desarrollado durante el semestre. Posibles alternativas para el proyecto incluyen el desarrollo de un software de seguridad/criptográfico o de investigación en algún tema del curso. Las ponderaciones serán establecidas al comienzo del semestre por el profesor.

V. Bibliografía

[1] Neal Koblitz , "*A course in number theory and cryptography*", 2ed., GTM 114, Springer, 1994.

[2] Alfred J. Menezes, Paul C. van Oorschot, Scott A. Vanstone, "*Handbook of Applied Cryptography*", CRC press, 1997.

[3] Bruce Schneier, "*Applied Cryptography: Protocols, Algorithms, and Source Code in C*", 2nd Edition Wiley, ISBN: 0471117099, 1996.

[4] Douglas R. Stinson. "*Cryptography - Theory and Practice*", Discrete Mathematics and its Applications. Chapman \& Hall / CRC Press, Boca Raton~FL, 3rd edition. ISBN 1584885084, 616pp, 2006.