FACULTAD DE CIENCIAS FÍSICAS Y MATEMÁTICAS UNIVERSIDAD DE CHILE

PROGRAMA DE CURSO

Código	Nombre
CC5301	**Introducción a la Criptografía Moderna**
Nombre en Inglés	

SCT	Unidades Docentes	Horas de Cátedra	Horas Docencia Auxiliar	Horas de Trabajo Personal
6	10	3	1,5	5,5

Requisitos	Carácter del Curso
CC3001, CC3102, (MA3403 / MA4701/ Autor).	Electivo

Resultados de Aprendizaje

Al finalizar el curso el alumno será capaz de:

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

Metodología Docente	Evaluación General
Clases teóricas y tareas	La evaluación se basa en un control, un proyecto y un examen (sin apuntes) más varis (entre 4 y 5) tareas cortas. El proyecto es desarrollado durante el semestre. Posibles alternativas para el proyecto incluyen: • El desarrollo de un software de seguridad/criptográfico. • Un artículo corto tipo “Estado de Arte” o de investigación en algún tema de curso. Cualquier tema o posible forma de proyecto queda a criterio del profesor. Las tareas consistirán en demostraciones y resolución de problemas, tanto teóricos como relativos a implementaciones en software. Se sigue la ponderación que se plantea a continuación: NC = (C1+NProyecto + EX)/3 NT = (NT1+…+NTn)/n NF = 0,7*NC + 0,3*NT El examen no reemplazará la nota de control (C1). Para aprobar el curso se requiere: • NC>4.0 • NProyecto >=4.0 • NT >= 4.0

Unidades Temáticas

Número	Nombre de la Unidad	Duración en Semanas
1	Elementos Básicos	1 Semana

Contenidos	Resultados de Aprendizajes de la Unidad	Referencias a la Bibliografía
1. Introducción 2. Conceptos Básicos: objetivos de seguridad (privacidad, autentificación), adversarios, recursos. Seguridad demostrable. 3. Criptografía Clásica (cifrados de sustitución y variantes, ataques)	Entender los fundamentos conceptuales y teóricos presentes al utilizar y analizar algoritmos criptográficos en el contexto de seguridad computacional. Entender funcionamiento y limitaciones de esquemas de ciframiento clásico.	[Bellare, cap. 1-2] [Stinson, cap. 1]

Número	Nombre de la Unidad	Duración en Semanas
2	Criptografía Simétrica (Clave Privada) Parte I	2 Semanas

Contenidos	Resultados de Aprendizajes de la Unidad	Referencias a la Bibliografía
1. Cifradores de Bloque: Mdelos, ejemplos (DES, AES) 2.Funciones Pseudo-aleatorias 3.Encriptación Simétrica: Modelos de seguridad, construcción basadas en cifradores de bloque	Entender, utilizar y analizar algoritmos para encriptación simétrica.	[Bellare, cap. 3-5] [Stinson, cap. 3]

Número	Nombre de la Unidad	Duración en Semanas
3	Criptografía Simétrica, Parte II	2 semanas

Contenidos	Resultados de Aprendizajes de la Unidad	Referencias a la Bibliografía
1. Funciones unidireccionales y resistentes a colisiones: (MD5, SHA-1, SHA-256, otros), modelos de seguridad, el ataque de los cumpleaños. 2. Autentificación de Mensajes: modelos y ejemplos	Entender y utilizar herramientas del tipo funciones de hash. Entender, modelar y evaluar esquemas de autentificación de mensajes.	[Bellare, cap. 6-7] [Stinson, cap. 4]

Número	Nombre de la Unidad	Duración en Semanas
4	Criptografía Asimétrica (Clave Pública), Parte I	4 Semanas

Contenidos	Resultados de Aprendizajes de la Unidad	Referencias a la Bibliografía
1. Teoría de números Computacional 2. Primitivas basadas en teoría de números 3. Encriptación Asimétricas 4. Firmas Digitales	Entender los fundamentos matemáticos de primitivas criptográficas basadas en teoría de números. Diseñar, modelar, evaluar y utilizar herramientas de clave pública para privacidad y autentificación.	[Bellare, cap. 9-12] [Stinson, cap. 5-7] [Goldreich2, cap. 5-6]

Número	Nombre de la Unidad	Duración en Semanas
5	Criptografía en la Práctica	3 semanas

Contenidos	Resultados de Aprendizajes de la Unidad	Referencias a la Bibliografía
1. Infraestructura de Clave Pública (PKI) 2. Autentificación y Acuerdos de claves • Autentificación e identificación (passwords), vía terceras partes confiables (Needham-Schroeder, Kerberos) • Diffie-Hellman y intercambios de claves autenticado (AKE) • Canales seguros (SSL y Encriptación Autenticada) 3. Problemas al implementar algoritmos criptográficas.	Resolver problemas prácticos (autentificación, canales seguros) usando herramientas criptográficas. Identificar y evitar potenciales dificultades.	[Bellare, cap. 8] [HAC, cap. 10, 12-14] [PHS, cap. 11, 13]

Bibliografía

[Bellare] Mihir Bellare y Phil Rogaway, “Introduction to Cryptography, Lecture Notes”, University of California San Diego, 2006.
http://www.cse.ucsd.edu/users/mihir/cse107/classnotes.html

[Stinson], Douglas Stinson, “Cryptography, Theory and Practice”, Second edition, editorial Cgapman and Hall/CRC, 2002.

[Goldreich1] Oded Goldreich, “Foundations of Cryptography, Basic Tools”, Cambridge University Press, 2001.

[Goldreich2] Oded Goldreich, “Foundations of Cryptography, Basic Applications”, Cambridge University Press, 2004.

[HAC] Alfred J. Menezes Paul C. van Oorschot, Scott A. Vanstone, “ Handbook of Applied Cryptography”, CRC press, 1997.

[PHS] Josef Pieprzyk, Thomas Hardjono, Jennifer Seberry, “ Foundamentals of Computer Security”, Springer, 2003.

Vigencia desde:	Primavera 2010
Elaborado por:	Alejandro Hevia