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 Algoritmos y Estructuras de Datos, CC3102 Teoría de la Computación, MA3403 Probabilidades.	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/o primitivas basadas en teoría de números, entre otros.
- Diseñar y evaluar soluciones criptográficas para problemas aplicados (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 varias (entre 4 y 5) tareas. 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

FACULTAD DE CIENCIAS FÍSICAS Y MATEMÁTICAS UNIVERSIDAD DE CHILE

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] [KL, cap. 1-2]

Número	Nombre de la Unidad	Duración en Semanas
2	Criptografía Simétrica, Parte I	2 Semanas

Contenidos	Resultados de Aprendizajes de la Unidad	Referencias a la Bibliografía
1. Cifradores de Bloque: Modelos, ejemplos (DES, AES) 2. Funciones pseudo-aleatorias (PRFs) 3. Encriptación Simétrica: Modelos de seguridad (IND-CPA/CCA), construcción basadas en cifradores de bloque.	Entender, utilizar y analizar algoritmos para encriptación simétrica basados en cifradores de bloque.	[Bellare, cap. 3-5] [Stinson, cap. 3] [KL, cap 3,6]

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

Contenidos	Resultados de Aprendizajes de la Unidad	Referencias a la Bibliografía
1. Funciones unidireccionales y resistentes a colisiones: (SHA-1, SHA-256, SHA-3, otros), modelos de seguridad, el ataque de los cumpleaños, unidireccionalidad. 2. Autentificación de Mensajes: modelos, ataques, y construcciones (CBC-MAC, HMAC) 3. Encriptación Autenticada (EA): modelos, construcciones genéricas y particulares (GCM, IPsec), ataques (WEP). EA con datos asociados.	Entender y utilizar herramientas del tipo funciones de hash. Entender, modelar y evaluar esquemas de autentificación de mensajes. Entender y utilizar algoritmos de encriptación autenticada. Identificar ataques a algoritmos ya quebrados.	[Bellare, cap. 6-7] [Stinson, cap. 4] [Boneh, cap. 9] [KL, cap. 4,5]

Número	Nombre de la Unidad	Duración en Semanas
4	Criptografía Asimétrica (Clave Pública), Parte I	5 Semanas

Contenidos	Resultados de Aprendizajes de la Unidad	Referencias a la Bibliografía
1. Teoría de números Computacional y revisión de supuestos computacionales 2. Primitivas basadas en teoría de números 3. Encriptación Asimétricas 4. Firmas Digitales 5. Introducción a Criptografía en Curvas Elípticas	Entender los fundamentos matemáticos de primitivas criptográficas basadas en teoría de números y sus supuestos. Diseñar, modelar, evaluar y utilizar herramientas de clave pública para privacidad y autentificación. Entender los fundamentos de Curvas Elípticas.	[Bellare, cap. 9-12] [Stinson, cap. 5-7] [Boneh, cap. 10-13, 15,16] [KL, cap. 8,9,11,12]

Número	Nombre de la Unidad	Duración en Semanas
5	Criptografía en la Práctica	4 semanas

Contenidos	Resultados de Aprendizajes de la Unidad	Referencias a la Bibliografía
1. Infraestructura de Clave Pública (PKI) 2. Acuerdos de claves Diffie-Hellman e intercambios de claves autenticado (AKE) 3. Problemas al implementar algoritmos criptográficas.	Resolver problemas prácticos (acuerdos de claves) usando herramientas criptográficas. Identificar y evitar potenciales dificultades.	[Bellare, cap. 8] [HAC, cap. 10, 12-14] [PHS, cap. 11, 13] [Boneh, cap. 20,21] [KL, cap. 10]

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”, Third edition, editorial Chapman and Hall/CRC, 2006.

[KL], Jonathan Katz, Yehuda Lindell, “Introduction to Modern Cryptography”, 2nd edition, editorial Chapman and Hall/CRC, 2015.

[Boneh], Dan Boneh, “A Graduate Course in Applied Cryptography”, 2016, Disponible online
http://crypto.stanford.edu/~dabo/cryptobook

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

Vigencia desde:	Semestre Primavera 2016
Elaborado por:	Alejandro Hevia