FACULTAD DE CIENCIAS FÍSICAS Y MATEMÁTICAS UNIVERSIDAD DE CHILE

PROGRAMA DE CURSO

Código	Nombre			
CC6301	TOPICOS EN CRIPTOGRAFIA MODERNA			
Nombre en Inglés				
Topics in Modern Cryptography				
SCT	Unidades Docentes	Horas de Cátedra	Horas Docencia Auxiliar	Horas de Trabajo Personal
3	5	1,5		3,5
Requisitos			Carácter del Curso	
[(cc30a/cc3001),(cc30b/cc3102),(ma34a/ma3403)] / (ma47a/ma4701) / (cc51q/cc5301) / Autor			Electivo para Ingeniería Civil en Computación.	

Resultados de Aprendizaje

El propósito del curso es dotar al estudiante de herramientas de análisis tanto para proponer y evaluar formalmente modelos de seguridad, así como algoritmos y protocolos criptográficos dentro de una sub-área específica de investigación actual en criptografía.

Al finalizar el curso el alumno será capaz de:

- Razonar matemáticamente acerca de la seguridad algoritmos criptográficos en la sub-area estudiada.
- Modelar y analizar formalmente algoritmos criptográficos basados en herramientas y técnicas propuestas recientemente en la sub-área en estudio.
- Identificar problemas de investigación actuales e importantes en la sub-área en estudios.

Metodología Docente	Evaluación General
- Clases expositivas - Presentación de Papers por los estudiantes - Discusión.	La evaluación se basa en al menos 2 presentaciones de artículos (P1, P2), y un proyecto (P). El proyecto debe tener carácter de investigación y ser desarrollado durante el semestre. Cualquier tema o posible forma del proyecto será de común acuerdo con el profesor. Se sigue la ponderación que se plantea a continuación: NC = NProyecto NT = (P1+P2)/n NF = 0,7*NC + 0,3*NT 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	Revisión de la Literatura	0.5

Contenidos	Resultados de Aprendizajes de la Unidad	Referencias a la Bibliografía
1. Introducción a la Criptografía Demostrable. 2. Descripción de la sub-área a estudiar. Conceptos básicos. La sub-área en estudio podrá ser una de las siguientes: 1. Computación Multipartita Segura 2. Criptografía Funcional, basada en Identidad o variantes. 3. Anonimato y Votación Electrónica 4. Criptografía Post-Cuántica 5. Verificación Automática de Demostraciones criptográficas. 6. Criptografía Racional 7. Criptografía de Curvas Elípticas 8. Otras sujetas a relevancia y actualidad de la sub-área.	Al término de la unidad el alumno será capaz de entender los fundamentos conceptuales y teóricos presentes en las propuestas actuales (nociones, construcciones y demostraciones) en la sub-área.	[Goldreich1, Goldreich2, Bellare, Variable]

Número	Nombre de la Unidad	Duración en Semanas
2	Revisión de Artículos del Area	14,5

Contenidos	Resultados de Aprendizajes de la Unidad	Referencias a la Bibliografía
1. Lectura crítica, revisión y análisis de artículos en la sub-área. 2. Discusión crítica de los conceptos, propuestas y análisis.	Al término de la unidad el estudiante será capaz de entender, analizar conceptos, nociones de seguridad, algoritmos y construcciones en la sub-área.	[Variable]

FACULTAD DE CIENCIAS FÍSICAS Y MATEMÁTICAS UNIVERSIDAD DE CHILE

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/cse207/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.
- [Variable] Artículos de investigación publicados en los últimos 4 años en conferencias del área (Crypto, Eurocrypt, TCC, FOCS, STOC, Asiacrypt, PKC, PODC), énfasis dependiendo de la sub-área.

Vigencia desde:	Otoño 2011
Elaborado por:	Alejandro Hevia