PONTIFICIA UNIVERSIDAD CATOLICA DE CHILE
ESCUELA DE INGENIERIA
DEPARTAMENTO DE CIENCIA DE LA COMPUTACION

Criptografía y Seguridad Computacional - IIC3253
Programa de Curso
1er semestre - 2021

Horario cátedra	:	martes y jueves módulo 2
Horario ayudantía	:	miércoles módulo 6
Profesores	:	Marcelo Arenas (`marenas@ing.puc.cl`) y Martín Ugarte (`martin.ugarte@imfd.cl`)
Ayudantes	:	Nicholas Mc-Donnell (`namcdonnell@uc.cl`), Nicolás Andre Van Sint Jan (`nicovsj@uc.cl`)
Repositorio	:	`https://github.com/UC-IIC3253/2021`

Objetivo

El objetivo del curso es introducir al alumno a los conceptos fundamentales de criptografía y seguridad computacional, poniendo énfasis tanto en los aspectos formales necesarios para definir la criptografía de clave privada y la criptografía de clave pública, como a los aspectos prácticos necesarios para construir aplicaciones computacionales seguras en distintos ámbitos.

Evaluación

La evaluación del curso estará basada en tareas y un examen final oral. Las tareas incluiran ejercicios teóricos, diseño de algoritmos y construcción de programas. De esta manera se medirá tanto el aprendizaje de los conceptos fundamentales enseñados en el curso, como su aplicación en la solución de problemas concretos. El examen final oral incluirá toda la materia vista en el año.

Sea $\overline{T}$ el promedio de las tareas y E la nota del examen. Para aprobar el curso se debe tener que $\overline{T} \geq 3.95$ y $E \geq 3.95$, en cuyo caso la nota final del curso será $\overline{T}$.

Contenido

1. Introducción
   - *a*) Conceptos básicos: cifrado, autentificación y principio de Kerckhoffs
   - *b*) Modelos de cifrado simétrico y asimétrico
   - *c*) Noción de adversario y tipos de ataques
2. Criptografía simétrica o de clave privada

   a) Un primera aproximación: one-time pad (OTP)
   b) Códigos de autenticación de mensaje (MAC)
   c) Funciones de hash (criptográficas)
   d) Códigos de autentificación de mensaje basados en funciones de hash (HMAC).
   e) Función de derivación de claves basada en contraseña (PBKDF)
   f) Cifrado de bloque: DES, AES
3. Criptografía asimétrica o de clave pública
   a) Repaso de aritmética modular
   b) Algoritmos fundamentales en teoría de números
   c) El protocolo RSA
   d) El protocolo ElGamal
   e) Firmas digitales
   f) Autoridades certificadoras e infraestructura de clave pública (PKI)
4. Seguridad
   a) Implementaciones prácticas de protocolos criptográficos
   b) Seguridad en la Web
5. Criptomonedas
   a) El protocolo de Bitcoin
   b) Ethereum y contratos inteligentes
   c) La criptografía detrás de Monero
6. Una muy breve introducción a la ingeniería social

Bibliografía

1. Niels Ferguson y Bruce Schneier. *Practical Cryptography*. Wiley, primera edición, 2003.
2. Neal Koblitz. *A Course in Number Theory and Cryptography*. Springer, segunda edición, 1994.
3. Alfred Menezes, Paul van Oorschot y Scott Vanstone. *Handbook of Applied Cryptography*. CRC Press, primera edición, 1996.
4. Arvind Narayanan, Joseph Bonneau, Edward Felten, Andrew Miller y Steven Goldfeder. *Bitcoin and Cryptocurrency Technologies: A Comprehensive Introduction*. Princeton University Press, primera edición, 2016.
5. Sharon Conheady. *Social Engineering in IT Security: Tools, Tactics, and Techniques*. McGraw-Hill Education, primera edición, 2014.