PONTIFICIA UNIVERSIDAD CATÓLICA DE CHILE
ESCUELA DE INGENIERÍA
DEPARTAMENTO DE CIENCIA DE LA COMPUTACIÓN

Criptografía y Seguridad Computacional - IIC3253
Programa de Curso
1er semestre - 2023

Horario cátedra	:	martes y jueves módulo 2, sala K200
Horario ayudantía	:	miércoles módulo 6, sala A1
Profesores	:	Marcelo Arenas (`marenas@ing.puc.cl`)
		Martín Ugarte (`contacto@martinugarte.com`)
Ayudantes	:	Nicolas Berríos (`nb@uc.cl`)
		Susana Figueroa (`sfigueroa3@uc.cl`)
		Christian Klempau (`christian.klempau@uc.cl`)
Repositorio	:	`https://github.com/UC-IIC3253/2023`

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 escrito. Las tareas incluirán 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 escrito medirá la comprensión de conceptos elementales del curso y será reprobatorio.

Si $\overline{T}$ es el promedio de las tareas y $E \in \{\text{aprobado}, \text{reprobado}\}$ es el resultado del examen, la nota final del curso N se calculará como

$$N \quad := \quad \begin{cases} 3{,}9 & \text{si } \overline{T} \geq 3{,}95 \text{ y } E = \text{reprobado} \\ \overline{T} & \text{en otro caso} \end{cases}$$

La fecha del examen es el 6 de julio, desde las 8:30am hasta las 12:50pm (módulos 1, 2 y 3).

Contenidos del curso

1. Introducción

   a) Dos problemas fundamentales: cifrado y autentificación
   b) Principio de Kerckhoffs
   c) Principios de la criptografía moderna
   d) Noción de adversario y tipos de ataques

2. Definiciones y herramientas para la criptografía simétrica o de clave privada
   a) Una primera aproximación: one-time pad (OTP)
   b) Definición de esquema criptográfico, y definición sistema de cifrado simétrico
   c) Noción de perfect secrecy
   d) Concepto de permutaciones pseudo aleatoria (PRP)
   e) Demostración de que OTP no es una PRP
   f) Generalización de PRP a rondas arbitrarias y adversario con recursos acotados.

3. Definiciones y herramientas para la autentificación
   a) Definición de una función de hash
   b) Propiedades fundamentales de una función de hash: resistencia a preimagen y colisiones
   c) Códigos de autenticación de mensaje (MAC)

4. Construcciones prácticas de cifrado simétrico
   a) Redes de sustitución/permutación
   b) Algoritmo de cifrado simétrico AES (Advanced Encryption Standard)

5. Construcciones prácticas de funciones de hash y métodos de autentificación
   a) Construcción de Davies-Meyer de funciones de compresión
   b) Construcción de Merkle-Damgård de funciones de hash, y la función de hash SHA-2
   c) Códigos de autentificación de mensaje basados en funciones de hash (HMAC)

6. Criptografía asimétrica o de clave pública
   a) Repaso de aritmética modular
   b) Algoritmos fundamentales en teoría de números. Test de primalidad
   c) El protocolo RSA
   d) Grupos finitos, logaritmo discreto y el protocolo de Diffie-Hellman para compartir un secreto
   e) El protocolo criptográfico ElGamal
   f) La noción de firmas digital. Firmas digitales basadas en RSA, y firma de Schnorr

7. Seguridad en la Web
   a) Seguridad de comunicación en la Web y la infraestructura de clave pública (PKI)
   b) Seguridad en el manejo de sesiones en la Web
   c) Password-based key-derivation function (PBKDF)

8. Criptomonedas y el protocolo de Bitcoin

9. Una breve introducción a la ingeniería social

Bibliografía

1. Heiko Knospe. *A Course in Cryptography*. American Mathematical Society, 2019.
2. Jonathan Katz y Yehuda Lindell. *Introduction to Modern Cryptography*. Chapman and Hall/CRC, tercera edición, 2021.
3. Niels Ferguson y Bruce Schneier. *Practical Cryptography*. Wiley, primera edición, 2003.
4. Neal Koblitz. *A Course in Number Theory and Cryptography*. Springer, segunda edición, 1994.
5. Alfred Menezes, Paul van Oorschot y Scott Vanstone. *Handbook of Applied Cryptography*. CRC Press, primera edición, 1996.
6. Arvind Narayanan, Joseph Bonneau, Edward Felten, Andrew Miller y Steven Goldfeder. *Bitcoin and Cryptocurrency Technologies: A Comprehensive Introduction*. Princeton University Press, primera edición, 2016.
7. Sharon Conheady. *Social Engineering in IT Security: Tools, Tactics, and Techniques*. McGraw-Hill Education, primera edición, 2014.