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

**Criptografía y Seguridad Computacional - IIC3253**
**Programa de Curso**
**1er semestre - 2022**

| | | |
|---|---|---|
| **Horario cátedra** | : | martes y jueves módulo 2, sala B12 |
| **Horario ayudantía** | : | miércoles módulo 6, sala B12 |
| **Profesores** | : | Marcelo Arenas (`marenas@ing.puc.cl`)<br>Martín Ugarte (`contacto@martinugarte.com`) |
| **Ayudantes** | : | Lothar Droppelmann (`ldroppelmann@uc.cl`), José Dominguez (`jndominguez@uc.cl`), José Escobar (`jtescobar1@uc.cl`), Jacques Hasard (`jnhasard@uc.cl`) |
| **Repositorio** | : | `https://github.com/UC-IIC3253/2022` |

# 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

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

# Contenidos del curso

1. Introducción
   *a*) Modelos de cifrado simétrico y asimétrico

   b) Principio de Kerckhoffs, autentificación y firma digital
   c) Principios de la criptografía moderna
   d) Noción de adversario y tipos de ataques

2. Criptografía simétrica o de clave privada
   a) Un primera aproximación: one-time pad (OTP)
   b) La noción de perfect secrecy
   c) Permutaciones pseudo aleatorias (PRP's)
   d) Funciones de hash (criptográfica) y el modelo de random oracle
   e) Códigos de autenticación de mensaje (MAC) y códigos de autentificación de mensaje basados en funciones de hash (HMAC)
   f) Nociones de seguridad concreta y asintótica, y la definición de sistema de cifrado simétrico
   g) Noción de generador pseudo-aleatorio, y su uso para la construcción de un sistema de cifrado simétrico
   h) Los algoritmos de cifrado simétrico DES (Data Encryption Standard) y AES (Advanced Encryption Standard)

3. 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 problema de decisión de Diffie-Hellman
   e) El protocolo ElGamal y su generalización a grupos arbitrarios
   f) Firmas digitales basadas en ElGamal y grupos finitos. Firma de Schnorr

4. 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 functions (PBKDF)

5. Criptomonedas y el protocolo de Bitcoin

6. Una breve introducción a la ingeniería social

# Bibliografía


1. Jonathan Katz y Yehuda Lindell. *Introduction to Modern Cryptography*. Chapman and Hall/CRC, tercera edición, 2020.

2. Niels Ferguson y Bruce Schneier. *Practical Cryptography*. Wiley, primera edición, 2003.

3. Neal Koblitz. *A Course in Number Theory and Cryptography*. Springer, segunda edición, 1994.

4. Alfred Menezes, Paul van Oorschot y Scott Vanstone. *Handbook of Applied Cryptography*. CRC Press, primera edición, 1996.

5. Arvind Narayanan, Joseph Bonneau, Edward Felten, Andrew Miller y Steven Goldfeder. *Bitcoin and Cryptocurrency Technologies: A Comprehensive Introduction*. Princeton University Press, primera edición, 2016.

6. Sharon Conheady. *Social Engineering in IT Security: Tools, Tactics, and Techniques*. McGraw-Hill Education, primera edición, 2014.