Pontificia Universidad Católica de Chile
Departamento de Ciencias de la Computación
IIC3253 – Criptografía y Seguridad Computacional
Profesor Marcelo Arenas - Martín Ugarte (Sección 1)
Primer Semestre del 2025

# Ayudantía 02

PRP

Ayudante: Diego Rodríguez Cid – darodriguez6@uc.cl

---

## Repaso de conceptos

## PRP

Una familia de *permutaciones pseudoaleatorias* (PRP) es una colección de funciones $\{F_k(\cdot)\}$ indexadas por una clave secreta $k$, cada una de las cuales es una permutación sobre $\{0,1\}^n$.
Informalmente, "se ve" como una permutación aleatoria para cualquier adversario eficiente que no conozca la clave.

## Juego para definir una PRP

1. El verificador elige un número $b \in \{0,1\}$ "al azar"
   a) En caso de que $b = 0$, se elige una clave $k \in K$ (el espacio de llaves) según la distribución $Gen$ y se define $f(x) = Enc_k(x)$
   b) En caso de que $b = 1$, se elige una permutación $\pi$ y se define $f(x) = \pi(x)$
2. Adversario elige una palabra $y$ y el verificador le responderá con $f(y)$. Este paso es repetido $q$ veces.
3. Adversario debe indicar si $b = 0$ o $b = 1$.

Dado este juego, el esquema criptográfico será una PRP si no existe un adversario cuya probabilidad de ganar el juego sea mayor a $1/2$.

## Problema 1. ¿Es OTP una PRP?

Diseñe una estrategia o demuestre que no existe estrategia para ganar el juego definido anteriormente.

## Problema 2. OTP basado en XOR

Considere $F_k(x) = x \oplus k$, con $x, k \in \{0,1\}^5$. ¿Es este esquema una PRP?

## Problema 3

Considere la siguiente función $F_k$ sobre el dominio $\{0,1\}^n$.

$$F_k(x) \;=\; \begin{cases} x \oplus k, & \text{si } x \text{ es par,} \\ x, & \text{si } x \text{ es impar.} \end{cases}$$

1. ¿Qué condición se debe cumplir en la función descrita para que sea una permutación? *hint:* Debe cumplir con ser biyectiva.
2. Asumiendo que se cumple esa condición, ¿corresponde a una PRP?