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

**Criptografía y Seguridad Computacional - IIC3253**
**1er semestre del 2022**

**Alumno: José Baboun**

# Tarea 1

## Pregunta 2

Tomemos el juego de Pseudo-random permutation de clases y consideramos que $(Gen, Enc, Dec)$ es una pseudo-random permutation (PRP) si no existe un adversario que pueda ganar el juego con una probabilidad significativamente mayor a $\frac{1}{2}$.

En base a esto, demostrar que para cierto esquema criptográfico existe una estrategia utilizable por un adversario que le permita obtener una probabilidad de ganar el juego mayor a $\frac{1}{2}$ implica que este esquema no es una PRP.

Luego, para el esquema definido en la tarea, definamos la siguiente estrategia.

- El adversario elige $y = 0^n$ como mensaje
- Si el primer bit de $f(y)$ es igual a 0, entonces el adversario elige $b' = 0$
- Si el primer bit de $f(y)$ es igual a 1, entonces el adversario elige $b' = 1$

Notamos que como no se eligen llaves que partan con 1 entonces si el primer bit es igual a 0 entonces el adversario siempre respondera correctamente cuando $b = 0$

Para simplificar la notación diremos que $\mathbb{P}(\text{Adversario gane}) = \mathbb{P}(AG)$. Luego, tenemos que

$$\mathbb{P}(AG) = \mathbb{P}(b = 0)\mathbb{P}(AG|b = 0) + \mathbb{P}(b = 1)\mathbb{P}(AG|b = 1)$$

$$= \frac{1}{2}\mathbb{P}(AG|b = 0) + \frac{1}{2}\mathbb{P}(b = 1)$$

$$\frac{1}{2}1 + \frac{1}{2}\frac{1}{2} = \frac{3}{4}$$

Notamos que $\frac{3}{4}$ es una probabilidad significativamente mayor a $\frac{1}{2}$. Concluímos que el esquema no es un PRP.