NOMBRE: Ignacia Baeza Nº LISTA:

PUNTAJE:

Pontificia Universidad Católica de Chile
Escuela de Ingeniería
Departamento de Ciencia de la Computación

IIC3253 — Criptografía y Seguridad Computacional — 1' 2022

Tarea 1 – Respuesta Pregunta 2

Para demostrar esto se propone el siguiente juego (análigo al juego visto en clases):

1. Verificador elige $b \in \{0,1\}$ con distribución uniforme (tira una moneda)
   - Si $b = 0$, entonces elige una clave $k \in K$ según la distribución Gen y define $f(x) = Enc(k, x)$
   - Si $b = 1$, entonces elige una permutación π con distribución uniforme y define $f(x) = \pi(x)$
2. El adversario elige una palabra $y \in \{0,1\}^n$, el verificador responde con $f(y)$
3. El paso 2. es repetido q veces
4. El adversario indica si $b = 0$ o $b = 1$, y gana si su elección es correcta

Sabemos que *Gen* no permite claves cuyo primer bit sea 0, y que el resto de las claves son elegidas con distribución uniforme.
Ahora para demostrar que este esquema no es PRP demostraremos que la probabilidad de que el adevrsario gane es superior a $\frac{3}{4}$.
Calculamos la probabilidad de ganar:

$$P(Ganar) = P(Ganar|b = 0) + P(Ganar|b = 1)$$

Como sabemos que $P(b = 0) = P(b = 1) = \frac{1}{2}$, tenemos:

$$P(Ganar) = \frac{1}{2} * P(Ganar|b = 0) + \frac{1}{2} * P(Ganar|b = 1)$$

Tenemos que $P(Ganar|b = 0) = 1$ ya que al ver una llave el adversario sabrá que es la llave.

Calculamos $P(Ganar|b = 1) = \frac{CasosFavorables}{CasosTotales}$

Sabmos que los casos favorables $(\frac{2^n}{2})!$ ya que segun el enunciado *Gen* sólo acepta las claves cuyo primer bit es 1 y estas son elegidas con distirbución normal uniforme. Tenemos que los casos totales son $(2^n)!$, lo cual nos deja con:

$$P(Ganar|b = 1) = 1 - \frac{(2^{n-1})!}{(2^n)!} = 1 - \frac{1}{2^n}$$

Por lo que:

$$P(Ganar) = \frac{1}{2} * 1 + (1 - \frac{1}{2^n})$$
$$= \frac{1}{2} + \frac{1}{2} - \frac{1}{2^{n+1}}$$

$$= 1 - \frac{1}{2^{n+1}}$$

Cuando tomamos el caso borde $n = 1$, tenemos que:

$$P(Ganar) = 1 - \frac{1}{2^2}$$

$$= 1 - \frac{1}{4}$$

$$= \frac{3}{4}$$

Por lo que la probabilidad de que el adversario gane siempre sera mayor o igual a $\frac{3}{4}$