Samuel Zúñiga [sezuniga1@uc.cl] 16637747

Tarea 1 - Pregunta 2

Debemos demostrar que nuestro esquema criptográfico (Gen, Enc, Dec) no es una PRP, es decir, que existe un adversario que puede ganar el juego con probabilidad $\frac{3}{4}$ (la cual se considera significativamente mayor a $\frac{1}{2}$) en una ronda.

Probabilidad de ganar

$$P(\text{El adversario gane el juego}) =$$

$$P(\text{El adversario gane el juego} \mid b = 0) \cdot P(b = 0)$$

$$+$$

$$P(\text{El adversario gane el juego} \mid b = 1) \cdot P(b = 1)$$

Con esto tenemos:

- $P(\text{El adversario gane el juego} \mid b = 0) = 1$. Si el verificador eligió $b = 0$, entonces $f(x) = Enc(k, x)$. El adversario tomó una palabra y y el verificador respondió con $f(y)$. Como suponemos que el adversario tiene infinita capacidad computacional, entonces es posible que el adversario itere sobre todo el espacio de llaves, hasta comprobar que con alguna llave k, obtuvo $f(y)$. De esta forma el adversario encontrará la llave con probabilidad 1.
- $P(b = 0) = \dfrac{1}{2}$
- $P(b = 1) = \dfrac{1}{2}$
- Para calcular $P(\text{El adversario gane el juego} \mid b = 1)$ debemos calcular la probabilidad de que la permutación $\pi(y)$ sea distinta de la encriptación $Enc(k_i, y)$ para alguna de las llaves posibles del espacio $\mathcal{K}$. Como el primer bit de la llave es fijo, entonces para las llaves de largo n, tenemos 2^{n-1} posibles llaves, por lo que las posibles llaves vienen dadas por k_i con $1 \leq i \leq 2^{n-1}$. Con esto tenemos:

$$P(\text{Permutación} \neq \text{Encriptación}) = P(\bigwedge_{i=1}^{2^{n-1}} \pi(y) \neq Enc(k_i, y))$$

$$=$$

$$1 - P(\bigvee_{i=1}^{2^{n-1}} \pi(y) = Enc(k_i, y))$$

Además tenemos que $P(\pi(y) = Enc(k_i, y))$ puede calcularse como $\frac{\text{casos favorables}}{\text{casos totales}}$. Esto es, la probabilidad de que la encriptación escogida con la llave k_i sea la misma que la dada por la permutación $\pi(y)$. Por lo tanto tenemos

$$1 - \sum_{i=1}^{2^{n-1}} P(\pi(y) = Enc(k_i, y))$$

$$=$$

$$1 - \sum_{i=1}^{2^{n-1}} \frac{(2^n - 1)!}{2^n!}$$

$$=$$

$$1 - \sum_{i=1}^{2^{n-1}} \frac{1}{2^n} = 1 - \frac{2^{n-1}}{2^n} = 1 - \frac{1}{2} = \frac{1}{2}$$

Por lo tanto la probabilidad de ganar viene dada por:

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

lo cual es significativamente mayor que $\frac{1}{2}$, por lo tanto el esquema criptográfico no es una PRP.