Criptografía y Seguridad Computacional - IIC3253
Tarea 1
Solución pregunta 2

Sean q y n dos números naturales tales que $6 \leq q \leq n$, y sea (Gen, Enc, Dec) un esquema criptográfico definido sobre los espacios $\mathcal{M} = \mathcal{C} = \{0,1\}^n$ y $\mathcal{K} = \{0,1\}^{nq-1}$. En esta pregunta usted debe demostrar que este esquema no es una pseudo-random permutation (PRP) con q rondas. En particular, debe demostrar que el adversario gana el juego que define una PRP con una probabilidad mayor o igual a $\frac{1}{2} + \frac{1}{6}$.

Solución. Sea (Gen, Enc, Dec) un esquema criptográfico arbitrario definido sobre los espacios $\mathcal{M} = \mathcal{C} = \{0,1\}^n$ y $\mathcal{K} = \{0,1\}^{nq-1}$. Suponemos que este esquema es perfectamente correcto, lo cual implica que para cada $k \in \{0,1\}^{nq-1}$, la función $Enc_k : \{0,1\}^n \to \{0,1\}^n$ es una permutación (es decir, es una función biyectiva).

Considere la definición de pseudo-random permutation (PRP) dada en clases. Para demostrar que el esquema anterior no es una PRP con q rondas, usamos un adversario que ejecuta los siguientes pasos:

- El adversario entrega z_1, ..., z_q al verificador, donde $z_i \in \{0,1\}^n$ para cada $i \in \{1, \ldots, q\}$ y $z_i \neq z_j$ para cada $i, j \in \{1, \ldots, q\}$ tal que $i \neq j$. El adversario recibe como respuesta $f(z_1)$, ..., $f(z_k)$.
- El adversario verifica se existe $k \in \{0,1\}^{nq-1}$ tal que $f(z_i) = Enc_k(z_i)$ para cada $i \in \{1, \ldots, q\}$. Si esta condición se cumple, entonces el adversario indica que $b = 0$, sino indica que $b = 1$.

Note que para implementar el segundo paso se deben considerar 2^{nq-1} claves en el peor de los casos. Vale decir, el adversario es un algoritmo de tiempo exponencial, lo cual no es un problema puesto que la definición de PRP no impone restricciones sobre su tiempo de funcionamiento.

Necesitamos calcular la probabilidad de que el adversario gane el juego, lo cual está dado por la siguiente expresión:

$$\begin{aligned}
&\Pr(\text{Adversario gane el juego}) = \\
&\quad \Pr(\text{Adversario gane el juego} \mid b = 0) \cdot \Pr(b = 0) + \\
&\qquad \Pr(\text{Adversario gane el juego} \mid b = 1) \cdot \Pr(b = 1) = \\
&\frac{1}{2} \cdot \Pr(\text{Adversario gane el juego} \mid b = 0) + \frac{1}{2} \cdot \Pr(\text{Adversario gane el juego} \mid b = 1).
\end{aligned}$$

Si $b = 0$, entonces el verificador debe haber encriptado los mensaje z_1, ..., z_q con una clave $k \in \{0,1\}^{nq-1}$. Tenemos entonces que el adversario elige $b = 0$ y gana el juego. Se concluye que $\Pr(\text{Adversario gane el juego} \mid b = 0) = 1$. Si $b = 1$, entonces el verificador escoge al azar una permutación $\pi : \{0,1\}^n \to \{0,1\}^n$ y responde en el juego con el valor $f(z) = \pi(z)$. En este caso, tenemos que el adversario pierde el juego si existe $k \in \{0,1\}^{nq-1}$ tal que $f(z_i) = Enc_k(z_i)$ para

cada $i \in \{1, \ldots, q\}$. Vale decir,

$$\begin{aligned}
\Pr(\text{Adversario pierda el juego} \mid b = 1) &= \Pr_{\pi}\left(\bigvee_{k \in \{0,1\}^{nq-1}} \bigwedge_{i=1}^{q} \pi(z_i) = Enc_k(z_i)\right) \\
&\leq \sum_{k \in \{0,1\}^{nq-1}} \Pr_{\pi}\left(\bigwedge_{i=1}^{q} \pi(z_i) = Enc_k(z_i)\right) \\
&= \sum_{k \in \{0,1\}^{nq-1}} \frac{(2^n - q)!}{(2^n)!} \\
&= \frac{2^{nq-1}}{\prod_{i=0}^{q-1}(2^n - i)}.
\end{aligned}$$

Sea f la función definida como $f(n, q) = \frac{2^{nq-1}}{\prod_{i=0}^{q-1}(2^n - i)}$. Es posible demostrar que $f(6, 6)$ es el mayor valor de esta función en el conjunto de puntos $\{(n, q) \in \mathbb{N} \times \mathbb{N} \mid 6 \leq q \leq n\}$. Calculando el valor de $f(6, 6)$, concluimos que:

$$\Pr(\text{Adversario pierda el juego} \mid b = 1) \leq f(6, 6) < \frac{2}{3}.$$

Tenemos entonces que $\Pr(\text{Adversario gane el juego} \mid b = 1) \geq \frac{1}{3}$, de lo cual se concluye que:

$$\begin{aligned}
&\Pr(\text{Adversario gane el juego}) = \\
&\quad \frac{1}{2} \cdot \Pr(\text{Adversario gane el juego} \mid b = 0) + \frac{1}{2} \cdot \Pr(\text{Adversario gane el juego} \mid b = 1) \geq \\
&\quad \frac{1}{2} \cdot 1 + \frac{1}{2} \cdot \frac{1}{3} = \frac{1}{2} + \frac{1}{6},
\end{aligned}$$

que era lo que queríamos demostrar.