Criptografía y Seguridad Computacional - IIC3253
Tarea 1
Solución pregunta 2

Considere un esquema criptográfico (Gen, Enc, Dec) definido sobre los espacios $\mathcal{M} = \mathcal{K} = \mathcal{C} = \{0,1\}^n$. Suponga además que Gen no permite claves cuyo primer bit sea 0, y que el resto de las claves son elegidas con distribución uniforme. Demuestre que este esquema no es una pseudo-random permutation con una ronda, si $\frac{3}{4}$ es considerada como una probabilidad significativamente mayor a $\frac{1}{2}$.

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

- El adversario entrega $y = 0^n$ al verificador y recibe como respuesta $f(y)$.
- Si $f(y) = Enc(k, y)$ para algún $k \in \{0,1\}^n$ tal que el primer bit de k es 1, entonces el adversario indica que $b = 0$, sino indica que $b = 1$.

Nótese que para implementar el segundo paso se deben considerar 2^{n-1} claves k 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:

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

Si $b = 0$, entonces el verificador debe haber encriptado el mensaje $y = 0^n$ con una clave $k \in \{0,1\}^n$ tal que el primer bit de k es 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 $f(y) = \pi(y)$. En este caso, tenemos que el adversario pierde el juego si $f(y) = Enc(k, y)$ para algún $k \in \{0,1\}^n$ tal que el primer bit de k es 1. Vale decir,

$$\begin{aligned}
\Pr(\text{Adversario pierda el juego} \mid b = 1) &= \Pr_{\pi}\left(\bigvee_{\substack{k \in \{0,1\}^n : \\ \text{el primer bit de } k \text{ es } 1}} \pi(y) = Enc(k, y) \right) \\
&\leq \frac{2^{n-1} \cdot (2^n - 1)!}{(2^n)!} = \frac{1}{2}.
\end{aligned}$$

Tenemos entonces que $\Pr(\text{Adversario gane el juego} \mid b = 1) \geq \frac{1}{2}$, de lo cual se concluye que:

$$\begin{aligned}\Pr(\text{Adversario gane el juego}) \; = \\ \frac{1}{2} \cdot \Pr(\text{Adversario gane el juego} \mid b = 0) + \frac{1}{2} \cdot \Pr(\text{Adversario gane el juego} \mid b = 1) \; \geq \\ \frac{1}{2} \cdot 1 + \frac{1}{2} \cdot \frac{1}{2} \; = \; \frac{3}{4},\end{aligned}$$

que era lo que queríamos demostrar.