Enunciado Pregunta 4

Sean M, K y C espacios de mensajes, llaves y textos cifrados, respectivamente, tales que $M = K = C = \{0,1\}^n$ con $n \geq 1$. Para un sistema criptográfico (Enc, Dec) sobre M, K y C, se define el siguiente juego con parámetros $r, q \geq 1$:

(1) El verificador escoge $b \in \{0,1\}$ con distribución uniforme.

  (1.1) Si $b = 0$, entonces el verificador escoge con distribución uniforme $K' \subseteq K$ tal que $|K'| = r$.

  (1.2) Si $b = 1$, entonces el verificador escoge con distribución uniforme una permutación $\pi : M \to M$.

(2) Para $i = 1, 2, \ldots, q$ se realizan los siguientes pasos.

  (2.1) El adversario elije un mensaje $m_i \in M$.

  (2.2) Si $b = 0$, entonces el verificador responde de la siguiente forma. Si $m_i \neq m_j$ para cada $j \in \{1, \ldots, i-1\}$, entonces el verificar escoge $k \in K'$ con distribución uniforme y entrega la respuesta $Enc(k, m_i)$. Si $m_i = m_j$ para algún $j \in \{1, \ldots, i-1\}$, entonces el verificador entrega la misma respuesta que en el paso j (vale decir, la misma respuesta que para el mensaje m_j).

  (2.3) Si $b = 1$, entonces el verificador entrega la respuesta $\pi(m_i)$.

(3) El adversario indica si $b = 0$ o $b = 1$, y gana si su elección es la correcta.

El sistema criptográfico (Enc, Dec) se dice un r-pseudorandom permutation (r-PRP) si no existe un adversario que pueda ganar el juego anterior con una probabilidad significativamente mayor a $\frac{1}{2}$. Nótese que el concepto de pseudorandom permutation visto en clases corresponde con esta noción para $r = 1$.

Considerando $M = K = C = \{0,1\}^{128}$, demuestre que OTP no es un 1000-PRP si consideramos un juego con 40 rondas ($q = 40$) y una probabilidad que gane el adversario mayor a igual a $\frac{3}{4}$ (en este caso $\frac{3}{4}$ se considera significativamente mayor a $\frac{1}{2}$).

Solución Pregunta 4

La estrategia del adversario es la siguiente. El adversario construye 40 mensajes distintos m_1, ..., m_{40}, vale decir, $m_i \neq m_j$ para todo $i, j \in \{1, \ldots, 40\}$ tales que $i \neq j$. Para estos 40 mensajes, el verificador construye 40 respuestas c_1, ..., c_{40} según el protocolo descrito anteriormente. Finalmente, el adversario verifica si $m_i \oplus c_i = m_j \oplus c_j$ para algún par $i, j \in \{1, \ldots, 40\}$ tal que $i \neq j$. Si esta condición es cierta, entonces el adversario responde 0 (indica que el verificador está usando $b = 0$), y en caso contrario responde 1.

Para la estrategia anterior para el adversario, tenemos que demostrar que

$$\Pr[\text{Adversario gane el juego}] \quad \geq \quad \frac{3}{4}.$$

Sabemos que

$$\Pr[\text{Adversario gane el juego}] = \Pr[\text{Adversario gane el juego} \mid b = 0] \cdot \Pr[b = 0] + \Pr[\text{Adversario gane el juego} \mid b = 1] \cdot \Pr[b = 1], \quad (1)$$

y $\Pr[b = 0] = \Pr[b = 1] = \frac{1}{2}$. Tenemos que calcular las probabilidades restantes. En primer lugar, consideramos $b = 0$, y suponemos que $k_1, \ldots, k_{40}$ son las claves escogidas con distribución uniforme desde el conjunto $K' \subseteq K$, con $|K'| = 1000$. Nótese que en este caso el verificador debe escoger 40 claves dado que los mensajes $m_1, \ldots, m_{40}$ son distintos. Tenemos entonces que

$$\begin{aligned}
\Pr[\text{Adversario gane el juego} \mid b = 0] &= \Pr\left[\bigvee_{1 \le i < j \le 40} m_i \oplus c_i = m_j \oplus c_j\right] \\
&= \Pr\left[\bigvee_{1 \le i < j \le 40} k_i = k_j\right] \\
&= 1 - \Pr\left[\bigwedge_{1 \le i < j \le 40} k_i \neq k_j\right] \\
&= 1 - \prod_{i=1}^{40} \frac{1000 - (i-1)}{1000} \\
&\ge 1 - 0.46 = 0.54
\end{aligned}$$

Este último cálculo fue realizado con la ayuda de `https://www.wolframalpha.com`, también se podría hacer utilizando Python.

Consideremos ahora el caso $b = 1$, y supongamos que Π es el conjunto de todas las permutaciones $\pi : M \to M$, donde $M = \{0,1\}^{128}$. Tenemos que

$$\begin{aligned}
\Pr[\text{Adversario gane el juego} \mid b = 1] &= \Pr\left[\bigwedge_{1 \le i < j \le 40} m_i \oplus c_i \neq m_j \oplus c_j\right] \\
&= \Pr_{\pi \leftarrow \Pi}\left[\bigwedge_{1 \le i < j \le 40} m_i \oplus \pi(m_i) \neq m_j \oplus \pi(m_j)\right] \\
&= 1 - \Pr_{\pi \leftarrow \Pi}\left[\bigvee_{1 \le i < j \le 40} m_i \oplus \pi(m_i) = m_j \oplus \pi(m_j)\right] \\
&= 1 - \Pr_{\pi \leftarrow \Pi}\left[\bigvee_{1 \le i < j \le 40} m_i \oplus \pi(m_i) \oplus m_j = \pi(m_j)\right] \\
&\ge 1 - \sum_{1 \le i < j \le 40} \Pr_{\pi \leftarrow \Pi}\left[m_i \oplus \pi(m_i) \oplus m_j = \pi(m_j)\right] \\
&= 1 - \sum_{1 \le i < j \le 40} \frac{1}{2^{128}} \\
&= 1 - \frac{40 \cdot 39}{2} \cdot \frac{1}{2^{128}} \ge 0.99
\end{aligned}$$

Este último cálculo también fue realizado con la ayuda de `https://www.wolframalpha.com`. Utilizando en la ecuación (1) las dos cotas inferiores obtenidas, llegamos a que

$$\Pr[\text{Adversario gane el juego}] \ge 0.54 \cdot 0.5 + 0.99 \cdot 0.5 = 0.765 > 0.75,$$

lo cual era lo que teníamos que demostrar.