Criptografía - Tarea 1

Matías Correa
15634183

<u>Pregunta 4</u>| Tomando $M = k = C = \{0,1\}^{128}$, mostrar que OTP no es un 1000-PRP en un juego con 40 rondas y una probabilidad mayor a 75% de que gane el adversario.

Se procederá a mostrar que existe una estrategia para que el adversario gane (A.G.) con $Pr[A.G.] > 3/4$

Se define la clase de funciones

$$flip_i : \{0,1\}^{128} \longrightarrow \{0,1\}^{128} \quad , \quad i \in [1, \dots, 40]$$

de manera que $m' = flip_i(m)$ es equivalente a m con su i-ésimo bit flippeado.

Se define también $\langle 0 \rangle$ como la cadena de 128 bits 0. Así, $m \text{ XOR } m = \langle 0 \rangle \quad \forall m \in \{1,0\}^{128}$

De la misma manera se sigue que
$$flip_i(m) \text{ XOR } flip_j(m) = flip_{i,j}(\langle 0 \rangle) \quad , \quad i \neq j . (1)$$

Se entiende $flip_{i,j}(m) = flip_i(flip_j(m)) = flip_j(flip_i(m))$

<u>Estrategia del Adversario:</u> el conjunto de 40 mensajes a enviar será

$$M' = \{flip_1(\langle 0 \rangle), flip_2(\langle 0 \rangle), \dots, flip_{40}(\langle 0 \rangle)\}.$$

El conjunto de respuestas que el Verificador envía a los 40 mensajes de $\mathcal{M}'$ es $\mathcal{C}'$.

$$\mathcal{C}' = \{ c \mid c = \underset{k \leftarrow k'}{Enc}(k, m) \text{ si } b = 0 \text{ ó } c = \Pi(m) \text{ si } b = 1, \forall m \in \mathcal{M}' \}$$

Entonces, para cada par $m_i, m_j \in \mathcal{M}' \times \mathcal{M}'$, con $i \neq j$, el Adversario chequea si $c_i \text{ XOR } c_j = flip_{i,j}(\langle 0 \rangle)$ (2)

La intuición detrás de esto es que, si el verificador repitió su clave $k \in k'$ cuando encriptó m_i y m_j, entonces:

$$\begin{aligned} c_i \text{ XOR } c_j = (m_i \text{ XOR } k) \text{ XOR } (m_j \text{ XOR } k) &= (m_i \text{ XOR } m_j) \text{ XOR } (k \text{ XOR } k) \\ &= flip_{i,j}(\langle 0 \rangle) \text{ XOR } \langle 0 \rangle \\ &= flip_{i,j}(\langle 0 \rangle) \end{aligned}$$

De esta manera el Adversario puede determinar si el Verificador está usando OTP. Sólo necesita que en las 40 rondas ocurra una colisión en las extracciones aleatorias que el Verificador realiza sobre k'.

El cálculo de la probabilidad de ocurrencia de dicha colisión sigue la misma lógica que la Paradoja del Cumpleaños. Así, con $|k'| = 1000$:

$$\Pr[\text{colisión en } k'] = 1 - \frac{1000!}{1000^{40} \cdot 960!} = 0{,}546$$

Siempre que (2) se cumpla, el Adversario responderá que $b = 0$ (esto es, que el Verificador usa OTP). Esto ocurrirá el 54,6% de las veces que así sea. Sin embargo, es posible que si $b = 1$, la permutación Π usada por el Verificador satisfaga (2) para algún par m_i, m_j.

En clases se calculó que la probabilidad de ocurrencia de ese evento para una función π con dominio de cardinalidad n es:

$$\Pr[\text{par en } \pi] = \frac{1}{2^n - 1}$$

Dado que ahora tenemos 40 pares, y reescribiendo el predicado para satisfacer el problema en cuestión:

$$\Pr_{\substack{m_i, m_j \in M' \\ i \neq j}}[\pi(m_i) = flip_{i,j}(p) \mid \pi(m_j) = p] = C_2^{40} \cdot \frac{1}{2^{128} - 1} = 2.3 \cdot 10^{-36} \approx 0.$$

Nota: de (1) se sigue que $m \text{ XOR } flip_{i,j}(m) = flip_{i,j}(\langle 0 \rangle)$.

Del resultado anterior se concluye que la probabilidad que (2) no se satisfaga (y por ende el Adversario responda que $b=1$) cuando $b=1$, es practicamente 100%.

$$\Pr[\text{Adv. responda } b=1 \mid b=1] = 1 - \frac{C_2^{40}}{2^{128}-1} \approx 1.$$

Finalmente, usando el teorema de Probabilidades Totales, calculamos la probabilidad de que el Adversario Gane (A. G.) el juego en 40 rondas contra OTP:

$$\begin{aligned}\Pr[A.G.] &= \Pr[A.G. \mid b=0] \cdot \Pr[b=0] + \Pr[A.G. \mid b=1] \cdot \Pr[b=1] \\ &= \Pr[\text{colisión en } K'] \cdot 1/2 + 1 \cdot 1/2 \\ &\approx 0{,}546 \cdot 0{,}5 + 0{,}5 = 0{,}77 > 0{,}75\end{aligned}$$

$\therefore$ OTP no es un 1000 - PRP