Pontificia Universidad Católica de Chile
Departamento de Ciencia de la computación
IIC3253 - Criptografia y Seguridad Computacional

Tarea 1

23 de abril de 2021

1º semestre 2021

José Manuel Domínguez - 17637449

Pregunta 4

Como vimos en clases para que el adversario ganara con una probabilidad significativamente mayor a 1/2 y solo una llave se necesitaban de 2 rondas. El adversario gana si logra descifrar cual fue el método que se usó para encriptar.

En ese caso dijimos que el adversario mandaría un mensaje m_1 y un segundo mensaje $\overline{m_1}$ (complemento del mensaje 1) cosa de que si el adversario elegía OTP se podía hacer el xor ($\oplus$) entre las 2 respuestas:

$$(m_1 \oplus k) \oplus (\overline{m_1} \oplus k)$$

como xor ($\oplus$) tiene propiedad conmutativa esto se puede reescribir como :

$$(m_1 \oplus k) \oplus (k \oplus \overline{m_1})$$

Ahora por propiedad asociativa esto se puede escribir de la siguiente forma:

$$m_1 \oplus (k \oplus k) \oplus \overline{m_1}$$

Luego sabemos que $x \oplus a = 0$ con esto nos queda:

$$m_1 \oplus 0 \oplus \overline{m_1}$$

que es lo mismo que

$$m_1 \oplus \overline{m_1}$$

Por último el xor ($\oplus$) entre un mensaje y su complemento queda como 1^l (o l unos) donde l es el largo del mensaje. Entonces el adversario lo que hace es decir OTP si ve un string de

l unos y permutación en otro caso. La única posibilidad de que el adversario pierda es si la permutación justo dio 2 mensajes que al aplicarles xor($\oplus$) estos crean un string de solo unos.

El siguiente problema es una idea similar a la anterior solo que en este caso hay 1000 llaves para elegir y 40 rondas para jugar. En este caso debemos probar como el adversario podría ganar con una probabilidad mayor o igual a $\frac{3}{4}$ si la función de encriptación es OTP.

Similar a la idea anterior asumamos que el adversario elige OTP como función de encriptación (b = 0). En este caso el adversario manda 40 mensajes (distintos) al verificador pero este puede elegir entre 1000 llaves distintas. Como vimos antes si se usa la misma llave para encriptar entonces el adversario puede hacer xor($\oplus$) entre las dos respuestas y sería lo mismo que hacer xor($\oplus$) entre los dos mensajes.

$$(m_1 \oplus k) \oplus (m_2 \oplus k) = (m_1 \oplus m_2)$$

Como el adversario sabe los 40 mensajes que mandó y tiene las 40 respuesta solo hace falta que una llave coincida para estar bastante seguro que el verificador escogió OTP (b = 0). Ya que este puede hacer todas las combinaciones de xor($\oplus$) entre mensajes.

$$\begin{aligned} &m_1 \oplus m_2 \\ &m_1 \oplus m_3 \\ &\vdots \\ &m_{39} \oplus m_{40} \end{aligned}$$

Este también puede hacer todas las combinaciones entre las respuestas. Diremos que $e_j = Enc(k, m_j)$ con $j \in \{1, ..., 40\}$.

$$\begin{aligned} &e_1 \oplus e_2 \\ &e_1 \oplus e_3 \\ &\vdots \\ &e_{39} \oplus e_{40} \end{aligned}$$

Entonces el adversario ve si tiene 1 par de $e_i \oplus e_j$ que coinciden con $m_a \oplus m_b$ con $a, b, i, j \in \{1, .., 40\}$, si es que es así este podría estar bastante seguro que el adversario eligió OTP (b = 0).

La probabilidad que una llave se repita dentro de 1000 eligiendo 40 de forma al azar se calcula con la paradoja del cumpleaños. Esto es 1 - P() de que no se repitan las llaves. La probabilidad que no se repitan las llaves es:

$$\frac{1000!}{1000^{40}(1000-40)!} = 0{,}45$$

Ahora la probabilidad de que se repita al menos 1 llave eligiendo 40 es:

$$1 - 0{,}45 = 0{,}55$$

Entonces el adversario para ganar el juego elige b = 1 si es que no existe ningún par de mensajes $e_i \oplus e_j$ que coinciden con $m_a \oplus m_b$ con $a, b, i, j \in \{1, .., 40\}$. y b = 0 si es que sí.

Esto nos deja con una probabilidad ≈ 1 en el caso de que se elija b = 1 (existe una probabilidad muy pequeña que las permutaciones den un par $e_i \oplus e_j$ que coincidan con $m_a \oplus m_b$). En el caso de que b = 0 la probabilidad es de que gane el adversario es de 0,55. Por lo tanto la probabilidad de que gane el adversario es de $\approx \frac{1}{2} * 0{,}55 + \frac{1}{2} * 1 \approx 0{,}775 \geq 0{,}75$. Lo que demuestra que OTP no es un 1000-PRP si consideramos 40 rondas.