Pontificia Universidad Católica de Chile
Escuela de Ingeniería
Departamento de Ciencias de la Computación

IIC3253 - Criptografía y Seguridad Computacional

Sebasthian von Bergen (15635635)

Tarea 1 – Respuesta Pregunta 4

Sea m_0 un mensaje cualquiera. Si $b = 0$ entonces se esta utilizando OTP:

$$f(m_0) = m \oplus k_0$$

Podemos extraer el valor de la llave elegida en este caso, k_0:

$$\begin{gathered} f(m_0) \oplus m_0 = (m_0 \oplus k_0) \oplus m_0 \\ f(m_0) \oplus m_0 = (m_0 \oplus m_0) \oplus k_0 \\ f(m_0) \oplus m_0 = 0 \oplus k_0 \\ k_0 = f(m_0) \oplus m_0 \end{gathered}$$

Logramos extraer el valor de k_0. Si ahora eligimos el siguiente mensaje m_1 como:

$$\begin{gathered} m_1 = f(m_0) \\ m_1 = m_0 \oplus k_0 \\ f(m_1) = (m_0 \oplus k_0) \oplus k_1 \end{gathered}$$

Podemos extraer el valor de k_1 usando el proceso anterior

$$k_1 = f(m_1) \oplus m_1$$

Repetimos estre proceso $q = 40$ veces y logramos extraer 40 llaves $k_i, i \in [0, 39]$. Si alguna de estas llaves se repite, podemos predecir que estamos en el caso $b = 0$, utilizando OTP. La probabilidad de esto es:

$$Pr[k_i \neq k_j, i, j \in [0, q]]$$

Esto significa que cada vez que el verificador elige una llave k_i tendria que haber elegido una que no habia sido utilizada.

$$Pr[k_i \neq k_j, j \in [0, i]] = \tfrac{1000-i}{1000}$$

Hay que multiplicar cada una de estas probabilidades para las $q = 40$ rondas:

$$\frac{1000-0}{1000} * \frac{1000-1}{1000} * ... * \frac{1000-(q-1)}{1000}$$
$$\frac{1}{1000}^q * \frac{1000!}{(1000-q)!}$$

Entonces, para el caso $q = 40$:

$$Pr[k_i \neq k_j, i, j \in [0, 39]] = \frac{1}{1000}^{40} * \frac{1000!}{960!}$$
$$Pr[k_i \neq k_j, i, j \in [0, 39]] = 0.4536280292870613$$

La probabilidad de que el verificador haya elegido claves k distintas para las 40 rondas es 0.45, esto significa que con probabilidad $1 - 0.45 = 0.55$ alguna de las claves k se repetira. El proceso de desicion del adversario entonces es:

1. Elige m_0 inicial
2. por las siguientes q veces:
   (a) recibe el retorno $f(m_i)$
   (b) aisla la clave k_i
   (c) elige m_{i+1} igual a $f(m_i)$
3. si existe al menos 2 k_i que sean iguales, decide que $b = 0$.
4. Si todos los k_i son distintos, decide $b = 1$

En el caso de que $b = 1$, entonces se esta utilizando una funcion de permutacion. Como no sabemos que funcion se esta utilizando, haremos el mismo proceso y obtendremos valores para las llaves $k_i^{'}$ virtuales que no fueron realmente utilizados. El caso en el que una llave $k_i^{'}$ sea igual a otra llave $k_j^{'}$ es cuando:

$$\pi(m_i) = m_0 \oplus k_0^{'} \oplus k_1^{'} \oplus ... \oplus k_j^{'} \oplus k_{j+1}^{'} \oplus ... \oplus k_i^{'}$$
$$\pi(m_i) = m_0 \oplus ... \oplus k_{j-1}^{'} \oplus k_{j+1}^{'} \oplus ... k_{i-1}^{'} \oplus (k_j^{'} \oplus k_i^{'})$$
$$\pi(m_i) = \pi(m_{i-1}) \oplus k_j^{'},\ j \in [1, i-1]$$

Si se cumple la afirmacion de arriba entonces tendremos un falso positivo. La probabilidad de que esto ocurra en alguna iteracion i de las $q = 40$ (ignoramos la primera porque no puede haber colision con solo 1 elemento) es:

$$Pr[\pi(m_i) = \pi(m_{i-1}) \oplus k_j, j \in [1, i-1]]$$

Entonces en cada iteracion, para que de un falso positivo, la permutacion π tiene que haber elegido uno de los j mensajes que habrian satisfecho la igualdad.

$$Pr[\pi(a) = b] = \frac{1}{2^{128}}$$
$$Pr[\pi(m_i) = \pi(m_{i-1}) \oplus k_j^{'}, j \in [1, i-1] = \sum_{l=1}^{j} \frac{1}{2^{128}} = \frac{j}{2^{128}}$$

Sumando estas probabilidades para todas las iteraciones:

$$\sum_{j=1}^{39} \frac{j}{2^{128}} = \frac{780}{2^{128}}$$

El valor de esta probabilidad es minusculo asi que podemos ignorarlo. Evaluando la probabilidad de que gane el adversario:

$$Pr[b = 0] * (1 - Pr[k_i \neq k_j, i, j \in [0, 39]|b = 0) + Pr[b = 1] * (1 - Pr[\pi(m_i) = \pi(m_{i-1}) \oplus k_j, j \in [1, i], i \in [1, 39]|b = 1])$$
$$0.5 * 0.55 + 0.5 * 1^* = 0.775$$
$$\frac{3}{4} = 0.75 \leq 0.775$$

Como nuestra probabilidad de exito es mayor a $\frac{3}{4}$, podemos decir que OTP no es 1000-PRP con $q = 40$ y el tamaño de los conjuntos $n = 128$