PONTIFICIA UNIVERSIDAD CATÓLICA DE CHILE
ESCUELA DE INGENIERÍA
DEPARTAMENTO DE CIENCIAS DE LA COMPUTACIÓN

IIC3253 - Criptografía y Seguridad Computacional
1er semestre del 2021
Vicente Merino

Tarea 1

Parte 4

Una par de ideas de que no hacer: La estrategia del adversario debería evitar mandar mensajes reptidos, ya que si mandamos dos veces el mensaje m, independiente de lo que haya elegio el verificador como función de verificación, me devolverá dos veces $\pi(m)$ o dos veces $Enc(k, m)$ (con k fijo). Por lo que si hacemos $\oplus$ entre las dos respuestas, en cualquier caso nos dará 0, sin poder sacar ninguna información de lo que utilizó el verificador.

Lo que podemos hacer es lo siguiente: elegir todos los m_i distintos entre sí. Si es que existe un par tal que $f(m_i) \oplus f(m_j) = m_i \oplus m_j$, lo más probable es que haya sido porque se eligió la misma llave en la respuesta y por lo tanto el adversario indica $b = 0$, si es que esto no ocurre, entonces el adversario indica $b = 1$.

¿Por qué esto funciona? Veamos en el caso que el adversario haya elegido $b = 0$, dado que todos los mensajes son distintos, el verificador siempre daría una respuesta distinta y para que exista al menos un par de mensajes que cumpla la propiedad enunciada, lo que debe ocurrir es que al menos se haya elegido un par de llaves iguales (ya que $Enc(k, m_i) \oplus Enc(k, m_j) = m_i \oplus k \oplus m_j \oplus k = m_i \oplus m_j$). Esto lo podemos enunciar de la siguiente forma:

$$Pr(\text{al menos un par de mensajes cumplen } m_i \oplus m_j = Enc(k_i, m_i) \oplus Enc(k_j, m_j))$$

$$= Pr(\text{al menos un par de llaves iguales } (m_i = m_j)) = 1 - Pr(\text{todas las llaves distintas})$$

$$= 1 - \prod_{i=0}^{39} \frac{1000 - i}{1000} \approx 0{,}5464$$

Notar que la última probabilidad se calcula de esta forma, debido a que primero tengo 1000 sobre 1000 mensajes distintos para elegir, después 1000 - 1 (porque ya elegí 1) sobre 1000, luego 1000-2 sobre 1000 y así...
Notar que aquí si elijo llaves distintas puede pasr que $m_i \oplus m_j$ y $Enc(k_i, m_i) \oplus Enc(k_j, m_j)$ sean muy parecidos, pero como las llaves no son las mismas, entonces si o si va a haber por lo menos un bit de diferencia.

Ahora debemos ver cuando el verificador eligió $b = 1$. En este caso el adversario ganará si es que no existe ningún par de mensajes, en que $m_i \oplus m_j = \pi(m_i) \oplus \pi(m_j)$. Intuitivamente, como son permutaciones podemos intuir que esta probabilidad es muy cercana a 1, pero aún así debemos calcularla. Para que se cumpla la

propiedad, se debe cumplir que $\pi(m_i) = m_i \wedge \pi(m_j) = m_j$, o bien, $\pi(m_i) = m_j \wedge \pi(m_j) = m_i$. De aquí podemos concluir lo siguiente: ninguna permutación hecha a cualquier mensaje, debe ser igual a si mismo u otro mensaje enviado.

Pensemos en la probabilidad de que todos los 40 mensajes estén asignados todos entre ellos, lo podemos pensar igual que como en clases con la tabla, la cantidad de permutaciones totales posibles son $2^{128}!$, la cantidad de permutaciones de la parte de abajo de la tabla (los mensajes no enviados), es $(2^{128} - 40)!$ y la cantidad de formas en que puedo permutar los 40 mensajes es $40!$.
Luego $Pr(40 \text{ mensajes asignados entre si mismos}) = \dfrac{(2^{128} - 40)!40!}{2^{128}!}$, ahora en general:

$$Pr(n \text{ mensajes asignados entre si mismos}) = \frac{(2^{128} - n)!n!}{2^{128}!} \approx 0 \quad \forall n \in \{1, \ldots, 40\}$$

Luego, la probabilidad de que haya alguna asignación permutación-mensaje es la suma de esta probabilidad entre $n = 1$ a 40, que resulta en 0. Luego la probabilidad buscada es:

$$Pr(\text{no hay ninguna asignación}) = 1 - Pr(\text{hay alguna asignación}) \approx 1$$

Ahora, tenemos que la probabilidad de que el adversario gane es:

$$Pr(\text{adversario gane}) = Pr(\text{adversario gane} \mid b = 0)Pr(b = 0) + Pr(\text{adversario gane} \mid b = 1)Pr(b = 1)$$

$$\approx 1/2 \cdot 0{,}5464 + 1/2 \cdot 1 = 0,7732 > 3/4$$

Luego, queda demostrado que OTP no es un 1000-PRP con $q = 40$, ya que con la estrategia elegida tenemos más de 3/4 de probabilidades de ganar.