NOMBRE: Benjamín Farías Valdés

N.ALUMNO: 17642531

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

IIC3253 — Criptografía y Seguridad Computacional — 1' 2022

Tarea 1

Pregunta 4

Dada una función de hash criptográfica (Gen, h), donde el recorrido de la función se encuentra en $\{0,1\}^{l(n)}$ para un n dado, se define el siguiente juego denominado *Hash-Img*(n), con el fin de demostrar la noción de **resistencia a pre-imagen:**

1. El verificador genera una llave $s = Gen(1^n)$ (con 1^n un parámetro de seguridad dado) y se la entrega al adversario.
2. El verificador **elige un mensaje cualquiera** $m \in \{0,1\}^{l'(n)}$ (donde $l'(n) > l(n)$), y le entrega $h^s(m)$ al adversario.
3. El adversario elige un mensaje m'.
4. El adversario gana el juego si $h^s(m') = h^s(m)$.

Dado el juego anterior, diremos que **la función de hash es resistente a pre-imagen** si para todo adversario que funciona como un algoritmo aleatorizado de tiempo polinomial, existe una función despreciable $f(n)$ tal que:

$$Pr(\text{Adversario gane } \textit{Hash-Img}(n)) \leq f(n)$$

Ahora demostraremos que si (Gen, h) es **resistente a colisiones**, entonces también es **resistente a pre-imagen.** Para comenzar, tenemos que por ser resistente a colisiones, todo adversario que funciona como un algoritmo aleatorizado de tiempo polinomial debe satisfacer lo siguiente:

$$Pr(\text{Adversario gane } \textit{Hash-Col}(n)) \leq f(n)$$

Esto significa que dada una llave s, y un adversario cualquiera que elige dos mensajes distintos m_1 y m_2:

$$Pr(h^s(m_1) = h^s(m_2)) \leq f(n)$$

Si tomamos $m_1 = m$ y $m_2 = m'$, es decir, el **primer mensaje elegido como el mensaje del verificador y el segundo mensaje como el elegido por el adversario** (en el juego *Hash-Img*(n)), se debe cumplir lo siguiente según la resistencia a colisiones:

$$Pr(h^s(m) = h^s(m')) \leq f(n)$$

Esto se satisface debido a que los mensajes elegidos en ambos juegos pueden ser cualquiera, y **en particular también pueden ser el par** (m, m')**.** La probabilidad anterior no es más que la probabilidad de ganar del adversario en el juego *Hash-Img*(n) (considerando el m y m' como se indicó arriba):

$$Pr(\text{Adversario gane } \textit{Hash-Img}(n)) \leq f(n)$$

Como esto es cierto para todo adversario polinomial aleatorizado, entonces se concluye que (Gen, h) es **resistente a pre-imagen**, demostrando lo pedido.