NOMBRES: Benjamín Lepe

N.ALUMNO: 17641756

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

IIC3253 — Criptografía y Seguridad Computacional — 1' 2022

Tarea 1 - Pregunta 4

El juego para definir la resistencia a preimagen sería el siguiente:

1. El verificador genera una llave $s = Gen(1^n)$ y la utiliza para generar un mensaje encriptado $h(s, m) = x$. Luego le entrega s y x al adversario.
2. El adversario elige una palabra m'.
3. Si $h(s, m') = x$ entonces el adversario gana.

Ahora, hay que demostrar que si (Gen, h) es resistente a colisiones, entonces (Gen, h) es resistente a preimagen. Para esto debemos notar que la probabilidad de que el adversario escoja dos mensajes que tengan una misma imagen es muy baja (siempre menor o igual a una función despreciable $f(n)$). Esto quiere decir que la función de encriptación tiende a ser inyectiva, es decir, cada mensaje tiene a lo más una imagen (en la mayoría de los casos). Sabiendo esto, podemos decir entonces que es muy probable que cada mensaje tenga un hash diferente, por lo tanto, si nos dan el resultado de un hash será muy difícil encontrar el mensaje original que se utilizó para generarlo, lo que implica finalmente que la probabilidad de que el adversario gane es muy baja si es que la función de hash es resistente a colisiones. Dicho esto, entonces queda demostrado que si (Gen, h) es resistente a colisiones, entonces (Gen, h) será resistente a preimagen.