PONTIFICIA UNIVERSIDAD CATÓLICA DE CHILE
ESCUELA DE INGENIERÍA
DEPARTAMENTO DE CIENCIA DE LA COMPUTACION

Criptografía y Seguridad Computacional - IIC3253
1er semestre del 2022

Alumno: José Baboun

Tarea 1

Pregunta 4

Para definir la resistencia a preimagen definiremos el siguiente juego basado en $Hash - Col(n)$. Se asume la existencia de un adversario que, en palabras simples, quiere ser capaz de generar un par de elementos x' para un mensaje y y una llave s.

Definamos el juego $preimagen(n)$ de una forma más formal. Consiremos una función de hash (Gen, H)

1. El verificador genera una llave $s = Gen(1^n)$
2. El verificador elige un mensaje secreto x_1 y genera $h = H^s(x_1)$. Le entrega h y s al adversario
3. El adversario gana el juego si responde con x_2 tal que $H^s(x_2) = h = H^s(x_1)$

A partir de este juego podemos definir que un par (Gen, H) es resistente a preimagen si para todo adversario que funciona como un algoritmo aleatorizado en tiempo polinomial existe una función despreciable $f(n)$ tal que

$$Pr[\text{Adversario gane } preimagen(n)] \leq f(n)$$

Ahora, demostraremos que si (Gen, H) es resistente a colisiones, entonces (Gen, H) es resistente a preimagen.

Por contradicción supongamos que (Gen, H) es resistente a colisiones pero no a preimagen. Luego, con una probabilidad no despreciable un valor x_2 para todo valor dado $h = H(x_1)$ tal que se cumple que $H(x_2) = h = H(x_1)$ para algún x_1 elegido. Notamos que esto no puede pasar por la resistencia a colisiones. Llegamos a una contradicción y concluímos que resistencia a colisiones implica resistencia a preimagen.