PONTIFICIA UNIVERSIDAD CATOLICA DE CHILE
ESCUELA DE INGENIERIA
DEPARTAMENTO DE CIENCIA DE LA COMPUTACION

Criptografía y Seguridad Computacional - IIC3253
Tarea 1
Tomás Valenzuela

Pregunta 4

Considere el juego *Hash-Col*(n) mostrado en clases para definir la noción resistencia a colisiones. Utilizando este tipo de juegos, defina la noción de resistencia a preimagen para una función de hash (Gen, h). Además, demuestre que si (Gen, h) es resistente a colisiones, entonces (Gen, h) es resistente a preimagen.

Respuesta

Noción de preimagen

Se crea el juego *Hash-Pre* para definir la noción de resistencia a preimagen, el cual tiene los siguientes pasos:

1. El verificador genera un Hash x y se lo entrega al adversario.
2. El adversario elige un mensaje m.
3. El adversario gana el juego si $h(m) = x$ y en caso contrario pierde.

Una función de hash (Gen, h) es resistente a preimagen si para todo adversario que funciona como un algoritmo aleatorizado de tiempo polinomial existe una función despreciable $f(n)$ tal que:

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

Demostración

(Por contradicción) Suponemos que existe una función de hash (Gen, h) que es resistente a colisiones pero no a preimagen. Esto significa que no se pueden encontrar 2 mensajes m_1 y m_2 tales que $h(m_1) = h(m_2)$ pero que dado un hash x se pueda encontrar un m tal que $h(m) = x$. Ahora, dado que el dominio de (Gen, h) es mucho más grande que el recorrido, necesariamente existe algún hash x que tenga al menos 2 preimágenes m_1 y m_2 tales que $h(m_1) = h(m_2) = x$. Luego, sabiendo que esta función no es resistente a preimagen se pueden encontrar estos m_1 y m_2, lo que contradice que se cumpla la resistencia a colisiones ya que esos 2 mensajes encontrados llevan al mismo hash (se encuentra una colisión). Por lo que necesariamente si (Gen, h) es resistente a colisiones, esta debe también ser resistente a preimagen.