Pontificia Universidad Católica de Chile
Departamento de Ciencias de la Computación
IIC3253 – Criptografía y Seguridad Computacional
Profesor Marcelo Arenas y Martin Ugarte
Primer Semestre del 2025

Ayudantía 3

Funciones de hash

Ayudante: Cristóbal Rojas – cristobalrojas@uc.cl

Definiciones y conceptos preliminares

Funciones Hash Criptográficas

Una función hash criptográfica es un par de algoritmos (Gen, h) donde:

- Gen es un algoritmo aleatorizado de tiempo polinomial que toma como entrada un parámetro de seguridad 1^n y genera una clave s.
- h es un algoritmo determinístico de tiempo polinomial que toma como entrada la clave s y un mensaje $m \in \{0,1\}^*$, y devuelve un hash $h^s(m) \in \{0,1\}^{\ell(n)}$, donde ℓ es una función polinomial fija.

Propiedades de seguridad

Las funciones hash criptográficas deben satisfacer las siguientes propiedades de seguridad:

1. **Resistencia a preimagen:** Dado un valor hash y, debe ser computacionalmente inviable encontrar cualquier mensaje x tal que $h^s(x) = y$.
2. **Resistencia a colisiones:** Debe ser computacionalmente inviable encontrar cualquier par de mensajes distintos x y x' tal que $h^s(x) = h^s(x')$.

Funciones despreciables

Una función $f : \mathbb{N} \to \mathbb{R}_{\geq 0}$ es despreciable si para todo polinomio $p : \mathbb{N} \to \mathbb{N}$, existe un entero n_0 tal que para todo $n > n_0$:

$$f(n) < \frac{1}{p(n)}$$

El juego Hash-Col

Para formalizar la noción de resistencia a colisiones, se define el juego Hash-Col(n):

1. El verificador genera $s = Gen(1^n)$ y se lo entrega al adversario.
2. El adversario elige mensajes m_1 y m_2 con $m_1 \neq m_2$.
3. El adversario gana el juego si $h^s(m_1) = h^s(m_2)$, y en caso contrario pierde.

Una función hash (Gen, h) se dice resistente a colisiones si para todo adversario probabilístico de tiempo polinomial $\mathcal{A}$, existe una función despreciable $negl(n)$ tal que:

$$\Pr[\mathcal{A} \text{ gana Hash-Col}(n)] \leq negl(n)$$

Problemas

Problema 1

Sean (Gen_1, h_1) y (Gen_2, h_2) dos funciones hash. Definamos (Gen, h) de manera que Gen ejecuta Gen_1 y Gen_2 para obtener las claves s_1 y s_2, respectivamente. Luego definimos $h^{s_1,s_2}(x) = h_1^{s_1}(x) \| h_2^{s_2}(x)$, donde $\|$ denota la concatenación.

Demuestre que si al menos una de (Gen_1, h_1) y (Gen_2, h_2) es resistente a colisiones, entonces (Gen, h) es resistente a colisiones.

Problema 2

Sea (Gen, h) una función hash resistente a colisiones. ¿Es $(Gen, \hat{h})$ definida por

$$\hat{h}^s(x) \stackrel{\text{def}}{=} h^s(h^s(x))$$

necesariamente resistente a colisiones?

Problema 3

Entrega una definición formal para el juego Hash-PreImg, es decir, el juego que representa la noción de resistencia a preimagen para una función de hash (Gen, h).