DEPARTAMENTO DE CIENCIAS DE LA COMPUTACIÓN
ESCUELA DE INGENIERÍA
PONTIFICIA UNIVERSIDAD CATÓLICA DE CHILE

IIC3253 - Criptografía y Seguridad Computacional (I/2023)

Ayudantía 5

Ayudantes: Chris Klempau (christian.klempau@uc.cl)

1. Funciones de Hash

1.1. Definiciones

¿Cuáles son las definiciones formales de las siguientes propiedades y definiciones para una función de hash criptográfica?

a. Función de hash criptográfico:

b. Generador de *keys*:

c. Función de hash *keyed*:

d. Función de compresión:

e. Requerimiento principal - resistencia a colisiones:

1.2. Dependencia pura del input

Explique por qué el *output* de una función de Hash debe depender de **todos** los bits de su input. ¿Qué ocurriría en caso contrario?

1.3. Concatenación R.C

Sean (Gen_1, h_1) y (Gen_2, h_2) dos funciones de hash criptográficas. Se define (Gen, h) como:

$$h^{s_1,s_2}(x) = h_1^{s_1}(x)||h_2^{s_2}(x)$$

Demuestre que si al menos una de (Gen_1, h_1) ó (Gen_2, h_2) es R.C, entonces (Gen, h) es R.C.

2. Merkle-Damgård

2.1. Padding

¿Por qué en la construcción de Merkle-Damgård $Pad(m)$ se incluye el largo del mensaje? ¿Qué propiedad necesaria se rompería en caso contrario?

2.2. Ataque de extensión de largo

Considere una función de hash $\mathcal{H}$ usando la construcción de Merkle-Damgård.

- Demuestre que un adversario que conoce el hash $H(m)$ de un mensaje m, pero no m en sí, puede generar un mensaje m' y calcular el hash $H(m||m')$.
- ¿Qué implicancia tiene lo anterior en usar Merkle-Damgård para verificar integridad de mensajes?

3. Davies-Meyer

Sea Enc una función de encriptación que cumpla con todos los requisitos necesarios de seguridad ($pseudo - randomness$ y esquema criptográfico $ideal$). Demuestre que h, una versión de Davies-Meyer modificada, NO es resistente a colisiones (en contraste a la construcción de Davies-Meyer original, que sí lo es).

$$h(u||v) = Enc_u(v) \oplus u$$