

Elementos Criptograficos

Juli No

7 de abril de 2024

1. Funcion Hash

Un hash es una funcion que genera una salida de tamaño constante independientemente de la entrada recibida, es decir, sea h la funcion Hash y sea m una entrada tenemos:

$$H = h(m)$$

El tamaño de la salida es la cantidad de bits que especifique la funcion hash, ejemplo: SHA-256 tiene 256 bits, es decir que genera una salida cuya tamaño son 256 bits ($256/8 = 32$ caracteres si hablamos de ascii)

Una característica muy importante que tienen o deben tener la funcion Hash es que no es invertible, es decir, dado $H = h(m)$ no puede encontrarse o es extremadamente difícil de encontrar $h^{-1}(H) = m$

1.1. Colisiones

Se conoce como colision al hecho de generar 2 hashes (salidas) iguales a partir de 2 mensajes distintos, es decir:

$$H = h(m_1), H = h(m_2), m_1 \neq m_2$$

1.2. Probabilidad de una Colision

Supongamos una funcion hash de 4 bits de tamaño de salida, los posibles estados que tendremos sera: **0000, 00001, 0010, 0011, 0100, 01001, 0110, 0111, 1000, 1001, 1010, 1011, 1100, 1101, 1110, 1111**. Tenemos 16 estados posibles, dado que cada estado tiene la misma probabilidad de ocurrencia tenemos que la probabilidad del estado es:

$$P_e = \frac{1}{2^4} = \frac{1}{16}$$

De manera mas general, si el algoritmo de hashing genera una salida de n bits la probabilidad de una colision viene dada por:

$$P_c = \frac{1}{2^n}$$

1.3. Propiedades

- **Facilidad de calculo:** $h(m) = H$ rapido de calcular
- **Unidireccionalidad:** Dado $h(m) = H$ es muy difícil encontrar m a partir de H
- **Compresion:** Dado m la salida H debe ser siempre el mismo tamaño
- **Difusion:** Un cambio en un bit para la entrada m generan 2 H_s completamente distintos

- **Resistencia simple a colisiones:** Sea $h(m_1) = H$, encontrar $H = h(m_2)$ con $m_1 \neq m_2$ debe ser computacionalmente difícil
- **Resistencia fuerte a colisiones:** Debe ser computacionalmente difícil encontrar 2 mensajes (M_1, M_2) al azar que produzca el mismo H. Por la paradoja del cumpleaños la probabilidad de ocurrencia de esto es $1/2^{n/2}$

1.4. Estructura Merkle-Damgard

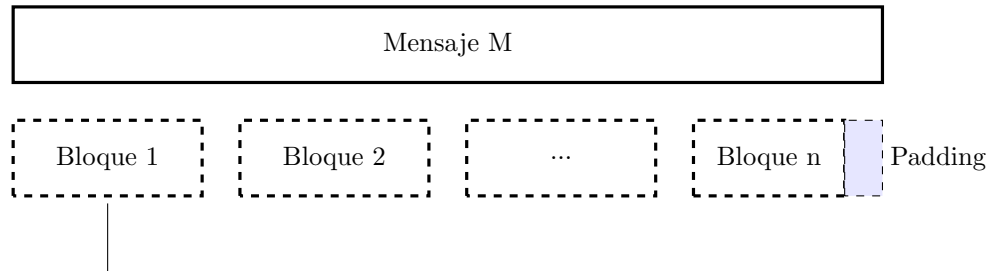
Habla un poco sobre esta estructura

1.5. Funciones Hash Conocidas

A continuacion una descripcion de las funciones Hash mas conocidas y/o usadas

2. Criptografia Simetrica Bloque

Sea M un mensaje de M bytes ($M \cdot 8$ bits waooo), en este tipo de cifra o cifrado los mensajes de entrada o texto claro se dividen en bloques:



- El mensaje M se divide en n bloques
- El Criptograma C sera la concatenacion de $c_1 + c_2 + \dots + c_{n-1} + c_n$
- No se puede cifrar bloques de forma independiente. Para ello usaremos algun "modo de cifra" como por ejemplo **CBC**(Cypher Book Chaining), **CTR** o **GCM** (Galois Counter Mode)