Cryptographic hash functions

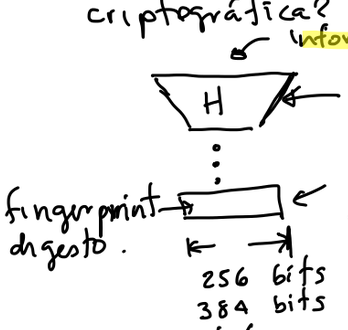
jueves, 11 de noviembre de 2021 11:49

Integridad

Detectar, posibles alteraciones a la información

Las funciones hash criptográficas proveen integridad.

¿Qué es una función hash criptográfica?



SHA2 : Estándar actual

¿Dónde se utilizan?

* Para las firmas digitales
* Para proteger contraseñas

$pwd \rightarrow [H] \rightarrow H(pwd)$

$pwd' \rightarrow [H] \rightarrow H(pwd')$

¿ $H(pwd) = H(pwd')$?

* Verificar integridad de archivos que se descargan de internet
* Generador pseudoaleatorio.

Formalmente:

Una función hash criptográfica es una función de un solo sentido (one-way function)

Es fácil calcular $h(x)$, dado x, pero dado $h(x)$ es computacionalmente muy difícil recuperar x

Es fácil calcular $h(x)$, dado x pero no existe $h^{-1}(x)$

Nota: no necesitan una llave

Birthday problem

Si el tamaño del digesto de una función hash es de 256 bits entonces tendré 2^{256} posibles resultados, comparado con el número de datos de entrada es posible que dados m y m' $h(m) = h(m')$

MD5: Message digest

SHA : Secure Hash Algorithm

SHA-1 : 160 bits

Seguridad de las funciones hash criptográficas

Para que una función hash sea segura debe ser resistente a colisiones

Resistencia a pre-imagen:

* Es fácil calcular $y = H(m)$, dado $m \in \{0,1\}^*$, pero dado y es computacionalmente difícil hallar m

Resistencia a colisiones débiles

Dado $m \in \{0,1\}^*$ debe ser computacionalmente difícil hallar $m' \neq m$ tal que $H(m) = H(m')$

Resistencia a colisiones fuertes

Es computacionalmente difícil hallar $m, m' \in \{0,1\}^*$ $m \neq m'$, tales que $H(m) = H(m')$

Ejemplo de una función hash defectuosa

$m \rightarrow [H] \rightarrow |H(m)| = 3$ bits

8 posibles resultados

$m = m_1, m_2 \cdots m_t$

$|m_i| = 3$ bits.

$H(m) = m_1 \oplus m_2 \oplus \cdots \oplus m_t$

SHA3 → NIST

¿Cuáles son los tamaños del digesto de SHA-3?

¿Cuántas propuestas hubo?

¿Quiénes las propusieron?

¿cuántas etapas hubo?

¿Quiénes son los finalistas? y cuantos

→ ¿Cómo usar la biblioteca criptográfica para implementar las funciones hash criptográficas?