M: espacio de mensajes

$M = \{0,1\}^*$

H: espacio de valores de hash

$H = \{0,1\}^{128}$

$h: M \rightarrow H$

- Resistente a preimagen

1) Facil de calcular $h(m)$

dado x, no es posible encontrar $h(m) = x$

$h : M \to H$ $\qquad H = \{0,1\}^{\ell}$

$M = \{0,1\}^*$

ℓ : largo de hash

r : largo de los bloques

$$m = m_1 \cdots m_k$$

$$|m_i| = r$$

$$h' : \{0,1\}^{\ell} \times \{0,1\}^{r} \to \{0,1\}^{\ell}$$

H_0 : estado inicial fijo

$H_0 \in \{0,1\}^{\ell}$

$H_1 = h'(H_0, m_1)$

$H_2 = h'(H_1, m_2)$

$$H_i = h'(H_{i-1}, m_i)$$

$H_k = h'(H_{k-1}, m_k)$

$h(m) = H_k$

$h(D) = X$

$\neq$

$h(D')$

MDS

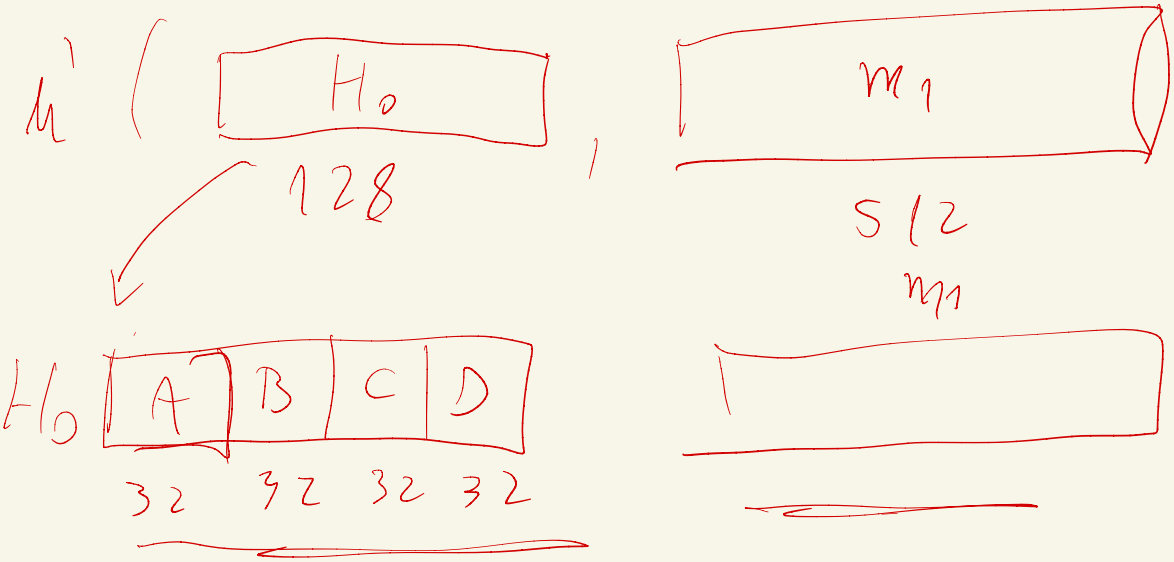
$h: \{0,1\}^* \to \{0,1\}^{128}$

$l = 128$

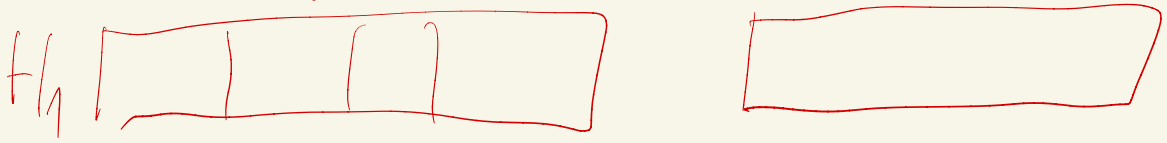
$r = 512$

$m = m_1 \cdots m_k$

$|m_i| = 512$



$\wedge, \vee, \neg, XOR$



MD5 : 128 bits

Secure hash algorithm (SHA)

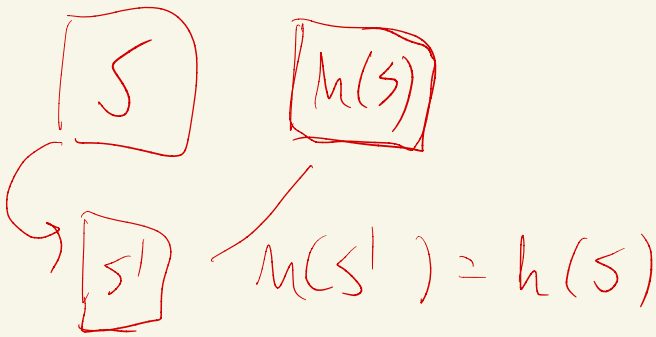
SHA-1 160 bits

SHA-256 256 bits

Resistente a colisiones: no existe un algoritmo eficiente que pueda encontrar colisiones

encontrar m_1, m_2 : $h(m_1) = h(m_2)$

$m_1 \neq m_2$



RANDOM ORACLE MODEL

$h : M \to H$

h es un random oracle model si para una secuencia de mensajes $m_1, m_2, \ldots$

① Si m_i es un mensaje nuevo ($m_i \neq m_j$ para cada $j \in \{1, \ldots, i-1\}$)

$h(m_i)$ es escogido al azar con distribución uniforme desde H

② Si $m_i = m_j$ para $j \in \{1, \ldots, i-1\}$: $h(m_i) = h(m_j)$

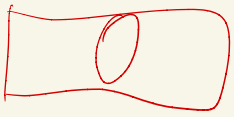
$m_1 = 0 \_ 00$

$m_2 = 0 \_ 01$

$H = \{0,1\}^{128}$

$h(m_1) = h(m_2) + 1$

↳ $\frac{1}{2^{128}}$

m 

- Ataque de la extensión del largo

$h(m)$ ✓

m ✗

$h : M \to H \qquad H = \{0,1\}^{128}$

$H_i = h'(H_{i-1}, m_i)$

$m = m_1 \dots m_k$

$|m| = \ell$

$h' : \{0,1\}^{128} \times \{0,1\}^{512} \to \{0,1\}^{128}$

$h(m)$ ✓ $\qquad |m| \qquad 512 \mid |m|$

$h(m \| m')$

$m = m_1 \dots m_k$

$m' = m'_1 \dots m'_s$

$h: M \to \{0,1\}^{128}$

$h': \{0,1\}^{128} \times \{0,1\}^{512} \to \{0,1\}^{128}$

$m = m_1 \| \dots \| m_k$

512

$h(m)$, $512 \| |m|$

$h(m \| m')$ $512 \| |m'|$

$m' = m'_1 \| \dots \| m'_s$

$m \| m' = m_1 \| \dots \| m_k \| m'_1 \| \dots \| m'_s$

$H_1 = h'(H_0, m_1)$

$H_k = h'(H_{k-1}, m_k)$ → $h(m)$

$H_{k+1} = h'(H_k, m'_1) \dots$

$h(m)$ $\quad |m| = 540$

$h(\underline{m} \,||\, \underline{x} \,||\, m')$

Colisión de mensajes parciales

$h(m) = h(m') \rightsquigarrow H_h$

$\Rightarrow h(m \,||\, \underline{m''}) = h(m' \,||\, \underline{m''})$

$512 \mid |m| \qquad 512 \mid |m'|$

$h(m) = h(m')$

$H_i = h'(H_{i-1}, m_i)$

$m \longmapsto h(m)$

$m \longmapsto h(m \,||\, h(m))$

$h_f(m) = h(m \,||\, h(m))$

Colisión de mensajes parciales:

$h(m) = h(m') \Rightarrow h(m \,||\, x) = h(m' \,||\, x)$

512 | |m|

512 | |m'|

$h_d(m) = h_d(m')$

$\Downarrow \Rightarrow ?$

$h_d(m \| x) = h_d(m' \| x)$

$h(m \| h(m)) = h(m' \| h(m'))$

$\Downarrow \Downarrow ?$

$h(m \| x \| h(m \| x)) = h(m' \| x \| h(m' \| x))$

$h_1(m) \longrightarrow h_2(m \| x)$