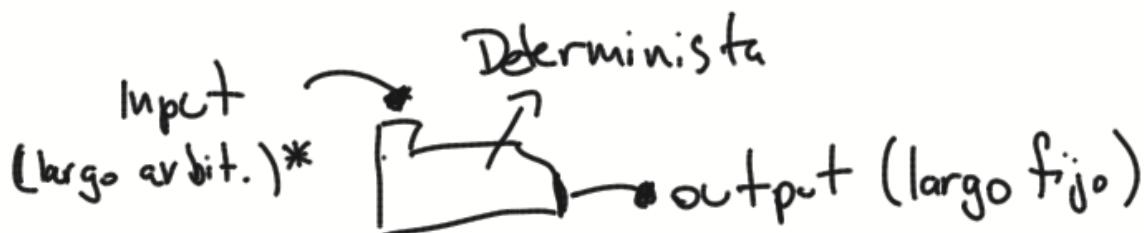


## Funciones de hash



1) Resiste a colisiones

No puedo encontrar  $m_1 \neq m_2$  tq  $h(m_1) = h(m_2)$

2) Resiste a pre-imagen.

Si me dan  $h(m)$ , no puedo encontrar  $m$ .

3)  $h$  debe ser "fácil" de calcular.

4) Correlación en el input no implica correlación en el output, y viceversa.

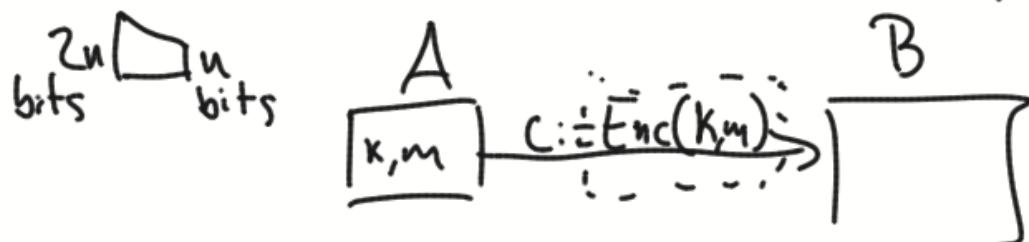
- Strict avalanche criterion,

- Bit independence



¿Cómo llegamos a  $h$ ?

Trámites de construir  $h'$  para largo fijo (input)



Podríamos usar  $\underline{h}' = \text{Enc}$ ?

$$H_0 = \text{Enc}(k_0, m_0) *$$

$$m'_0 = \underline{\text{Dec}}(K'_0, H_0)$$

$$1) \text{ Encuentre } m'_0 \text{ y } K'_0 \text{ tq } \underline{\text{Enc}}(K'_0, m'_0) = H_0.$$

Entonces: cómo construir  $h'$ ?

$$\underline{\text{Enc}}(\underline{\text{Enc}}(K_0, m_0), m_0) = H'_0$$

$$m'_0 = \text{Dec}(K'_0, H'_0) \Rightarrow \underline{\text{Enc}}(K'_0, m'_0) = H_0$$

$$K'_0 = \underline{\text{Enc}}(K''_0, m'_0)$$

$$\begin{aligned} \underline{\text{Enc}}(\underline{\text{Enc}}(K'_0, m'_0), m'_0) &= \\ &= \underline{\text{Enc}}(K'_0, m'_0) = H'_0 \end{aligned}$$

No implica colisiones,  
ni pre-imagen.  
Podría servir

Def  $h'$  como  $\underline{\text{Enc}}(K, m) \oplus K$

Thm: Si  $\text{Enc}$  es un "ideal cypher" entonces  
 $h'$  es resistente a colisiones y pre-imágenes.

$\underline{\text{Enc}}(K, m) \oplus K$  se conoce como la  
constr. de Davies-Meyer.

DM nos da  $h'$  que es para largo  $2n$ .

Cómo extendemos  $h'$  a  $h$  para largo arbitrario.

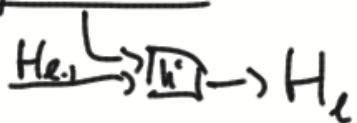
$$m = \overline{m_0 \mid m_1 \mid m_2 \mid \dots \mid m_{l-1}}$$

$$N = H_0 \xrightarrow{} h' \xrightarrow{} H_1 \xrightarrow{} h' \xrightarrow{} H_2 \xrightarrow{} h' \dots \xrightarrow{} H_{l-1} \xrightarrow{} h'$$

$$H_l := h(m)$$

$$m = \overline{m_1 \mid m_2 \mid \dots \mid m_{l-1}}$$

三



Si  $h'$  es resistente a colisiones entrouces, como  $H_e = H'_e$ , tenemos  $m_{hi} = m'_{e-1}$  y  $H_{j-1} = H'_{e-1}$ .

$$\text{Contra } H_{\ell-1} = H'_{\ell-1}$$

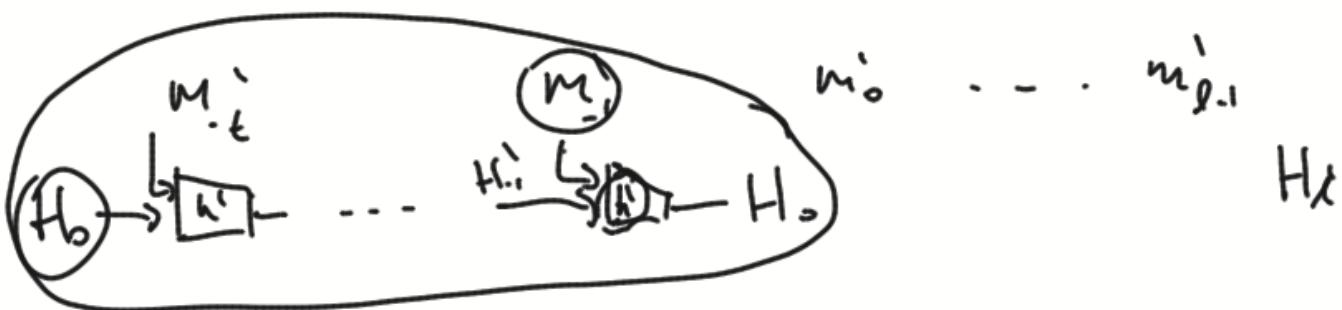
$$h'(H_{\ell-2}, m_{\ell-2}) = h'(H'_{\ell-2}, m'_{\ell-2})$$

$$\Rightarrow H_{e-2} = H'_{e-2} \quad m_{e-2} = m'_{e-2}$$

• • •

$$H_0 = H_0' \quad m_0 = m_0'$$

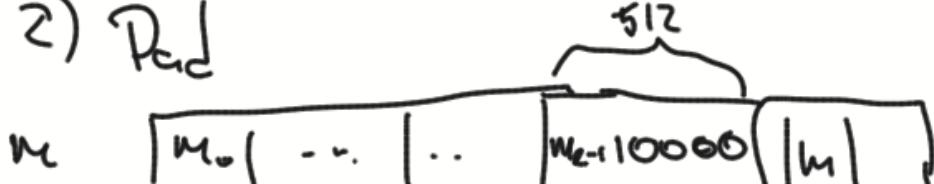
$$m^i m_1^i \dots m_\alpha^i \dots m_e^i$$



1) H<sub>o</sub> debe ser un

"nothing-up-my-sleeve number"

2) Rad



La constr. completa basada en la idea de padding con el largo, se conoce como la const. de Merkle-Damgård

$P_{\text{ad}}(n)$  es una func que cumple

- $m \in$  prefijo de  $\text{Pad}(m)$
  - $|m_1| = |m_2|$  entonces  $|\text{Pad}(m_1)| = |\text{Pad}(m_2)|$  \*
  - $|m_1| \neq |m_2| \Rightarrow$  el último bloq de  $\text{Pad}(m_1)$   
es  $\neq$  al último bloq de  $\text{Pad}(m_2)$
  - $\Rightarrow h$  se porta bien ssi  $h'$  se porta bien











