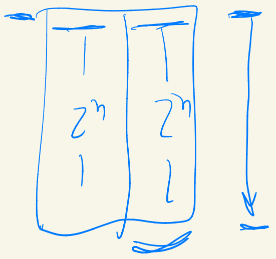
PSEUDO RANDOM PERMUTATION (PRP)

$$\begin{tikzcd} & k \in K \arrow[r] & f(x)=Enc(k,x) \\ V: b \in \{0,1\} \arrow[ur, "b=0"] \arrow[dr, "b=1"'] & & \\ & \Pi \arrow[r] & f(x)=\Pi(x) \end{tikzcd}$$

$$|K| = |M| = 2^n$$

Π:



A: $m \in M$ → V: $f(m)$

A repite el paso anterior q veces

paso final:

A debe decidir si $f(x)=Enc(k,x)$ o si f era una permutación

OTP no es un PRP con $q=2$

$$\begin{tikzcd} & m_1 & V: f(m_1) \\ A: \arrow[ur] \arrow[dr] & & \\ & \overline{m_1} & V: f(\overline{m_1}) \end{tikzcd}$$

$(m_1 \text{ XOR } k) \text{ XOR } (\overline{m_1} \text{ XOR } k)$

si $b=0 \Rightarrow \underline{f(m_1)} \ \underline{\text{XOR}} \ \underline{f(\overline{m_1})} = 1 \ldots 1$

si $b=0 \Rightarrow \Pi(m_1) \text{ XOR } \Pi(\overline{m_1}) = 1 \ldots 1$

puede pasar

$$\Pi(\overline{m_1}) = \overline{\Pi(m_1)}$$

$$\boxed{\begin{array}{c} \Pr\left(\underline{\Pi(\overline{m_1}) = \overline{\Pi(m_1)}}\right) = \dfrac{1}{2^n - 1} \\ \| \\ \Pr\left(\Pi(m_1) \text{ XOR } \Pi(\overline{m_1}) = 1 \ldots 1\right) \end{array}}$$

$$\Pr(\text{Adversario gane}) =$$

$$\underbrace{\Pr(\text{Adversario gane} \mid b=0)}_{1} \cdot \overbrace{\Pr(b=0)}^{\frac{1}{2}}$$

$$+ \underbrace{\Pr(\text{Adversario gane} \mid b=1)}_{\left(1 - \frac{1}{2^n - 1}\right)} \cdot \underbrace{\Pr(b=1)}_{\frac{1}{2}}$$

$$\Pr(\text{Adversario gane}) = \boxed{\begin{array}{l} 1 \cdot \frac{1}{2} \\ + \left(1 - \frac{1}{2^n - 1}\right) \cdot \frac{1}{2} \end{array}}$$

$$n = 128$$

M : espacio de mensaje

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

H : espacio de posible valores para mi función de hash

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

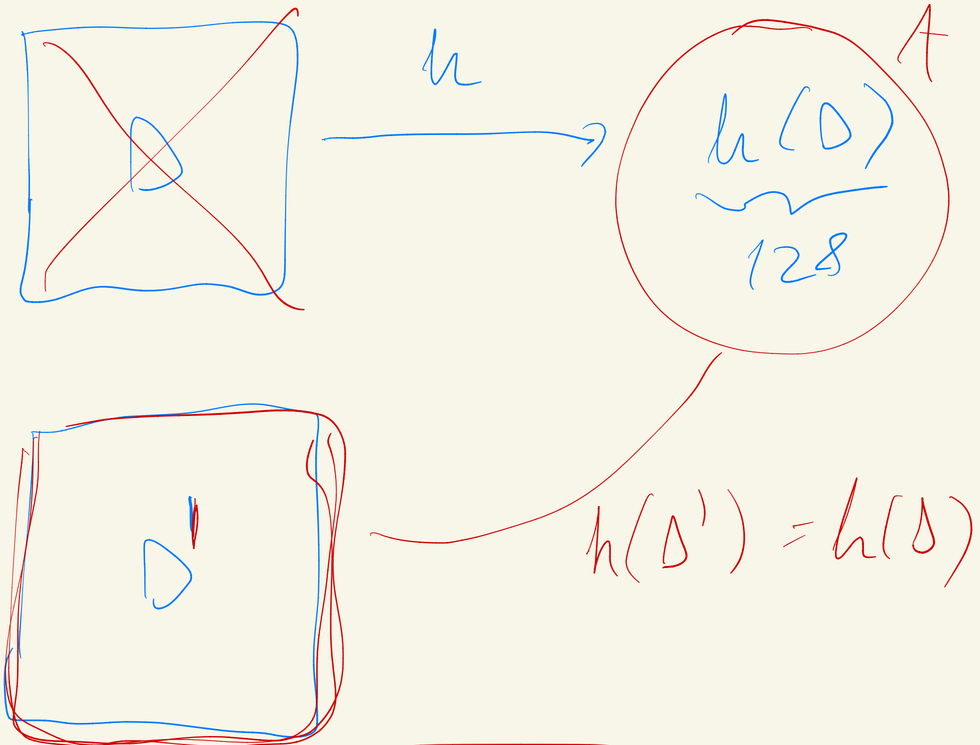
$$\boxed{h : M \to H}$$

"Resistente a preimagen"

→ h sea fácil de calcular.

→ "h^{-1}" sea difícil de calcular

no hay un algoritmo eficiente que dado $x \in H$, calcule m tal que $h(m) = x$



$$\boxed{h(D') = h(D)}$$

funzioni di hash per una tabella di hash

$$\underline{h(X) = ((A X + B) \bmod C)}$$

$$\boxed{h(x) = (Ax + B) \bmod C}$$

$$h(x+C) = (A(x+C) + B) \bmod C$$

$$= (Ax + \underbrace{\cancel{AC}}_{0} + B) \bmod C$$

y, encontrar x tal que

$$h(x) = y$$

$$h(Cm + y - B) =$$

$$(A(Cm + y - B) + B) \bmod C$$

$$(Ay - AB + B) \bmod C$$

$$= y$$

$$h(x) = (229x + 149) \cancel{\bmod 641}$$

$$y \Rightarrow \text{¿}h(x) = y\text{?}$$

$$229x + 149 = y$$

$$\boxed{x = \frac{y - 149}{229}} \leftarrow$$

$$(229x + 149 \equiv y) \bmod 641$$

$$229x \equiv y - 149 \bmod 641$$

$$\boxed{14 \cdot 229 \bmod 641 = 1}$$

$$\underbrace{\cancel{14 \cdot 229}}_{1} x \equiv 14 \cdot y - 14 \cdot 149 \bmod 641$$

$$3 \cdot b \equiv 1 \mod 11$$

$$\boxed{2} \cdot b \equiv 1 \mod \boxed{8}$$

$$a \cdot b \equiv 1 \mod c$$

$$x \equiv 14(y-149) \mod 641$$

$$h(\underline{32481}) = \boxed{134}$$

$$14(134-149) \mod 641$$

$$(14 \cdot -15) \mod 641$$

$$-210 \bmod 641$$

$$= 431$$

$$h(431) = (229 \cdot 431 + 149) \bmod 641$$

$$= \underline{\underline{134}}$$

$$h : \underset{\substack{\downarrow \\ \text{espacio} \\ \text{de mensaje}}}{M} \to \underset{\substack{\downarrow \\ \text{espacio de valores} \\ \text{de hash}}}{H}$$

$M = \{0,1\}^*$ $\qquad$ $H = \{0,1\}^{128}$

$m \in M$

$$m = \boxed{\underbrace{m_1}_{\hookrightarrow\ \underline{512}\ \text{bits}} \mid m_2 \mid \cdots \mid m_k}$$

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

$h'(x, y)$ $\qquad$ $|x| = 128$

$|y| = 512$

H_i: estados $\quad |H_i| = \{0,1\}^{128}$

H_0: estado inicial fijo

$$m = m_1 \; m_2 \; \ldots \; m_k$$

$$H_1 = h'(H_0, \boxed{m_1})$$

$$H_2 = h'(H_1, m_2)$$

$$\vdots$$

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

$$\vdots$$

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

$$\boxed{h(m) = H_k}$$

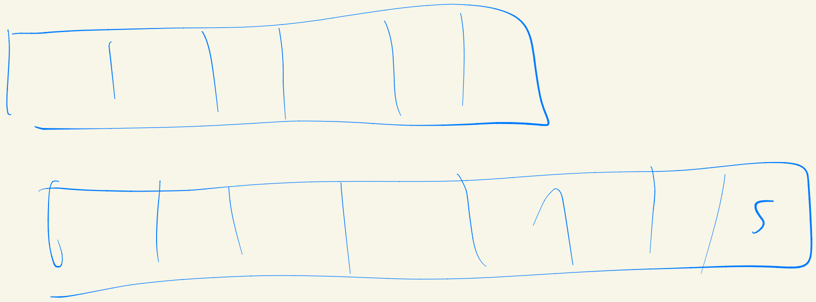
$$\underline{h(m)} = \underline{h(m')}$$

$$h(mX) = h(m'X)$$

$X = X_1 - - X_\ell$

$m =$

$m' =$



$H_k = h(m)$ $\qquad$ $h'(H_k, X_1)$

$\qquad\qquad\qquad\qquad \|$

$H'_s = h(m')$ $\qquad$ $h'(H'_s, X_1$

$m \longmapsto h(m)$

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