2021-04-20

Today 9:30 AM — IIC 3253

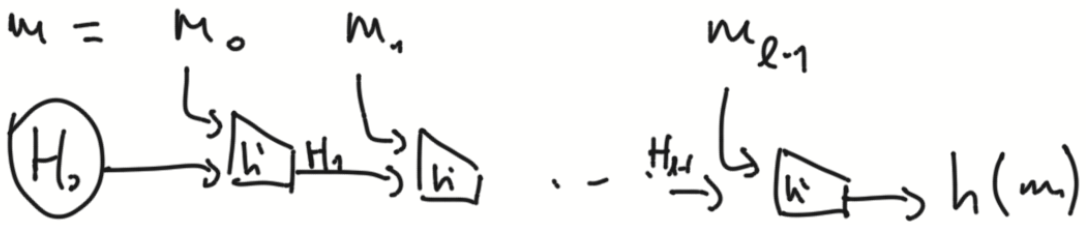
Recordatorio:

Partimos con $Enc(K, m)$ y queremos llegar 1° a h' = función de hash de largo fijo.

$h' : \{0,1\}^{2n} \to \{0,1\}^n$

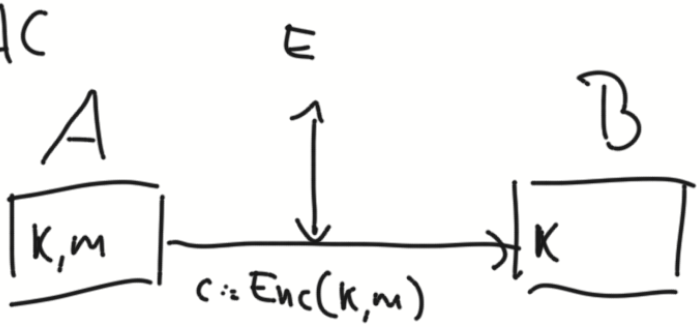
$Enc(K, m) =: h'(K \| m)$ mala idea!!

$h'(H_0, m) := Enc(H_0, m) \oplus H_0$ (Davies-Meyer)

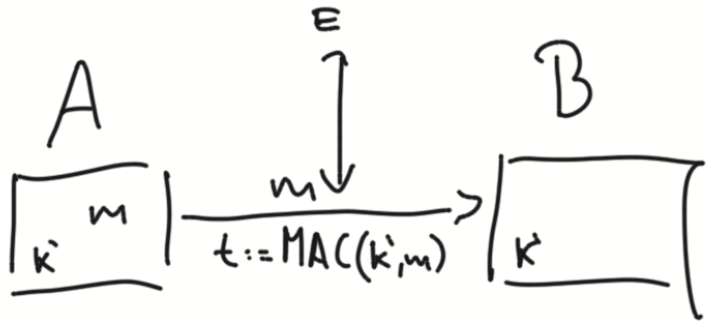


Construcción Merkle-Damgård

MAC

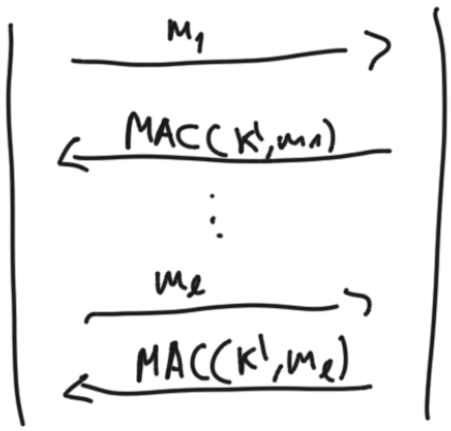


A le pide al banco transferir $<\$2^{20}$ a E



Adv V

elegir k' al azar



Adv gana si puede producir $m \notin \{m_1, \dots, m_\ell\}$ junto con $MAC(k', m)$

Funciona, para largo fijo, $MAC(k', m) = Enc(k', m)$?
Si sup Enc es indistinguible de una PRP.
¿Qué puede hacer Adv? "Absolutamente nada" Dem?
- Víctor

Suponiendo $MAC = M'$ para largo fijo, lo podamos extender a largo arbitrario

- $M = M'\left(k', \bigoplus_{i=0}^{\ell-1} m_i\right)$ ✗

- $M = \left(M'(k', m_0), M'(k', m_1), \dots, M'(k', m_{\ell-1})\right)$

$- M = \left(M^1(k', 1 \| m_0), M^1(k', 2 \| m_1), \ldots, M^1(k', l \| m_{l-1}) \right)$

$M(m_1) = (t_0, \ldots, t_{l-1}), \quad M(m_2) = (t'_0, \ldots, t'_{l-1})$