IIC3253

HMAC

Partimos con AES como ejemplo de cifrado

→Modos de operación para largo arbitrario

→Función de compresión (Davies-Meyer)

→Función de hash (Merkle-Damgård)

→MAC?

HMAC

Hash-based message authentication code

Construyendo un MAC Mac en
base a una función de hash h

¿Qué pasa si definimos $Mac_k(m) = h(k||m)$?

Recordemos el juego que definía un buen MAC

1. El verificador genera una llave k
2. El adversario envía $m_0 \in \mathcal{M}$
3. El verificador responde $Mac_k(m_0)$
4. Los pasos 2 y 3 se repiten tantas veces como quiera el adversario
5. El adversario envía (m, t), siendo m un mensaje que no se había enviado antes

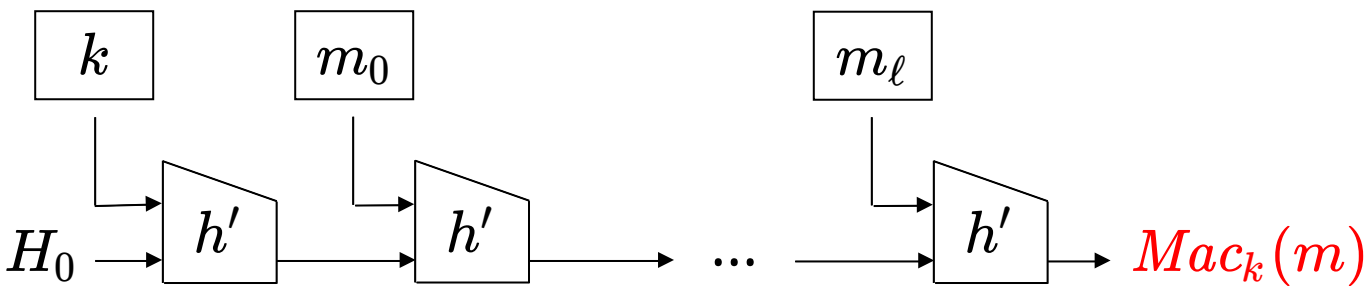
El adversario gana si $Verify_k(t, m) = 1$

¿Qué pasa si definimos $Mac_k(m) = h(k||m)$?

Pensemos que estamos usando SHA-2

¿Puede el adversario ganar el juego?

Simplificación: el largo de k es un bloque



Donde $k\, m_0\, \cdots\, m_\ell$ es en realidad $Pad(k||m)$

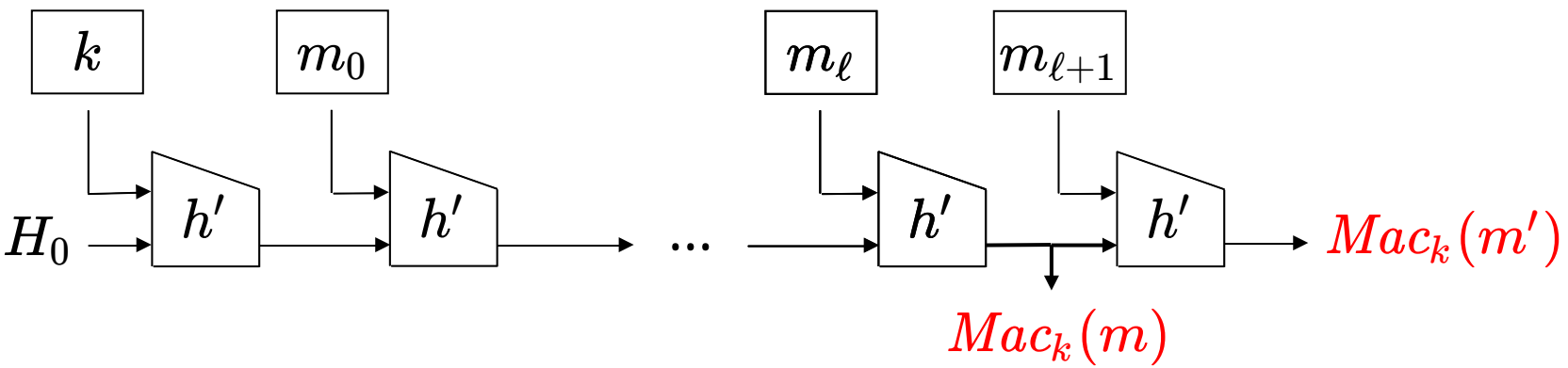
En particular $m \neq\ m_0\, \cdots\, m_\ell$

¿Cómo se ve $Pad(Pad(k||m))$?

$$Pad(Pad(k||m)) = k\, m_0\, \cdots\, m_\ell\, m_{\ell+1}$$

$$Pad(Pad(k||m)) = k\, m_0 \cdots m_\ell\, m_{\ell+1}$$

Por lo tanto el adversario puede calcular



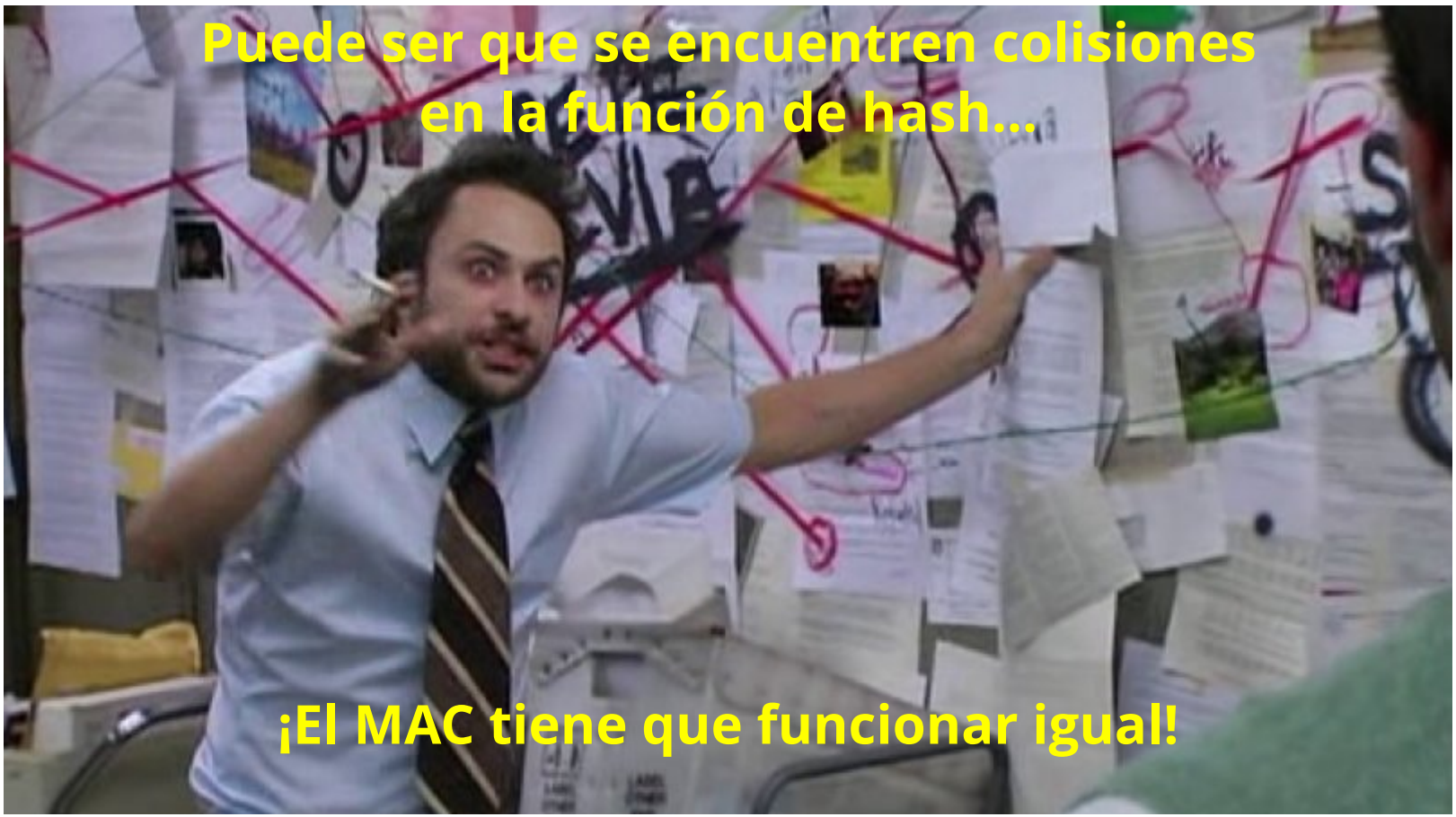
Donde $m' = m_0 \cdots m_\ell$

Length extension attacks

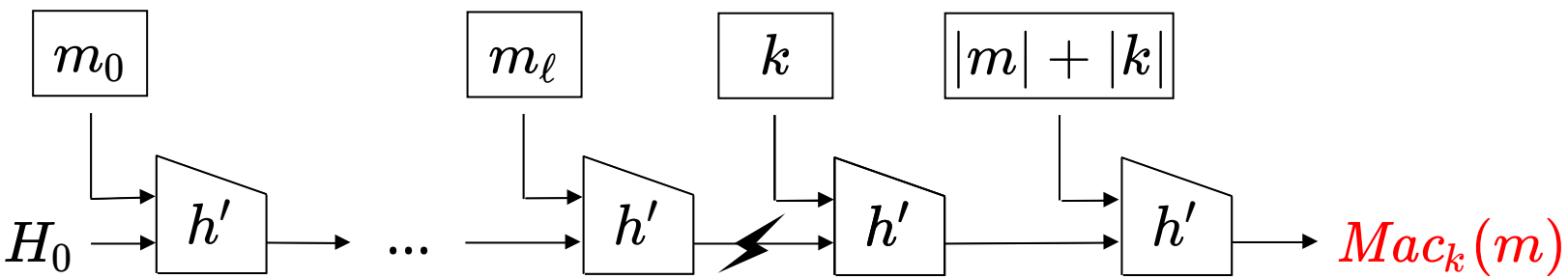
¿Y si tratamos con $Mac_k(m) = h(m||k)$?

¿Podemos hacer ataques de extensión de largo?

No, pero seamos más paranóicos


Puede ser que se encuentren colisiones
en la función de hash...
¡El MAC tiene que funcionar igual!

$$Mac_k(m) = h(m||k)$$



Una colisión de dos mensajes del mismo largo implica romper el MAC

¿Qué hacemos entonces?

Podemos tratar varias cosas, pero lo que podemos *intuir* que es seguro es

$$Mac_k(m) = h(k_1 \,||\, h(k_2 \,||\, m))$$

Donde k_1 y k_2 ocupan exactamente un bloque, son distintas, se derivan de forma determinista a partir de k y no se pueden obtener sin k

El estándar se define de la siguiente forma

$$k' = \begin{cases} h(k) & k \text{ usa más de un bloque} \\ k & \text{e.o.c.} \end{cases}$$

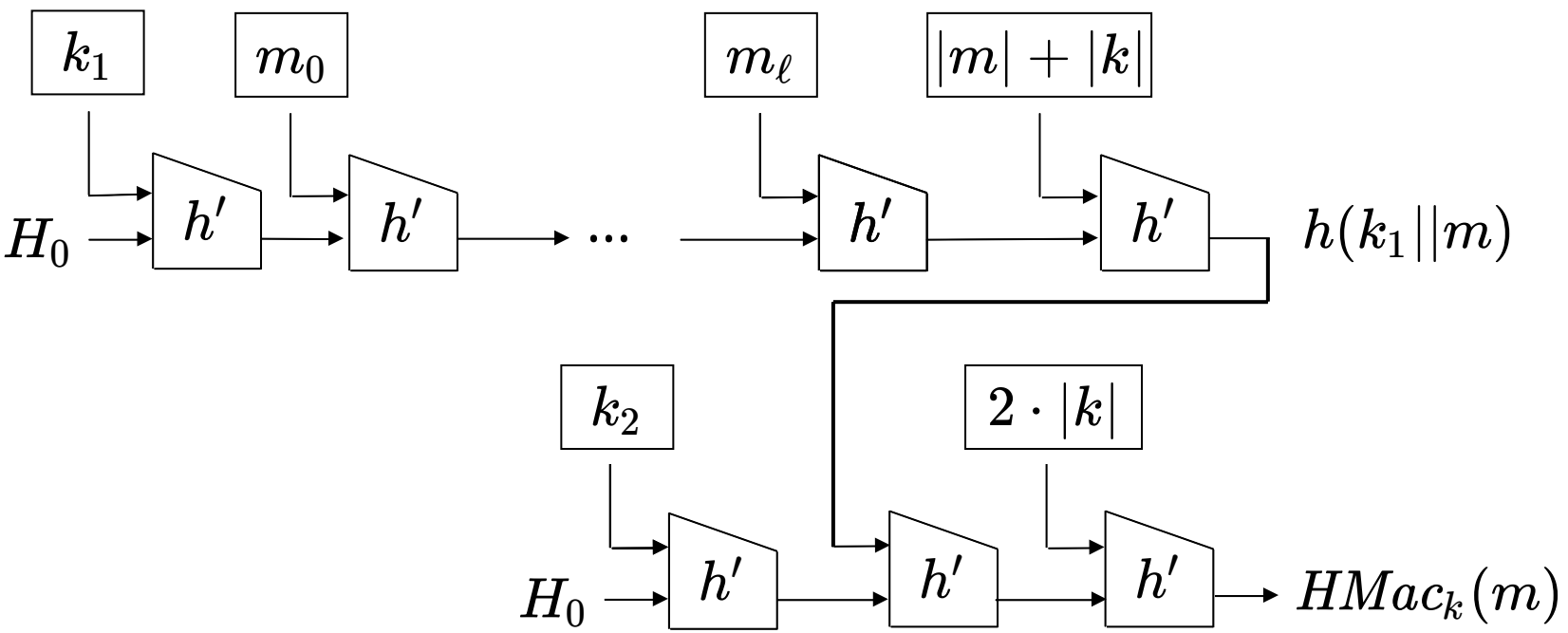
$$k_1 = k' \oplus \texttt{36} \cdots \texttt{36} \qquad k_2 = k' \oplus \texttt{5c} \cdots \texttt{5c}$$

```
5c = 01011100

36 = 00110110
```

$$HMac_k(m) = h(k_2 \,||\, h(k_1 \,||\, m))$$

$$HMAC_k(m) = h(k_2 || \, h(k_1 || m))$$



Wikipedia

No se conocen ataques prácticos para HMAC-MD5, suponiendo que el atacante no conoce la llave