1) HMAC : MAC à partir de hachages

HMAC utilise SHA-1.

La clé est hachée avec le message.

a) • préfixe MAC : pMAC :

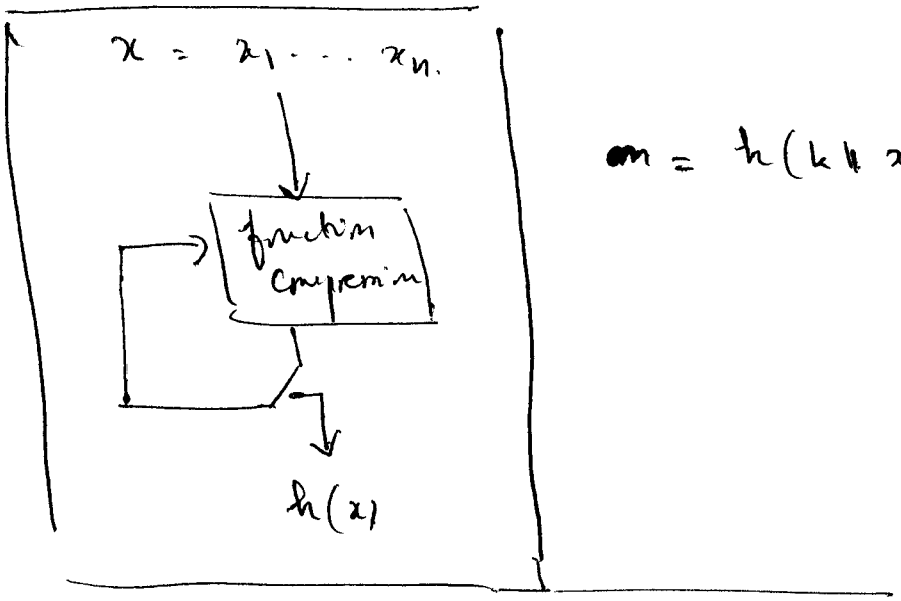
$$m = MAC_k(x) = h(k \| x).$$

b) • suffixe MAC : sMAC :

$$m = MAC_k(x) = h(x \| k).$$

a) Attaque de p.MAC : $m = h(k \| x)$.

On suppose que h est construit par (voir chap. hachage)



$m = h(k \| x_1, \ldots x_n)$.

A C B

$x = (x_1, \ldots, x_n)$

$m = h(k \| x_1, \ldots, x_n)$

Σ interception : (x, m) ←

x_0

$(x_1, \ldots, x_n, x_{n+1})$

$m_0 = h(m \| x_{n+1})$.

(x_0, m_0) ←

$m' = h(k \| x_1 \ldots x_n x_{n+1})$

$m' = m_0 \Rightarrow$

valide.