b) Attaque de DMAC : $m = h(x \| k)$

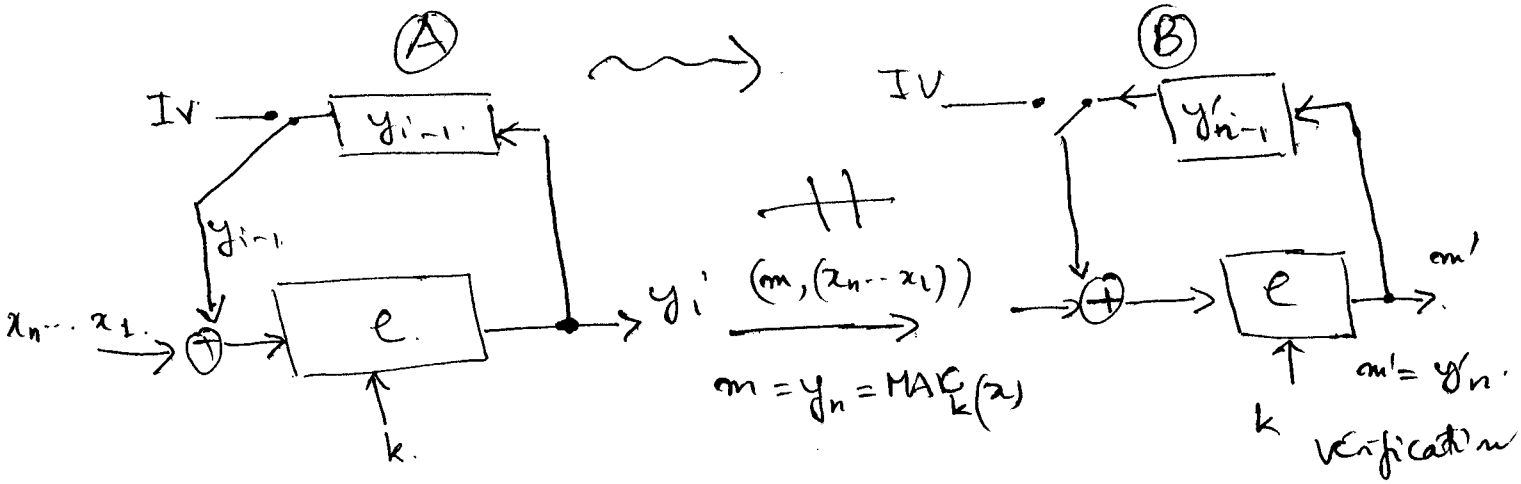
Supposons que O peut trouver x et x_0. $h(x) = h(x_0)$.

$m_0 = h(x \| k) = h(x_0 \| k)$: nature itérative de MAC. permet cette attaque.

2) MAC à partir de B-cryptage :

ex. mode CBC. (cipher Bloc chaining mode).

On obtient un mode CBC_MAC : $x = x_1 \dots x_n$.



$$\begin{cases} y_1 = e_k(x_1 \oplus IV) \\ y_i = e_k(x_i \oplus y_{i-1}) \quad i \geq 2 \end{cases}$$

$m = MAC_k(x) = y_n$.

Avec le DES, utilisé par les banques.

- on peut utiliser Galois Counter MAC.