2021-05-18

May 18, 11:17 AM — IIC 3253

$|k| = n \quad |m| = l$

$Enc(k, m) = c \quad |c| = l$

NIST: National Institute of Standards and Technology

Llamado para AES

advanced enc. standard

"the extent to which the output is indist. from a random permutation"

$k \leftarrow K$

$Enc(k, m)$ sea PRP para m

$2l \cdot 2^l$

No podemos guardar tanta información !!

$F_k := Enc(k, \cdot)$

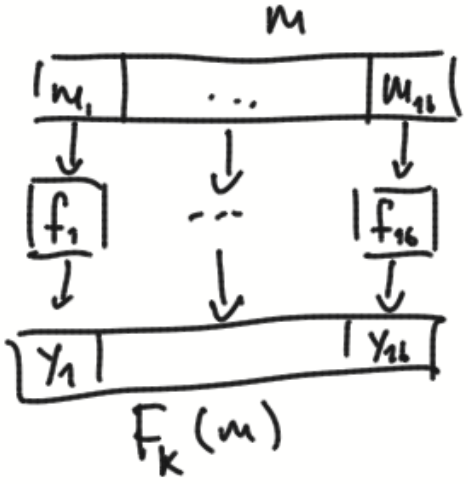
$\ell = 128$

Sup $f_1 \dots f_{16}$ son permutaciones de $\{0,1\}^8$

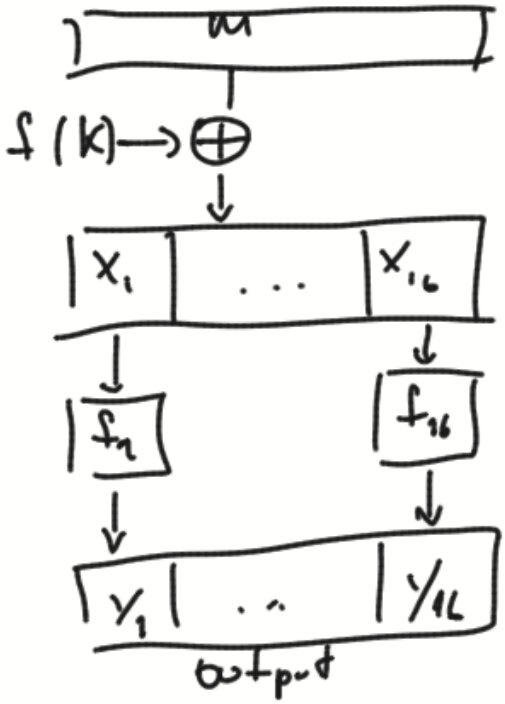
Dividimos m en bytes (bloques de 8 bits)

$m_1 \dots m_{16}$

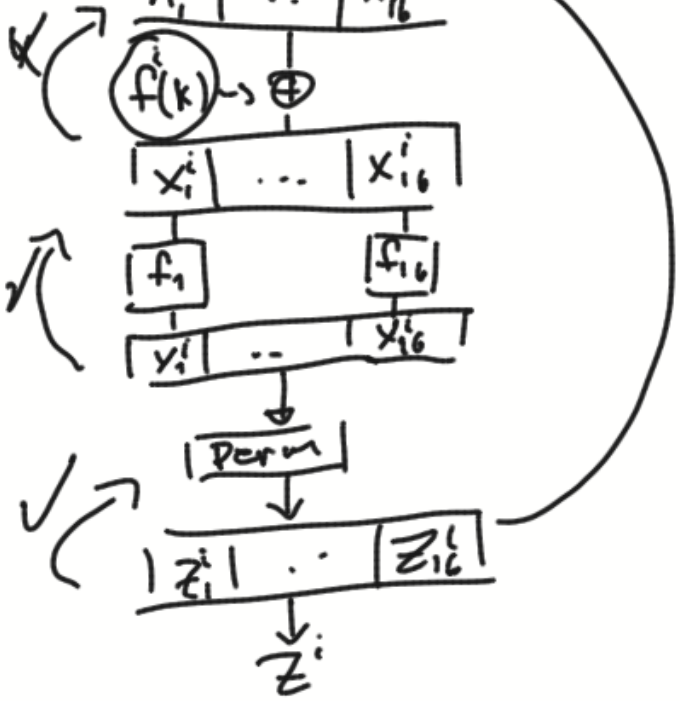
Def $F_k(m) := f_1(m_1) \| f_2(m_2) \| \dots \| f_{16}(m_{16})$



Pésima idea!!!



Mala idea!!!



$|f^i(k)_1| = 8$

Red de sustitución/permutación

output

$F_k(m) := z^{12}$