2021-05-20

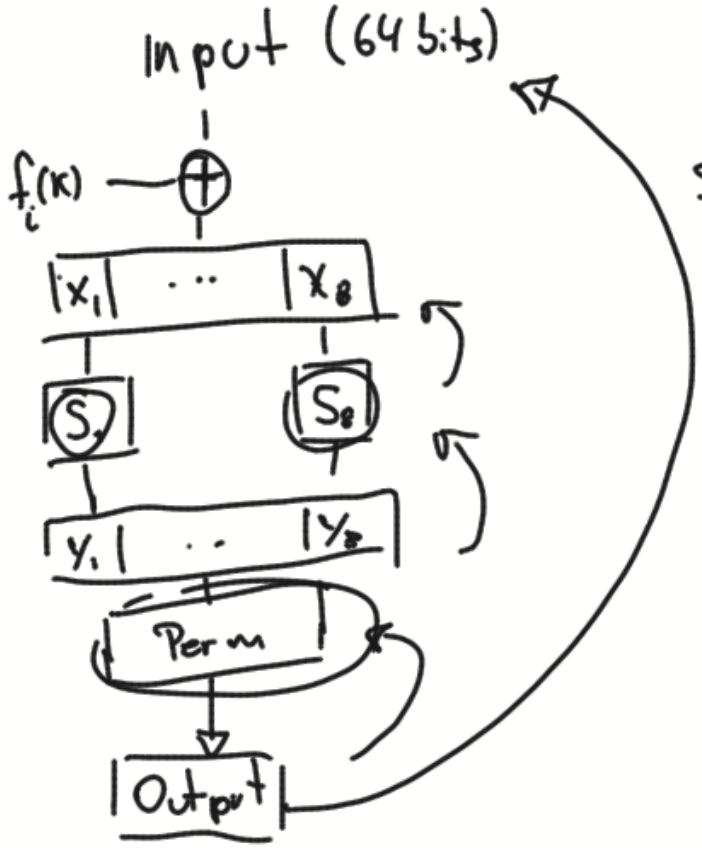
May 20, 11:25 AM

IIC 3253

PRP en 64 bits

Mucha memoria!!

Generar PRP en base a perm. de largo menor



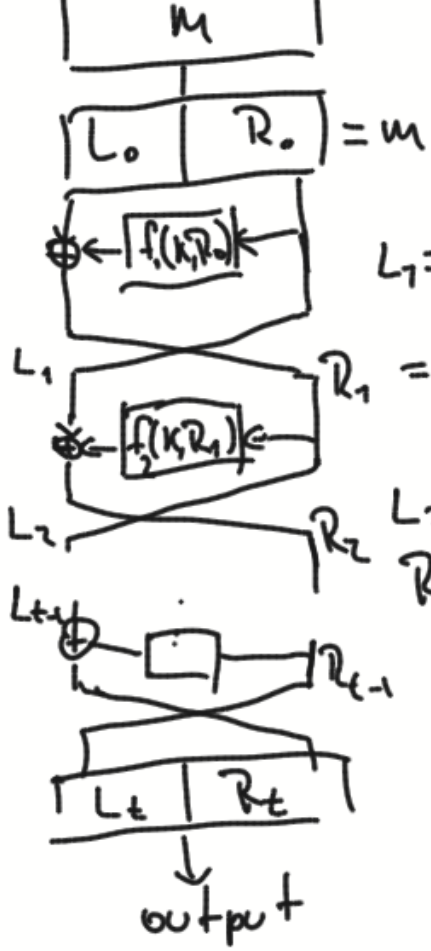
S/P - Network

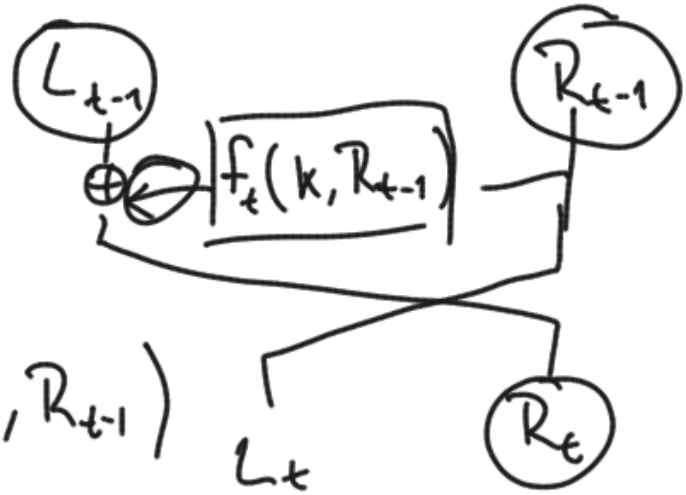
Substitution - permutation

- Invertible
- Efecto avalancha

Base de AES

Redes de Feistel (Base de DES)





Es invertible? ✓

$L_{t-1} = R_t \oplus f_t(K, R_{t-1})$

$R_{t-1} = L_t$

Efecto avalancha → más adelante.

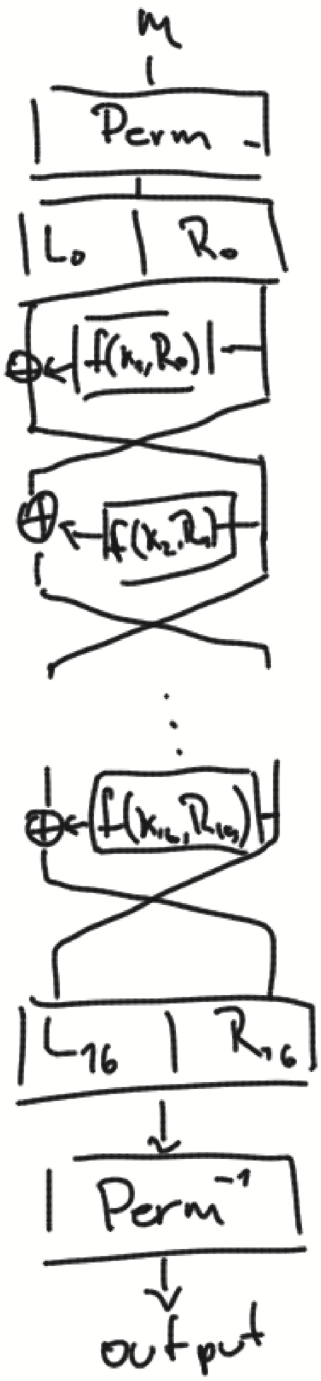
Cuántas rondas?

$L_1 = R_0$

Pésima idea!!!...

más rondas? veamos ej concreto.

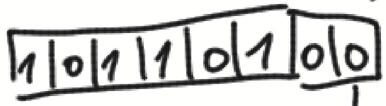
DES (Data Encryption Standard)



$|m|=64$

$|k|=64$, con 8 bits de paridad

$|k|=56$



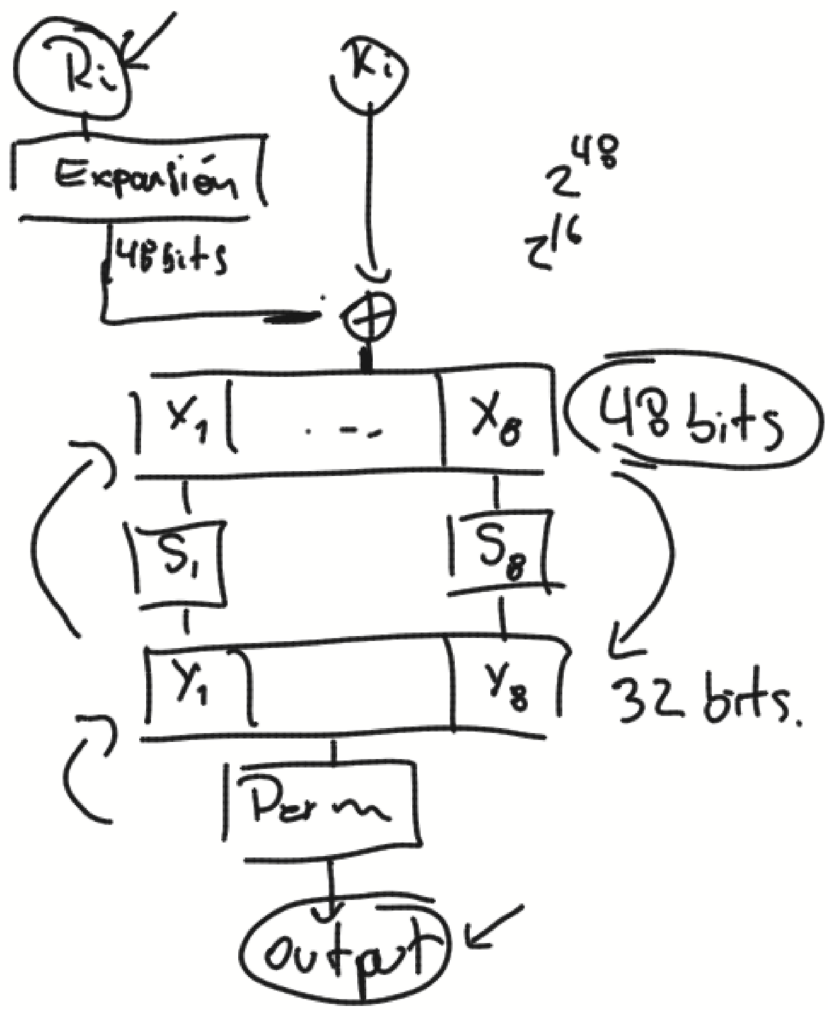
→ 0 si hay cant. par de 1s
1 eoc.

Qué es f?

Es una S/P-Network de 1 ronda.

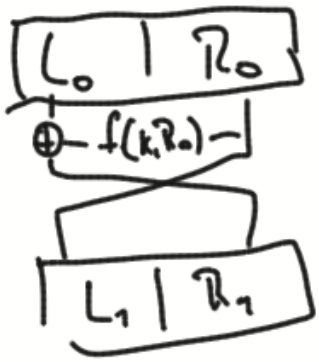
El input es R_i (además de K_{i+1})

$|R_i|=32$ $|K_{i+1}|=48$ bits



Las S-boxes toman 6 bits
y retornan 4-bits.

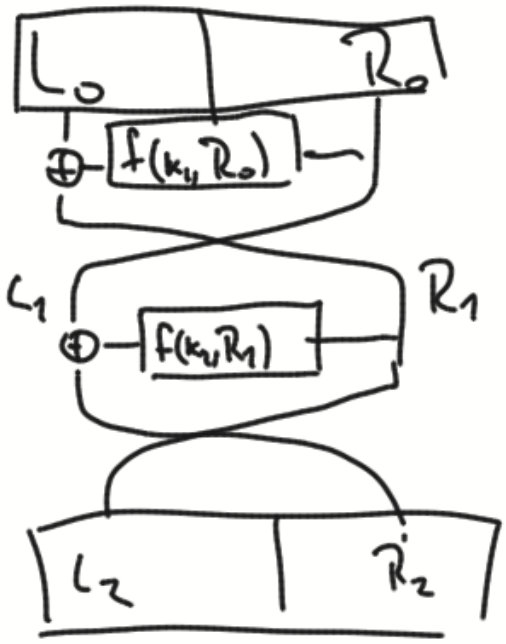
Podemos obtener la llave si suponemos
DES con 1 ronda y tenemos $(m, DES(m))$?



$L_1 = R_0$

$f(K_1, R_0) = L_0 \oplus R_1$

Ataque en 2 rondas



$L_1 = R_0$

$R_1 = L_0 \oplus f(K_1, R_0)$!

$L_2 = R_1$

$R_2 = L_1 \oplus f(K_2, R_1)$!

$\rightarrow f(k_1, R_0) = L_2 \oplus L_0$

$\rightarrow f(K_2, L_2) = R_2 \oplus R_0$