Justification : (2 16)

- Étant donné k, trouver k_{16} :

ma $C_0 = C_{16}$ et $D_0 = D_{16}$. D'où k_{16} après PC-I :

$$\begin{aligned} k_{16} &= PC-2(C_{16}, D_{16}) \\ &= PC-2(C_0, D_0) \\ &= PC-2(PC-I(k)). \end{aligned}$$

- $$\begin{aligned} k_{15} &= PC-2(C_{15}, D_{15}) \\ &= PC-2(RS_2(C_{16}), RS_2(D_{16})) \end{aligned}$$

Right shift.

$$= PC-2(RS_2(C_0), RS_2(D_0)).$$

$k_{14}, k_{13}, \ldots$ s'obtiennent par RS

- ma : Ronde i decryptage inverse Round$_{16-i+1}$ du crypt.

- $$\begin{aligned} (L_0^d, R_0^d) = IP(y) &= IP(IP^{-1}(R_{16}, L_{16})) \\ &= (R_{16}, L_{16}) \end{aligned}$$

$\Rightarrow$ $L_0^d = R_{16}$ et $R_0^d = L_{16} = R_{15}$.

- Ronde$^d_1$ inverse Ronde$_{16}$:

$$L_1^d = R_0^d = L_{16} = R_{15}.$$

$$\begin{aligned} R_1^d &= L_0^d \oplus f(R_0^d, k_{16}) = R_{16} \oplus f(L_{16}, k_{16}) \\ &= L_{15} \oplus f(R_{15}, k_{16}) \oplus f(R_{15}, k_{16}) = L_{15} \end{aligned}$$

etc. $\boxed{L_i^d = R_{16-i} \text{ et } R_i^d = L_{16-i}}$