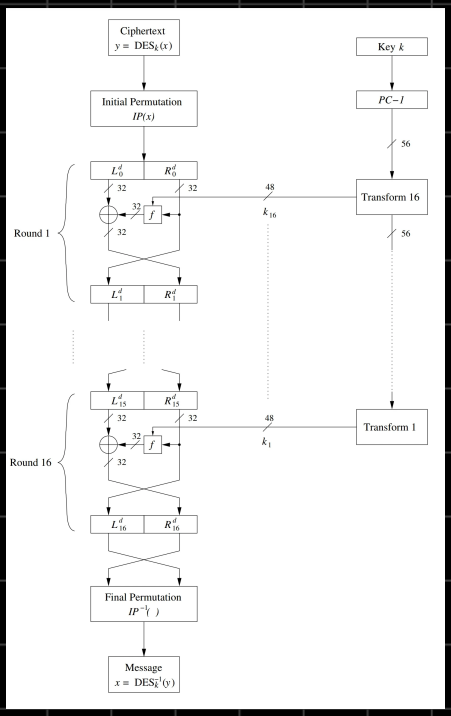
3.4. Descifrado

Esencialmente es la misma función que en el cifrado ← llave privada
↳ DES está basado en una red Feistel

* Comparado con el cifrado, sólo el esquema de llaves se invierte
↳ Ronda 1 de descifrado ⟷ subllave k_{16}
Ronda 2 " " ⟷ " k_{15}
⋮
Ronda 16 " " ⟷ " k_1



→ Esquema de llaves invertido

Dada la llave inicial k, ¿podemos generar fácilmente k_{16}?

Tenemos que $C_0 = C_{16}$ y $D_0 = D_{16}$, entonces

$$\begin{aligned} k_{16} &= PC\text{-}2(C_{16}, D_{16}) \\ &= PC\text{-}2(C_0, D_0) \\ &= PC\text{-}2(PC\text{-}1(k)) \end{aligned}$$

¿Cómo obtener k_{15}?

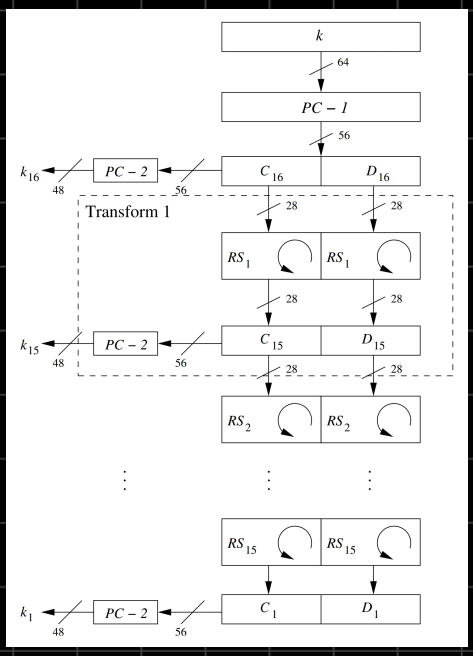
Necesitamos C_{15} y D_{15}, que se derivan de C_{16} y D_{16} a través de rotaciones hacia la derecha (RS):

$$\begin{aligned} k_{15} &= PC\text{-}2\,(C_{15}, D_{15}) \\ &= PC\text{-}2\,(RS_2(C_{16}), RS_2(D_{16})) \\ &= PC\text{-}2\,(RS_2(C_0), RS_2(D_0)) \end{aligned}$$

¿Y las demás llaves?

Se sigue un proceso similar, vía rotaciones a la derecha.

* $Ronda_D$ 1 → no se rota la llave
* $Ronda_D$ 2, 9, 16 → las dos mitades se rotan a la derecha un bit
* $Ronda_D \neq 1, 2, 9, 16$ → las dos mitades se rotan a la derecha dos bits



→ Descifrado en redes de Feistel

¿Por qué el descifrado es esencialmente lo mismo que el cifrado?

Idea básica: el descifrado invierte a DES ronda por ronda.

↳ $Ronda_D$ 1 ⟷ $Ronda_C$ 16, ..., $Ronda_D$ 16 ⟷ $Ronda_C$ 1

Notemos lo siguiente: si $y = DES_k(x)$,

$$(L_0^d, R_0^d) = IP(y) = IP(IP^{-1}(R_{16}, L_{16})) = (R_{16}, L_{16})$$

$$\Rightarrow \begin{aligned} L_0^d &= R_{16} \\ R_0^d &= L_{16} = R_{15} \end{aligned}$$

Ahora veamos que la primera ronda de descifrado revierte la última ronda de cifrado. Para esto, notemos que

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

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

Este es un proceso iterativo que continúa en las siguientes rondas:

$$L_i^d = R_{16-i} \qquad R_i^d = L_{16-i} \qquad i = 0, \ldots, 16$$

Entonces $L_{16}^d = R_0$ y $R_{16}^d = L_0$. Finalmente,

$$IP^{-1}(R_{16}^d, L_{16}^d) = IP^{-1}(L_0, R_0) = IP^{-1}(IP(x)) = x$$