→ Au début, on applique $IP(x)$ une permutation ;
le résultat obtenu est partagé en L_0, R_0.

on applique ensuite

ronde i $\begin{cases} L_i = R_{i-1} & \text{(copie)} \\ R_i = L_{i-1} \oplus f(R_{i-1}, k_i) \end{cases}$

noter que la partie gauche seulement est cryptée ici par f, au rond prochain, l'autre partie est cryptée (swapping).

⇒ la substance du chiffrement est donc dans la fonction f, qui réalise la Confusion et la diffusion. C'est une fonction non-linéaire, utilisant la clé k_i, qui est surjective.

(2) Structure interne du DES :

Les blocs constituants le DES sont :
PI et PI^{-1}, les rondes du DES, la fonction f et l'ordonnancement des clés.

(2.1) PI et PI^{-1} : permutation (fixe tables) permettant d'arranger les choses. Facile à réaliser hardware.