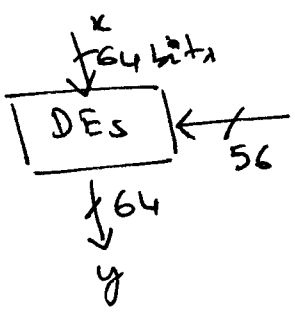
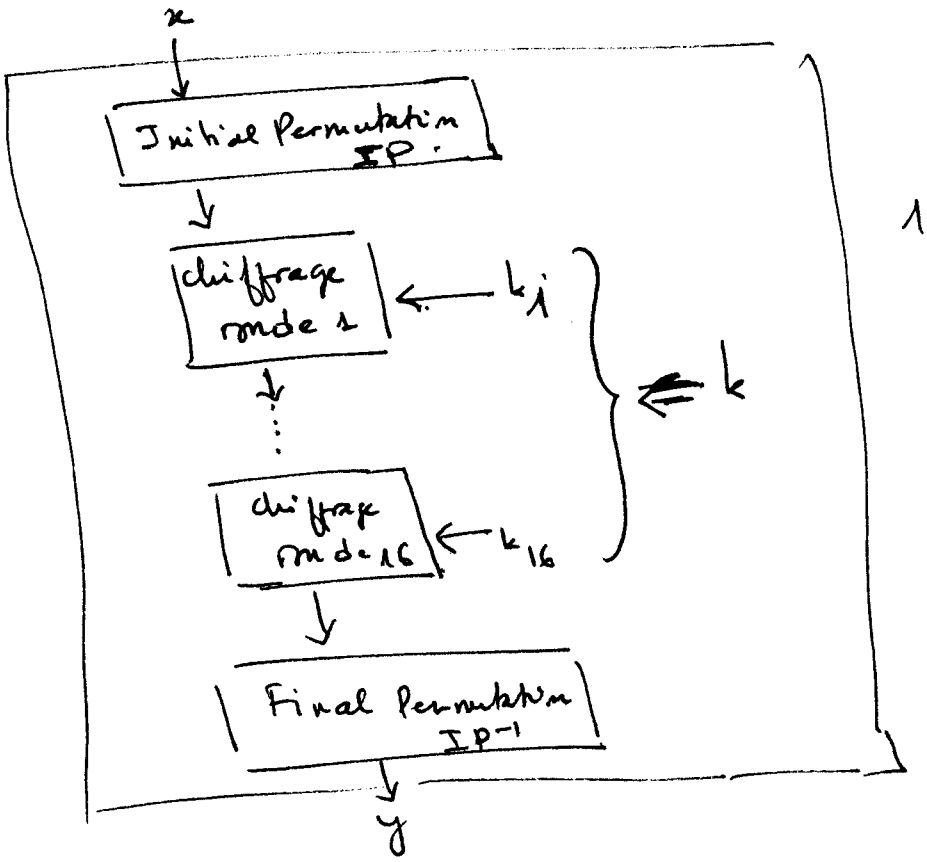
(1) L'Algorithme DES : chiffrement par bloc de taille 64 bits :



Le B. chiffrage est fait itérativement : chaque étape (qu'on va appeler ronde) exécute les mêmes opérations ; il y a 16 rondes. chaque ronde a une clé k_i extraite de k.



16 rondes du DES.

La structure des rondes (identiques) est basée sur le réseau de Fiestel facile à implémenter et aussi la méthode de décryptage consiste à ordonnancer la clé k_i en ordre inverse

Le réseau de Fiestel consiste en 16 rondes avec l'entrée (L_0, R_0)