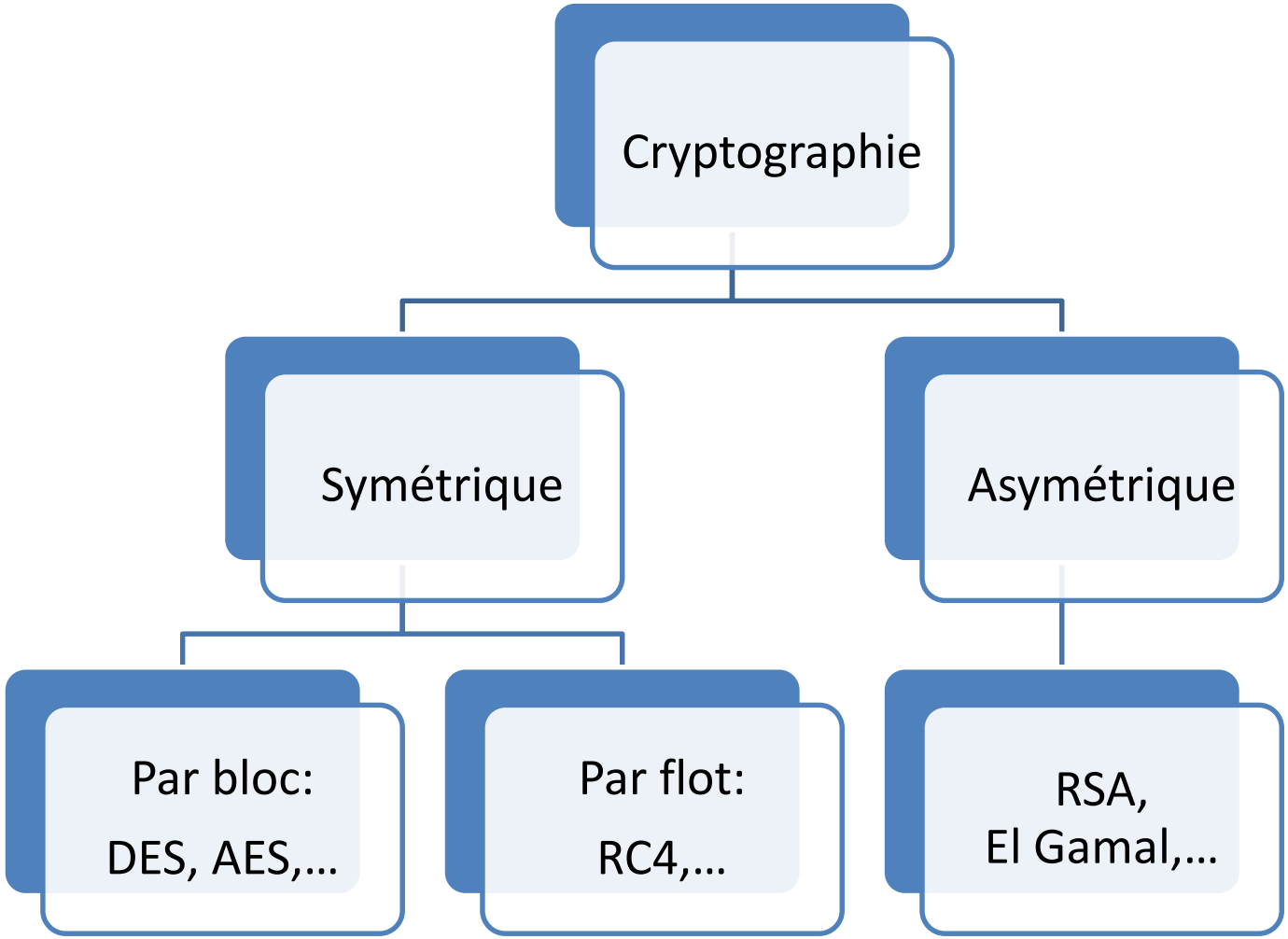




# Chiffrement Symétrique

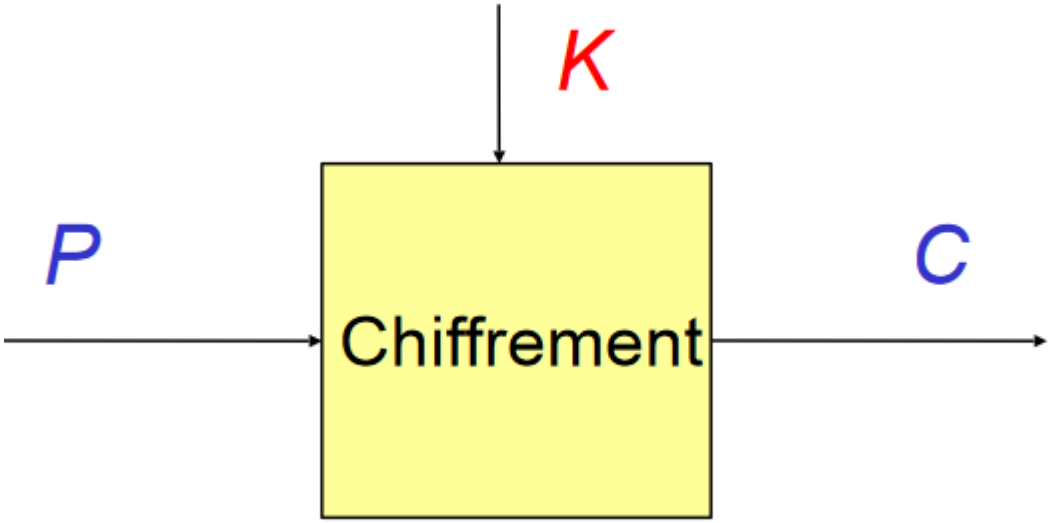
Pr. Mustapha JOHRI

# La Cryptographie moderne



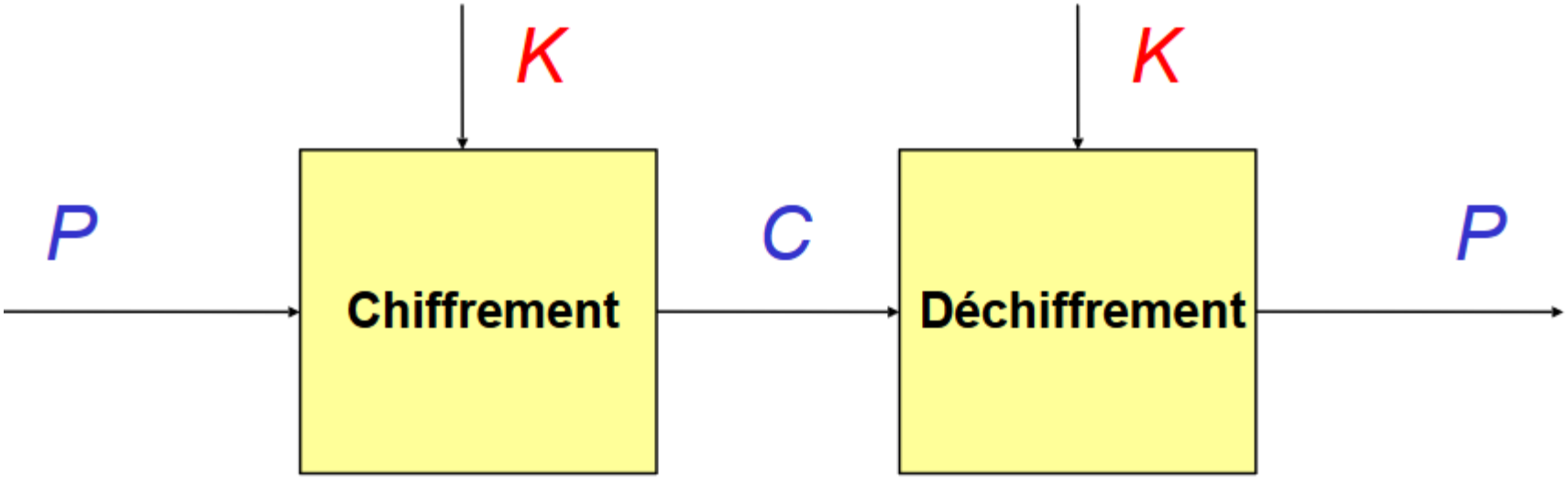
# Chiffrement Symétrique

- **Définition** : Un algorithme de chiffrement symétrique transforme un message en clair P avec une clé secrète K. Le résultat est un message chiffré C



# Chiffrement Symétrique

- La fonction de chiffrement doit être inversible



# Chiffrement Symétrique

- On distingue deux grandes catégories

Chiffrement par flot

- P est traité bit par bit
- Algorithmes :
  - RC4, E0/1(Bluetooth) , A5/1(GSM )

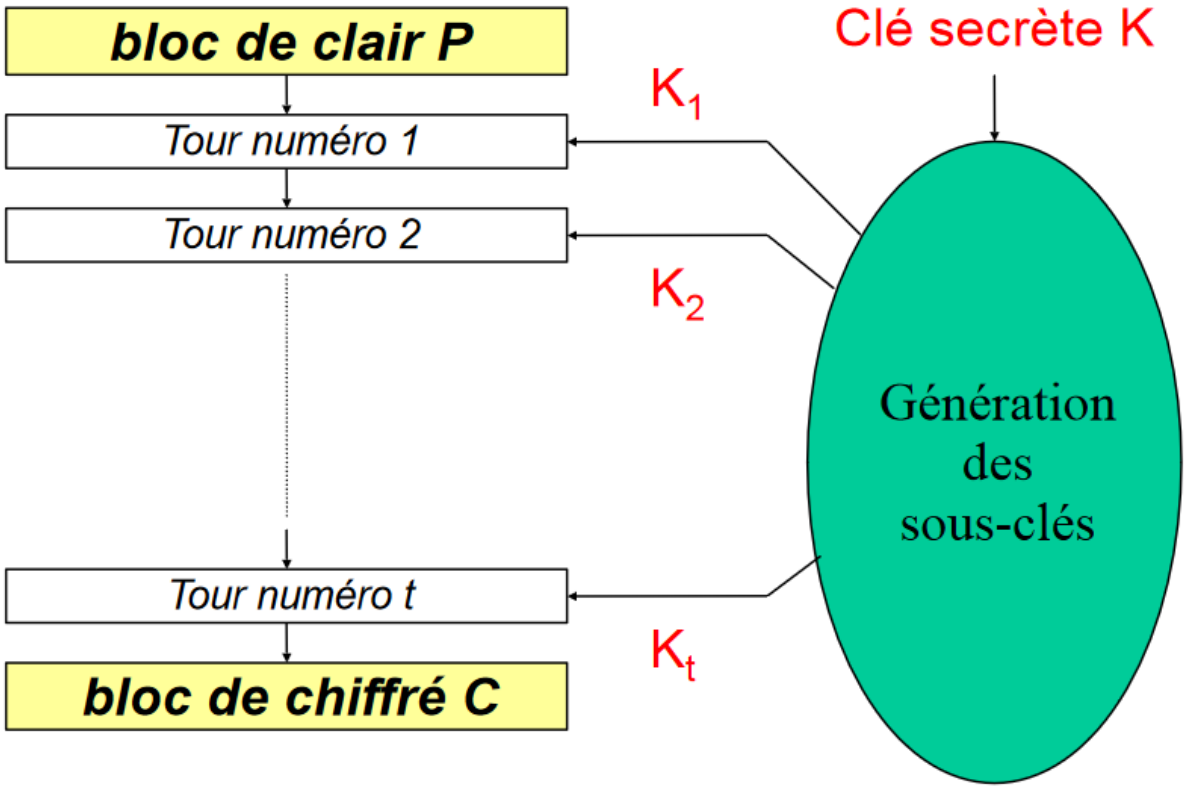
Chiffrement par bloc

- P est traité par blocs de données (ex: 64 bits ou 128 bits)
- Algorithmes :
  - DES (mots de passe Unix)
  - AES, IDEA(e-mail), RC6,

# Chiffrement par bloc

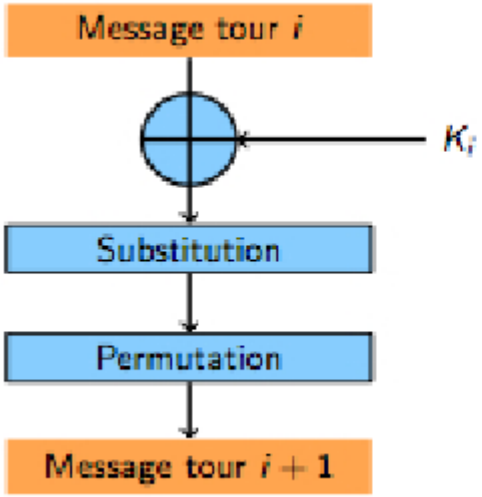
# Chiffrement par blocs

- Schéma général



# Chiffrement par blocs

- Entre deux tours successives :




- addition de la sous-clef $K_i$
- couche de substitution
- couche de transposition

# Data Encryption Standard:

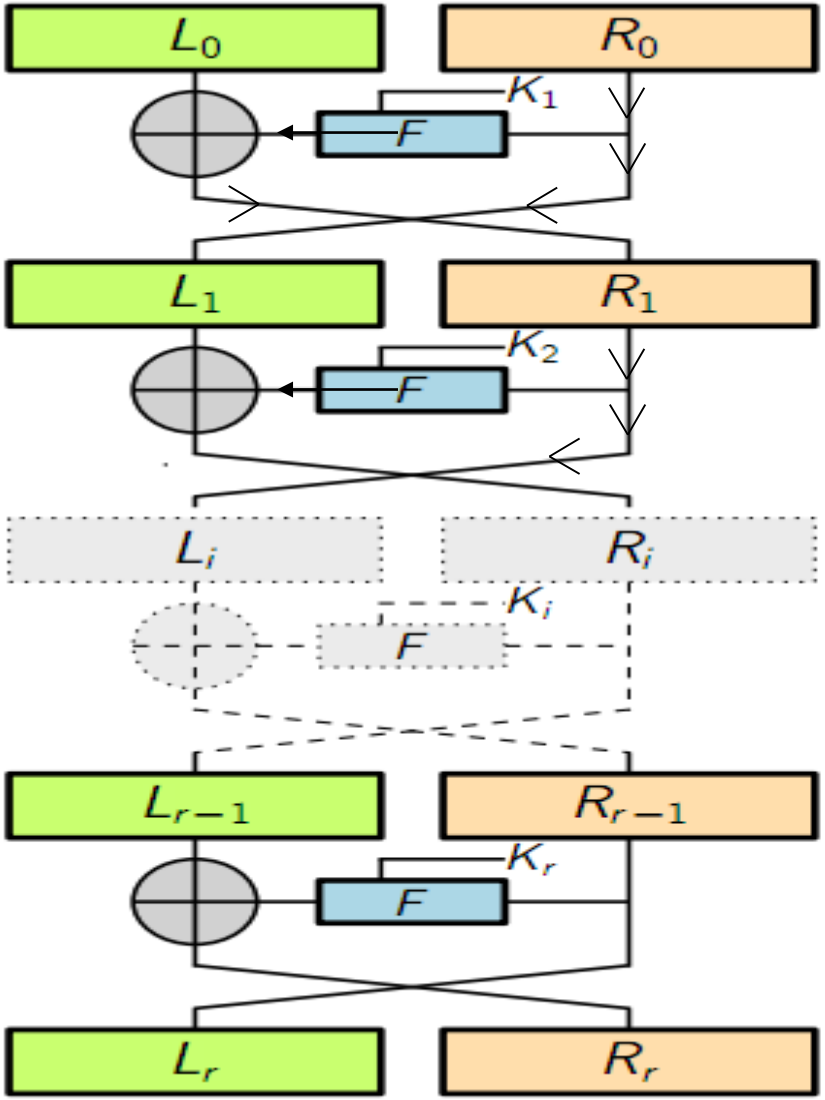
# DES

# Description de DES

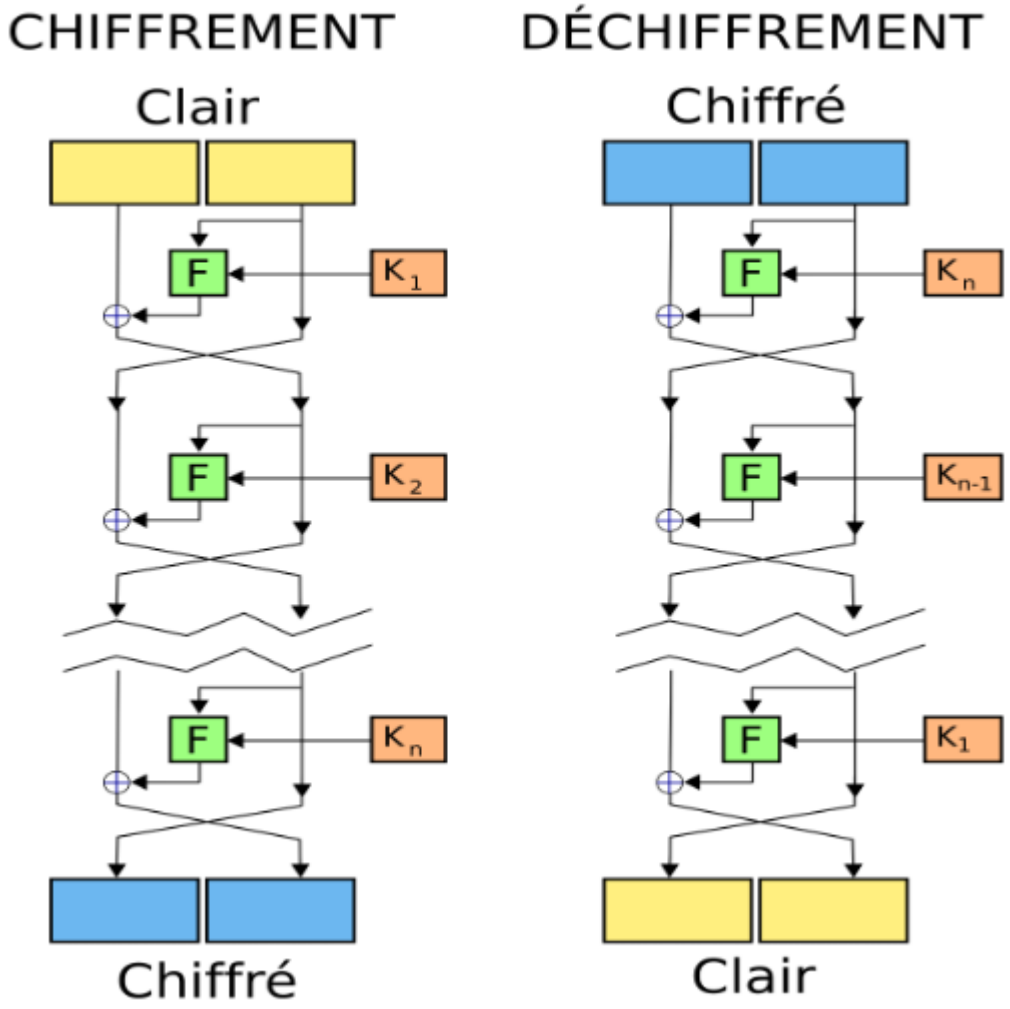
- Crée par **IBM**.
- Approuvé en tant que **standard de chiffrement** aux États-Unis en 1976.
- «Amélioré» par la NSA (**National Security Agency)**
- Utilise des **blocs de taille n = 64 bits**.
- Utilise une **clef de taille 56 bits**.
- Basé sur le principe d'un **réseau de Feistel à 16 tours.**

# Description des réseaux de Feistel

**Chiffrement**: un bloc de texte en clair est découpé en deux ; la transformation de ronde est appliquée à une des deux moitiés, et le résultat est combiné avec l'autre moitié par ou exclusif. **Les deux moitiés sont alors inversées pour l'application de la ronde suivante.**



# Description des réseaux de Feistel

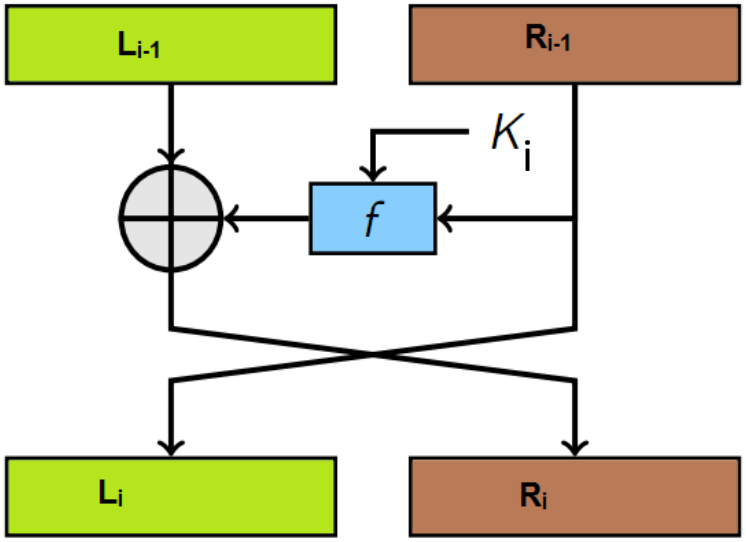


# Description des réseaux de Feistel

- La taille de bloc doit être paire, on divise le bloc en deux: $m=(L_0, R_0)$.
- n tours.
- Chaque tour transforme $(L_{i-1}, R_{i-1})$ en $(L_i, R_i)$ où :

- Pour i=1,…,n

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



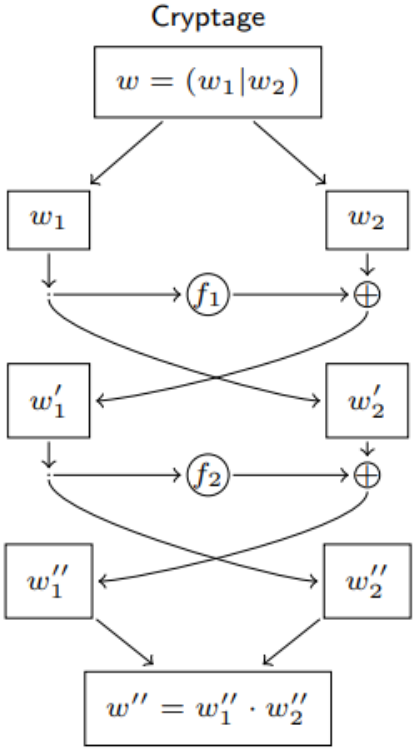

- La **sortie** est $(L_n, R_n)$
- Fonction de tour **inversible**

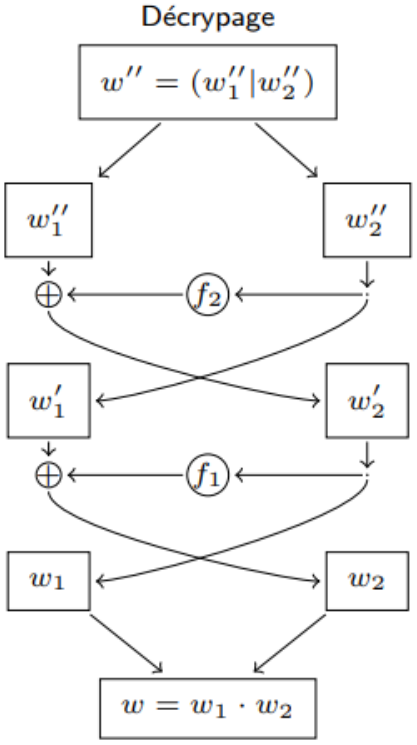
même si F ne l'est pas !!

# Description des réseaux de Feistel

**Exercice :** On considère le diagramme de Feistel suivant sur 2 tours en acceptant en entrée des mots binaire w codés sur 6bits, avec

| m | $f_1(m)$ | $f_2(m)$ |
|---|---|---|
| 000 | 101 | 010 |
| 001 | 100 | 001 |
| 010 | 011 | 110 |
| 011 | 000 | 111 |
| 100 | 001 | 110 |
| 101 | 101 | 011 |
| 110 | 010 | 001 |
| 111 | 110 | 100 |

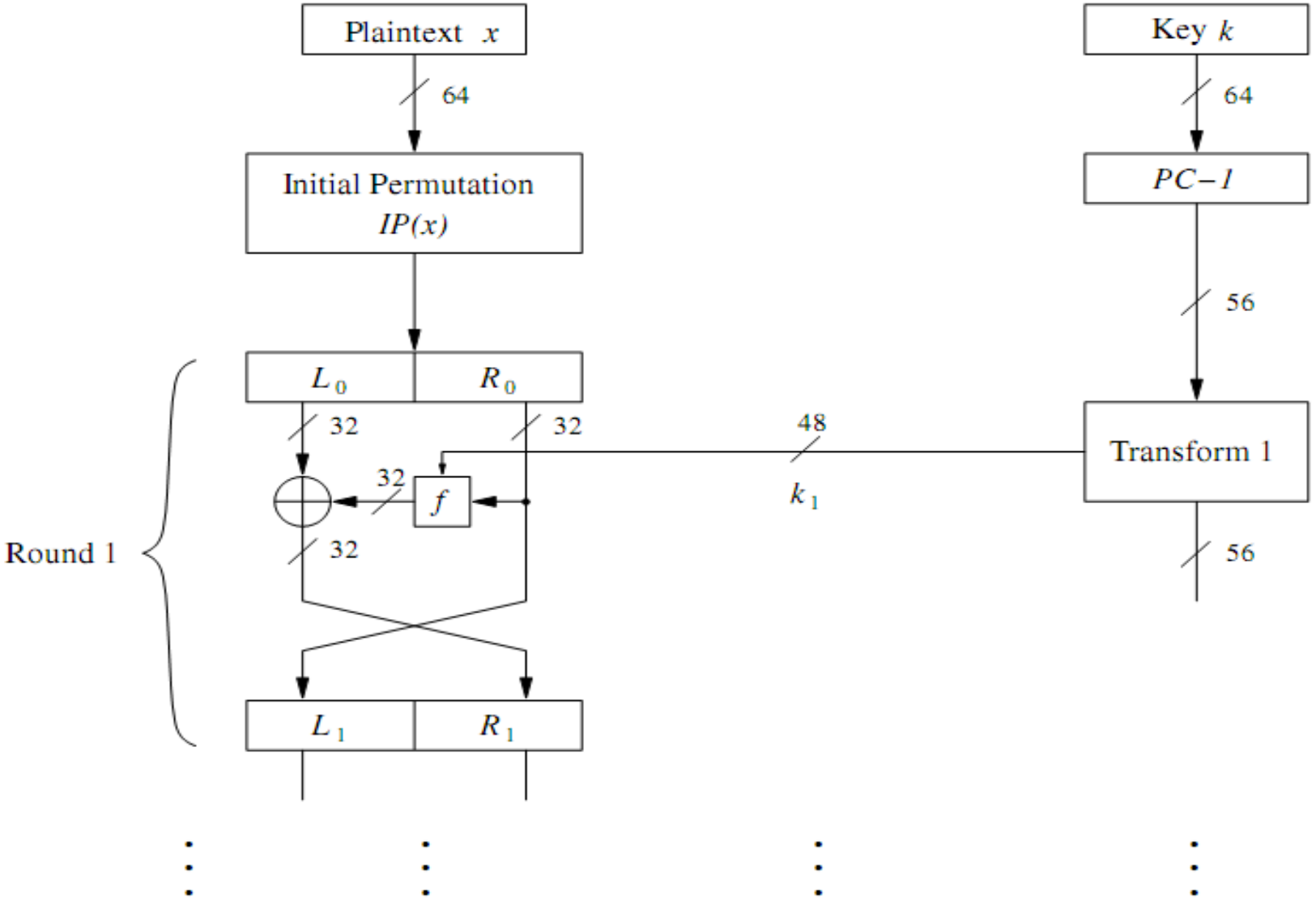


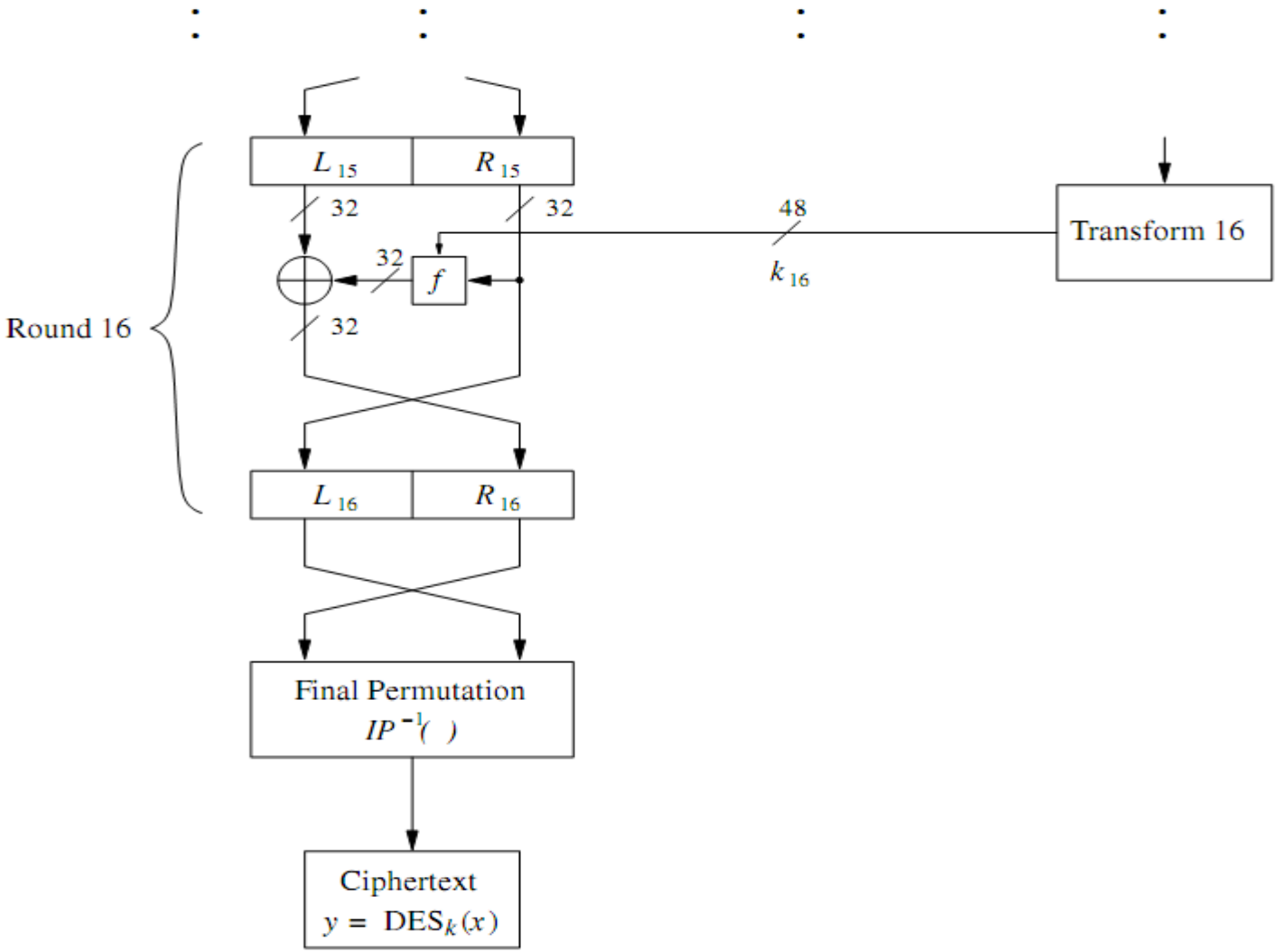

- Coder le message m = 101110 → **C =010011**
- Décoder le message c=111010

# Description de DES:

## schéma général



# Description de DES: schéma général



# Description de DES: permutation

- la transformation IP et la transformation inverse $IP^{-1}$ sont des permutations définies par les tableaux ci-dessous :

| $IP$ | | | | | | | |
|---|---|---|---|---|---|---|---|
| 58 | 50 | 42 | 34 | 26 | 18 | 10 | 2 |
| 60 | 52 | 44 | 36 | 28 | 20 | 12 | 4 |
| 62 | 54 | 46 | 38 | 30 | 22 | 14 | 6 |
| 64 | 56 | 48 | 40 | 32 | 24 | 16 | 8 |
| 57 | 49 | 41 | 33 | 25 | 17 | 9 | 1 |
| 59 | 51 | 43 | 35 | 27 | 19 | 11 | 3 |
| 61 | 53 | 45 | 37 | 29 | 21 | 13 | 5 |
| 63 | 55 | 47 | 39 | 31 | 23 | 15 | 7 |

Initial permutation $IP$

| $IP^{-1}$ | | | | | | | |
|---|---|---|---|---|---|---|---|
| 40 | 8 | 48 | 16 | 56 | 24 | 64 | 32 |
| 39 | 7 | 47 | 15 | 55 | 23 | 63 | 31 |
| 38 | 6 | 46 | 14 | 54 | 22 | 62 | 30 |
| 37 | 5 | 45 | 13 | 53 | 21 | 61 | 29 |
| 36 | 4 | 44 | 12 | 52 | 20 | 60 | 28 |
| 35 | 3 | 43 | 11 | 51 | 19 | 59 | 27 |
| 34 | 2 | 42 | 10 | 50 | 18 | 58 | 26 |
| 33 | 1 | 41 | 9 | 49 | 17 | 57 | 25 |

Final permutation $IP^{-1}$

- La signification de IP est que le 58ème bit devient le 1er bit, le 50ème devient le 2ème, et ainsi de suite.

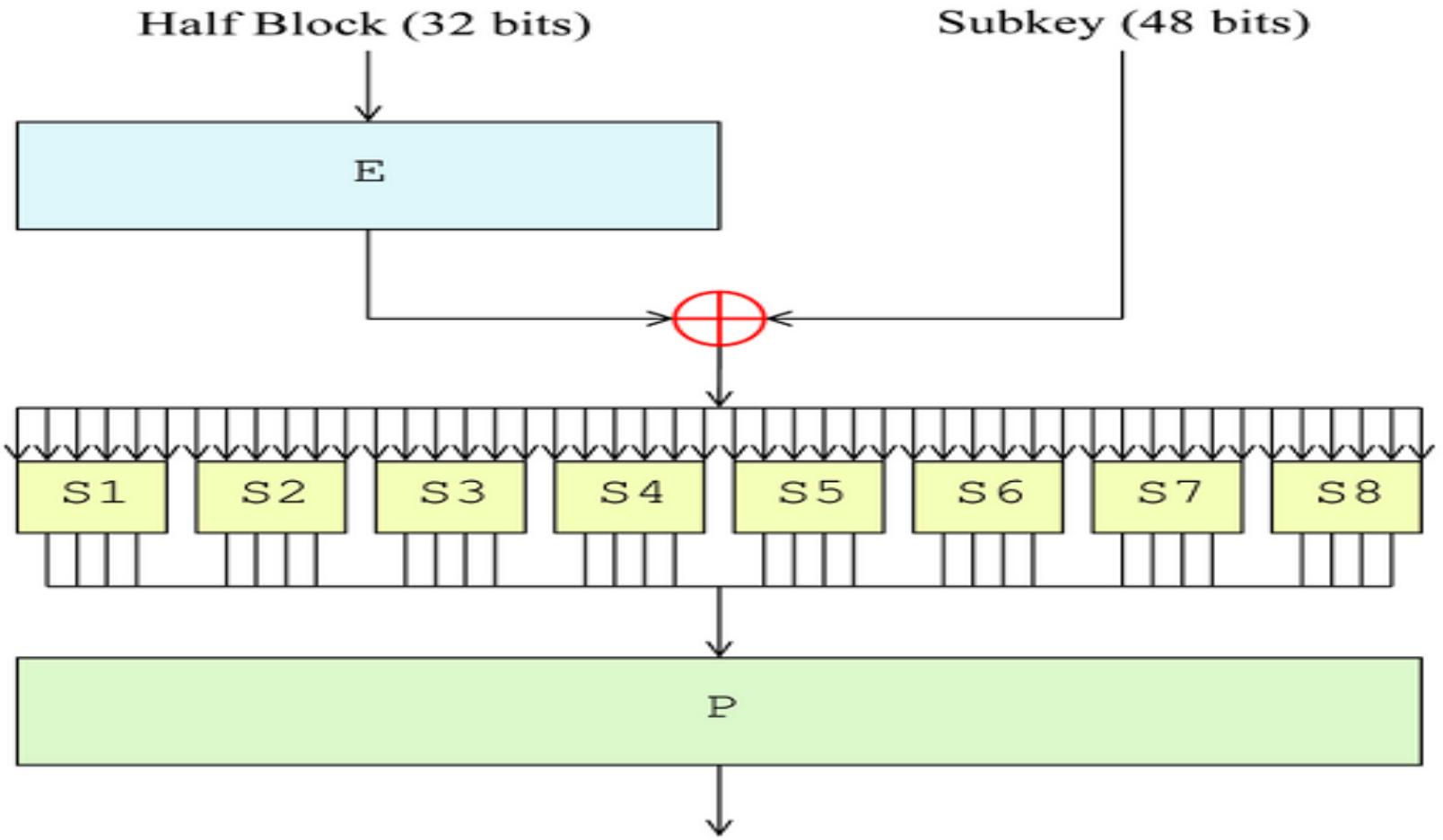
- De même pour $IP^{-1}$, le premier bit du résultat est le bit 40, le deuxième bit du résultat est le bit 8, etc.

# Description de DES: détails

- Une permutation initiale, IP est appliquée sur les 64 bits du bloc.
- La permutation inverse est appliquée à la fin du chiffrement.
- 16 clefs de rondes $K_1,\ldots,K_{16}$ de 48 bits chacune sont déduites des 56 bits de la clef principale.

- Pour chaque ronde du réseau de Feistel, on utilise la fonction $f(R_{i-1},k_i)=P(S(E(R_{i-1})+k_i))$ où:
  - E est une expansion fixée de 32 bits vers 48 bits,
  - S est composé de 8 applications fixées de 6 bits vers 4 bits, appelées S-boxes.
  - P est une permutation fixée sur 32 bits.

# Description de DES: fonction f




$$f(R_{i-1}, K_i) = P(S(E(R_{i-1}) \oplus K_i))$$

# Description de DES: fonction f

- Cette fonction f fait intervenir:
  - l'opération E qui transforme un bloc de 32 bits en un bloc de 48 bits,
  - les opérations S1 à S8 qui transforment des groupes de 6 bits en groupes de 4 bits,
  - la permutation P qui agit sur un bloc de 32 bits.

# Description de DES: fonction f

| $E$ | | | | | |
|---|---|---|---|---|---|
| 32 | 1 | 2 | 3 | 4 | 5 |
| 4 | 5 | 6 | 7 | 8 | 9 |
| 8 | 9 | 10 | 11 | 12 | 13 |
| 12 | 13 | 14 | 15 | 16 | 17 |
| 16 | 17 | 18 | 19 | 20 | 21 |
| 20 | 21 | 22 | 23 | 24 | 25 |
| 24 | 25 | 26 | 27 | 28 | 29 |
| 28 | 29 | 30 | 31 | 32 | 1 |

| $P$ | | | | | | | |
|---|---|---|---|---|---|---|---|
| 16 | 7 | 20 | 21 | 29 | 12 | 28 | 17 |
| 1 | 15 | 23 | 26 | 5 | 18 | 31 | 10 |
| 2 | 8 | 24 | 14 | 32 | 27 | 3 | 9 |
| 19 | 13 | 30 | 6 | 22 | 11 | 4 | 25 |

- Le 1er bit de E(R) est le bit 32, le 2ème est le bit 1, etc.
- la permutation P, le 1er bit est le bit 16, le 2ème le bit 7, etc.

# Description de DES: S-Boxes

S-box $S_1$

| $S_1$ | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 0 | 14 | 04 | 13 | 01 | 02 | 15 | 11 | 08 | 03 | 10 | 06 | 12 | 05 | 09 | 00 | 07 |
| 1 | 00 | 15 | 07 | 04 | 14 | 02 | 13 | 01 | 10 | 06 | 12 | 11 | 09 | 05 | 03 | 08 |
| 2 | 04 | 01 | 14 | 08 | 13 | 06 | 02 | 11 | 15 | 12 | 09 | 07 | 03 | 10 | 05 | 00 |
| 3 | 15 | 12 | 08 | 02 | 04 | 09 | 01 | 07 | 05 | 11 | 03 | 14 | 10 | 00 | 06 | 13 |

S-box $S_2$

| $S_2$ | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 0 | 15 | 01 | 08 | 14 | 06 | 11 | 03 | 04 | 09 | 07 | 02 | 13 | 12 | 00 | 05 | 10 |
| 1 | 03 | 13 | 04 | 07 | 15 | 02 | 08 | 14 | 12 | 00 | 01 | 10 | 06 | 09 | 11 | 05 |
| 2 | 00 | 14 | 07 | 11 | 10 | 04 | 13 | 01 | 05 | 08 | 12 | 06 | 09 | 03 | 02 | 15 |
| 3 | 13 | 08 | 10 | 01 | 03 | 15 | 04 | 02 | 11 | 06 | 07 | 12 | 00 | 05 | 14 | 09 |

S-box $S_3$

| $S_3$ | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 0 | 10 | 00 | 09 | 14 | 06 | 03 | 15 | 05 | 01 | 13 | 12 | 07 | 11 | 04 | 02 | 08 |
| 1 | 13 | 07 | 00 | 09 | 03 | 04 | 06 | 10 | 02 | 08 | 05 | 14 | 12 | 11 | 15 | 01 |
| 2 | 13 | 06 | 04 | 09 | 08 | 15 | 03 | 00 | 11 | 01 | 02 | 12 | 05 | 10 | 14 | 07 |
| 3 | 01 | 10 | 13 | 00 | 06 | 09 | 08 | 07 | 04 | 15 | 14 | 03 | 11 | 05 | 02 | 12 |

# Description de DES: S-Boxes

S-box $S_4$

| $S_4$ | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 0 | 07 | 13 | 14 | 03 | 00 | 06 | 09 | 10 | 01 | 02 | 08 | 05 | 11 | 12 | 04 | 15 |
| 1 | 13 | 08 | 11 | 05 | 06 | 15 | 00 | 03 | 04 | 07 | 02 | 12 | 01 | 10 | 14 | 09 |
| 2 | 10 | 06 | 09 | 00 | 12 | 11 | 07 | 13 | 15 | 01 | 03 | 14 | 05 | 02 | 08 | 04 |
| 3 | 03 | 15 | 00 | 06 | 10 | 01 | 13 | 08 | 09 | 04 | 05 | 11 | 12 | 07 | 02 | 14 |

S-box $S_5$

| $S_5$ | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 0 | 02 | 12 | 04 | 01 | 07 | 10 | 11 | 06 | 08 | 05 | 03 | 15 | 13 | 00 | 14 | 09 |
| 1 | 14 | 11 | 02 | 12 | 04 | 07 | 13 | 01 | 05 | 00 | 15 | 10 | 03 | 09 | 08 | 06 |
| 2 | 04 | 02 | 01 | 11 | 10 | 13 | 07 | 08 | 15 | 09 | 12 | 05 | 06 | 03 | 00 | 14 |
| 3 | 11 | 08 | 12 | 07 | 01 | 14 | 02 | 13 | 06 | 15 | 00 | 09 | 10 | 04 | 05 | 03 |

S-box $S_6$

| $S_6$ | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 0 | 12 | 01 | 10 | 15 | 09 | 02 | 06 | 08 | 00 | 13 | 03 | 04 | 14 | 07 | 05 | 11 |
| 1 | 10 | 15 | 04 | 02 | 07 | 12 | 09 | 05 | 06 | 01 | 13 | 14 | 00 | 11 | 03 | 08 |
| 2 | 09 | 14 | 15 | 05 | 02 | 08 | 12 | 03 | 07 | 00 | 04 | 10 | 01 | 13 | 11 | 06 |
| 3 | 04 | 03 | 02 | 12 | 09 | 05 | 15 | 10 | 11 | 14 | 01 | 07 | 06 | 00 | 08 | 13 |

# Description de DES: S-Boxes

S-box $S_7$

| $S_7$ | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 0 | 04 | 11 | 02 | 14 | 15 | 00 | 08 | 13 | 03 | 12 | 09 | 07 | 05 | 10 | 06 | 01 |
| 1 | 13 | 00 | 11 | 07 | 04 | 09 | 01 | 10 | 14 | 03 | 05 | 12 | 02 | 15 | 08 | 06 |
| 2 | 01 | 04 | 11 | 13 | 12 | 03 | 07 | 14 | 10 | 15 | 06 | 08 | 00 | 05 | 09 | 02 |
| 3 | 06 | 11 | 13 | 08 | 01 | 04 | 10 | 07 | 09 | 05 | 00 | 15 | 14 | 02 | 03 | 12 |

S-box $S_8$

| $S_8$ | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 0 | 13 | 02 | 08 | 04 | 06 | 15 | 11 | 01 | 10 | 09 | 03 | 14 | 05 | 00 | 12 | 07 |
| 1 | 01 | 15 | 13 | 08 | 10 | 03 | 07 | 04 | 12 | 05 | 06 | 11 | 00 | 14 | 09 | 02 |
| 2 | 07 | 11 | 04 | 01 | 09 | 12 | 14 | 02 | 00 | 06 | 10 | 13 | 15 | 03 | 05 | 08 |
| 3 | 02 | 01 | 14 | 07 | 04 | 10 | 08 | 13 | 15 | 12 | 09 | 00 | 03 | 05 | 06 | 11 |

# DES: fonctionnement des S-Boxes

Exemple : Supposons que le texte à transformer soit 101100 à l'entrée de S1.

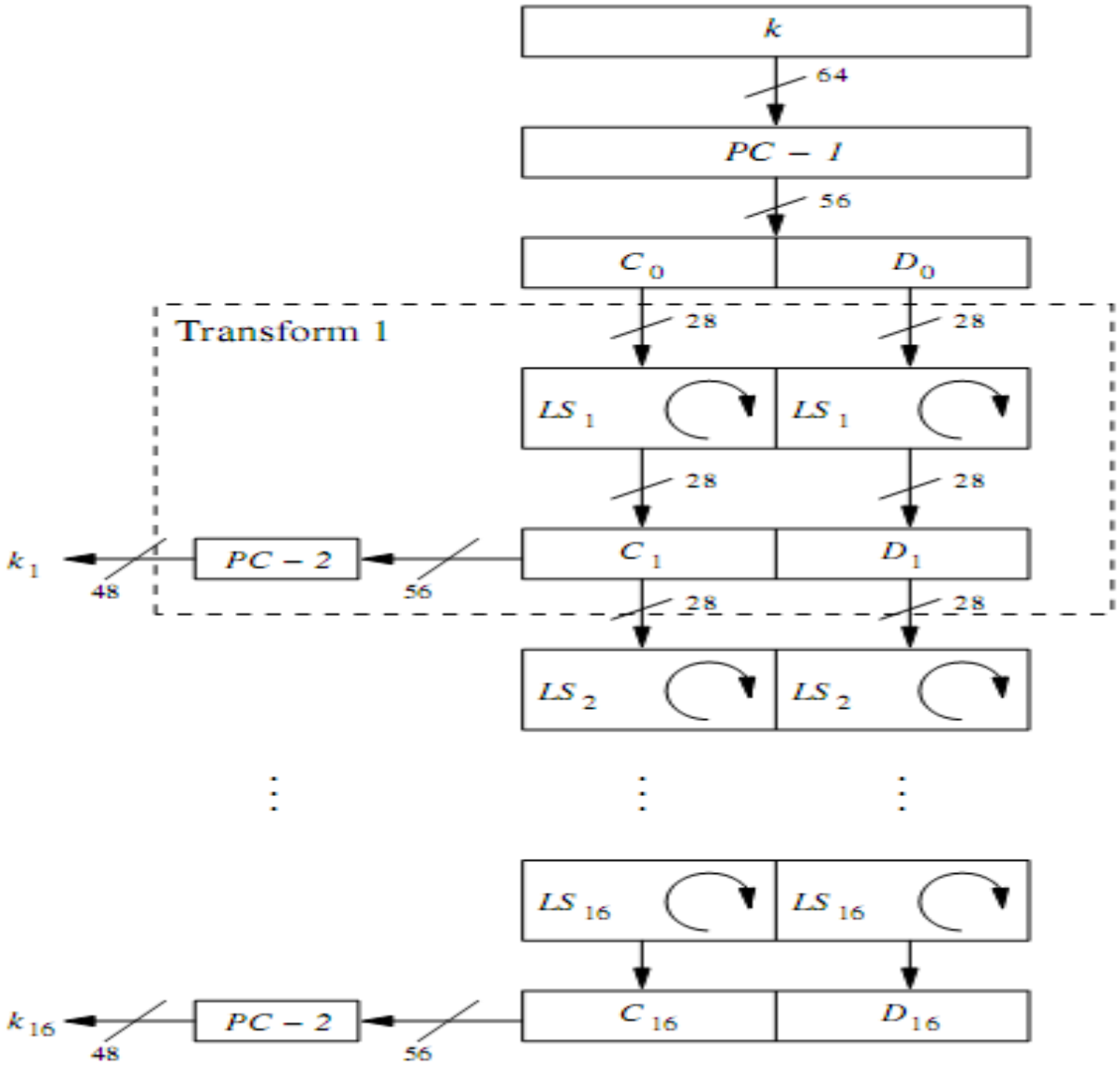
- On sépare le premier bit (1) et le dernier bit (0) que l'on concatène (10 soit 2 en décimal) ;
- Les quatres bits restant constituent le nombre 0110, soit 6 en décimal.
- A l'intersection de la ligne 2 et de la colonne 6 de la matrice S1, on obtient 2, soit sur 4 bits, 0010.
- Ainsi 101100 se transforme en 0010

# DES: procédé de diversification de clés

- Étant donné les 64 bits de K, on enlève les bits de parité et l'on ordonne les autres suivant une permutation PC-1.

1. On note $C_0D_0$ =PC-1(K) où $C_0$ est composée des 28 premiers bits de PC-1(K) et $D_0$ des 28 restants.
2. Pour i compris entre 1 et 16, on calcule
   - $C_i = LS_i(C_{i-1})$
   - $D_i = LS_i(D_{i-1})$ où $LS_i$ est une rotation circulaire.
   - $K_i = PC\text{-}2(C_iD_i)$.

# DES: procédé de diversification de clés



# DES: procédé de diversification de clés

- Les clés sont produites sur 48 bits, à partir de la clé de départ K, suivant un processus faisant intervenir les permutations PC-1 et PC-2 :

| $PC-1$ | | | | | | | |
|---|---|---|---|---|---|---|---|
| 57 | 49 | 41 | 33 | 25 | 17 | 9 | 1 |
| 58 | 50 | 42 | 34 | 26 | 18 | 10 | 2 |
| 59 | 51 | 43 | 35 | 27 | 19 | 11 | 3 |
| 60 | 52 | 44 | 36 | 63 | 55 | 47 | 39 |
| 31 | 23 | 15 | 7 | 62 | 54 | 46 | 38 |
| 30 | 22 | 14 | 6 | 61 | 53 | 45 | 37 |
| 29 | 21 | 13 | 5 | 28 | 20 | 12 | 4 |

| $PC-2$ | | | | | | | |
|---|---|---|---|---|---|---|---|
| 14 | 17 | 11 | 24 | 1 | 5 | 3 | 28 |
| 15 | 6 | 21 | 10 | 23 | 19 | 12 | 4 |
| 26 | 8 | 16 | 7 | 27 | 20 | 13 | 2 |
| 41 | 52 | 31 | 37 | 47 | 55 | 30 | 40 |
| 51 | 45 | 33 | 48 | 44 | 49 | 39 | 56 |
| 34 | 53 | 46 | 42 | 50 | 36 | 29 | 32 |

# DES: procédé de diversification de clés

- les décalages à gauche sont circulaires : le bit sortant à gauche est réintroduit à droite.

- Toutefois, le décalage est effectué une fois ou deux fois suivant les clés comme le montre le tableau ci-dessous :

| Numéro de clé | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Nombre de décalages | 1 | 1 | 2 | 2 | 2 | 2 | 2 | 2 | 1 | 2 | 2 | 2 | 2 | 2 | 2 | 1 |

# Critique de DES

- La critique du DES est de nos jours aisée car la clé de 64 (en fait 56 bits) est trop courte et on peut la deviner par essais successifs de combinaisons de 56 bits.

- Démonstration de John Gilmore (janvier 1999) : on peut trouver la clé DES avec une machine en 22h et 15 min.

- DES tend à être remplacé par d'autres systèmes comme AES(Advanced Encryption Standard).

# Double DES

## Double DES

Deux chiffrements successifs avec deux clefs différentes, i.e. :

$$c = \mathrm{DES}_{K_1}\left(\mathrm{DES}_{K_2}(m)\right).$$

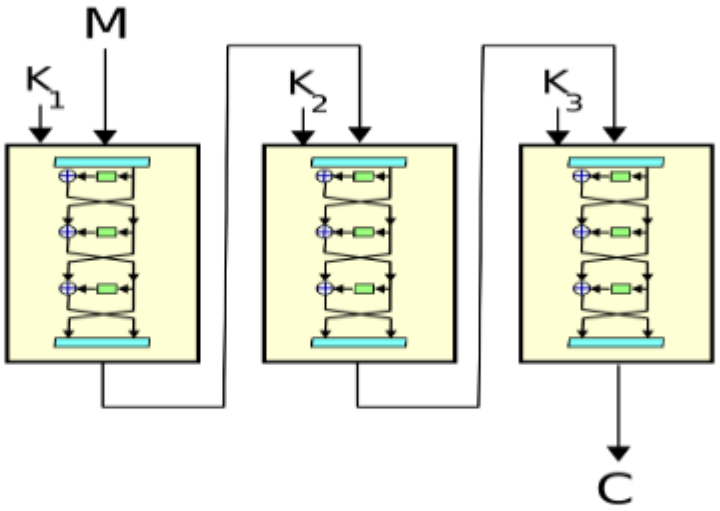
Pour le déchiffrement :

$$m = \mathrm{DES}^{-1}_{K_2}\left(\mathrm{DES}^{-1}_{K_1}(c)\right).$$

# Triple DES

On l'utilise avec 2 ou 3 clefs.

$$c = \mathrm{DES}_{K_1}\left(\mathrm{DES}^{-1}_{K_2}\left(\mathrm{DES}_{K_3}(m)\right)\right).$$




- EMV
  - VISA
  - MasterCard
  - American Express
  - J Smart - JCB