Module: Cryptographie

3ème année licence en Informatique

Par : Prof. Cherif Foudil

Chapitre 4

Partie 2: Cryptographie Moderne

1- Cryptographie symétrique

- Par bloc
- par flux

2- Cryptographie Asymétrique

L'arrivée de l'informatique

La machine Enigma

Créée et fabriquée par les militaires Allemands après la défaite de 1918,

Ils pensent qu'ils ont trouvé la machine idéale pour la cryptographie,

Le fonctionnement:

Le codage effectué par la machine **Enigma** est à la fois simple et astucieux. Chaque lettre est remplacée par une

autre, l'astuce est que la substitution change d'une lettre à l'autre.

Concrètement, le circuit électrique est constitué de plusieurs éléments en chaîne :

La machine d'ENIGMA

1-Le tableau de connexions : il permet d'échanger des paires de l'alphabet, deux à deux, au moyen de fiches. Il y a 6 fiches qui permettent donc d'échanger 12 lettres. Par exemple, dans le tableau suivant (avec simplement 6 lettres), on a échangé A et C, D et F, tandis que B et D restent invariants.

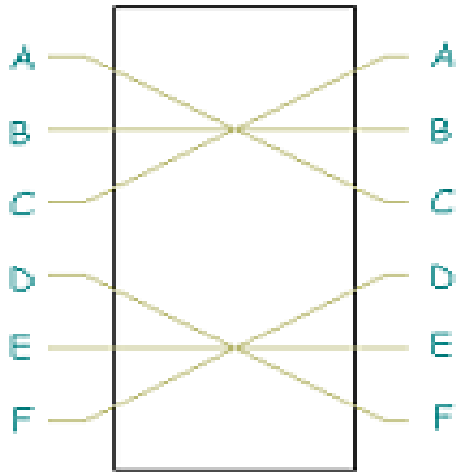
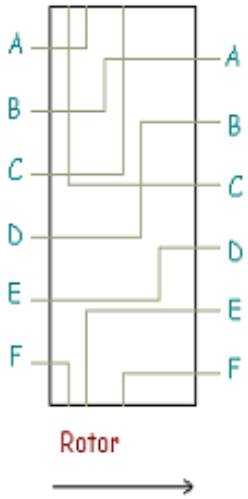


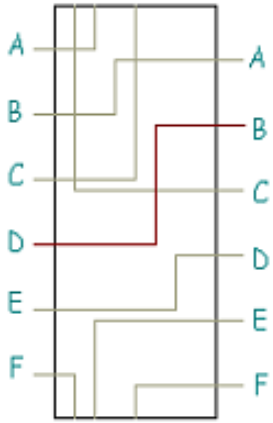
Tableau de connexions

La machine d'ENIGMA

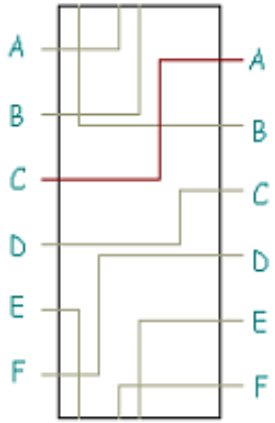
2-Les rotors : un rotor est un cylindre qui fait correspondre, a chaque lettre en entrée une autre lettre. Les rotors sont montés à la suite les uns des autres. La machine Enigma disposera, au gré de ses évolutions successives, de 3 à 6 rotors. On a le choix de les placer dans l'ordre que l'on souhaite (ce qui constituera une partie de la clé).



Entrée	Sortie
A	E
B	A
C	F
D	B
E	D
F	F

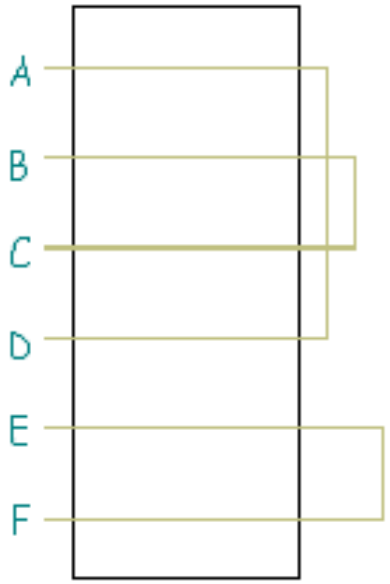


Le rotor tourne



La machine d'ENIGMA

3-Le réflecteur : Au bout des 3 rotors se situe une dernière permutation qui permet de revenir en arrière. On permute une dernière fois les lettres 2 par 2, et on les fait retraverser les rotors, et le tableau de connexion.



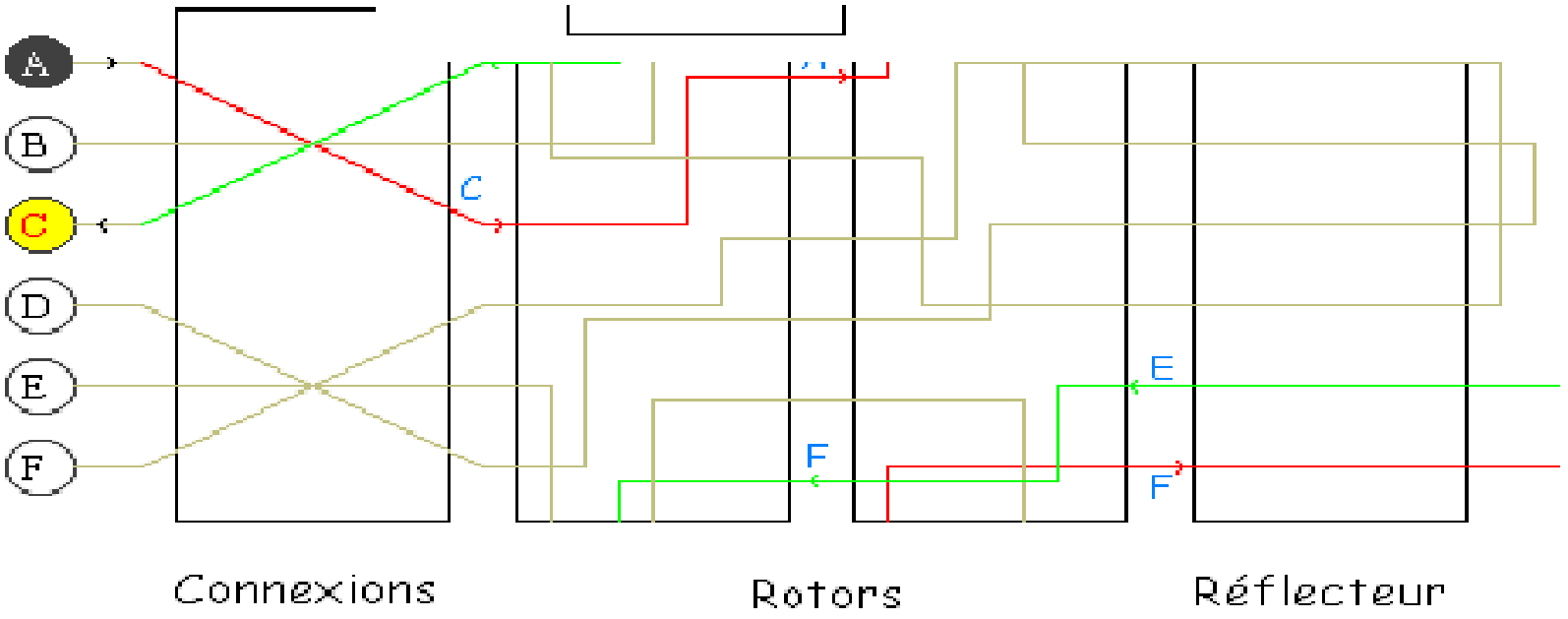
A est permuté avec D, B est permuté avec C, et E avec F.

Le réflecteur

La machine d'ENIGMA

Résumons sur la machine simplifiée suivante (6 lettres, 2 rotors) comment est codée la lettre A :

- On traverse le tableau de connexions : on obtient C.
- On traverse les 2 rotors : on obtient successivement A et F.
- On traverse le réflecteur où on obtient E, puis on renvoie dans les rotors pour obtenir F.



La machine d'ENIGMA

Nombre de clés possibles

Il y a trois éléments à connaitre pour pouvoir coder un message avec la machine Enigma.

1. la position des 6 fiches du tableau de connexion : (12 lettres parmi 26, 6 paires de lettres parmi 12) Soit 100.391.791.500 possibilités.
2. l'ordre des rotors : il y a autant d'ordre que de façons d'ordonner 3 éléments : 3!=6.
3. la position initiale des rotors : chaque rotor ayant 26 éléments, il y a 26 puis 3 =17.576 choix.

   On multiplie tout cela, et on obtient plus de 10 puis16 possibilités, ce qui est énorme pour l'époque!

La machine d’ENIGMA

Les allemands ont une confiance totale en la machine Enigma, dont ils ont fabriqué 100.000 exemplaires.
Ils s'échangeront des communications radios cryptées, persuadés que jamais les Alliés ne les comprendront.

La cryptanalyse de la machine Enigma

Point forts et faiblesses

- L'une des failles de la machine Enigma est que jamais la lettre A ne sera codée par un A. Cela élimine un certain nombre de cas à inspecter.
- Une des autres faiblesse dépend plutôt du protocole utilisé par les allemands : certains opérateurs (par exemple, ceux qui informaient de la météo) prenaient peu de précautions et commençaient toujours leurs messages par les mêmes mots (typiquement "Mon général...").

La cryptanalyse de la machine Enigma

Travail des Anglais

- Les anglais connaissaient pour une partie du message à la fois le texte clair et le texte codé, ce qui aide à retrouver la clé.
- Et comme c'est la même clé qui sert pour toutes les machines Enigma de l'armée allemande pour un jour donné, une erreur de protocole dans un message peut compromettre la sécurité de tous les autres !

La cryptanalyse de la machine Enigma

Travail des Polonais

- Dès 1933 et jusqu'au début de la guerre, grâce au travail de trois mathématiciens polonais (Marian Rejewski, Jerzy Rózicki et Henryk Zygalski), le "Polski Biuro Szyfrów" sait décrypter les messages allemands, chiffrés avec la machine Enigma, exploitant une faille dans la procédure de début de transmission (Les opérateurs allemand saisissaient deux fois les trois premières lettres du message). Même si ces trois lettres sont inconnues, le nombre de câblages qui peuvent transformer ces trois lettres en une séquence particulière sont limités. Rejewski les appelle des « chaînes ». Ils ont travaillé beaucoup sur les chaines


Marian Rejewski


Jerzy Rózicki


Henryk Zygalski

La cryptanalyse de la machine Enigma

Travail de Allan Turring

- Les allemands ont résolu les failles et ont utilisé plus de rotors,

- La cryptanalyse d'Enigma était devenue entre temps une affaire britannique et américaine. C'est Alan Turing qui va s'occuper de l'analyse de l'Enigma.
- Turing est le chef du groupe à Bletchley Park, proche de Londres où se sont retrouvé tous les cryptologues et mathématiciens.

Le travail d'Alan Turing pour déchiffrer les messages allemands a profondément changé le cours de la seconde guerre mondiale.

« Parmi les nombreuses hypothèses circulant sur l'origine du logo d'Apple, l'une d'elle est que la pomme serait celle mordue par Turing », Puisque il meurt empoisonné en mangeant une pomme contenant du cyanure

La cryptographie moderne

- Les algorithmes de chiffrement classiques sont peu sûrs en général.
- Le chiffrement moderne utilise la puissance des ordinateurs modernes.
- Dans la cryptographie moderne, **les textes sont remplacés par des chiffres**. Via l'utilisation de la table ASCII,
- Les procédés de substitutions et de transpositions sont toujours utilisés, mais maintenant seulement sur des bits (0 et 1).
- On distingue deux types d'algorithmes à clés :

1- les systèmes de chiffrement symétriques

2- les systèmes asymétriques

La cryptographie Symétrique

En pratique la clef utilisée pour le déchiffrement est **identique** à celle utilisée pour le chiffrement.

⇒ L'avantage est que le chiffrement est très rapide.

⇒ Le défaut pratique l'émetteur et le récepteur doivent avoir la même clef pour communiquer, ce qui implique une transmission de clef et donc l'existence d'un canal sure.

D'autres problèmes:

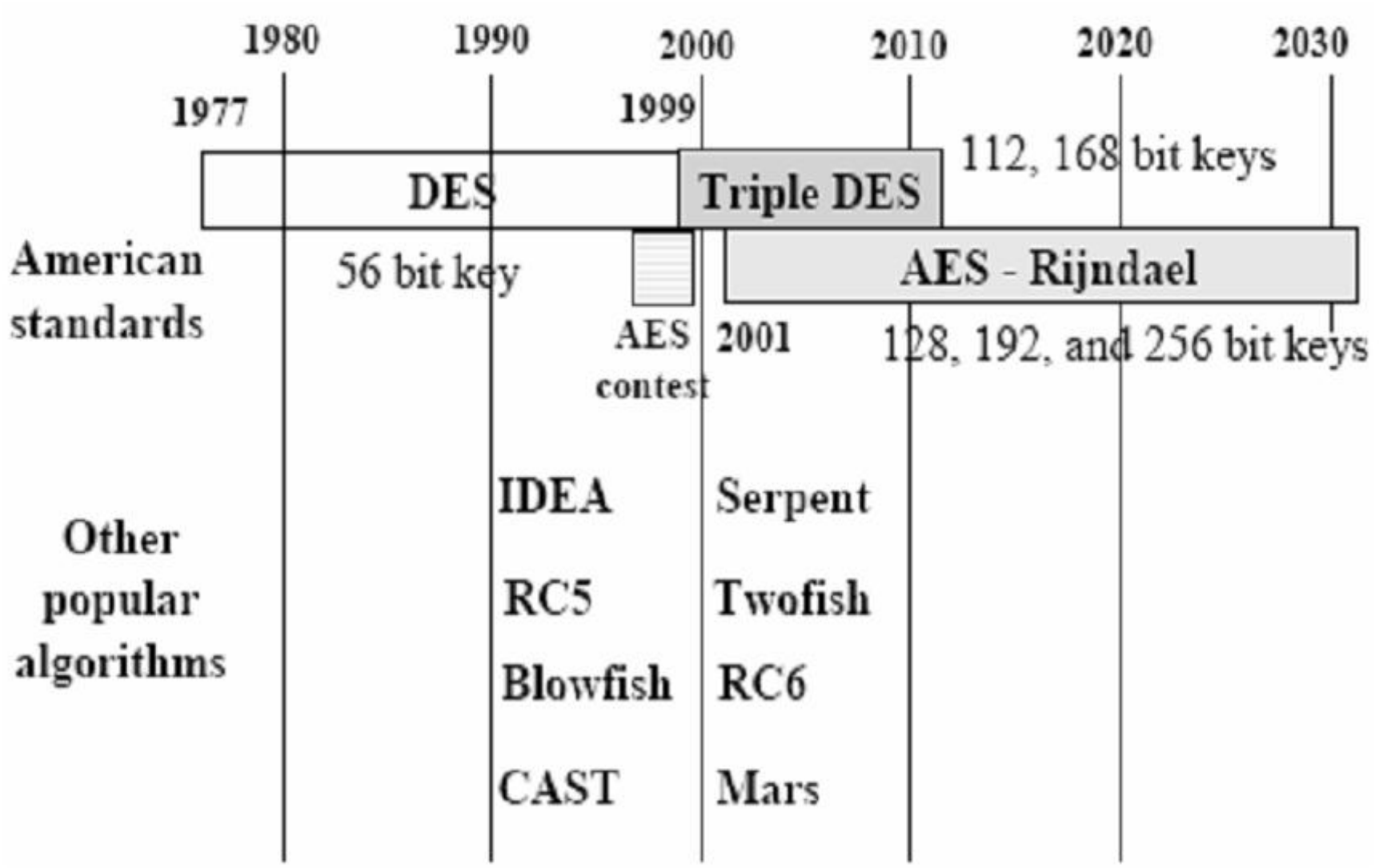
- Si la clé secrète est compromise (volée, piratée, ...) par un opposant, alors ce dernier pourra déchiffrer tous les messages encodés.

- Les clés doivent être distribuées secrètement : c'est très difficile à l'échelle planétaire (se rencontrer, utiliser un messager sûr, etc...).

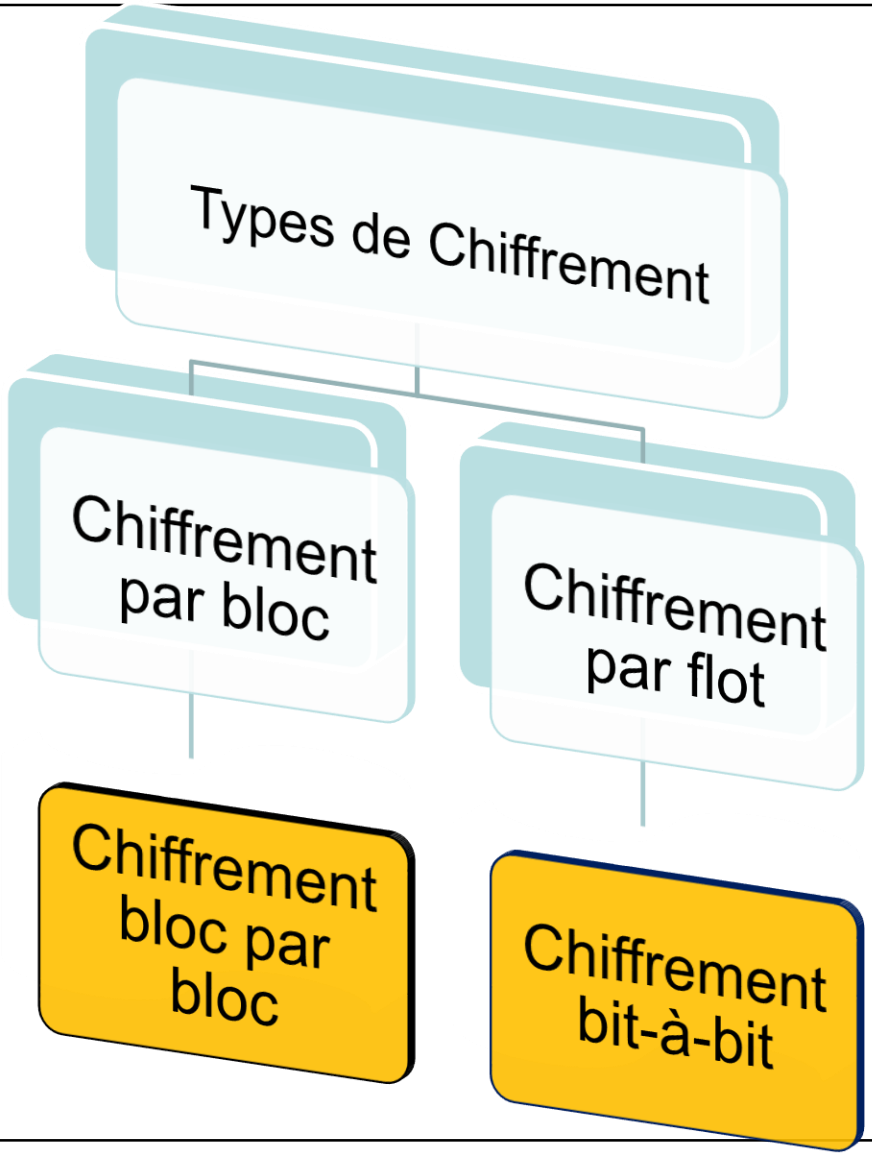
- Si une clé différente est utilisée pour chaque paire différentes d'utilisateurs du réseau, le nombre total des clés augmente très rapidement en fonction du nombre total d'utilisateurs. (problème de distribution des clés)

Exemples les plus connus : DES, triple DES, AES, RC4, masque jetable.

Historique de chiffrements symétriques



Deux catégories de chiffrement symétrique



Deux catégories de chiffrement symétrique

- **Chiffrements par blocs** [block ciphers] : ce sont des systèmes de chiffrement qui opèrent sur le message clair par grand groupes de bits (e.g., 64 bits).
- **Chiffrements par flots** [stream ciphers] : ce sont des systèmes de chiffrement qui opèrent sur le message clair par bit (ou quelque fois par petit groupement de bits).

Pratiquement les systèmes par flots opèrent sur les caractères, alors que ceux par blocs opèrent sur les mots.

Chiffrement par Blocs

Principe:

1. Le message est découpé en blocs (de 1,8,32 ou 64 bits),
2. Chaque bloc est chiffré indépendamment de la valeur des autres blocs

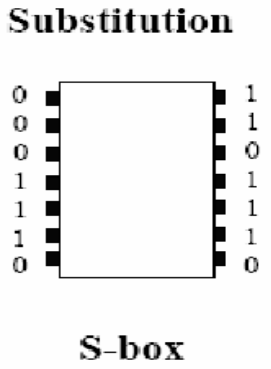
Le principe de Chiffrement par Blocs

L'idée générale du chiffrement par blocs est la suivante:

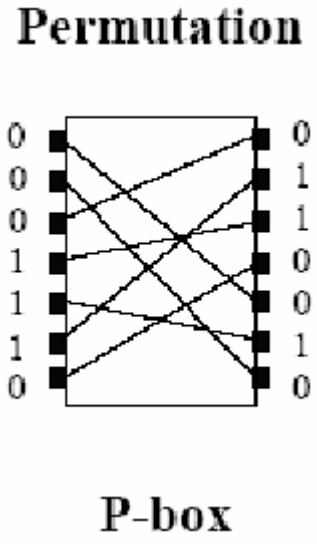
1) Remplacer les caractères par un code binaire
2) Découper cette chaîne en blocs de longueur donnée
3) Chiffrer un bloc en l'additionnant bit par bit à une clef.
4) Déplacer certains bits du bloc.
5) Recommencer éventuellement un certain nombre de fois l'opération 3.
6) Passer au bloc suivant et retourner au point 3 jusqu'à ce que tout le message soit chiffré.

Les catégories du chiffrement par Blocs

1- Chiffrement par substitution: Les substitutions consistent à remplacer des symboles ou des groupes de symboles par d'autres symboles ou groupes de symboles dans le but de créer de la confusion.



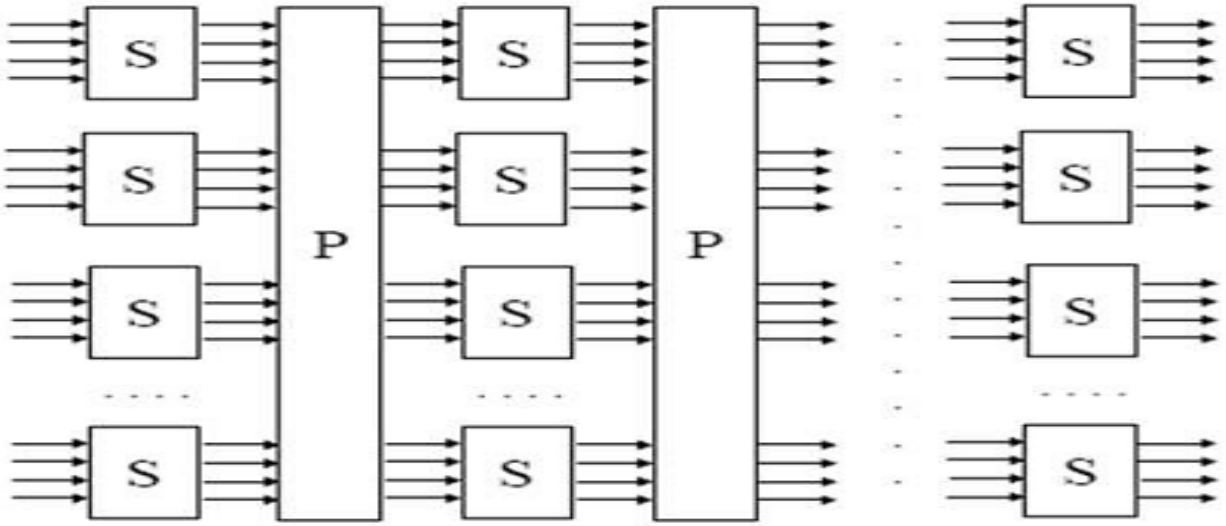
2- Chiffrement par transposition: Les transpositions consistent à mélanger les symboles ou les groupes de symboles d'un message clair suivant des règles prédéfinies pour créer de la diffusion. Ces Règles sont déterminées par la clé de chiffrement. Une suite de transpositions forme une permutation.



Les catégories du chiffrement par Blocs

3- Chiffrement par produit : C'est la combinaison des deux. Le chiffrement par substitution ou par transposition ne fournit pas un haut niveau de sécurité, mais en combinant ces deux transformations, on peut obtenir un chiffrement plus robuste.

On dit qu'un «round» est complété lors que les deux transformations ont été faites une fois (substitution et transposition).



1-Les chiffrements par blocs (Horst Feistel)

Inventé par **Horst Feistel** (1915 – 1990) et son chiffrement Lucifer (mots tronqués).

C'est un chiffre à **clé privée symétrique**.

C'est à dire que non seulement on utilise la même clé pour chiffrer et déchiffrer (Clé privée), mais on utilise le même algorithme pour chiffrer et déchiffrer (Comme le ROT13)

1-Les chiffrements par blocs

Inventé par Horst Feistel en 1973 (IBM).

Fonctionnement:

1. Dans une construction de Feistel, le bloc d'entrée d'un round est séparé en deux parties.
2. La fonction de chiffrement est appliquée sur la première partie du bloc et l'opération binaire OU-Exclusif est appliquée sur la partie sortante de la fonction de la deuxième partie. Ensuite les deux parties sont permutées et le prochain round commence.

1-Les chiffrements par blocs

L'algorithme contient n rondes.

Chaque ronde a la structure suivante pour le chiffrement et le déchiffrement:

La longueur de l'entrée est 2w (bits), celle de la clef est K

Diviser l'entrée en 2 moitiés L_0 et R_0

$L_1 = R_0$,

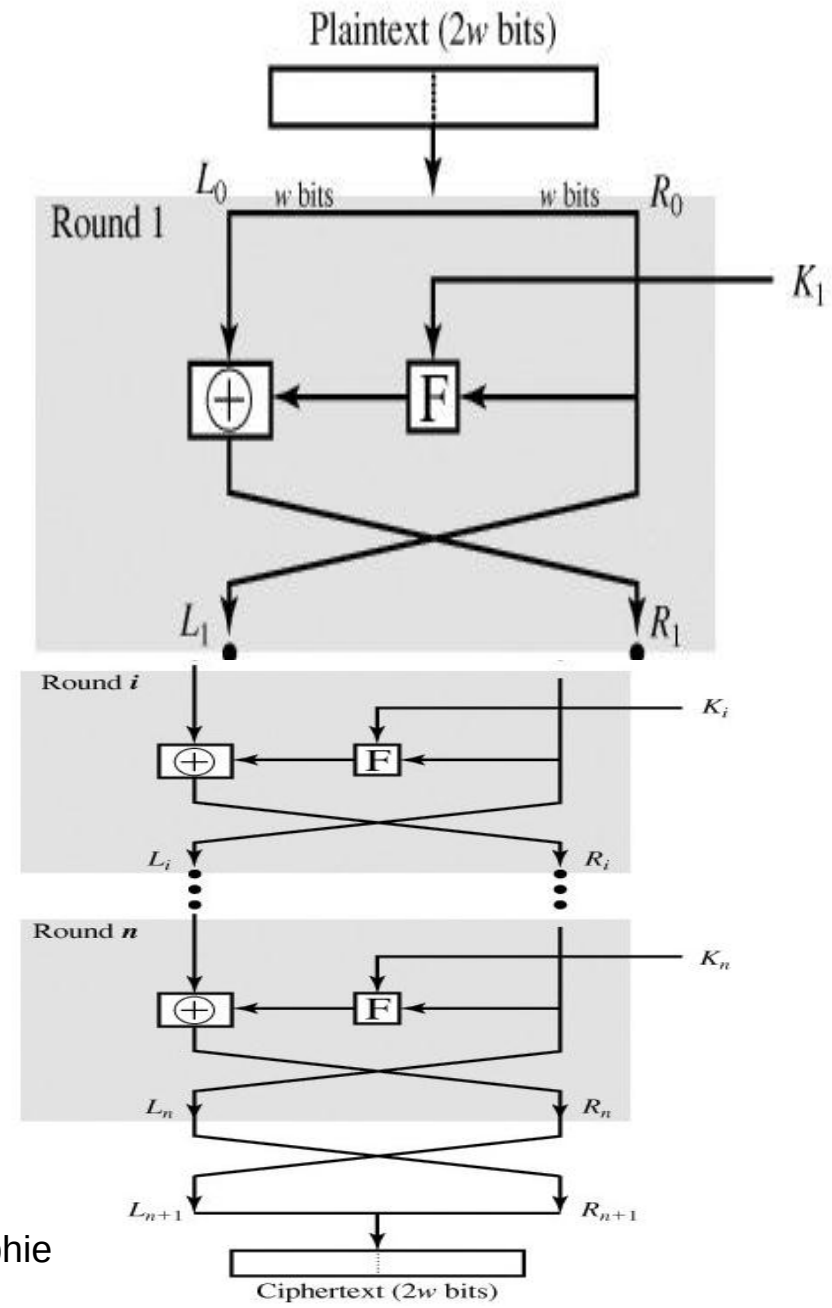
$R_1 = L_0 \oplus f(R_0, K)$

Dans la ronde suivante, on utilise (L_1, R_1) au lieu de (L_0, R_0), etc…

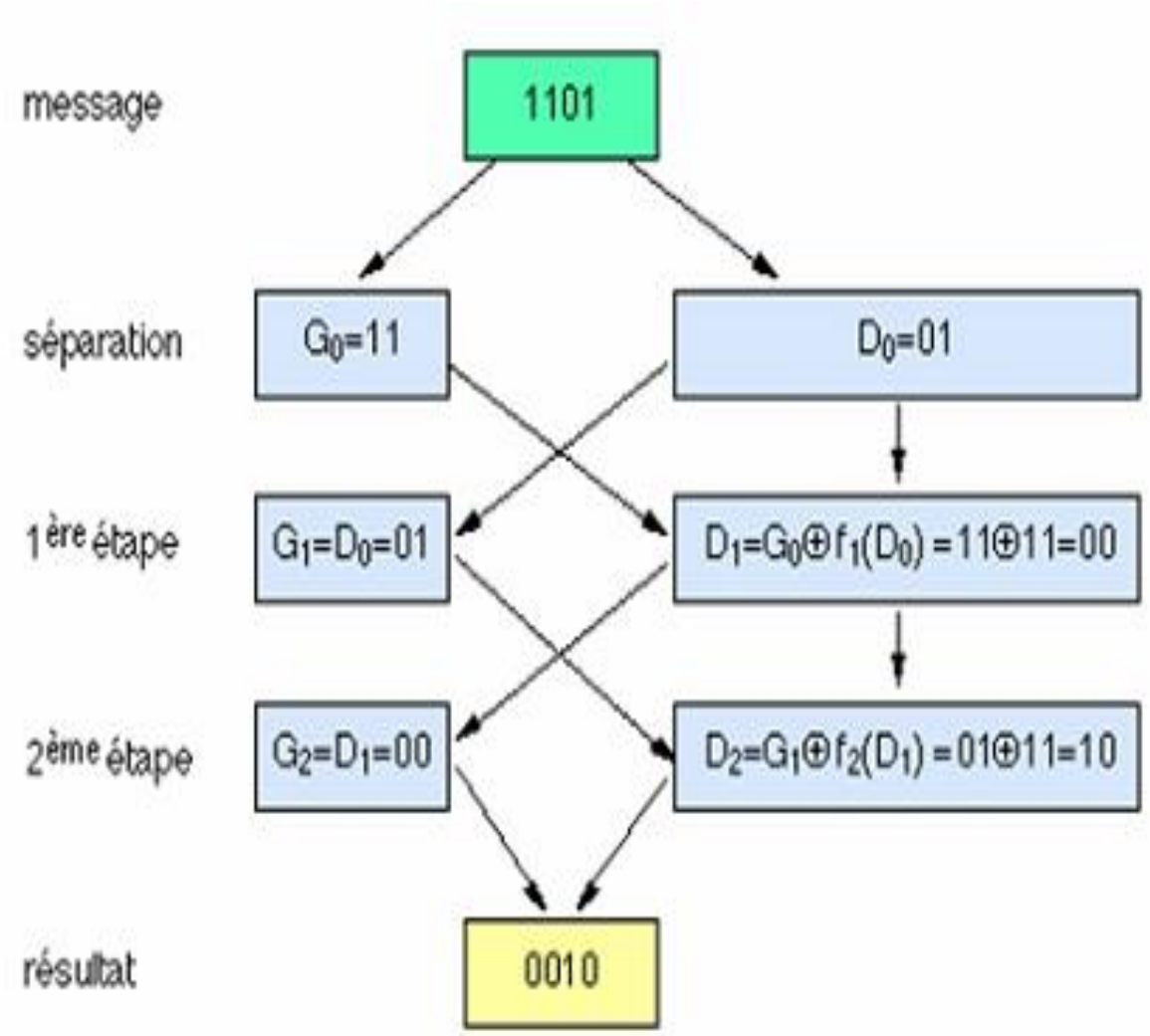
La fonction f est la même pour toutes les rondes mais une clef différente est utilisée à chaque ronde.

Structure de chiffrement de Feistel

- Taille d'un bloc: généralement 64 bits,
- Taille de la clé: 128 bits est réputée suffisante
- Nombre de rondes: typiquement 16
- Algorithme de génération des sous clés:
  une grande complexité renforce la sécurité
- Fonction de la ronde:
  Une fonction complexe est dure à analyser, mais, rend le chiffrement lent.



Exécution d'un schéma de Feistel



message	résultat
0000	0100
0001	1100
0010	1010
0011	0111
0100	0011
0101	1001
0110	1111
0111	0000
1000	1101
1001	0101
1010	0001
1011	1110
1100	1000
1101	0010
1110	0110
1111	1011

Exemple de chiffrement de Feistel

Principe de fonctionnement du schéma de Feistel avec un texte de 8 bits, une clé de 4 bits et 4 tours ou rondes.

Soit le « texte en clair » 0100 1001

Et la clé : 1010

F(D,K) = D + K

Exemple1 de chiffrement de Feistel

Ronde N° 1

Étape 1 : On découpe le bloc à chiffrer en deux parties.

G_0 et D_0 (pour Gauche, ronde N°0 et Droite N°0)

G_0 : **0100** D_0 : **1001**

Étape 2 : On calcul Z_0 un ou exclusif entre la clé et D_0 :

1001
1010

0011

Étape 3 : On calcul D_1 un ou exclusif entre Z_0 et G_0 : **0111**

Étape 4 : G_1 vaut D_0 : **1001**

Et voila, la 1ere ronde est finie.

Exemple de chiffrement de Feistel

Ronde N° 2

On recommence les mêmes manipulations,

On obtient Z_1 : **1101**
G_2 : **0111**
D_2 : **0100**

Ronde N° 3

Idem,

On obtient Z_2 : **1110**
G_3 : **0100**
D_3 : **1001**

Ronde N° 4 :

attention, la dernière ronde utilise un schéma différent :

Étape 1 : On calcul Z_4 un ou exclusif entre la clé et D_3 (ça , ca na change pas) : **0011**

Étape 2 : On calcul G_4 un ou exclusif entre Z_4 et G_3 : **0111**

Étape 3 : D_4 vaut D_3 : **1001**

Et voila. On à le cryptogramme : **0111 1001**

Exemple de déchiffrement de Feistel

Exercice à faire: Déchiffrez le cryptogramme suivant :
Sur le principe du schéma de Feistel avec un texte de 8 bits, une clé de 4 bits et 4 tours ou rondes.
Soit le « Cryptogramme » 0111 1001
Et la clé : 1010

Choix des paramètres

La réalisation d'un tel réseau dépend des choix effectués pour les paramètres suivants :

– Taille du bloc : si elle augmente, la sécurité augmente également

– Taille de clé : si elle augmente, la sécurité aussi

– Nombre de cycle : plus il y en a, plus la sécurité est renforcée

– Algorithme de génération des sous-clés : plus il est complexe, plus la compréhension est rendue difficile.

L'algorithme de DES
(Data Encryption Standard)

2-DES (Data Encryption Standard)

L'algorithme DES adapté comme standard en 1976.

DES a été l'algorithme officiel de l'administration américaine jusqu'en 1999.

L'algorithme DES transforme un bloc de 64 bits en un autre bloc de 64 bits.

Il manipule des clés individuelles de 56 bits, représentées par 64 bits. (8 bits pour la parité)

Le DES est un chiffre de Feistel légèrement modifié avec l'alphabet {0,1} et la longueur des blocs de 64 bits.

2-DES (Particularités)

Avantages de DES: algorithme de chiffrement symétrique standard pendant longtemps,

– il possède un haut niveau de sécurité,

– il est complètement spécifié et facile à comprendre,

– la sécurité est indépendante de l'algorithme lui-même,

– il est rendu disponible à tous, par le fait qu'il est public,

– il est adaptable à diverses applications (logicielles et matérielles),

– il est rapide et exportable,

– il repose sur une clé relativement petite, qui sert à la fois au chiffrement et au déchiffrement,

– il est facile à implémenter.

2-DES (Particularités)

C’est un algorithme de chiffrement à clef secrète. La clef sert donc à la fois à chiffrer et à déchiffrer le message. Cette clef a ici une longueur de 64 bits, c’est-à-dire 8 caractères, mais dont seulement 56 bits sont utilisés.

L’entière sécurité de l’algorithme repose sur les clefs puisque l’algorithme est parfaitement connu de tous. La clef de 64 bits est utilisée pour générer **16 autres clefs de 48 bits** chacune qu’on utilisera lors de chacune des 16 itérations du D.E.S. Ces clefs sont les mêmes quel que soit le bloc qu’on code dans un message

2-DES (Particularités)

Cet algorithme est relativement facile à réaliser matériellement et certaines puces chiffrent jusqu'à

1 Go de données par seconde.

Pour les industriels, c'est un point important notamment face à des algorithmes asymétriques, plus lents, tels que l'algorithme R.S.A.

2-DES (Algorithme principal)

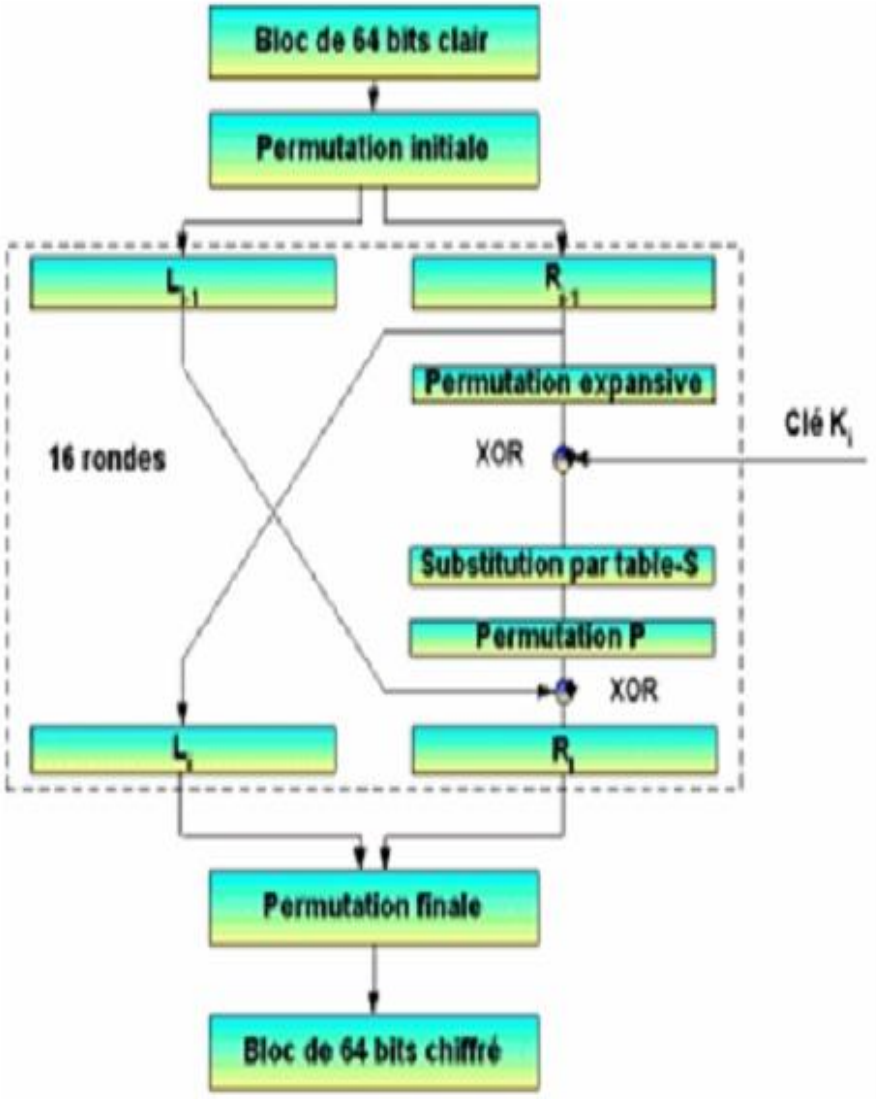
04 étapes:

1-Calcul de la clé: fabrication de 16 sous-clefs Ki

2-Permutation initiale

3-Calcul médian (16 fois): application d'un algorithme complexe appliqué en fonction de la clef.

4-Permutation finale



Etape 1: calcul de la clef

- La clef a une longueur de **64** bits, c'est-à-dire **8** caractères, mais dont seulement **56** bits sont utilisés (dans l'algorithme).
- Le nombre de clefs du DES est $2^{56} \approx 7.2*10^{16}$
- Exemple: (en Hex)

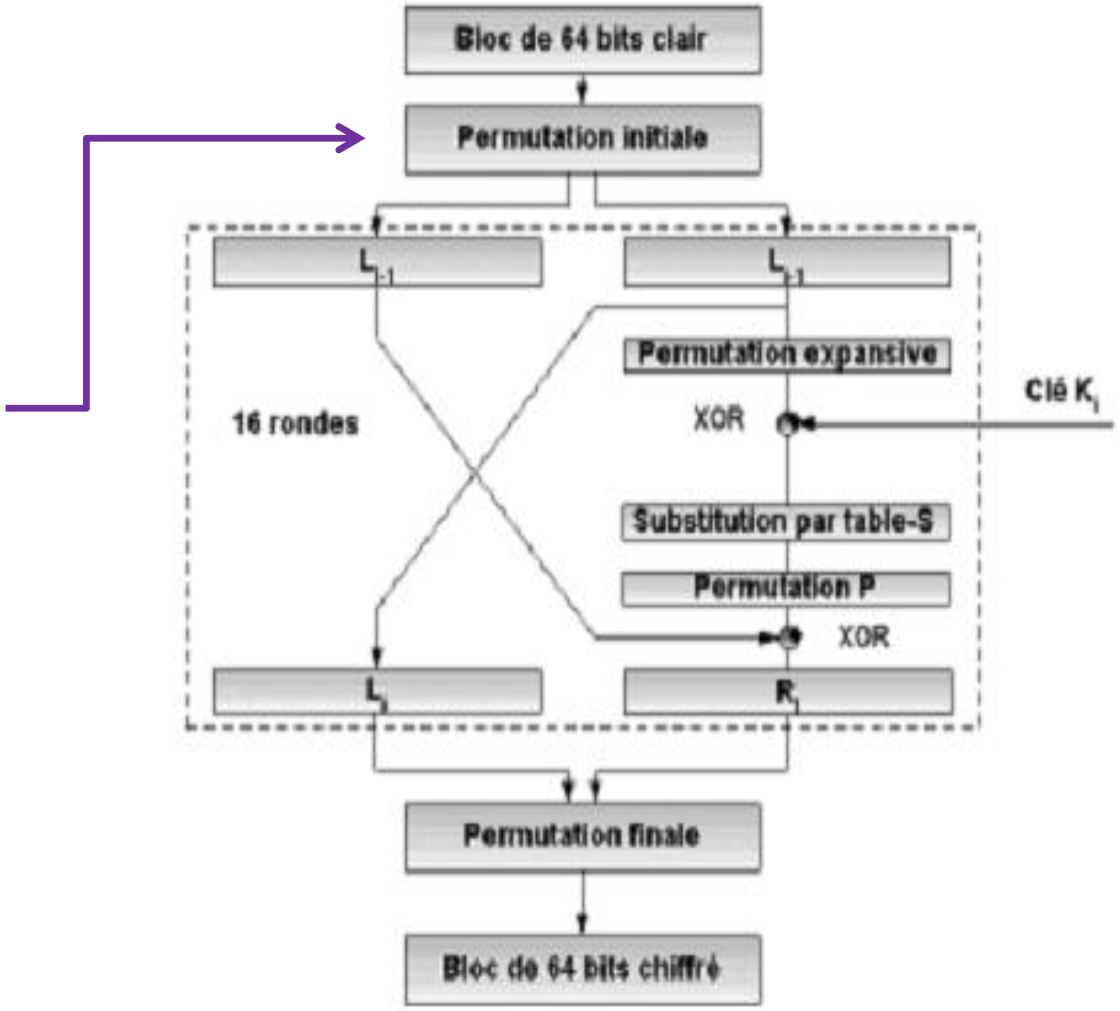
13 34 57 79 9B BC DF F1

Une clef valable pour le DES

0	0	0	1	0	0	1	1
0	0	1	1	0	1	0	0
0	1	0	1	0	1	1	1
0	1	1	1	1	0	0	1
1	0	0	1	1	0	1	1
1	0	1	1	1	1	0	0
1	1	0	1	1	1	1	1
1	1	1	1	0	0	0	1

Etape 2: Permutation initiale

Permutation initiale



Matrice de permutation initiale

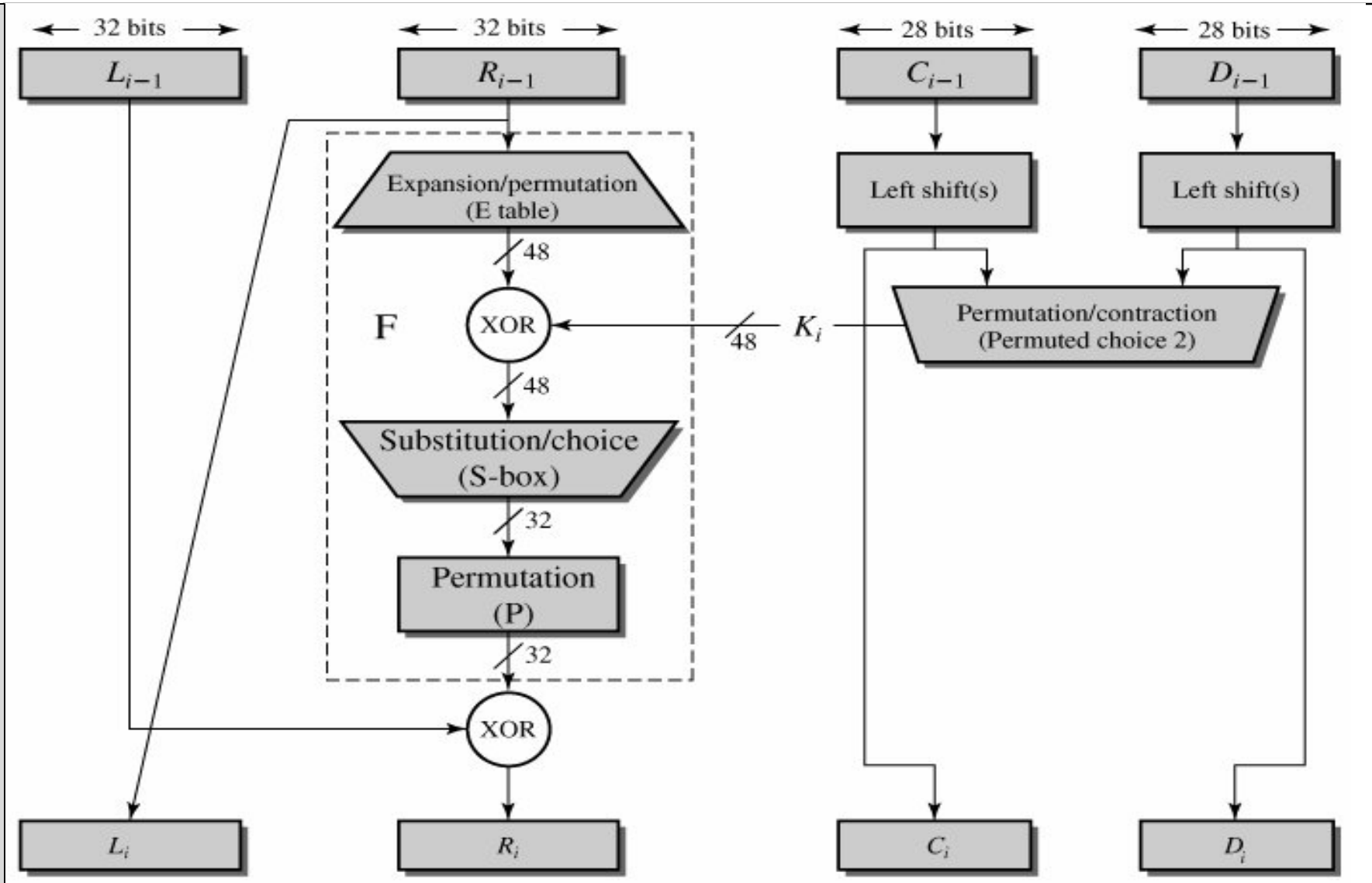
Les 64 bits du texte clair sont soumis à la permutation initiale (PI ou IP) pour produire le texte brouillé selon le tableau suivant: Le premier bit sera le bit 58, le second le bit 50, etc.

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

Etape 3:Calcul médian

- Les 64 bits initiaux de données sont divisés en 2 blocs (L et R).
- Itérations:
  - $Ln = R_{n-1}$
  - $R_n = L_{n-1} \oplus F(R_{n-1}, K_n)$
  - $K_n = G(K,n)$
- Avec
  - $L_n = t_1 \ldots t_{32}$
  - $R_n = t_{33} \ldots t_{64}$

Calcul médian



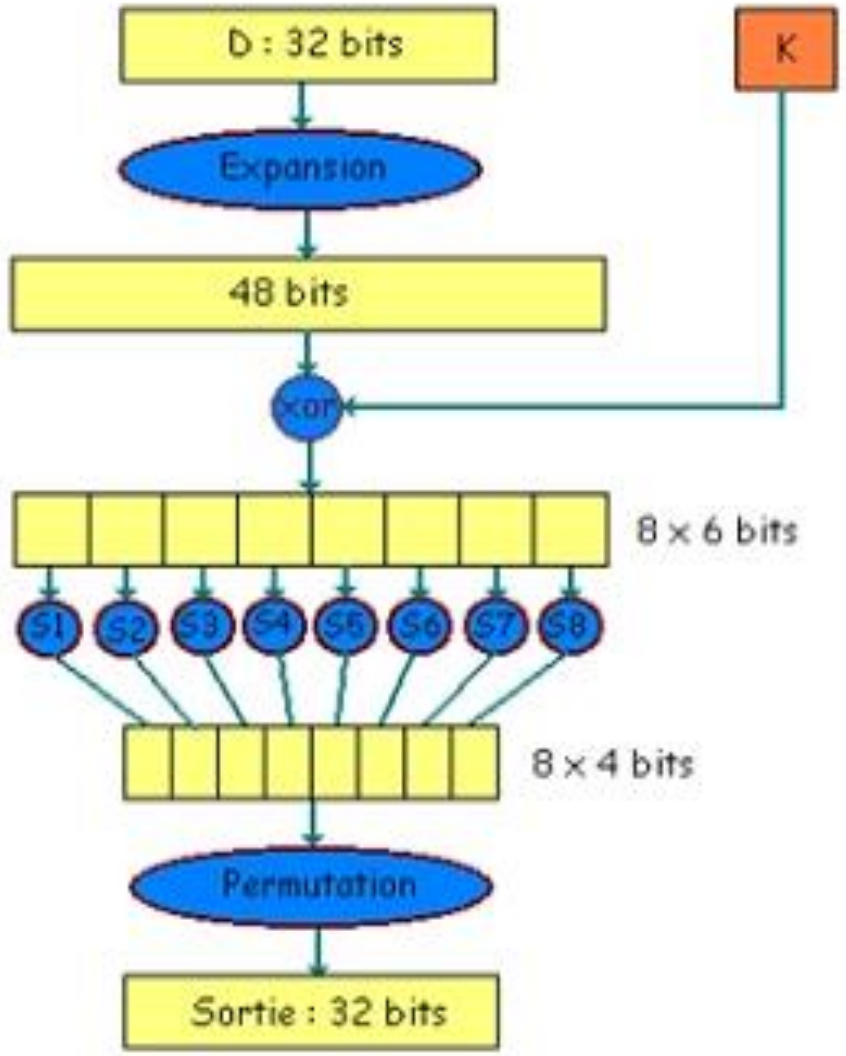
Calcul médian

Le calcul médian s'effectue en 16 itérations. On traite 2 blocs simultanément :

un bloc de 32 bits (données) et

un bloc de 48 bits (clés).

Le résultat forme un bloc de 32 bits.



Matrice d'extension

Expansion : Les 32 bits sont étendus à 48 bits grâce à une table d'expansion (également appelée matrice d'extension).

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

Calcul médian

Addition de la sous-clé : Le résultat de l'expansion est additionné (par une opération $\oplus$) à la sous-clé K_n correspondant à l'itération selon la formule :

$$E(R_{i-1}) \oplus K_i = B_1 B_2 \dots B_8$$

Les $B_1, B_2, ..., B_8$ sont des blocs de 6 bits :

$$B_j = b_1 b_2 b_3 b_4 b_5 b_6.$$

Transformations par S-Boxes : Chaque bloc B_j constitue ensuite l'entrée de l'opération de substitution réalisée sur base des S-Box.

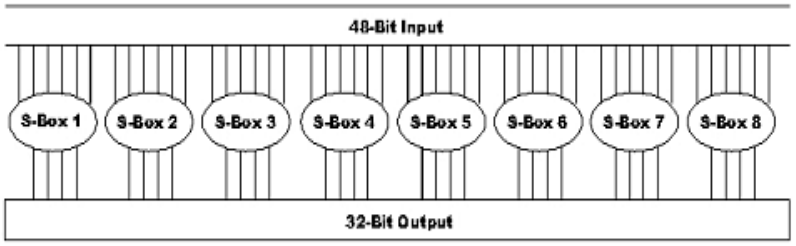


FIG. 5.14 – Transformations S-Box

Calcul médian

L'opération de substitution consiste pour chaque S-box à calculer :

- $b_1\ b_6$ = n° de ligne
- $b_2\ b_3\ b_4\ b_5$ = n° de colonne

N° de colonne

	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	14	4	13	1	2	15	11	8	3	10	6	12	5	9	0	7
1	0	15	7	4	14	2	13	1	10	6	12	11	9	5	3	8
2	4	1	14	8	13	6	2	11	15	12	9	7	3	10	5	0
3	15	12	8	2	4	9	1	7	5	11	3	14	10	0	6	13

N° de ligne

FIG. 5.15 – S-Box particulière

Calcul médian

Row	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	14	4	13	1	2	15	11	8	3	10	6	12	5	9	0	7
1	0	15	7	4	14	2	13	1	10	6	12	11	9	5	3	8
2	4	1	14	8	13	6	2	11	15	12	9	7	3	10	5	0
3	15	12	8	2	4	9	1	7	5	11	3	14	10	0	6	13
0	15	1	2	14	6	11	3	4	9	7	2	13	2	0	5	10
1	3	13	4	7	15	2	8	14	12	0	1	10	6	9	11	5
2	0	14	7	11	10	4	13	1	5	8	12	6	9	3	2	15
3	13	8	10	1	3	15	4	2	11	6	7	12	0	5	14	9
0	10	0	9	14	6	3	15	5	1	13	12	7	11	4	2	8
1	13	7	0	9	3	4	6	10	2	8	5	14	12	11	15	1
2	13	6	4	9	8	15	3	0	11	1	2	12	5	10	14	7
3	1	10	13	0	6	9	8	7	4	15	14	3	11	5	2	12
0	7	13	14	3	0	6	9	10	1	2	8	5	11	12	4	15
1	13	8	11	5	6	15	0	3	4	7	2	12	1	10	14	9
2	10	6	9	0	12	11	7	13	15	1	3	14	5	2	8	4
3	3	15	0	6	10	1	13	8	9	4	5	11	12	7	2	14
0	2	12	4	1	7	10	11	6	8	5	3	15	13	0	14	9
1	14	11	2	12	4	7	13	1	5	0	15	10	3	9	8	6
2	4	2	1	11	10	13	7	8	15	9	12	5	6	3	0	14
3	11	8	12	7	1	14	2	13	6	15	0	9	10	4	5	3
0	12	1	10	15	9	2	6	8	0	13	3	4	14	7	5	11
1	10	15	4	2	7	12	9	5	6	1	13	14	0	11	3	8
2	9	14	15	5	2	8	12	3	7	0	4	10	1	13	1	6
3	4	3	2	12	9	5	15	10	11	14	1	7	6	0	8	13
0	4	11	2	14	15	0	8	13	3	12	9	7	5	10	6	1
1	13	0	11	7	4	9	1	10	14	3	5	12	2	15	8	6
2	1	4	11	13	12	3	7	14	10	15	6	8	0	5	9	2
3	6	11	13	8	1	4	10	7	9	5	0	15	14	2	3	12
0	13	2	8	4	6	15	11	1	10	9	3	14	5	0	122	7
1	1	15	13	8	10	3	7	4	12	5	6	11	0	14	9	2
2	7	11	4	1	9	12	14	2	0	6	10	13	15	3	5	8
3	2	1	14	7	4	10	8	13	15	12	9	0	3	5	6	11

FIG. 5.16 – Les 8 S-Box du DES

Calcul médian

Transformations par P-Box (permutation du calcul médian) : L'opération de permutation est réalisée sur le résultat de la substitution des S-box et est basée sur la table de la figure 5.17.

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

FIG. 5.17 – Matrice de permutation du calcul médian

Etape 4: Permutation finale

Une fois le calcul médian terminé, on pratique la permutation inverse de la permutation initiale. Attention toutefois : il s'agit de l'inverse de la permutation initiale, en d'autres termes, cette table permet de retrouver la position de départ. Ce n'est pas l'inverse de la "matrice" de départ !

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

FIG. 5.19 – Permutation finale

2-DES (Data Encryption Standard)

Algorithme du calcul de la clé G(K, n)

La clé initiale est de **64** bits. Le calcul a lieu en **4** étapes:

❶ **Réduction à 56 bits:** les bits de parité sont enlevés.
On utilise la fonction PC1:

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

63

Algorithme du calcul de la clé G(K, n)

2. **Division en sous-clés de 28 bits:** le résultat de l'étape précédente (56 bits) est scindé en deux sous-clés de 28 bits.
3. **Rotation de la clé:** à chaque itération, chaque sous-clé de 28 bits subit une rotation d'1 ou 2 bits vers la gauche selon la table suivant:

Round number	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
Bits rotated	1	1	2	2	2	2	2	2	1	2	2	2	2	2	2	1

65

2-DES (Data Encryption Standard)

Algorithme du calcul de la clé G(K, n)

❹ **Réduction:** après concaténation des deux sous-clés précédentes, la clé résultante (56bits) est réduite à une sous-clé de 48 bits sur base de fonction PC2:

Le résultat de cette réduction est la sous-clé K_n additionnée avec $E(R_{n-1})$.

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

67

Questions ?

2-DES (Déchiffrement)

DES: Déchiffrement

- Il suffit d'appliquer le même algorithme mais inversé en tenant bien compte du fait que chaque itération du déchiffrement traite les mêmes paires de blocs utilisés dans le chiffrement.
  - $R_{n-1} = L_n$
  - $L_{n-1} = R_n \oplus F(R_n, K_n)$

69

2-DES (Cryptanalyse)

Cryptanalyse du DES

- Recherche exhaustive (2^{55})
- Cryptanalyse différentielle ($1991, 2^{47}$)
- Cryptanalyse linéaire ($1994, 2^{43}$)

73

2-DES (Cryptanalyse)

Cryptanalyse du DES

- Recherche exhaustive (Force brute)
  - Chiffrer un texte connu jusqu'a retrouver le chiffrement
  - Permet de connaitre la clef

Type d'attaquant	Budget	Outil	Clé de 40 bits	Clé de 56 bits
Simple hacker	Négligeable	Soft	1 semaine	Impossible
	300 €	Circuit prédiffusé	5 heures	38 ans
PME	7500 €	Circuit prédiffusé	*12 minutes*	18 mois
Grande entreprise	225 k€	Circuit prédiffusé	*24 secondes*	19 jours
	225 k€	ASIC	*0.18 seconde*	3 heures
Multinationale	7,5 M€	ASIC	*5 msec.*	6 minutes
Etat	225 M€	ASIC	0.2 msec.	12 secondes

Coût / performance d'une recherche exhaustive (1996)

75

2-DES (Cryptanalyse)

Cryptanalyse du DES: Recherche exhaustive

- Une telle machine a été construite en 1998. Deep Crack a coûté environ 200 000 dollars et pouvait casser la clé en moins d'une semaine.

77

2-DES (Cryptanalyse)

Cryptanalyse du DES: Recherche exhaustive

- Une telle machine a été construite en 1998. Deep Crack a coûté environ 200 000 dollars et pouvait casser la clé en moins d'une semaine.
- Le calcul distribué en utilisant les ordinateurs des particuliers (*distributed.net*, de plus de 100 000 ordinateurs) a prouvé son efficacité en cassant une clé en moins de 24 heures, suite à un test de 145 milliards de clés par seconde.

79

2-DES (Cryptanalyse)

Cryptanalyse du DES: La cryptanalyse différentielle

- La cryptanalyse différentielle découverte par Eli Biham et Adi Shamir en 1991 permet de trouver la clé en utilisant 2^{47} textes clairs choisis.
- Etude des différences de chiffrement entre des textes similaires.
- Utilise la comparaison du ou exclusif de deux entrées avec le ou exclusif des deux sorties correspondantes
- Permet de sélectionner des clefs probables

83

2-DES (Data Encryption Standard)

Cryptanalyse du DES: La cryptanalyse linéaire

- inventée par Mitsuru Matsui en 1994 est plus efficace.
- Utiliser des relations linéaires pour interpoler des bits de la clef
- On suppose qu'un adversaire dispose d'un grand nombre de paires de textes clairs et de textes correspondants tous chiffrés avec la même clé K inconnue (attaque à texte clair connu).
- Cette attaque nécessite 2^{43} couples (tous chiffrés avec la même clé) que l'attaquant a pu récupérer par un moyen ou un autre.

85

Autres cryptosystèmes à clef privée

Principaux algorithmes

- ***DES*** (Data Encryption Standard) a été élaboré par le NIST(National Institute of Standards and Technology) en 1977. Les informations sont chiffrées par blocs de 64 bits avec une clé de 56 bits. Cet algorithme est largement utilisé pour les applications financières. Il est généralement mis en œuvre en un mode dit de chainage de blocs (CBC, Cipher Block Chaining) ou le chiffrement d' un bloc dépend du précédent.

Autres cryptosystèmes à clef privée(2 DES)

- Suite aux failles du **DES**, quelques modifications ont été apportées, mais pas toujours avec succès. Ce fut notamment le cas avec le 2DES. Il faut tout d'abord choisir deux clefs k1et k2
- Le principe du 2DES est de chiffrer deux fois le message :E(k2, E(k1, m)) Il a été prouvé que 2DES était équivalent à un DES avec une clé de 57 bits. Il faut donc seulement deux fois plus de travail pour le briser ($2^{57} = 2*2^{56}$).
- Le 2DES est sensible à l'attaque Meet-in-the-middle, autrement dit, un intrus peut s'introduire dans l'échange et retrouver la clé utilisée

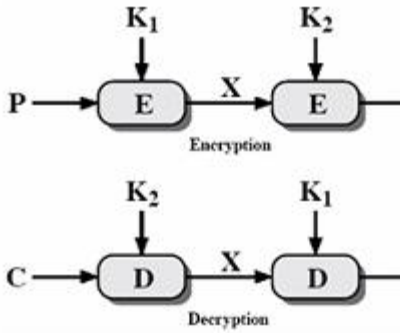


FIG. 5.23 – Double D

Autres cryptosystèmes à clef privée

- Les algorithmes ***Triple DES***, ***DESX*** (DES XORed), ***GDES*** (Generalized DES), ***RDES*** (Randomized DES) sont déduits de l'algorithme DES, il exploit des clés plus longues, rendant ainsi l' algorithme plus puissant.
- Le triple DES tire son nom du fait que l'on réalise trois niveaux de chiffrement ce qui donne une clé effective de chiffrement de 168 bits (56 bits trois trois).
  - ***Triple DES***,
  - ***DESX*** (DES XORed),
  - ***GDES*** (Generalized DES),
  - ***RDES*** (Randomized DES)

Autres cryptosystèmes à clef privée (3 DES)

Grâce à 2 clefs, on pratique 3 opérations :

$$E(k_1, D(k_2, E(k_1, m))).$$

C'est équivalent au fait de doubler la taille effective de la clé (ce qui est une longueur sûre actuellement). Il existe deux versions : la première utilise deux clés (cas de figure présenté ici), la seconde trois (le dernier chiffrement utilise une troisième clé).

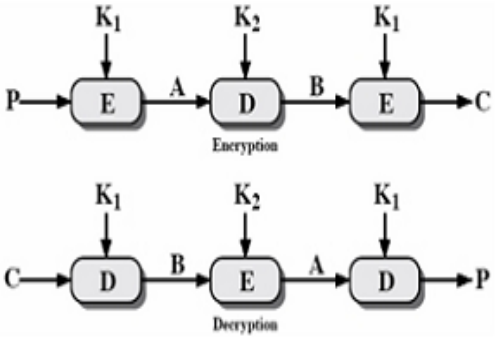


FIG. 5.24 – Triple DES

Il est très robuste contre toutes les attaques faisables connues. Cependant, il est beaucoup plus lent que le DES car on triple les opérations.

Autres cryptosystèmes (IDEA et Blowfish)

- ***IDEA*** (International Data Encryption Algorithm) élaboré conjointement par des chercheurs de l'école polytechnique fédéral de Zurich et de la société Ascom, **utilise une clé de 128 bits pour coder des blocs de données de 64 bits.**

Il est principalement utilisé par le protocole de messagerie sécurisé PGP (Pretty Good Privacy).

- **Blowfish** est un algorithme de chiffrement symétrique (c'est-à-dire « à clef secrète ») par blocs conçu par Bruce Schneier en 1993. **IL utilise une taille de bloc de 64 bits et la clé de longueur variable peut aller de 32 à 448 bits**.

Blowfish est environ 5 fois plus rapide que Triple DES et deux fois plus rapide que IDEA. Malgré son âge, il demeure encore solide du point de vue cryptographique. La version complète avec 16 tours est à ce jour entièrement fiable et la recherche exhaustive reste le seul moyen pour l'attaquer.

Autres cryptosystèmes à clef privée (AES)

- La progression de la puissance des ordinateurs a causé la mort du DES. Ce dernier n'est plus jamais utilisé lorsque la sécurité demandée est forte (utilisation militaire, documents "secrets", etc.). Pour cette tâche, on préfère utiliser l'algorithme connu sous le nom générique d'AES (Advanced Encryption Standard), issu d'un concours créé en raison des faiblesses avérées du DES. Le véritable nom de l'AES est le Rijndael, nom résultant de la contraction des noms de ses inventeurs : Rijmen et Deamen.

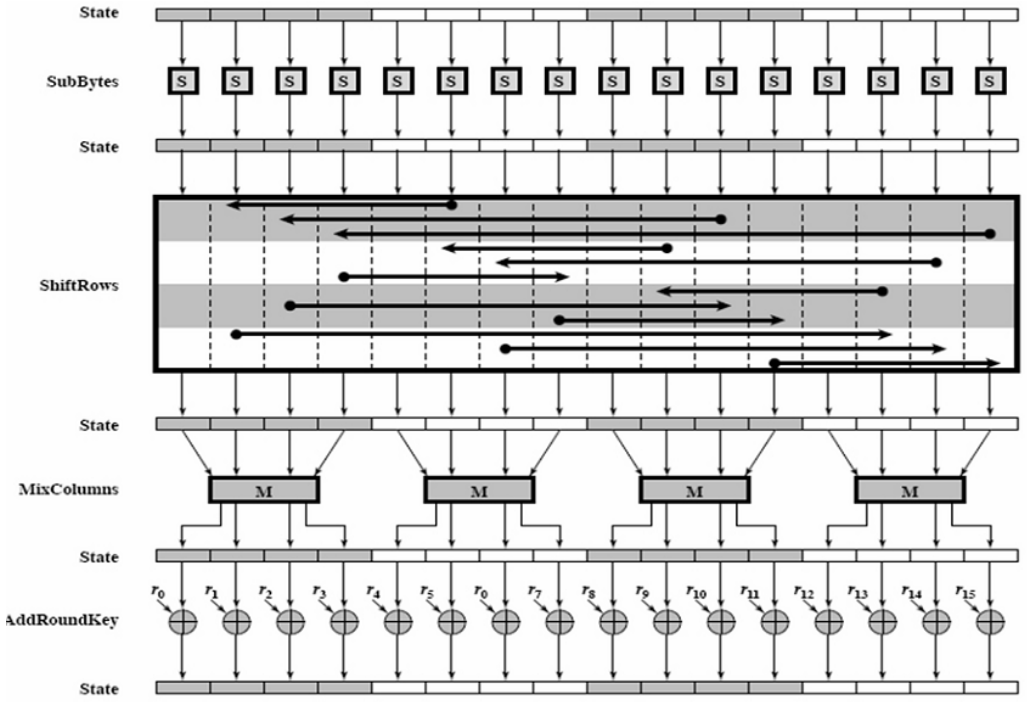
Il exploite des clés de 128 bits, 192 ou 256 bits sur des blocs de 128 bits.

L' AES est considéré rapide, facile à implémenter et ne requiert que peu de ressource mémoire. Actuellement, ce système demeure incassable et reste **le plus sûr des systèmes de chiffrement symétrique.**

Autres cryptosystèmes à clef privée (AES)

À chaque ronde, quatre transformations sont appliquées :

1. substitution d'octets dans le tableau d'état
2. décalage de rangées dans le tableau d'état
3. déplacement de colonnes dans le tableau d'état
4. addition d'une "clef de ronde" qui varie à chaque ronde



Cryptanalyse

- Les cryptanalyses des systèmes de chiffrement se base en général sur la découverte de la clé de chiffrement, sur l'analyse des messages indépendamment de la connaissance des clés.
- En réalité, La majorité des systèmes de chiffrement symétrique sont opérationnellement sécurisés .
- Avec le progrès scientifique dans le domaine de l'informatique et de l' électronique, les systèmes qui sont jugés actuellement sûrs ne le seront peut être plus dans le futur proche (ce qui est déjà le cas du DES simple avec une clé 56 bits) du fait de l' augmentation de la capacité et de la rapidité de traitement mises à disposition de la communauté.
- Le cryptanalyste peut par exemple tester plusieurs clés qui ne diffèrent les unes par rapport aux autre que de quelques bit sur un seul message pour deviner le comportement du système de chiffrement. Ensuite il va tenter de retrouver les messages originaux à partir des messages chiffrés sans avoir recours à l'utilisation effective de la clé des utilisateurs.

Comparaison

	DES	3DES	AES
Date	1976	1978	2000
Type de chiffrement	Chiffrement par blocs	Chiffrement par blocs	Chiffrement par blocs
Taille de blocs	64 bits	64 bits	128 bits
Taille de clefs	64 bits	128 à 192 bits	128, 192 et 256 bits
Sécurité	Faible	Moyenne	Haute

Chiffrement par flot