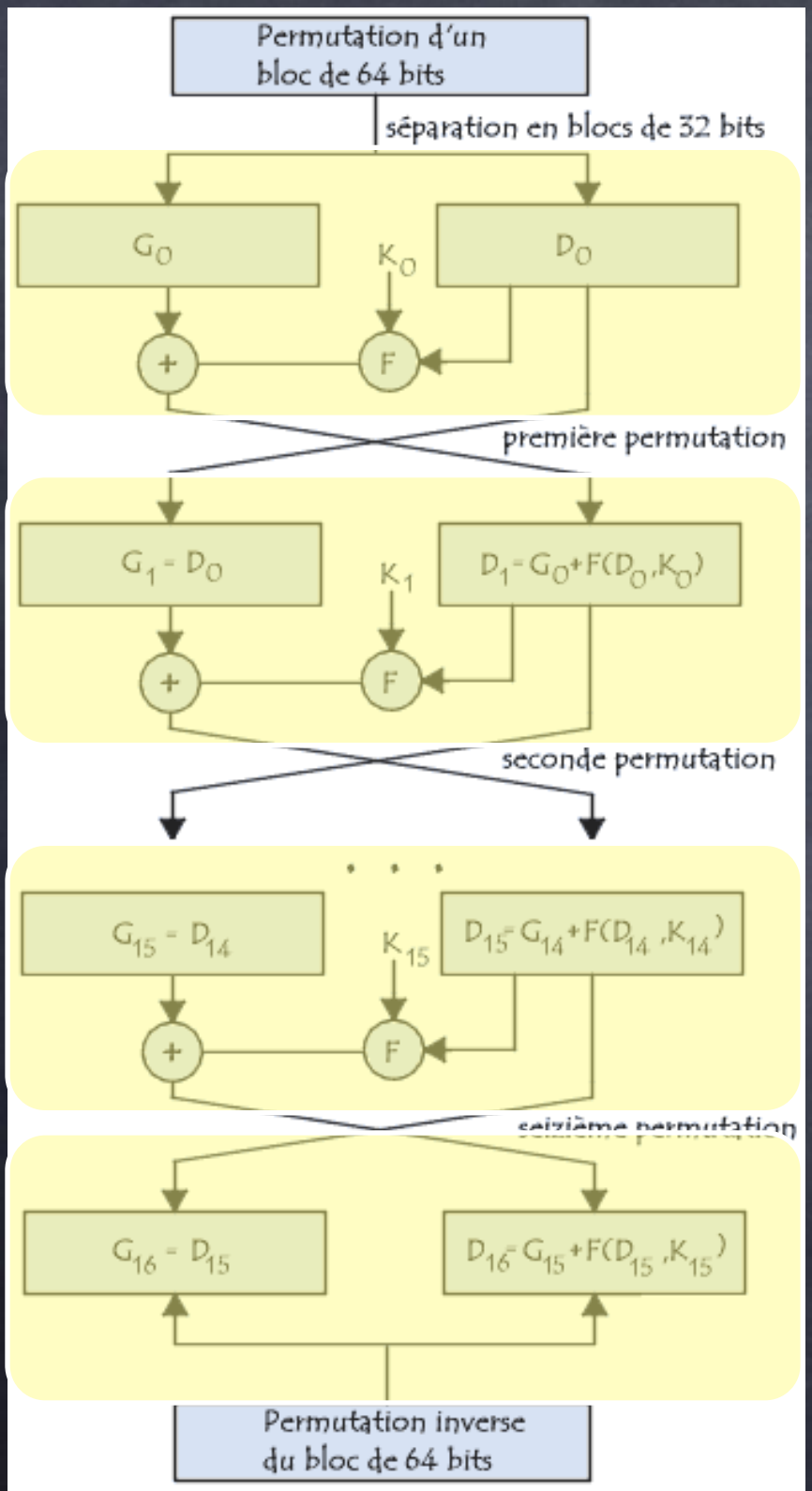
DES et AES

Cours de Crypto

Louis Salvail

DES

- 56 bits de clé.
- Blocs de 64 bits.
- Réseau de Feistel à 16 rondes.
- Les fonctions de ronde sont comme pour les réseaux du type substitution-permutation.
  - Substitutions: Réalisées par 8 S-boxes chacune étant 4-1
  - Permutations: Les sorties des S-boxes sont permutées.



Bloc de donées à chiffrer:

Ronde #1

Ronde #2

Ronde #15

Ronde #16

1	2	3	4	5	6	...	61	62	63	64

Permutation initiale

58	50	42	34	26	18	...	31	23	15	7

DES dérive 16 clés de 48bits, une pour chaque ronde, à partir d'une seule clé de 64(56) bits.

G_0 D_0 K_0

$G_1 = D_0$

$D_1 = F(D_0, K_0) + G_0$

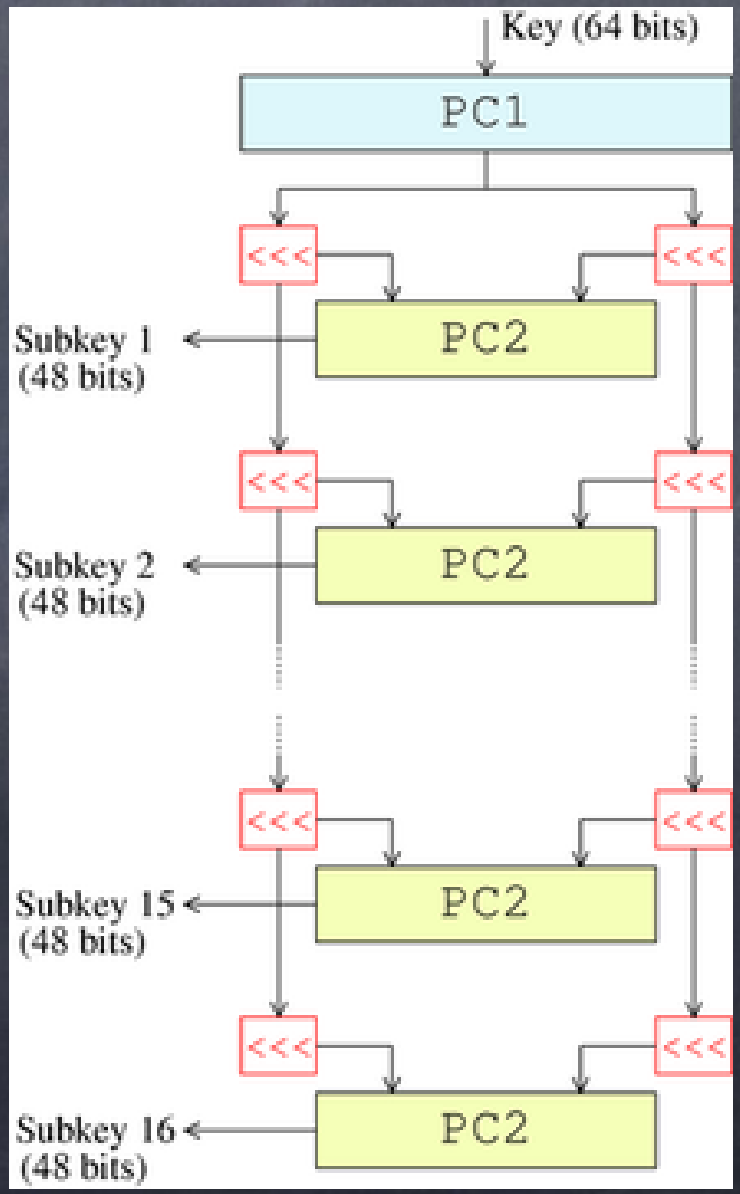
Ceci applique une substitution et une transposition (permutation)

Les clés DES sont codées sur 64 bits (8 octets) mais chaque octet contient un bit de parité (de sorte que la parité de chaque bloc est impaire). Le résultat est une clé effective de 64-8=56 bits!

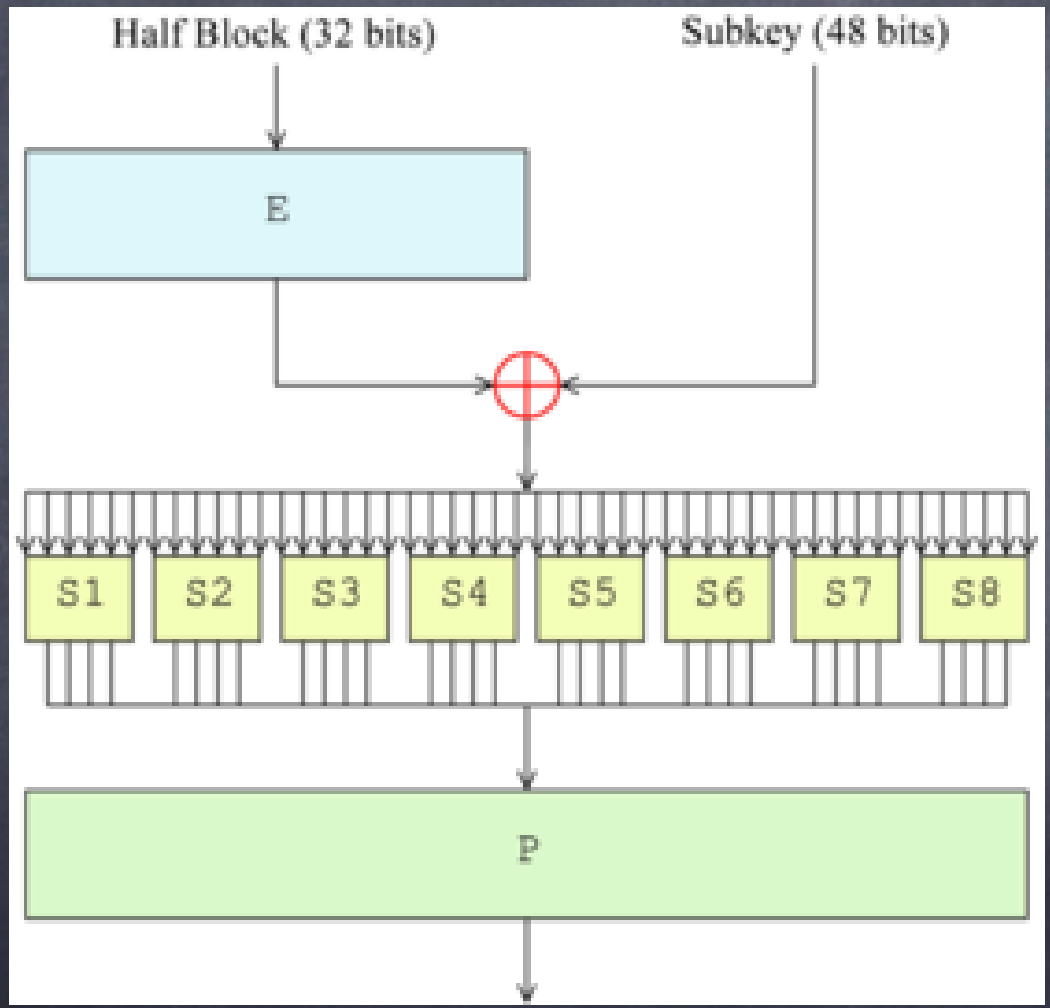
Dérivation des Clés pour les rondes DES

DES utilise sa clé de 56 bits qui est coupée en deux. Chaque partie de 28 bits est traitée séparément. À chaque tour, les deux sous-clés subissent une rotation vers la gauche par un ou deux bits (selon le tour). Des sous-clés de 48 bits sont ensuite extraites en prenant 24 bits dans chaque clé de 28 bits. Les 24 bits retenus varient selon les tours de telle façon que chaque bit soit utilisé dans approximativement 14 des 16 sous-clés employées dans les 16 tours.

Soit K=(KL,KR). La partie la plus à gauche des sous-clés provient toujours de KL tandis que la partie la plus à droite provient de KR



Fonctions de ronde



Les boîtes-S

Chaque Boîte-S accepte 6 bits et en produit 4.

B_6=101101

Milieu

S_6	0	1	10	11	100	101	110	111	1000	1001	1010	1011	1100	1101	1110	1111
0	10	1100	100	1	111	1010	1011	110	1000	101	11	1111	1101	0	1110	1001
1	1110	1011	10	1100	100	111	1101	1	101	0	1111	1010	11	1001	1000	110
10	100	10	1	1011	1010	1101	111	1000	1111	1001	1100	101	110	11	0	1110
11	1011	1000	1100	111	1	1110	10	1101	110	1111	0	1001	1010	100	101	11

bouts

Chaque ligne est une permutation

Attaque contre DES à une ronde

- La clé K1 pour la ronde 1 est de 48 bits.
- (x,y): y=(L1,R1) où L1=R0 et R1=L0+f1(R0),
  - f1(x1) = R1+x0,
  - Donc, à partir de la fin de f1(x1) nous pouvons parcourir la permutation de mixage à l'envers.
    - Ainsi, nous avons les sorties des S-boxes. Puisque chaque S-box est 4-1, nous avons 4 valeurs possibles pour l'input de chaque S-box.
    - Les inputs de toutes les S-boxes sont E(x1)+K1
    - Pour chaque portion de 6 bits de K1, il y a 4 candidats possibles.
    - Ce qui fait $4^{48/6}=2^{16}$ candidats!
    - Une nouvelle paire (x',y') permet de trouver K1 en temps essentiellement 2^{16}.

Attaque contre DES à deux rondes

- Maintenant la clé consiste en deux portions K1 et K2 de 48 bits chacune.
- y=(L2,R2), L1=R0=x1, R1=L0+f1(R0)=x0+f1(x1), L2=R1=x0+f1(x1), et R2=x1+f2(R1).
- L0, R0, L1, R1, L2, et R2 sont connus.
- Nous connaissons donc les entrées-sorties de f1 et f2!
- La même attaque que précédemment permettra donc de trouver K1 et K2 en le double du temps: $2*2^{16}$.
- Puisque plusieurs bits de K1 et K2 sont les même,

Attaque contre DES à trois rondes

- y=(L3,R3), puisque L1=R0 et R2=L3 nous avons que la seule valeur inconnue est R1=L2=L0+f1(R0).
- Nous n'avons plus les entrées-sorties d'acune fonction de ronde.
- On peut observer que f1(R0)=L0+R1=L0+L2 et que f3(R2)=L2+R3 ce qui donne:
  - (L0+L2)+(L2+R3)=L0+R3 qui est connu.
  - Nous connaissons les entrées de R0 pour f1 et R2=L3 pour f3 ainsi que le XOR de leurs sorties.
  - Nous allons utiliser ceci pour trouver la clé.

Attaque contre DES à trois rondes

- Puisque la partie gauche des sous-clés provient KL et la partie droite des sous-clés provient de KR
- Ceci implique que KL affecte seulement les 4 premières S-boîtes tandis que KR affecte seulement les 4 dernières S-boîtes.
- Puisque les permutations de fin de rondes sont connues, nous connaissons quels bits de la sortie d'une ronde proviennent de quelles S-boîtes.
- Nous allons traverser l'espace des clés pour chaque moitié de la clé maître. L'attaque sera de complexité environ $2*2^{28}$ au lieu de 2^{56}.
- L'attaque sera possible si nous pouvons vérifier la validité d'un essai.....

Attaque contre DES à trois rondes

- Soit kL un essai pour la partie gauche KL de K.
- Nous connaissons l'entrée R0 de f1 ce qui nous permet à partir de kL d'essayer une entrée pour les 4 premières S-boîtes.
- Nous pouvons donc calculer la moitié des bits de sortie de f1.
- Nous pouvons faire la même chose avec f3 puisque nous connaissons son entrée L3. Évidemment nous faisons ceci avec le même essai kL que pour f1.
- Les résultats peuvent être XORés pour vérifier si le résultat est consistant avec les 16 premiers bits de la valeur connue L0+R3.

Attaque contre DES à trois rondes

- Si kL=KL alors le test sera passé avec succès.
- Si kL<>KL alors nous nous attendons a ce qu'elle passe le test avec probabilité essentiellement 2^{-16} (car nous vérifions 16 bits des 32 bits de sortie).
- Il y a 2^{28} candidats pour kL ce qui nous donne $2^{28}/2^{16}=2^{12}$ possibilités pour KL.
- En faisant de même avec KR nous obtenons 2^{12} candidats pour celle-ci.
- Chaque combinaison pour kL et kR est possible ce qui nous donne 2^{24} candidats.
- L'attaque est conclue après une recherche exhaustive sur ces candidats à partir d'une nouvelle paire (x',y').
- La complexité totale est $2*2^{28} + 2^{24} < 2^{30}$ et l'espace nécessaire est $2*2^{12}$. Ceci est possible avec un ordinateur personnel.

Chiffrement double

- Vous avez obtenu (M, $C=E_{k2}(E_{k1}(M))$) et vous voulez trouvez K1, K2 en $2*2^{56}$ chiffrements et

Algo

1. Pour chaque K1 calcul z=EK1(M) est range (z,k1) dans liste L

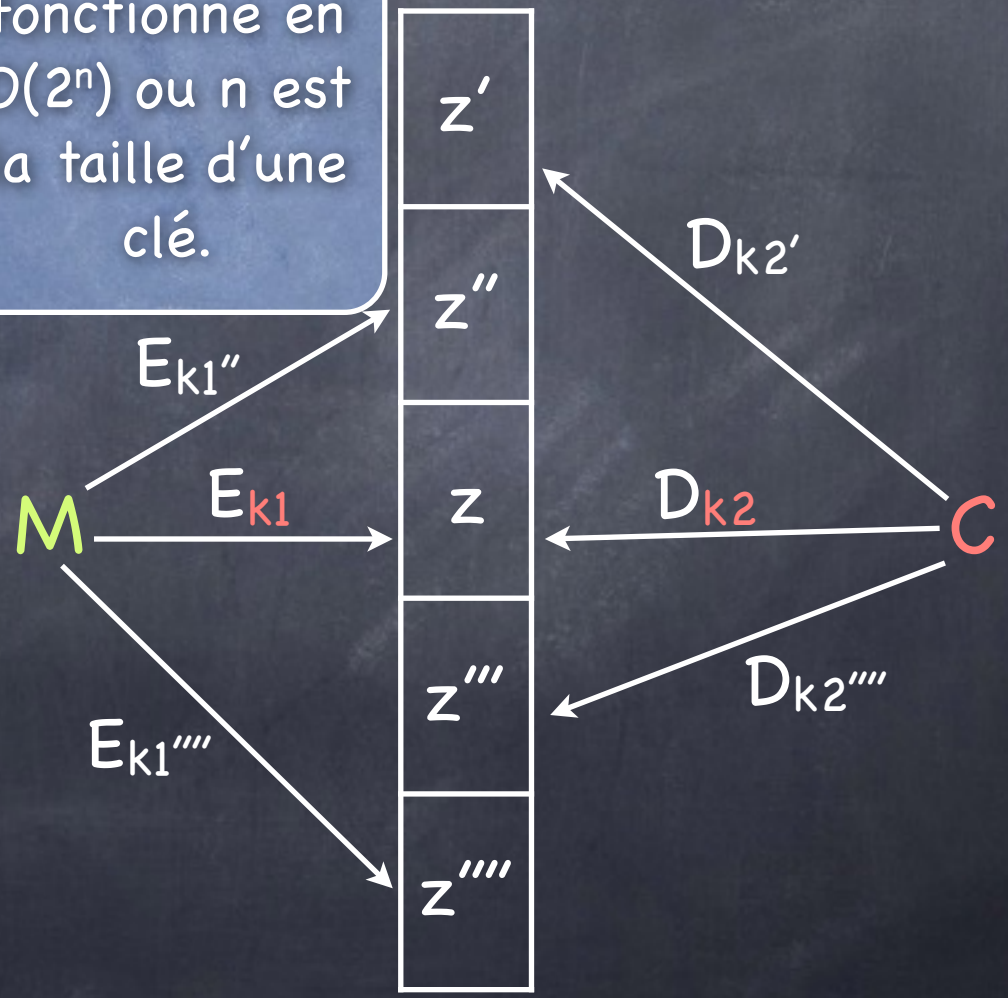
2. Pour chaque K2 calcul z=DK2(C) est range (z,k2) dans liste L'

3. Trier L et L' selon la première composante

4. Trouve un 'match' de la forme (z,k1) et (z,k2) dans L et L'. Ceci peut se faire en |L| visite puisque les listes sont triées.

5. Retourner k1,k2.

Cet algo fonctionne en $O(2^n)$ ou n est la taille d'une clé.



Triple DES (2 clés)

- $E_{K1}(D_{K2}(E_{K1}(M)))$ est proposé comme tel pour que si K1=K2 alors il s'agit d'un seul chiffrement DES. Autrement, E_{K2} ferait aussi bien le travail.
- L'attaque de la rencontre au milieu ne fonctionne pas car le chiffrement de M et le déchiffrement de C par une seule clé DES laisse un chiffrement ou déchiffrement au milieu. Pour pouvoir se rencontrer, un des deux bouts doit chiffrer et déchiffrer avec deux clés rendant l'attaque inutile...
- Il y a d'autres attaques sur triple DES. L'une demande un temps dans $O(2^n)$ (où n est la longueur d'une seule clé) mais aussi $O(2^n)$ paires (M,C) choisies ou C est le chiffrement de M avec la même clé.

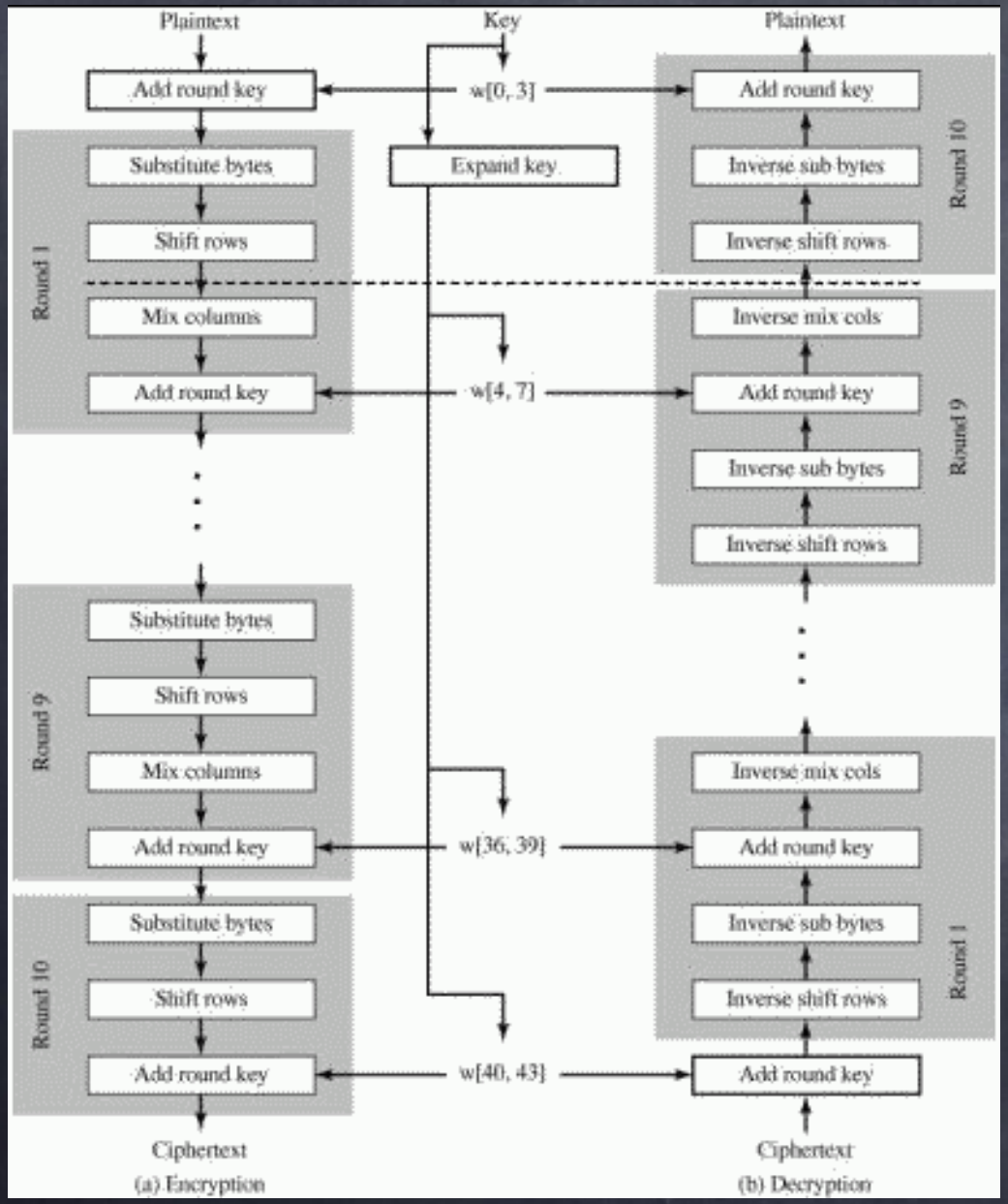
AES: Advanced Encryption Standard

- Le système DES à été remplacé pour un nouveau système appelé AES:Advanced Encryption Standard.
- Il est devenu le nouveau standard NIST en 2001.
  - Il chiffre des blocs de 128 bits,
  - avec des clés secrètes de 128(10 rondes), 192(12 rondes), ou 256 bits (14 rondes).
- Consomme peu de mémoire et est très efficace.

Les rondes

- AES dérive une clé de ronde de 128 bits à partir de la clé maîtresse de 128 bits.
- Elle est interprétée comme une matrice d'octets 4X4.
- L'input est placée dans une matrice d'octets 4X4 appelée l'état.
- L'état est modifié à chaque ronde à partir de la clé de ronde et d'une série de transformations.

AES

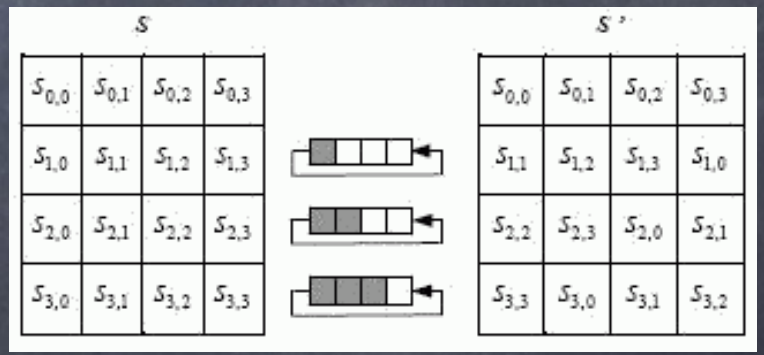


AddRoundKey:Calcul des XOR des octets du bloc à chiffrer avec la matrice de la clé courante.

SubByte:Substitue chaque octet du bloc à chiffrer.

Regardons le bloc courant comme une matrice 4X4 d'octets:

Shiftrows:Applique des rotations aux rangées 2,3,4 de la matrice.



Mixcol:Multiplie chaque colonne du bloc courant par une matrice. Les multiplications sont dans un corps fini et les additions des XOR.

$$\begin{bmatrix} s'_{0,c} \\ s'_{1,c} \\ s'_{2,c} \\ s'_{3,c} \end{bmatrix} = \begin{bmatrix} 02 & 03 & 01 & 01 \\ 01 & 02 & 03 & 01 \\ 01 & 01 & 02 & 03 \\ 03 & 01 & 01 & 02 \end{bmatrix} \begin{bmatrix} s_{0,c} \\ s_{1,c} \\ s_{2,c} \\ s_{3,c} \end{bmatrix}$$

Shiftrows+Mixcol forment le mixage....