4. Cryptographie Moderne
Cryptographie Symétrique

Noureddine AZZOUZA Riadh MEGHATRIA

[1] Université Djilali BOUNAAMA Khemis Miliana, Algérie

Cours de Sécurité Informatique, M2GLSD

Cryptographie moderne

la cryptographie moderne manipule des séquences binaires (le message à chiffrer est une suite de bits)

- les algorithmes sont connus de tous (ne sont pas secret)
- la sécurité repose uniquement sur le secret d'une clé.

Classes de cryptographie moderne

- Cryptographie symétrique
- Cryptographie asymétrique

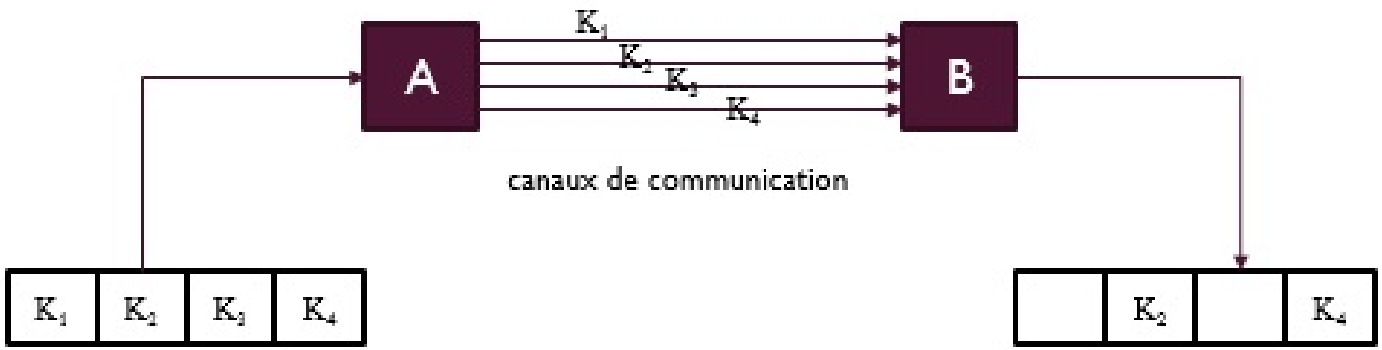
Transfert de clés

Canal de communication

Écoute du canal

Clé en plusieurs morceaux

Téléphone, courrier postal ...



Utilisation des clés

Chiffrement par logiciel

- Interruption du chiffrement (système multitâches)
- sauvegarde de la clé et du programme de chiffrement

Conséquence

risque de récupérer la clé par un attaquant ...

Stockage des clés

La clé est mémorisée par l'utilisateur

- Entrer la clé sous forme de bits
- Entrer sous forme d'une chaine de caractère —> transformée en suite de bits
- Découper la clé en 2 parties (utilisateur & système)

Duplication des clés

Responsable

- connaitre et sauvegarder toutes les clés (employés)

Risques

- utilisation des clé pour des fins personnelles
- partage de secret

Longévité des clés

- réduire le risque d'une éventuelle compromission des clés
- Aucune clé ne doit être utilisée pour une période indéfinie

Crypto-période

- durée de vie maximale d'une clé
- Date limité ou compteur d'utilisation

Gestion des clés

Se procurer la clé de quelqu'un :

- Directement de la personne concernée
- BDD centralisée
- BDD privée, gestion distribuée des clés

Modes de chiffrement

Chiffrement par bloc

ECB, CBC, CFB, OFB, BC, PCBC

Chiffrement à flot

ou chiffrement en continu

Notation

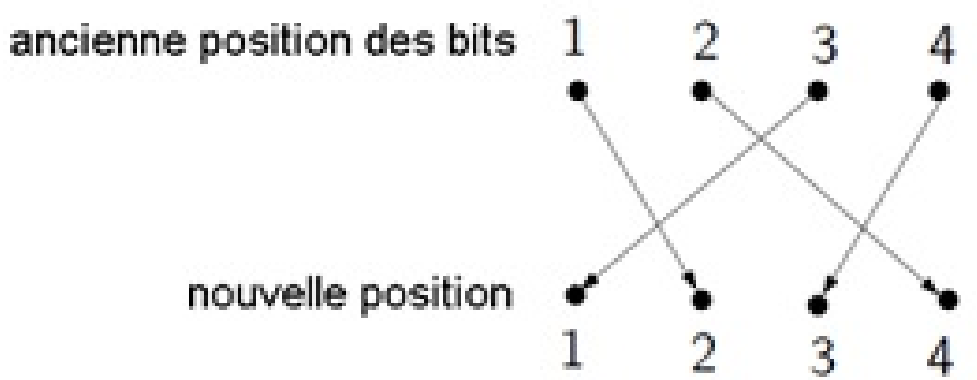
1. M : message en clair
2. C : le texte chiffré
3. E : la fonction de chiffrement
4. VI : la valeur d'initialisation
5. D : la fonction de déchiffrement

Opérations de chiffrement

- Permutation

Exemple : Permutation binaire

- M=101000100101
- Taille d'un bloc = 4
- Permutation P : {1, 2, 3, 4} –> {1, 2, 3, 4}
- Résultat : [P(1), P(2), P(3), P(4)] = [3, 1, 4, 2]



Opérations de chiffrement

- Substitution

Exemple : Substitution binaire

- M=10100010000
- Taille d'un bloc = 2
- Substitution S :

X	00	01	10	11
$\downarrow$	$\downarrow$	$\downarrow$	$\downarrow$	$\downarrow$
$S(X)$	11	10	01	00

Opérations de chiffrement

- XOR (OU Exclusif)

Exemple : OU Exclusif

- l'alphabet binaire $\sum = \{0,1\}$
- l'opérateur logique ou exclusif : $\oplus$
- Permutation P

$X \oplus Y$

X\Y	0	1
0	0	1
1	1	0

- Résultat : [0, 1, 0, 1,1] $\oplus$ [1, 1, 0, 0,1]= [1, 0, 0, 1,0].

Opérations de chiffrement

- Bijection de Feistel

Exemple : OU Exclusif

- une succession d'étapes ("rondes")
- effectuer une opération sur la moitié des données, inverse et combiner les deux parties
- Chiffrement :

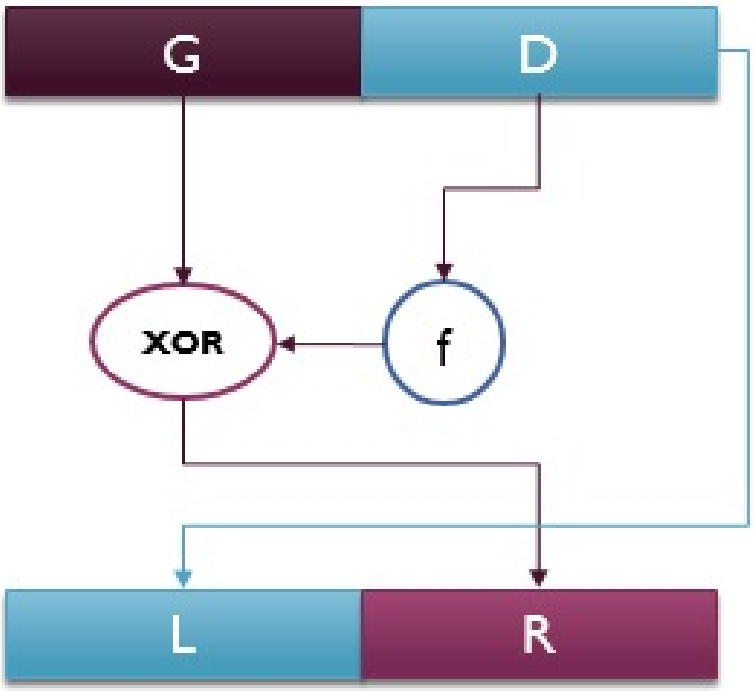
$$\begin{cases} L_i = R_{i-1} \\ R_i = L_{i-1} \bigoplus f(R_{i-1}, K_i) \end{cases}$$

- Déchiffrement :

$$\begin{cases} L_{i-1} = R_i \bigoplus f(I_i, K_i) \\ R_{i-1} = L_i \end{cases}$$

Opérations de chiffrement

- Bijection de Feistel



F : fonction presque aléatoire

Bloc (G, D) ⟶ (L, R) tel que

L = D

R = G XOR f(D).

Bijection : (L, R) ⟶ (G, D) tel que

D = L

G = R XOR f(D)

Electronic Code Book (ECB)

Principe

- le message M est découpé en blocs M_i de taille fixe.
- Chaque bloc est alors chiffré séparément par une fonction E_k, paramétrée par une clé k .
- un bloc sera toujours codé de la même manière.
- Chiffrement : $E_k(M_i) = C_i$
- Déchiffrement : $M_i = D_k(C_i)$ tel que $D_k = E_k^{-1}$

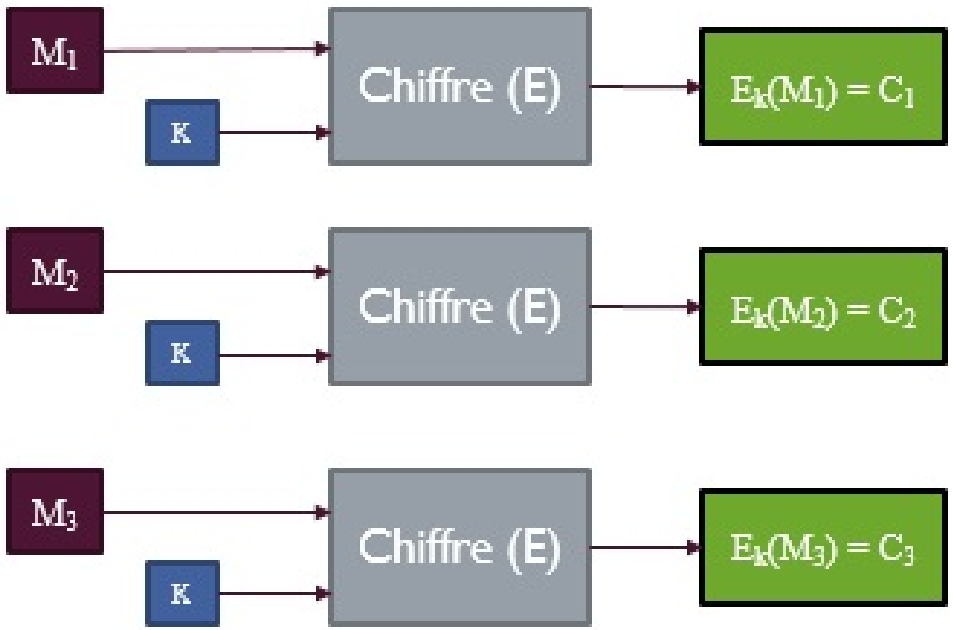
Electronic Code Book (ECB)

Avantages

- Le plus simple à utiliser.
- Blocs indépendants.

Inconvénients

- Attaque par répétition.



Electronic Code Book (ECB)

Exemple

- Chiffrer (2) messages en mode ECB.
- Taille du bloc l = 2
- Chiffrement du 1^er message
- Chiffrement du 2^eme message
- Comparaison
- John peut déduire facilement le salaire de Jack : 500000 chiffré en C91010

JOHN__105000
JACK__500000

JO | HN | __ | 10 | 50 | 00
Q9 | 2D | FP | VX | C9 | IO

JA | CK | __ | 50 | 00 | 00
LD | AS | FP | C9 | IO | IO

Q9 | 2D | FP | VX | C9 | IO
LD | AS | FP | C9 | IO | IO

Cipher Block Chaining (CBC)

Principe

- un bloc ne soit pas codé de la même manière (en 2 msg différents).
- Ajouter une Valeur Initiale VI aléatoire (ou C_0) .
- Le bloc est modifié par XOR avec le bloc chiffré précédent avant d'être lui même chiffré.
- Chiffrement : $C_i = E_k(m_i \bigoplus C_{i-1})$
- Déchiffrement : $M_i = C_{i-1} \bigoplus D_k(C_i)$

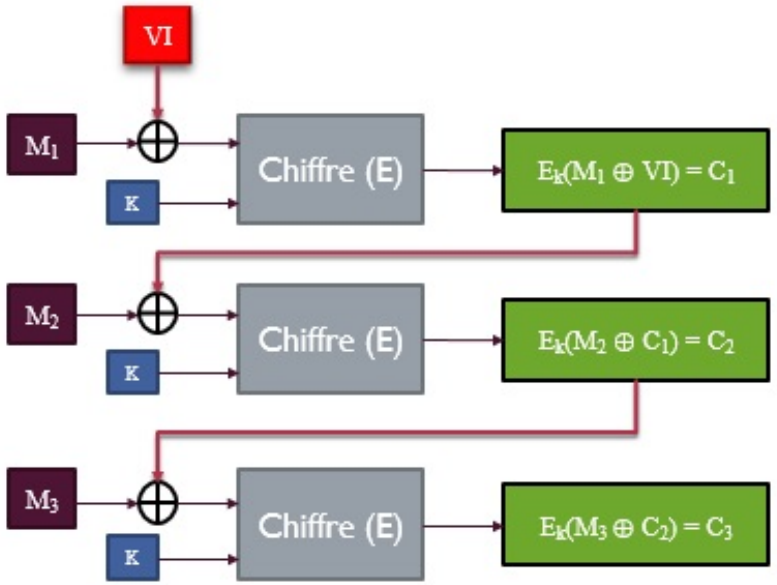
Cipher Block Chaining (CBC)

Avantages

- Le mode le plus utilisé.
- Même msg chiffré différemment car utilisation de VI.

Inconvénients

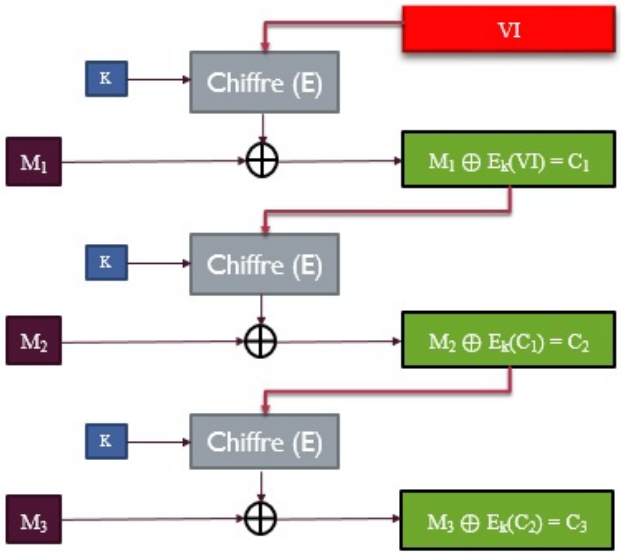
- Lenteur : il faut attendre le déchiffrement du msg précèdent pour déchiffrer un bloc.



Cipher FeedBack (CFB)

Principe

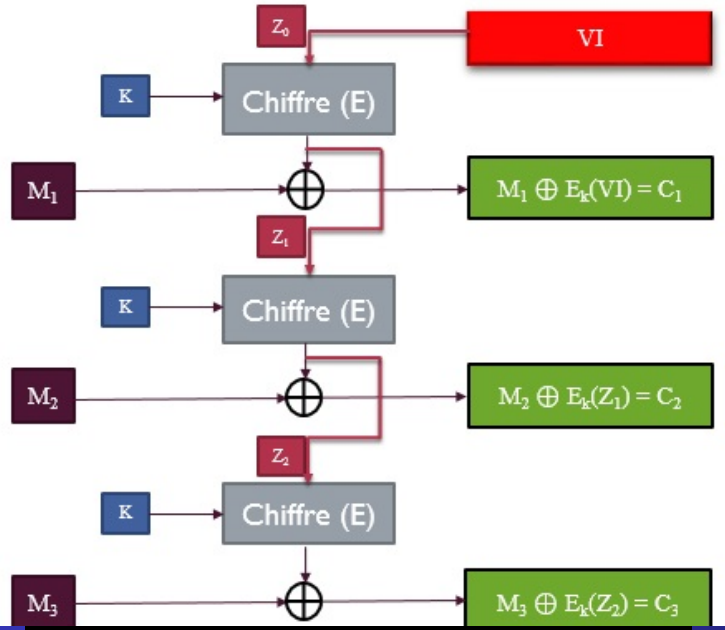
- le déchiffrement ne nécessite pas l'implémentation de la fonction : $D_k = E_k^{-1}$.
- Chiffrement : $C_i = M_i \bigoplus E_k(C_{i-1})$
- Déchiffrement : $M_i = C_i \bigoplus E_k(C_{i-1})$



Output FeedBack (OFB)

Principe

- permet d'avoir un chiffrement et un déchiffrement totalement symétrique.
- Chiffrement : $Z_0 = C_0; Z_i = E_k(Z_{i-1}); C_i = M_i \bigoplus Z_i$
- Déchiffrement : $Z_i = E_k(Z_{i-1}); M_i = C_i \bigoplus Z_i$



Counter-mode encryption (CTR)

Principe

- chiffrement de plusieurs blocs en parallèle.
- intervenir le chiffrement d ?un compteur de valeur initiale T
- Chiffrement : $C_i = M_i \bigoplus E_k(T + i)$
- Déchiffrement : $M_i = C_i \bigoplus E_k(T + i)$

Stream Cipher (SC)

Principe

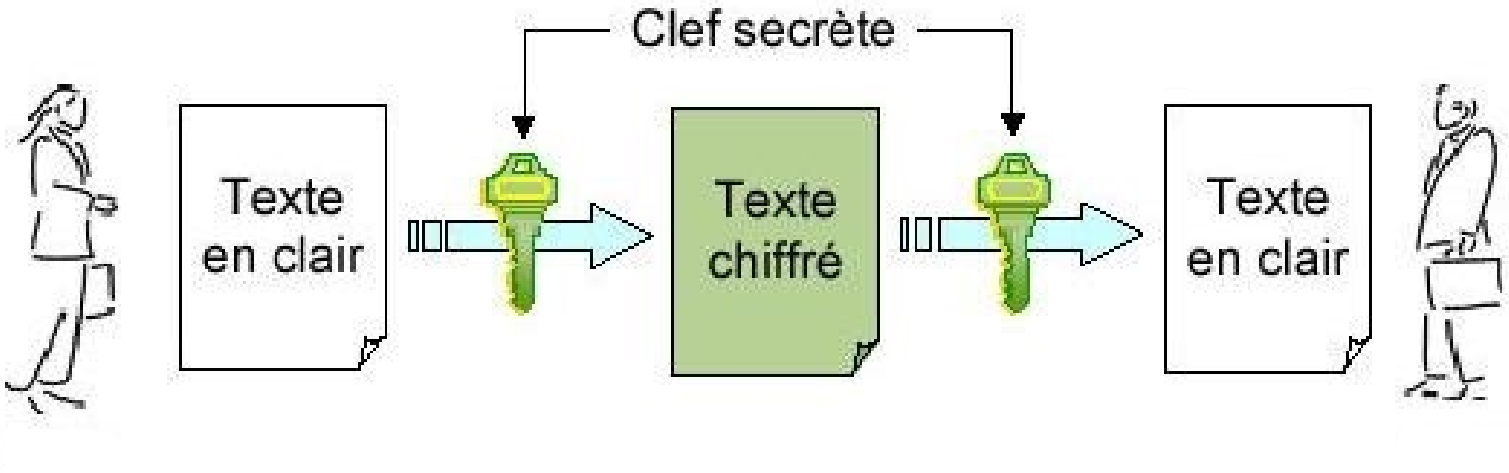
- Bit par bit (confidentialité absolue).
- XOR avec clé générée aléatoirement.
- Destinataire possédant suffisamment de clés

Propriétés

- Clé aussi longue que le message (n bits)
- Clé doit être une chaine de bits aléatoire
- Clé ne doit être utilisée qu'une seule fois

Cryptographie symétrique

1. Les algorithmes à clés secrètes ou symétriques sont des algorithmes où la clé de chiffrement peut être calculée à partir de la clé de déchiffrement et vice versa
2. Les clés sont identiques dans la plupart des cas
3. L'émetteur et le destinataire doivent se mettre d'accord sur cette clé afin d'être utilisé avant tout envoi de message.



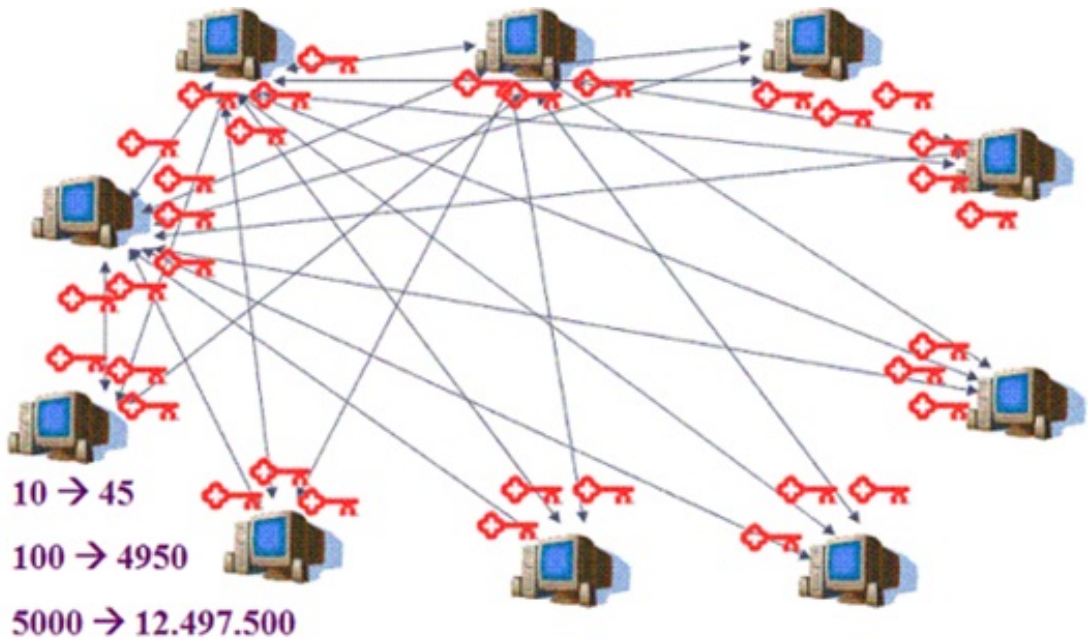
Cryptographie symétrique

Avantages

- Très sûr
- Résistant
- Rapide
- Facile à mettre en oeuvre

Inconvénients

- Distribution des clés
- Nombre de clés : n(n-1)/2
- Ajout d'utilisateurs



Cryptographie symétrique : Algorithmes

Algorithmes de chiffrement par bloc (Block Cipher)

- DES (clé de 56 bits codée sur 64 bits)
- 3DES (Encrypt-Decrypt-Encrypt avec 3 clés différentes (168 bits))
- IDEA (128 bits)
- CAST (128 bits)
- Blowfish (longueur de clé variable, jusqu'à 448 bits)
- AES (128, 192 ou 256 bits)

Algorithme DES

Algorithme DES

- Data Encryption Standard
- Publié en 1975 suite à l'appel d'offre de NBS en 1973
- Reprend les principes de Réseau de Feistel et une partie du système de cryptage Lucifer d'IBM
- la base des algorithmes récents : IDEA, CAST, RC5 ...
- Très populaire et utilisé dans les Transactions bancaires et les systèmes Unix

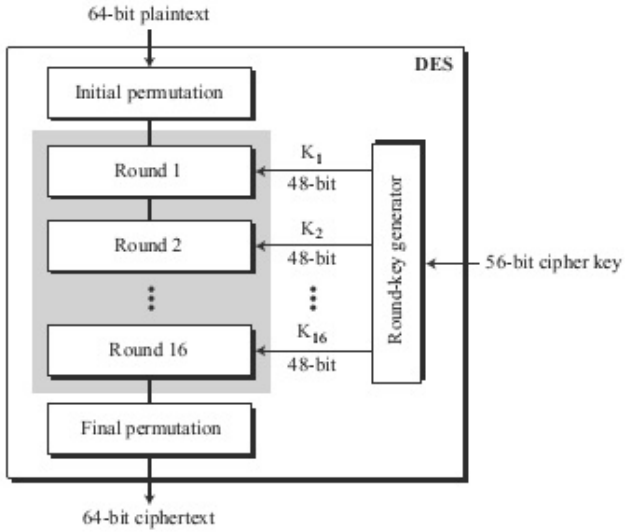
Propriétés

- Symétrique : clé secrète de 56 bits
- Réversible : un algorithme pour le codage/décodage
- Par bloc : message fractionné en bloc de 64 bits

Algorithme DES : Principe

Principe

1. Permutation initiale
2. Effectuer 16 itérations (tours ou rondes)
   - Dépend d'une sous-clé de 48 bits.
   - Plusieurs transpositions et substitutions selon un réseau de Feistel. Le bloc de 32 bits ayant le poids le plus fort (celui qui s'étend du bit 32 au bit 64) subira une transformation ;
3. Permutation finale inverse

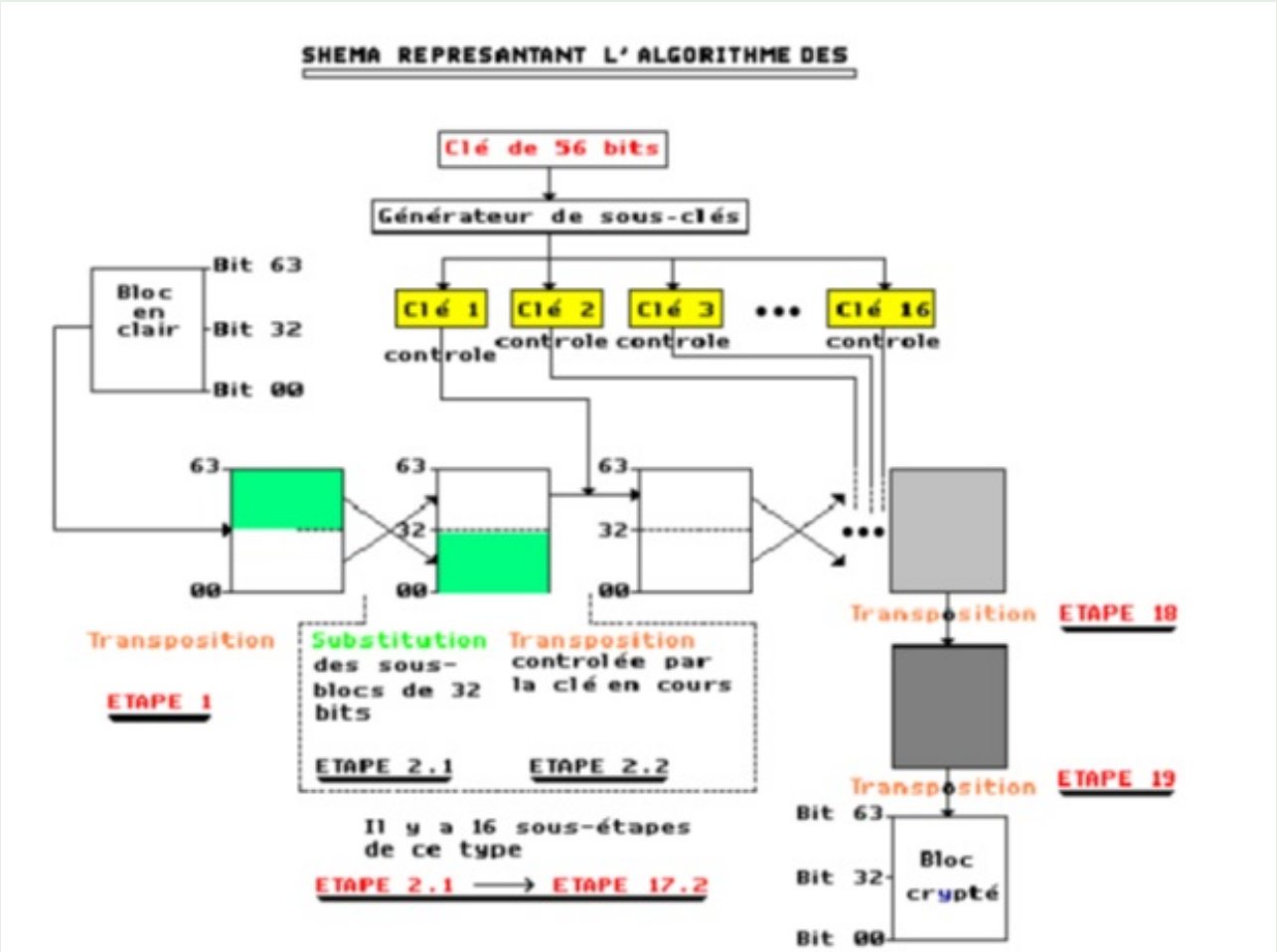


Paramètres

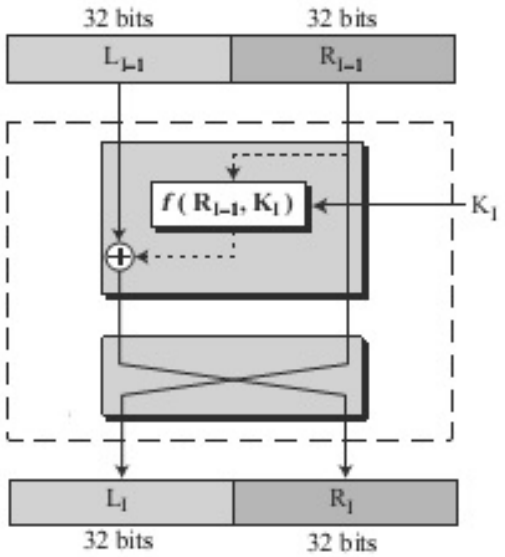
- Taille du bloc : 64 bits (8 octets)
- Taille de la clé : 56 bits
- bits restants (8, 16, 24, 32, 40, 48, 56) : bits de parité ou détection d'erreur
- Permutation et substitution réalisés par : P-box et S-Box

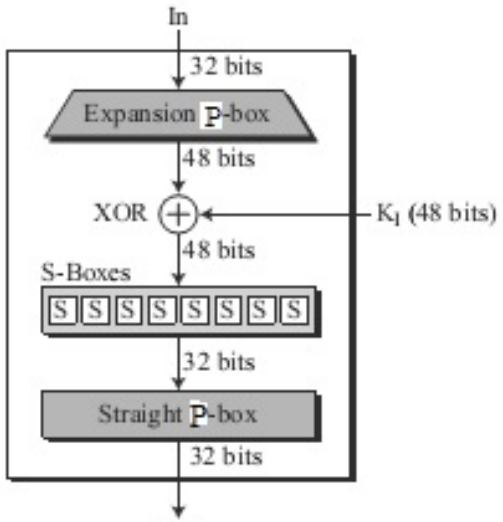
Algorithme DES : Étapes

Etapes

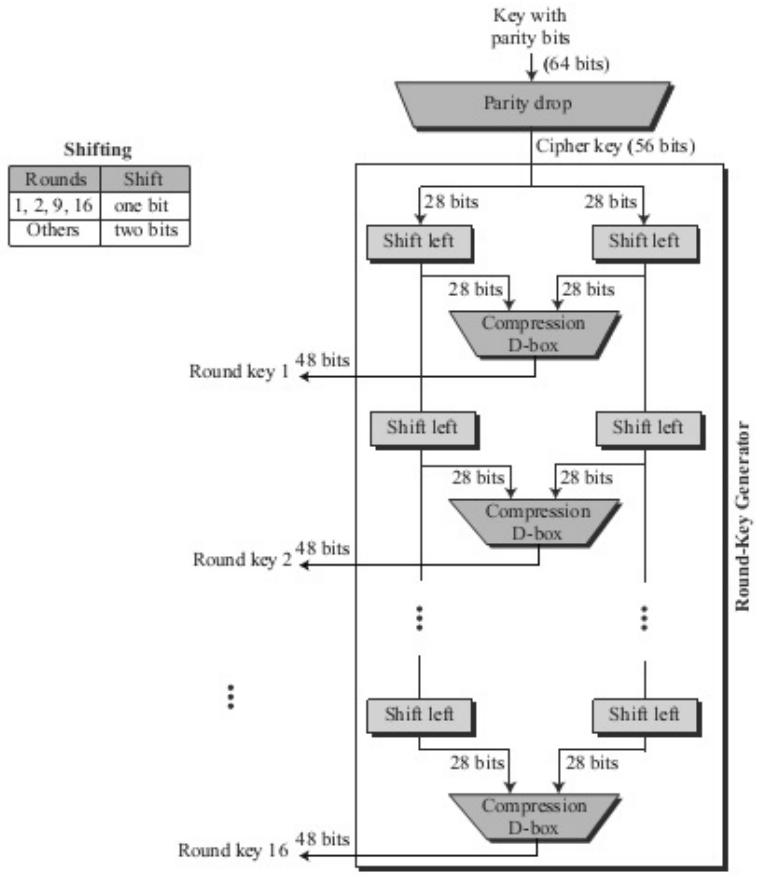


Algorithme DES : itération





Algorithme DES : Génération des Sous clé



Shifting

Rounds	Shift
1, 2, 9, 16	one bit
Others	two bits

Algorithme DES

Avantages

- Facile à implémenter
- Rapide
- Rapport qualité/performance

Inconvénients

- Vulnérable aux attaques par force brute
- Taille clé trop courte / les puissances de calcul actuels
- 1999 : la clé DES à été cassée en 22 heures

- 3DES : 3 fois DES successifs avec différentes clés

Algorithme AES

Algorithme AES

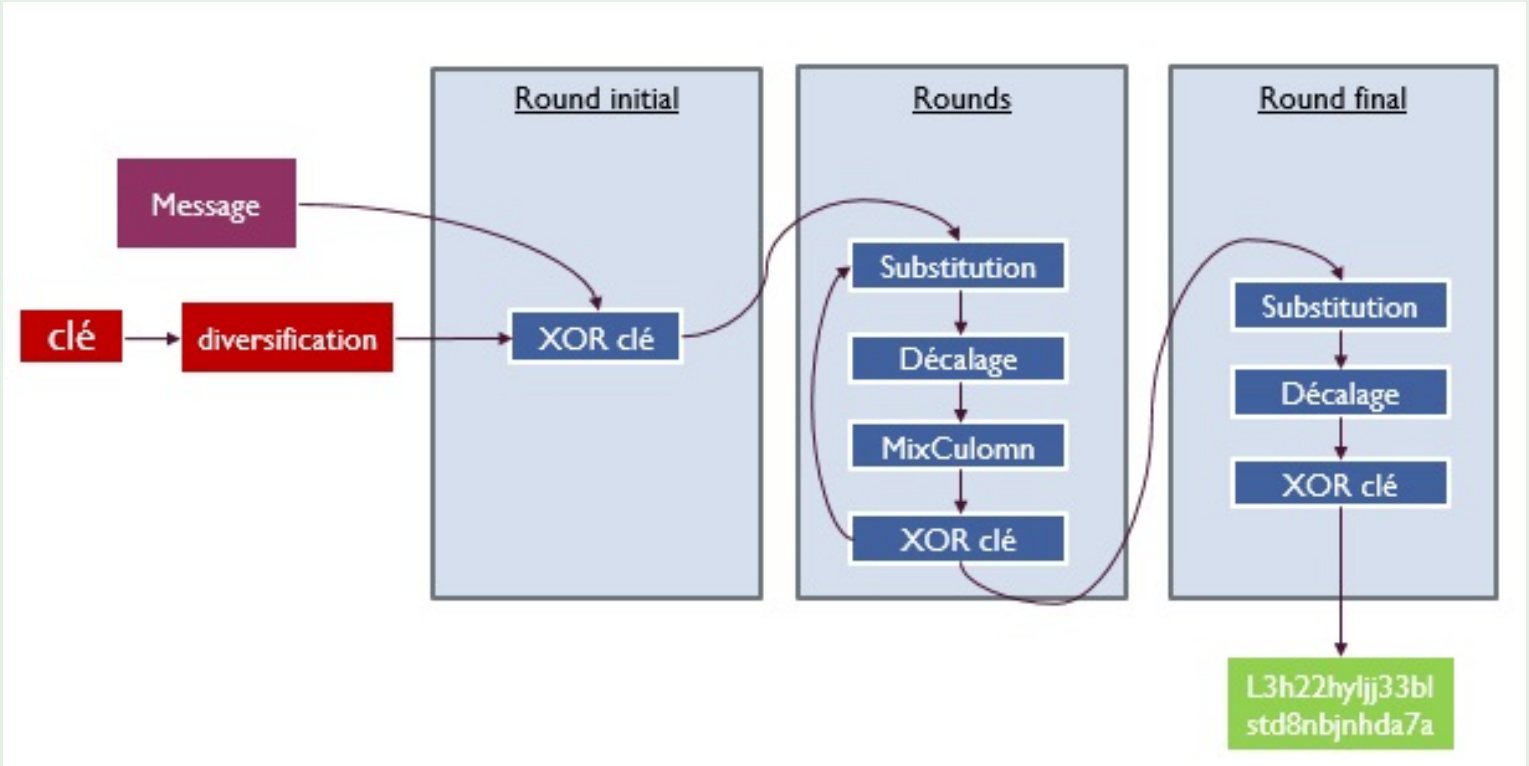
- A.E.S : Advanced Encryption Standard (Rijndael Cipher)
- 1997 : compétition lancée par NIST
- chiffrement par blocs de 128 (128, 192 ou 256)
- Le chiffrement est réalisé en d tours (10, 12 ou 14)

Avantages

- Plus sécurisé
- Plus rapide
- Le plus utilisé des algorithmes symétriques

Algorithme AES : Étapes

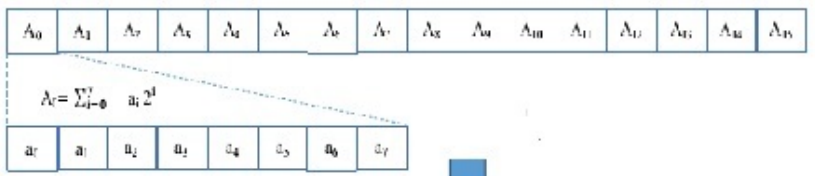
Etapes



Algorithme AES : Principe

Principe

1. Manipule des blocs de 128 bits (16 octets) sous forme de Matrice de 4 x 4 octets noté STATE
2. Calculer STATE = STATE $\bigoplus$ K
   1. Opération de substitution : SUBBYTES
   2. Opération de décalage : SHIFTROWS
   3. Opération : MIXCOLUMNS
   4. Opération XOR declé : ADDROUNDKEYS



A_0	A_4	A_8	A_{12}
A_1	A_5	A_9	A_{13}
A_2	A_6	A_{10}	A_{14}
A_3	A_7	A_{11}	A_{15}

STATE

Algorithme AES : Substitution (SUBBYTES)

Substitution

- Agit sur chaque octet
- utilise la table de substitution S-Box

Substitution

S-Box

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	63	7C	77	7B	F2	6B	6F	C5	30	01	67	2B	FE	D7	AB	76
1	CA	82	C9	7D	FA	59	47	F0	AD	D4	A2	AF	9C	A4	72	C0
2	B7	FD	93	26	36	3F	F7	CC	34	A5	E5	F1	71	D8	31	15
3	04	C7	23	C3	18	96	05	9A	07	12	80	E2	EB	27	B2	75
4	09	83	2C	1A	1B	6E	5A	A0	52	3B	D6	B3	29	E3	2F	84
5	53	D1	00	ED	20	FC	B1	5B	6A	CB	BE	39	4A	4C	58	CF
6	D0	EF	AA	FB	43	4D	33	85	45	F9	02	7F	50	3C	9F	A8
7	51	A3	40	8F	92	9D	38	F5	BC	B6	DA	21	10	FF	F3	D2

Algorithme AES : Décalage (SHIFTROWS)

Décalage

- Effectuer une permutation circulaire sur les éléments des lignes de la matrice B

Décalage

B_0	B_4	B_8	B_{12}
B_1	B_5	B_9	B_{13}
B_2	B_6	B_{10}	B_{14}
B_3	B_7	B_{11}	B_{15}

Première ligne non décalée

$2^{ième}$ ligne décalée à gauche d'une position

$3^{ième}$ ligne décalée à gauche de 2 positions

$4^{ième}$ ligne décalée à gauche de 3 positions

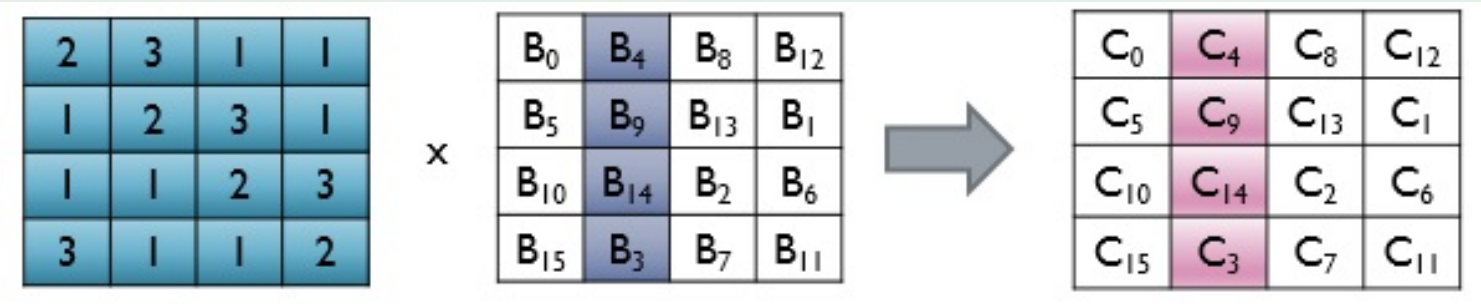
B_0	B_4	B_8	B_{12}
B_5	B_9	B_{13}	B_1
B_{10}	B_{14}	B_2	B_6
B_{15}	B_3	B_7	B_{11}

Algorithme AES : MIXCOLUMNS

MIXCOLUMNS

- Une transformation linéaire qui mixe les colonnes de la matrice
- Chaque colonne est multipliée par une matrice fixe C

MIXCOLUMNS



Algorithme AES : XOR clé (ADDROUNDKEYS)

ADDROUNDKEYS

- Cette opération consiste en un XOR de la matrice STATE résultant de l'opération MIXCOLUMNS et de la clef du tour
- Les sous clés sont générées dans l'étape de diversification

Algorithme AES : Diversification

Génération des clés

- Génération des sous clés pour les Rounds
- Les sous clés sont dérivées récursivement à partir de la clé initiale
- Utilisation d'un algorithme de diversification

Algorithme AES : Diversification

Diversification

1. G : une fonction qui réalise
   1. rotation entre les 4 octets en entrée
   2. substitution des octets à l'aide de l'S-box
2. RC (Round coefficient) est un coefficient ajouté à l'octets le plus à gauche
   1. RC[i]= $x^{i-1} mod x^8 + x^4 + x^3 + x + 1$
   2. RC[1] = x^0 = (00000001)2
   3. RC[2] = x^1 = (00000010)2
   4. ...
   5. RC[10] = x^9 = (00110110)2