Confidentialité I : Chiffrement symétrique

Cours 02

Ahmed Amou El Arby

Confidentialité par chiffrement

Une des principales méthodes pour assurer la confidentialité des données est le chiffrement.

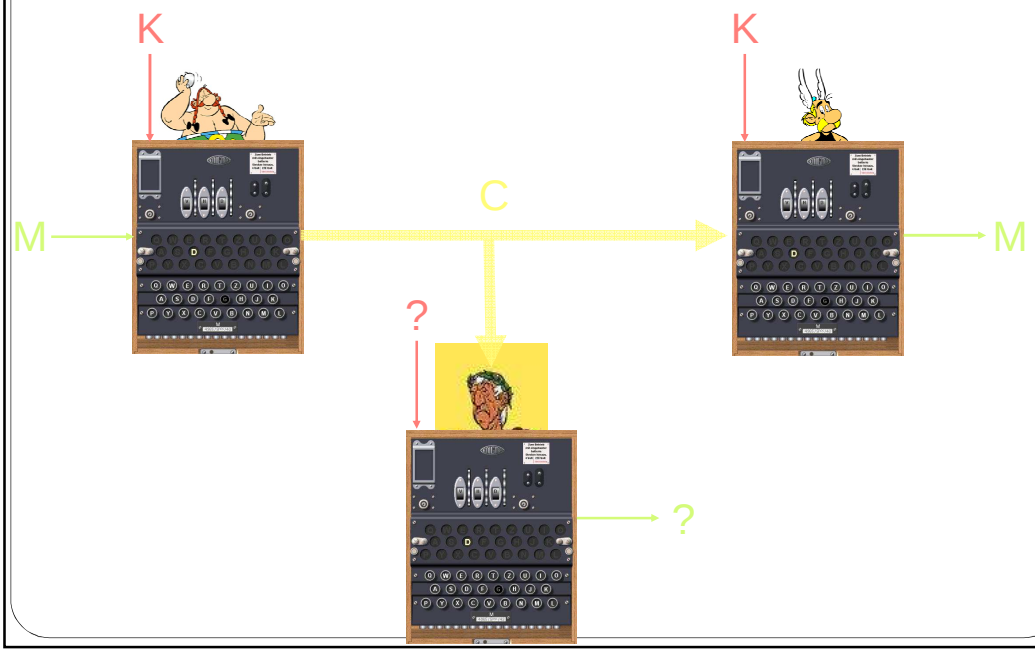
Les méthodes de chiffrement offrent deux outils qui fonctionnent à partir d'une clé :

$C := E_K(M)$ chiffre le message M avec la clé K ;

$D_{K'}(C)$ déchiffre le message C avec la clé K'.

Nous voulons que, sans connaître la clé K, $C=E_K(M)$ ne donne pas d'information sur M.

Le scénario



Le seul chiffre parfaitement sûr

A 0 B 1 Y 24 Z 25

F Y 5 24
29
3
D

Ce chiffre est appelé chiffre de **Vernam** ou **masque jetable** («one-time pad»)

nécessite une clé de 4 lettres!

K M

K M

QZAB

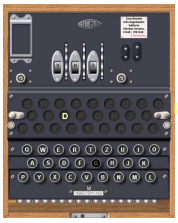
Q Q A
M Z L
L A L
P B O

QZAB

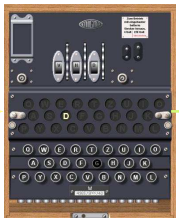
Q Q A
M Z L
L A L
P B O

Un message de 4 lettres

ALL
O



QML
P



ALL
O

Dans la pratique

Un système de chiffrement devrait nécessiter une clé secrète de longueur indépendante de la longueur du message à transmettre.

Un système de chiffrement devrait permettre de chiffrer plusieurs messages avec la même clé.

Malheureusement, il n'est pas possible qu'un tel système cache toute l'information sur le message clair même à un adversaire qui ne connaît rien sur la clé secrète!

Nous sommes dans l'impasse!

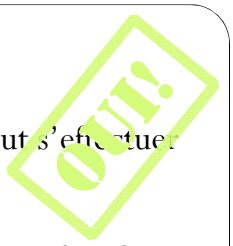
Une autre approche

Relaxons un peu la condition qu'un chiffre ne doit pas donner d'information sur le message clair :

> Un cryptogramme C ne doit pas donner d'information sur le message clair M à quiconque ne pouvant essayer les déchiffrements de C avec (presque) toutes les clés.
>
> Noter que si l'adversaire avait le temps de calculer tous les déchiffrements possibles de C, alors il pourrait sans doute déterminer de l'information sur M en conservant les messages qui sont bien formés.
>
> Une attaque de ce type est appelée « recherche exhaustive de clés ».

Notre notion de sécurité relaxée dira d'un système de chiffrement qu'il est sûr s'il ne peut être attaqué que par la recherche exhaustive de clés.

Est-ce raisonnable?



Supposons que le déchiffrement de C avec clé K peut s'effectuer en 1μs sur un ordinateur (ce qui est pas mal rapide).

Combien de temps est nécessaire pour effectuer une recherche exhaustive de clés lorsque la clé est de longueur :

16 bits? 2^{16} X 10^{-6}sec = 65536 X 10^{-6} = 0,06 sec.

32 bits? 2^{32} X 10^{-6}sec = 4295 secs.

64 bits? 15848931924611secs = 584 940 années.

128 bits? 2^{64} X 584 940 années >>>>>>> l'âge de l'univers!

Chiffres symétriques

Un chiffre est appelé symétrique si la clé de chiffrement est la même que celle pour le déchiffrement.

La clé peut être réutilisée pour le chiffrement de plusieurs messages.

Ces systèmes sont habituellement très performants!

La longueur des clés secrètes doit être assez grande pour exclure la recherche exhaustive des clés. Ceci n'est cependant pas une garantie de sécurité…

Un peu d'histoire

Le chiffre de César:

Chiffrement :

A->D, B->E, C->F,…, X->A, Y->B, Z->C.

Déchiffrement :

A->X, B->Y, C->Z,…, X->U, Y->V, Z->W.

Quand César transmettait le message :

UHWLUHCYRXV alors

RETIREZVOUS…..

Le chiffre de César n'a donc pas de clé secrète!!!!!

César avec une clé!

Nous pouvons facilement ajouter une clé au chiffre de César.

La clé est $0 \leq K \leq 25$ et indique le décalage appliqué à chaque lettre du message. Le chiffre de César est le cas spécial $K=3$.

Pour montrer que ce chiffre est peu sûr, essayez de déchiffrer :

ID RTHR UDMV IZH UT IZH UZHMBV!

26 clés possibles est bien trop peu!!!!

Alphabet mélangé

(chiffrement par substitution monoalphabétique)

Dans ce chiffre, la clé correspond à une permutation des lettres de l'alphabet :

[A,B,C,D,E,F,G,H,I,J,K,L,M,N,O,P,Q,R,S,T,U,V,W,X,Y,Z]

[D,H,Q,A,X,E,W,T,U,P,L,G,M,V,K,I,B,Y,Z,C,F,J,K,N,S,O]

ELEPHANTESQUE -> XGXITDVCXZBFX

Le nombre de clés possibles est $26! = 4.03 \text{ X } 10^{26} > 2^{91}$!

Est-ce sûr?

Cryptanalyse statistique

Remarquez qu'étant donné un message chiffré C, le tableau des fréquences des lettres de C contient les mêmes valeurs que celui des lettres du message clair M.

Si M est un message en français, la lettre la plus fréquente est 'E'. Ainsi, il est très probable que la lettre la plus fréquente de C soit en fait la version chiffrée de 'E'.

La procédure peut être répétée. La deuxième lettre la plus fréquente en français est le 'A'. On s'attend à ce que la lettre de C, deuxième quant à sa fréquence, devrait être la version chiffrée de 'A'.

En continuant ainsi, beaucoup d'information sur le message M peut être obtenue à partir de C.

Même avec plus de 2^{91} clés possibles, M n'est pas chiffré de façon sûre!

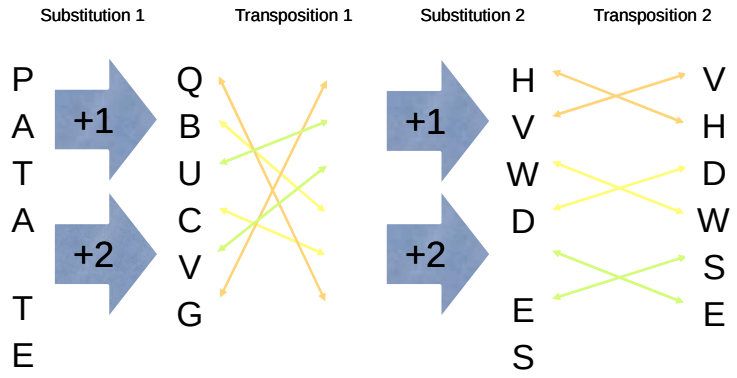
L'analyse fréquentielle a été découverte par Al Kindi au 9e siècle, peut-être en étudiant le Coran (il faut des textes écrits pour y parvenir!).

Substitutions et transpositions

Shannon (1949) propose d'utiliser des fonctions pour créer des transformations de mixage qui distribuent les messages intelligibles uniformément sur l'ensemble des messages chiffrés possibles.

Un exemple commun est l'utilisation de transpositions (permutations), de substitutions et d'opérations linéaires simples.

Évidemment, toutes ces opérations doivent être inversibles pour permettre le déchiffrement…



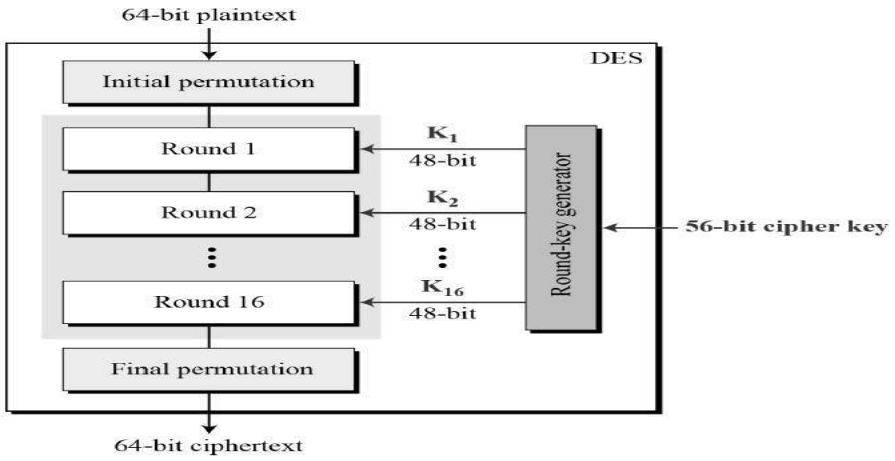
Data Encryption Standard (DES)

DES est un standard NIST (des années 1970) pour le chiffrement à clé secrète de blocs de données de taille fixe. Sa version la plus simple (et la moins sûre) :

Chiffre des blocs de données de 64 bits.

La clé secrète est longue de 56 bits (en fait 64 bits dont 8 bits servent à tester la parité de chaque bloc de 8 bits de clé).

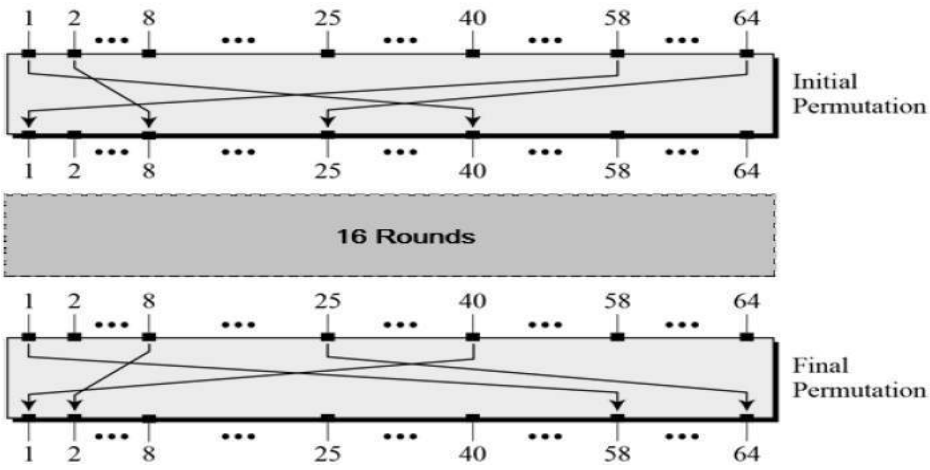
Data Encryption Standard (DES) (suite)



- DES se decompose en trois parties:
  - Initial and Final Permutation
  - Round Function
  - Key Generation

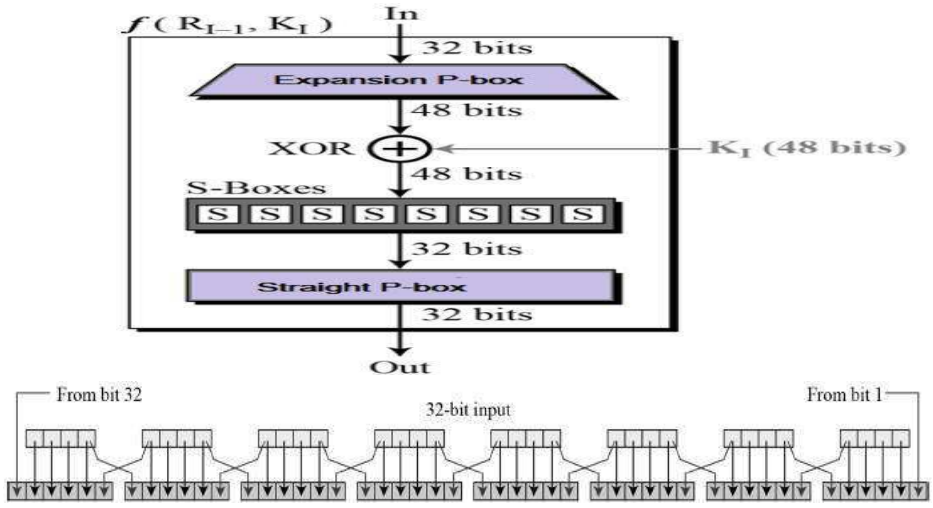
Data Encryption Standard (DES) (suite)

- Permutation Initiale et Final



Data Encryption Standard (DES) (suite)

- Fonction Rondes

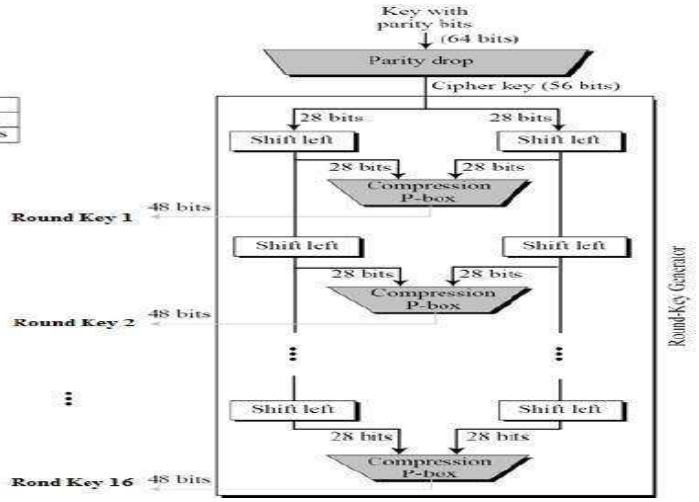


Data Encryption Standard (DES) (suite)

- Génération des Clefs

Shifting

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



L'insécurité de DES simple

Une clé de 56 bits n'est pas suffisante pour s'assurer qu'une fouille exhaustive des clés n'est pas possible. C'est probablement pourquoi ce système de chiffrement a été adopté comme tel (72,057,594,037,927,936 clés) :

De nombreux processeurs peuvent déchiffrer plus de 92 m[illions] 72 Billiards sec. Un grand organisme peut accomplir une fouille exhaustive en déchiffrant en parallèle à l'aide de plusieurs machines.

Des machines dédiées peuvent briser DES pour moins de 100 000 $ en quelques heures.

Des versions plus fortes ont été proposées. Triple-DES est un système de chiffrement avec 112 bits de clé très utilisé dans le monde bancaire:

$3DES_{KK'}(M) = DES_K(DES_{K'}^{-1}(DES_K(M)))$.

chiffrements plus 1 déchiffrement DES avec deux clés sont nécessaires pour éviter certaines attaques.

Briser DES (56 bits)

AES: Advanced Encryption Standard

Le système DES a été remplacé pour un nouveau système appelé AES : Advanced Encryption Standard.

Il est devenu le nouveau standard NIST en 2001.

Sa conception est similaire à celle de DES.

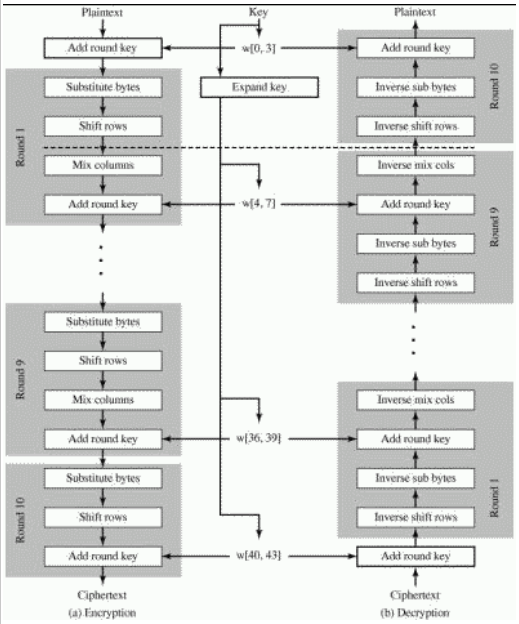
Il chiffre des blocs de 128 bits

avec des clés secrètes de 128, 192 ou 256 bits.

Consomme peu de mémoire et est très efficace.

Évidemment, il n'est pas plus sûr que DES, si un bon mode de fonctionnement n'est pas utilisé…

AES

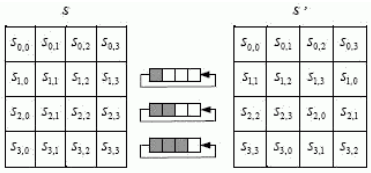


AddRoundKey : Calcul des XOR des octets du bloc à chiffrer avec la matrice de la clé courante.

SubByte : Substitue chaque octet du bloc à chiffrer.

Voyons 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.

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

Conclusion : chiffrement symétrique

Pour assurer que le chiffrement à clé secrète fonctionne comme il devrait :

Vous devez avoir un bon système de chiffrement par blocs,

Un mode de fonctionnement approprié et

Une bonne façon de choisir le vecteur d'initialisation.

Bien des réalisations posent IV=0, ce qui est une bien mauvaise idée....

Même dans ce cas, il se pourrait que le système ne soit pas sûr, car aucun de ceux-ci n'a été démontré comme tel.

Ces systèmes sont rapides : 1-10 Mo/sec sur un PC décent et beaucoup plus rapides sur du matériel dédié. Parfait pour le chiffrement de flux.

En général, à mesure que le nombre de messages chiffrés avec la même clé augmente, la sécurité se détériore.