Chapitre4 : La cryptographie

I- Introduction

- Définition et historique

II- cryptographie actuelle

III- Signatures et certificat numériques

IV- Applications de la cryptographie

I- Introduction

- Définition et historique

On parle de cryptographie depuis de Jules César qui envoyait des messages à ses généraux mais qui ne faisait pas confiance à ses facteurs.

- Lorsque ***Jules César*** envoyait des messages à ses généraux, il ne faisait pas confiance à ses messagers.

- Il remplaçait donc tous les **A** contenus dans ses messages par des **D**, les **B** par des **E**, et ainsi de suite pour tout l'alphabet.

- Seule la personne connaissant la règle du « **décalage par trois** » pouvait déchiffrer ses messages.

De la on a commencé à parler d'une information cachée modifiée, chiffré ..Etc, d'une manière générale. Aujourd'hui on retrouve la cryptographie dans plusieurs domaines.

De nos jours on retrouve de la cryptographie dans :

- Armée.
- Système bancaire.
- Internet (achat, identification).
- Téléphone portable.
- TV payante.
- Carte d'identité électronique.
- Vote électronique.

Pour protéger une information, on peut opter pour deux solutions :

- La Stéganographie : écriture couverte.
- La cryptographie

Dans la stéganographie, l'information n'est pas modifié, mais elle est plutôt cachée.

Durant l'antiquité, certains généraux rasaient le crâne de leurs esclaves, leur tatouaient un message et attendaient que les cheveux repoussent pour faire passer des informations importantes.

La stéganographie : écriture couverte

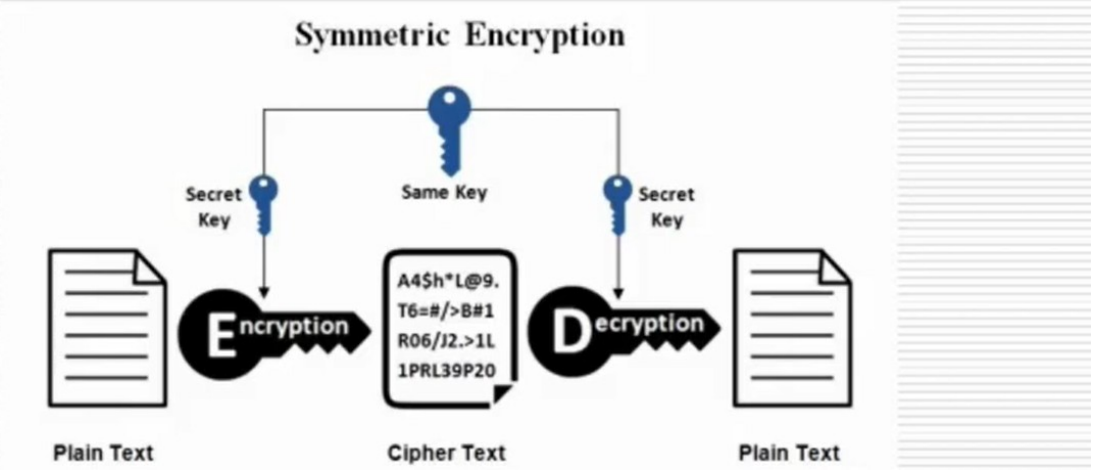
L'information est dissimulée au sein d'une autre information afin de la rendre invisible.

Il suffit de retrouver l'endroit où est cachée l'information dans le message pour retrouver le secret.

Par contre dans la cryptographie l'information est modifiée selon une méthode préétablie.

La cryptographie :

L'information est modifiée selon une méthode préétablie afin de la rendre incompréhensible.



C’est la méthode de chiffrement. Il s’agit de message clair qui va subir un certain nombre de modifications pour empêcher toute personne qui n’a pas les autorisations d’avoir accès à ces informations et faire des modifications, ou essayer de comprendre la signification ...Etc. La cryptographie, c’est beaucoup plus modifier l’information et non pas cacher l’information.

La cryptographie : Il existe deux grandes catégories :

- **Par transposition : l'ordre** des éléments d'une information est modifiée (**décalage** des caractères d'une phrase, pixels d'une image, ...)

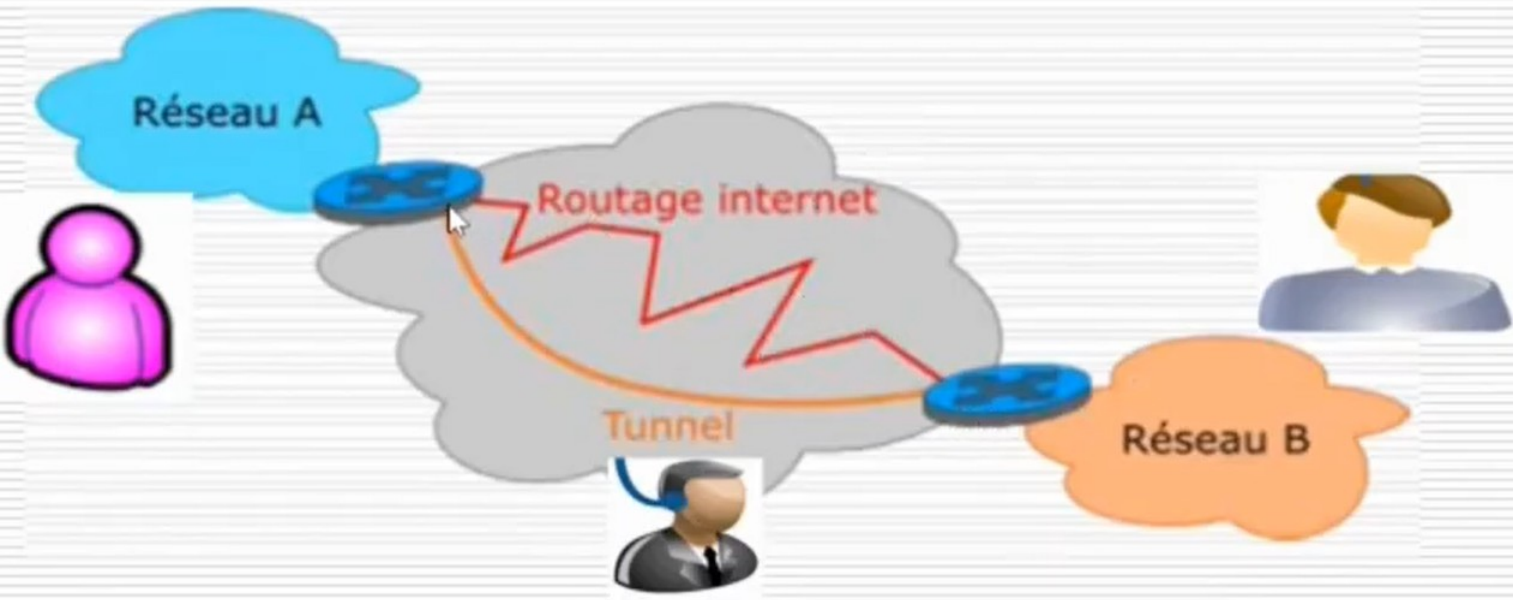
- **Par substitution** : les éléments d'une information sont **remplacés** par d'autres (**remplacer** tous les A par B, B par C, etc...)

II- cryptographie actuelle

Protagonistes traditionnels

- **Alice ou Anne** et **Bob** souhaitent se transmettre des données
- **Oscar ou Mallory**, un opposant qui souhaite espionner Alice et Bob.

Notre système de cryptographie, c'est de permettre par exemple à Bob et Ali de communiquer sur un canal de communication non sécurisé comme internet et d'empêcher le pirate d'avoir accès à cette information. C'est ça l'objectif de la cryptographie. Ça consiste à empêcher une personne intermédiaire de la communication entre Bob et Alice qui essaie d'espionner un canal de communication non sécurisé tel qu'internet, et on va essayer d'empêcher cette personne soit de le modifier, soit d'avoir accès à cette échange, soit de comprendre ce qui est échangé...Etc.



Message clair 'M': Cette expression désigne le message original n'ayant subi aucune modification

Clé: La clé désigne l'information permettant de chiffrer et de chiffrer/déchiffrer un message

Chiffrement:
Fonction de transformation d'un message M de telle manière à le rendre incompréhensible :

- Basé sur une fonction de chiffrement E
- On génère ainsi un message chiffré **C = E(M)**

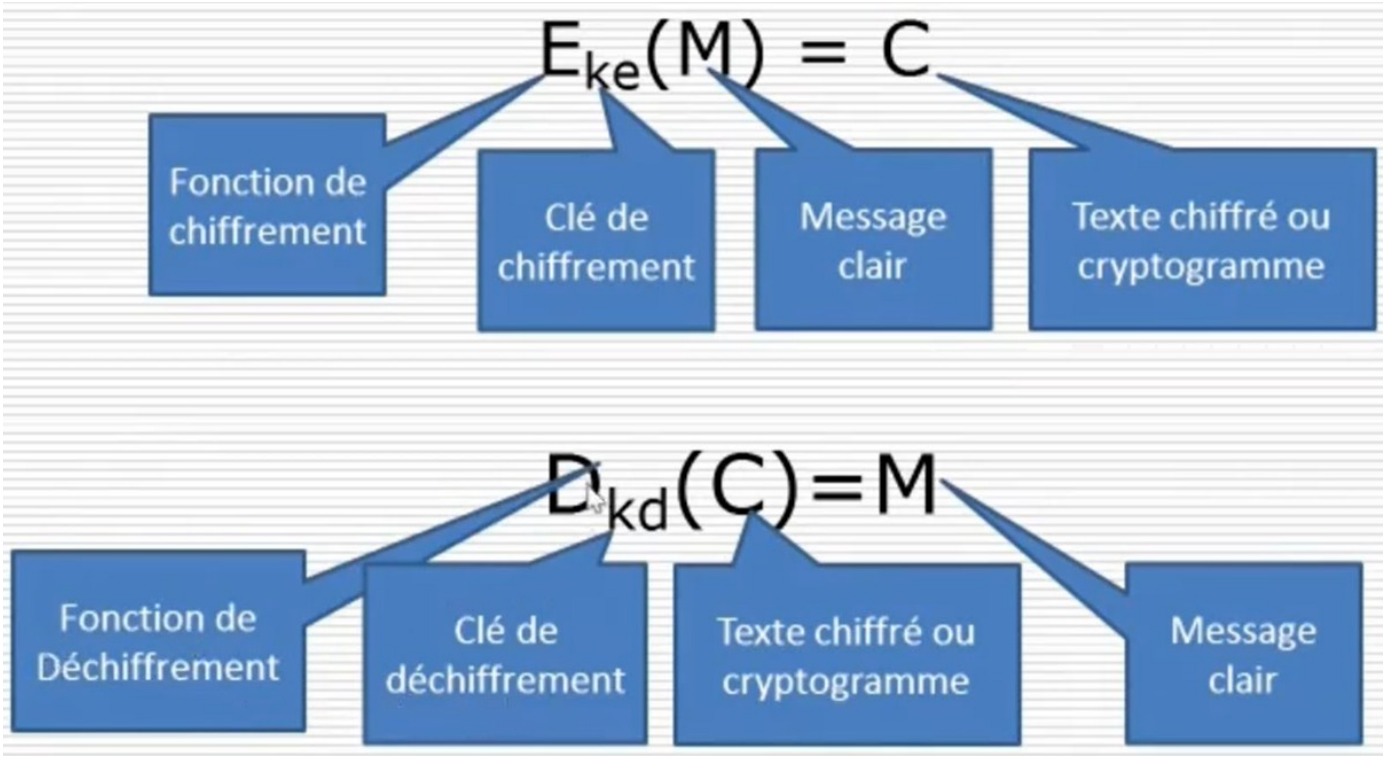
Déchiffrement:
Fonction de reconstruction du message clair à partir du message chiffré :

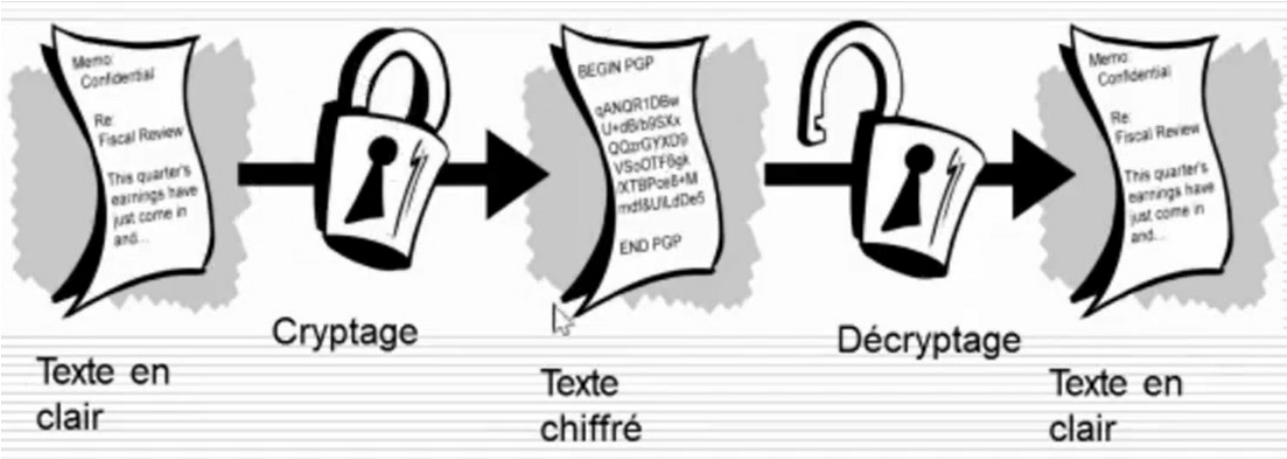
Basé sur une fonction de déchiffrement D
On a donc **D(C) = D(E(M)) = M**

En pratique : E et D sont généralement paramétrées par des clefs Ke et Kd :

- $E_{ke}(M) = C$
- $D_{kd}(C)=M$

Avec plus d'éclaircissement, nous avons les fonctions suivantes :


$E_{ke}(M) = C$
Fonction de chiffrement
Clé de chiffrement
Message clair
Texte chiffré ou cryptogramme
$D_{kd}(C) = M$
Fonction de Déchiffrement
Clé de déchiffrement
Texte chiffré ou cryptogramme
Message clair



Définitions
Cryptographie et cryptanalyse

- **La cryptographie** est la science qui utilise les mathématiques pour le cryptage et le décryptage de données.

- **La cryptanalyse** est l'étude des informations cryptées, afin d'en découvrir le secret.

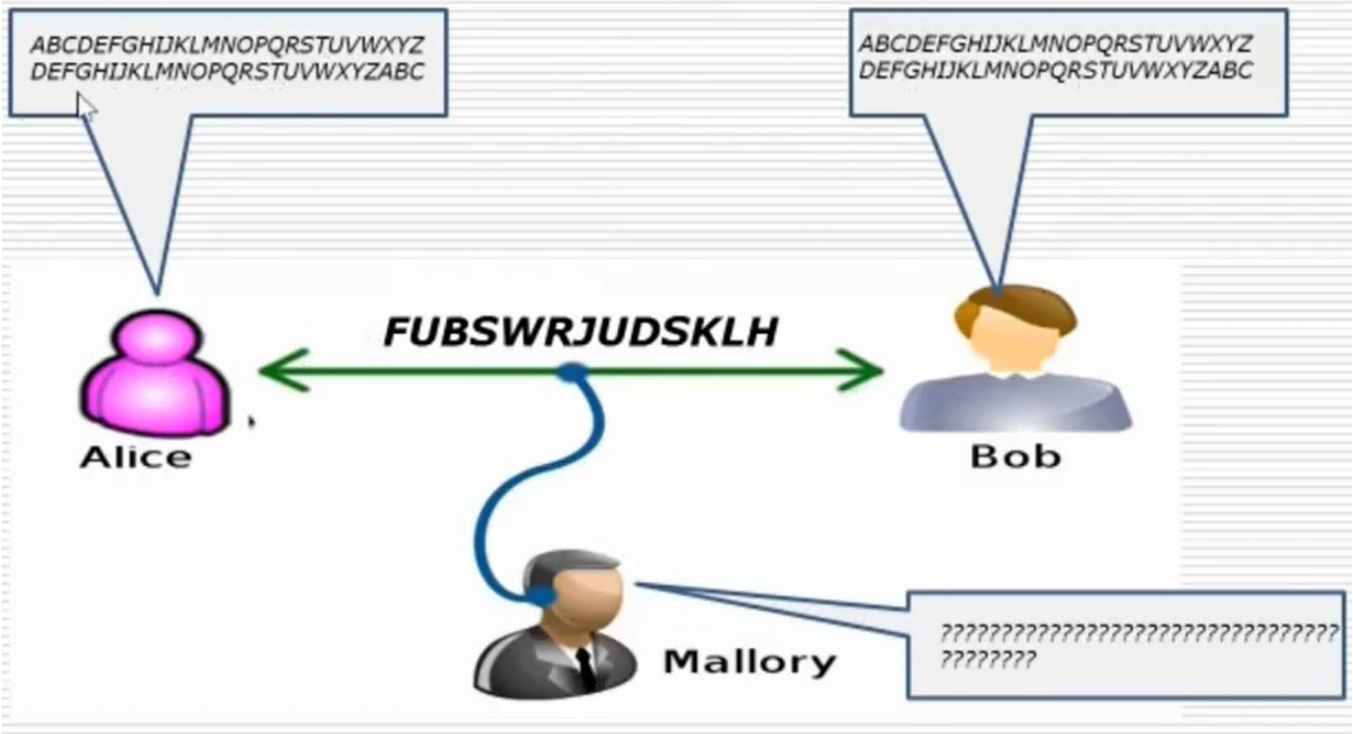
- **La cryptologie** englobe la cryptographie et la cryptanalyse

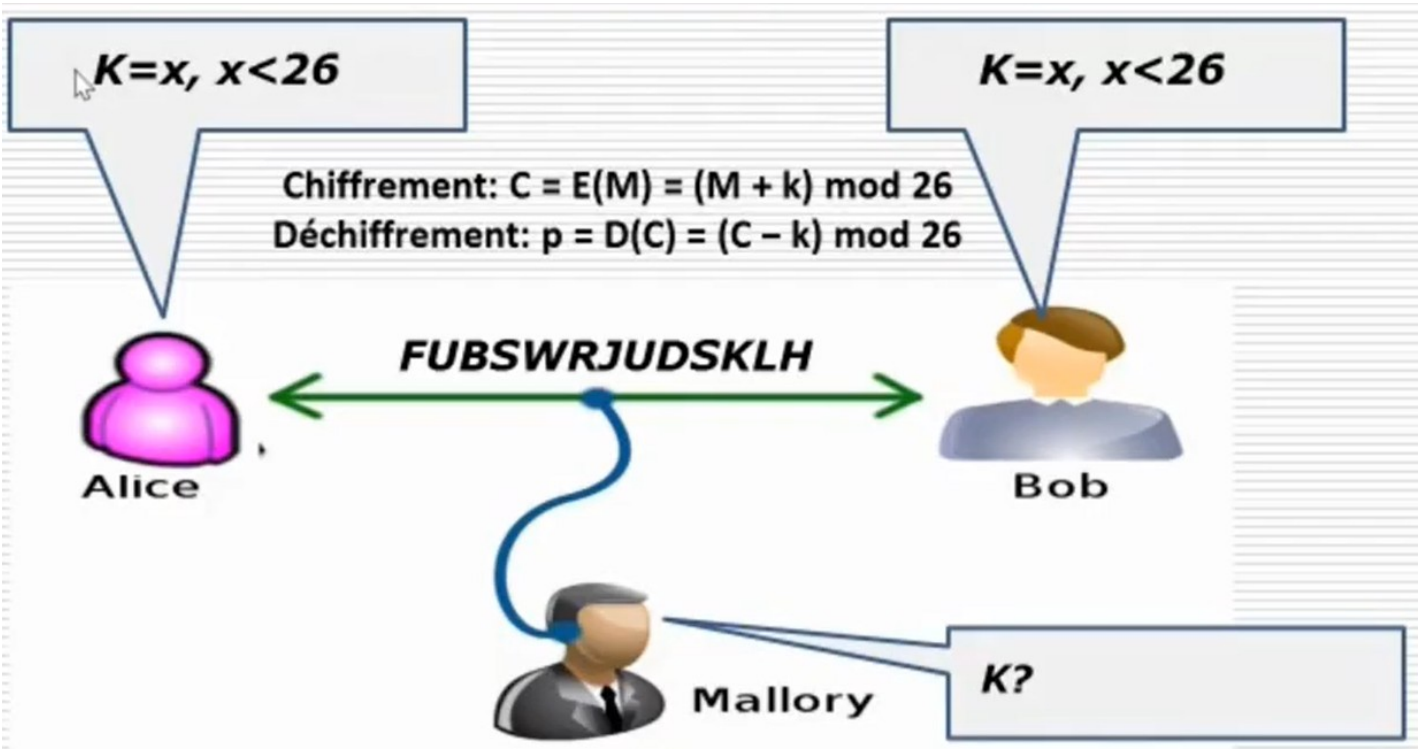
Le Chiffrement de César

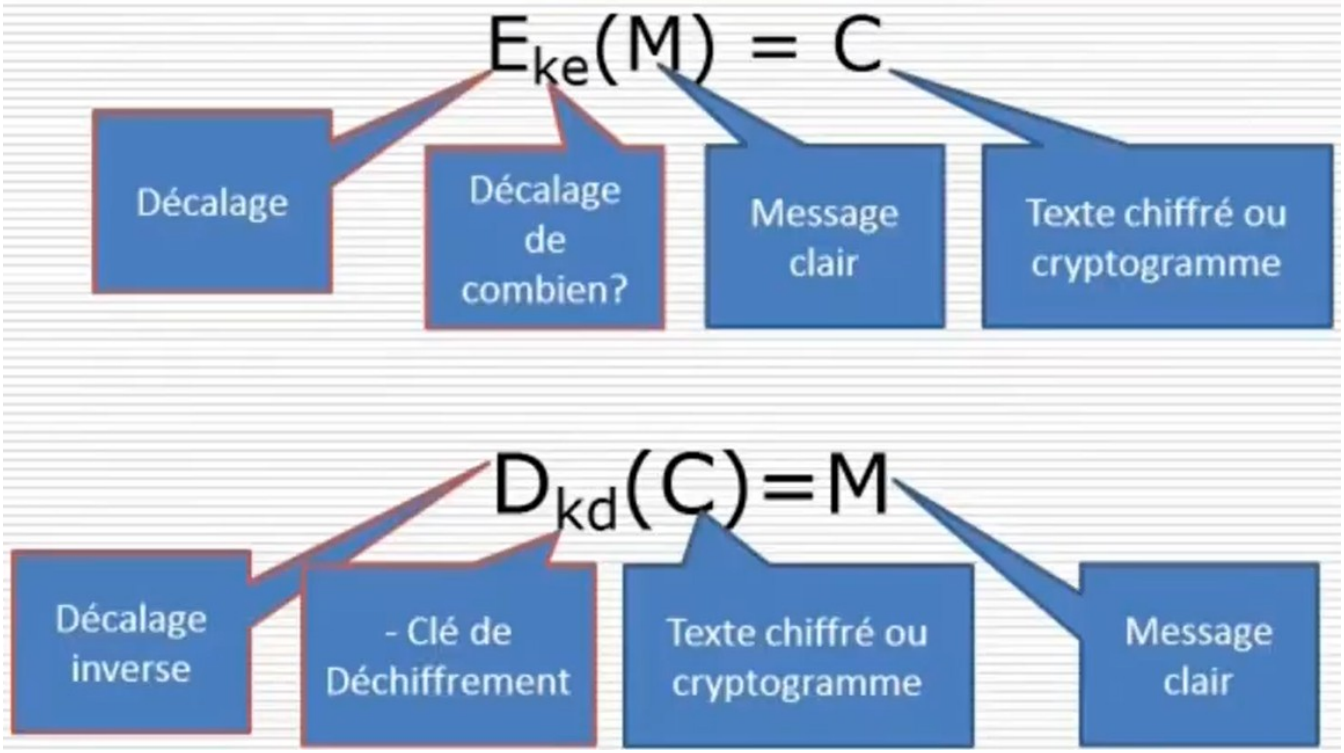
Consiste à décaler l'alphabet clair. Le décalage est la clé du chiffrement

Exemple :
On veut chiffrer le mot *CRYPTOGRAPHIE avec un* décalage de 3. Pour cela on écrit les alphabets clair et chiffré comme suit :

ABCDEFGHIJKLMNOPQRSTUVWXYZ
DEFGHIJKLMNOPQRSTUVWXYZABC
Et on remplace:
CRYPTOGRAPHIE ---> FUBSWRJUDSKLH




K=x, x<26
K=x, x<26
Chiffrement: C = E(M) = (M + k) mod 26
Déchiffrement: p = D(C) = (C – k) mod 26
FUBSWRJUDSKLH
Alice
Bob
Mallory
K?


$E_{ke}(M) = C$
Décalage
Décalage de combien?
Message clair
Texte chiffré ou cryptogramme
$D_{kd}(C) = M$
Décalage inverse
- Clé de Déchiffrement
Texte chiffré ou cryptogramme
Message clair

Chiffrement de César – Cryptanalyse

Faiblesse du chiffre de César:

- Il n'y a que 26 clés possibles !
- Donc étant donnée un message chiffré, il suffit de tester les 26 clés possibles pour retrouver le message clair.
- Cela se fait en quelques minutes !!

Solution:

Utiliser un alphabet chiffré aléatoirement

C'est ce qu'on appelle cryptanalyse par force brute.

Substitution aléatoire

Exemple :
ABCDEFGHIJKLMNOPQRSTUVWXYZ
OHGFEDCBUKJPNMIQRXSTLZXYWV

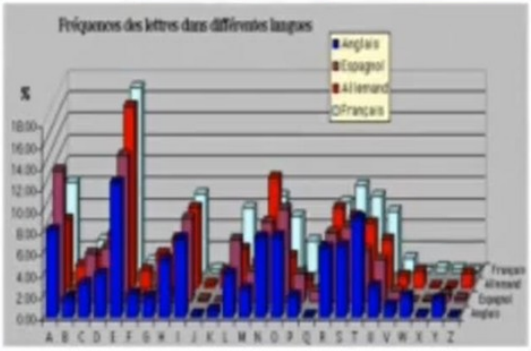
Dans ce cas, le nombre de clés possibles passe à **400 000 000 000 000 000 000 000 000 !!!**

Cryptanalyse:
Il est évident impossible de tester toutes les clés possibles, même une machine est incapable de le faire en un temps raisonnable (**300 000** ans pour un ordinateur très puissant !!).

Rang	Caractère	Nombre d'occurrences	Pourcentage
1	e	115 024 205	12,10
2	a	67 563 628	7,11
3	i	62 672 992	6,59
4	s	61 882 785	6,51
5	n	60 728 196	6,39
6	r	57 656 209	6,07
7	t	56 267 109	5,92
8	o	47 724 400	5,02
9	l	47 171 247	4,96
10	u	42 698 875	4,49
11	d	34 914 685	
12	c	30 219 574	
13	m	24 894 034	
14	p	23 647 179	
15	é	18 451 937	
17	g	11 684 140	
18	b	10 817 171	
19	v	10 590 858	
20	h	10 583 562	
21	f	10 579 192	
28	q	6 140 307	

Statistique selon la langue française

Rang	Caractère	Nombre d'occurrences	Pourcentage
1	h	115 024 205	12,10
2	j	67 563 628	7,11
3	e	62 672 992	6,59
4	k	61 882 785	6,51
5	u	60 728 196	6,39
6	p	57 656 209	6,07
7	w	56 267 109	5,92
8	x	47 724 400	5,02
9	r	47 171 247	4,96
10	v	42 698 875	4,49
		34 914 685	3,67
		30 219 574	3,18
		24 894 034	2,62
		23 647 179	2,49
		18 451 937	1,94
		11 684 140	1,23
		10 817 171	1,14
		10 590 858	1,11
		10 583 562	1,11
		10 579 192	1,11
		6 140 307	0,65



Statistique du texte chiffré

Pourtant il est possible là encore de casser ce chiffrement en quelques minutes !!

Dans la langue française, par exemple, on sait que la fréquence d'apparition de chaque lettre est à peu près stable. Il suffit donc à:

- Mesurer la fréquence d'apparition de chaque lettre d'un texte chiffré
- Comparer avec la table des fréquences des lettres françaises
- Déduire l'alphabet chiffré

Autres systèmes classiques

- Les homophones (solution pour attaque par stat)
- Chiffre affine (polynôme)
- Chiffre de Playfair (Chiffrement polygraphique)
- Chiffre de Hill (Matrices)
- Chiffre de Vigenère (amélioration du chiffre de César)
- Chiffre de Vernam (masque jetable)
- Transpositions
- ...
- La machine Enigma
- ...

Au prochain cours nous parlerons de la cryptographie moderne.

Cryptographie moderne