Institut Supérieur des Mathématique Appliquées et d'Informatique

Cours : Cryptographie

Enseignante : Dhikra Saffar Amira

1ere année mastère ASSIR

Plan

- **Chapitre I :** Introduction à la cryptographie
- **Chapitre II :** La cryptographie classique
- **Chapitre III :** Complément mathématique
- **Chapitre IV :** Le chiffrement par bloc
- **Chapitre V:** Chiffrement par clé publique

Institut Supérieur des Mathématique Appliquées et d'Informatique

Chapitre I

Introduction à la Cryptographie

Enseignante : Dhikra Saffar Amira

1ere année mastère ASSIR

Vocabulaire de base

- **Cryptologie :** Il s'agit d'une science mathématique comportant deux branches : la cryptographie et la cryptanalyse

- **Cryptographie :** La cryptographie est l'étude des méthodes donnant la possibilité d'envoyer des données de manière confidentielle sur un support donné.

- **Chiffrement :** Le chiffrement consiste à transformer une donnée (texte, message, ...) afin de la rendre incompréhensible par une personne autre que celui qui a créé le message et celui qui en est le destinataire.

- **Déchiffrement:** La fonction permettant de retrouver le texte clair à partir du texte chiffré.

Vocabulaire de base

- **Texte chiffré :** Appelé également cryptogramme, le texte chiffré est le résultat de l'application d'un chiffrement à un texte clair.
- **Clef :** Il s'agit du paramètre impliqué et autorisant des opérations de chiffrement et/ou déchiffrement.
- **Algorithme symétrique**, la clef est identique lors des deux opérations.
- **Algorithmes asymétriques**, la clef diffère pour les deux opérations
- **Cryptanalyse :** Opposée à la cryptographie, elle a pour but de retrouver le texte clair à partir de textes chiffrés en déterminant les failles des algorithmes utilisés.
- **Cryptosystème :** Il est défini comme l'ensemble des clés possibles (espace de clés), des textes clairs et chiffrés possibles associés à un algorithme donné.

Objectifs

- **La confidentialité d'informations**

- Historiquement la première utilisation

- Concept permettant de s'assurer que l'information ne peut être lue que par les personnes autorisées

- **L'authentification**

- S'assurer de l'identité de l'émetteur du message

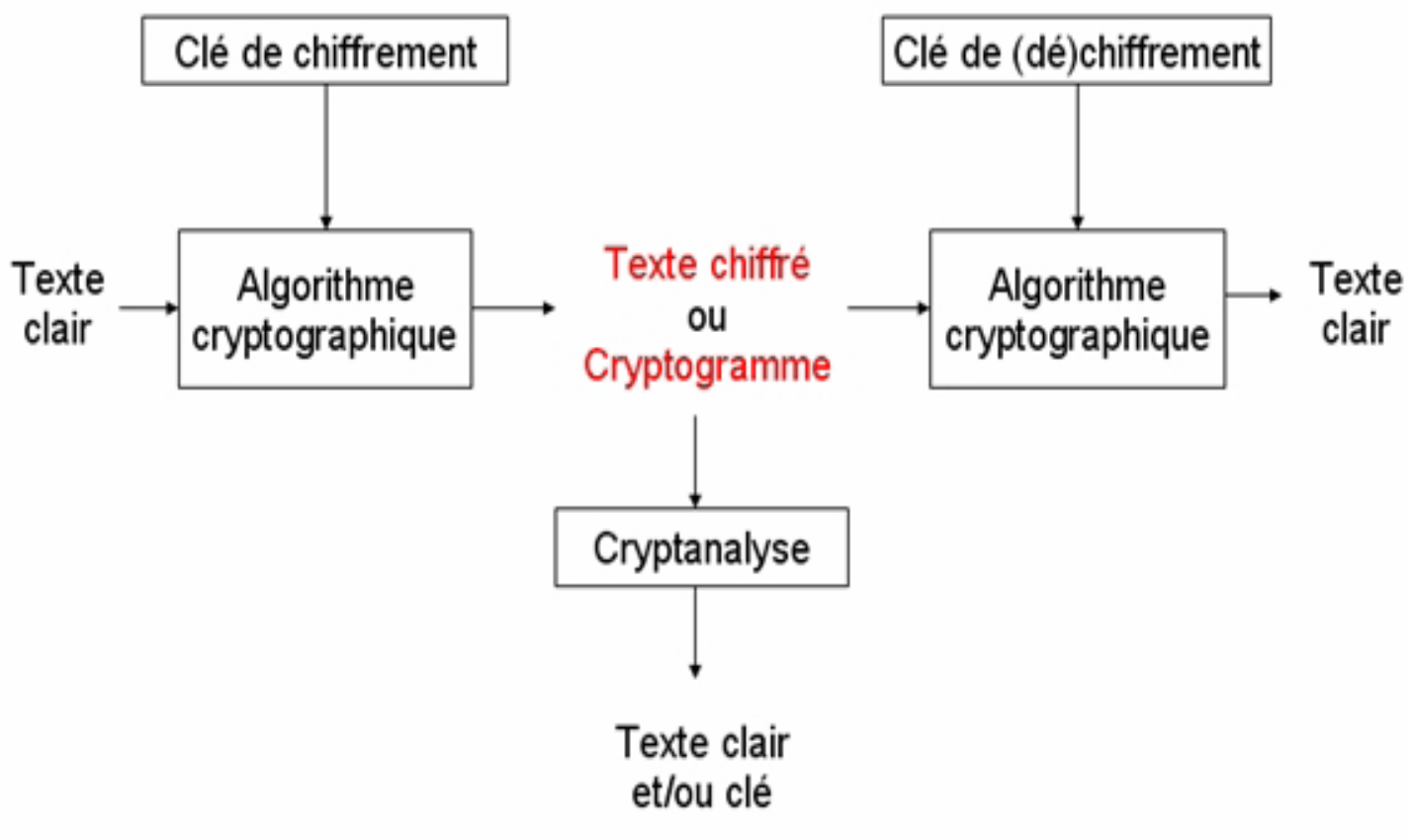
- **Le contrôle d'intégrité**

- Détecter toute altération d'information (stockée ou transmise)

- **La non-répudiation**

- Empêcher un expéditeur de pouvoir nier son envoi

Vocabulaire de base



Protocole de chiffrement

Notation

- En cryptographie, la propriété de base est que

M = D(E(M))

– M représente le texte clair,

– C est le texte chiffré,

– K est la clé (dans le cas d'un algorithme à clé symétrique), Ek et Dk dans le cas d'algorithmes asymétriques,

– E(x) est la fonction de chiffrement

– D(x) est la fonction de déchiffrement.

Les principaux concepts cryptographique

- Crypto système à clé symétrique
- Crypto système à clé publique
- Fonction de hachage
- Protocoles cryptographiques

- Confidentialité
- Intégrité
- Authentification

Crypto système à clé symétrique

- Caractéristiques :

- Les clés sont identiques : KE = KD = K,

- La clé doit rester secrète,

- Les algorithmes les plus répandus sont le DES, AES, 3DES, ...

- Ces algorithmes sont basés sur des opérations de transposition et de substitution des bits du texte clair en fonction de la clé,

- La taille des clés est souvent de l'ordre de 128 bits. Le DES en utilise 56, mais l'AES peut aller jusque 256,

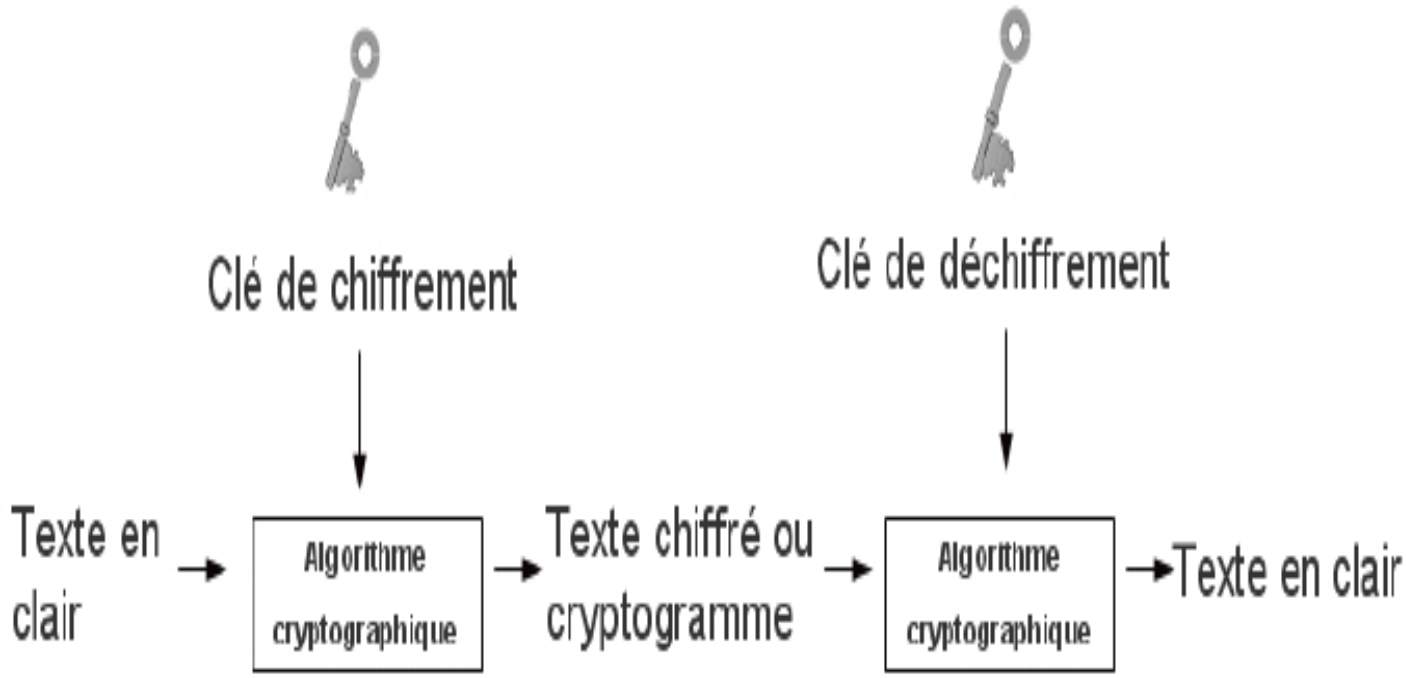
Crypto système à clé symétrique

- L'avantage principal de ce mode de chiffrement est sa rapidité,

- Le principal désavantage réside dans la distribution des clés : pour une meilleure sécurité, on préfèrera l'échange manuel.

- Pour de grands systèmes, le nombre de clés peut devenir conséquent. C'est pourquoi on utilisera souvent des échanges sécurisés pour transmettre les clés. En effet, pour un système à N utilisateurs, il y aura $N.(N-1)/2$ paires de clés.

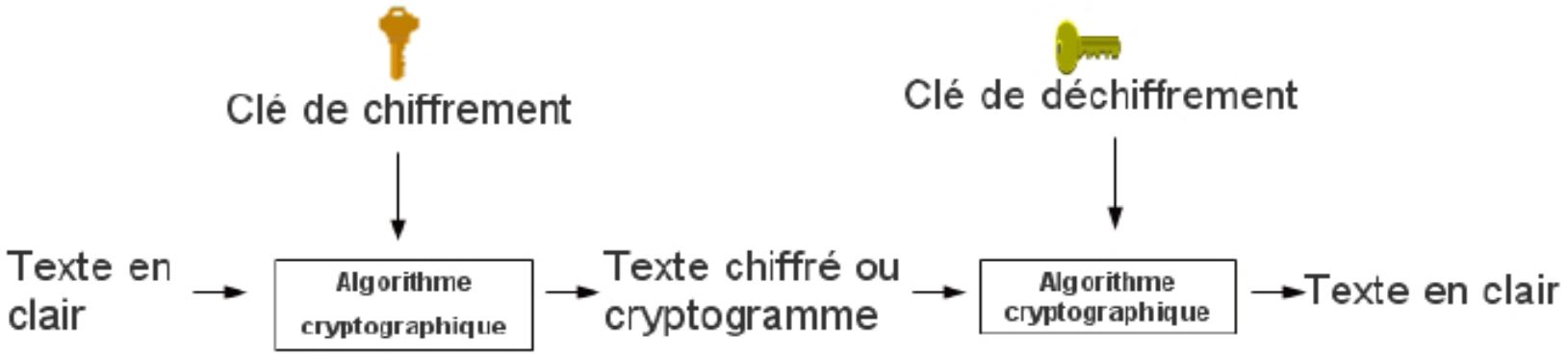
Crypto système à clé symétrique



Crypto système à clé publique

- Caractéristiques :

– Une clé publique PK (symbolisée par la clé verticale),
– Une clé privée secrète SK (symbolisée par la clé horizontale),
– Propriété : La connaissance de PK ne permet pas de déduire SK,
– $D_{SK}(E_{PK}(M)) = M$,
– L'algorithme de cryptographie asymétrique le plus connu est le RSA,



Crypto système à clé publique

- Les algorithmes se basent sur des concepts mathématiques tels que l'exponentiation de grands nombres premiers (RSA), le problème des logarithmes discrets (ElGamal), ou encore le problème du sac à dos (Merkle-Hellman).

- La taille des clés s'étend de 512 bits à 2048 bits en standard.

- Chaque utilisateur conserve sa clé secrète sans jamais la divulguer. Seule la clé publique devra être distribuée.

Crypto système à clé publique

- Au niveau des performances, le chiffrement par voie asymétrique est environ 1000 fois plus lent que le chiffrement symétrique.

- Cependant, à l'inverse du chiffrement symétrique où le nombre de clés est le problème majeur, ici, seules n paires sont nécessaires. En effet, chaque utilisateur possède une paire (SK, PK) et tous les transferts de message ont lieu avec ces clés.

- La distribution des clés est facilitée car l'échange de clés secrètes n'est plus nécessaire.

Fonction de hachage

- Un message clair de longueur quelconque doit être transformé en un message de longueur fixe inférieure à celle de départ.
- Le message réduit portera le nom de "Haché" ou de "Condensé".
- Intérêt : Utiliser ce condensé comme empreinte digitale du message original afin que ce dernier soit identifié de manière univoque.
- Caractéristiques :

1) Ce sont des fonctions unidirectionnelles :

A partir de H(M) il est impossible de retrouver M

2) Ce sont des fonctions sans collisions :

A partir de H(M) et M il est impossible de trouver M'≠M

tel que H(M') = H(M).

Protocoles cryptographiques

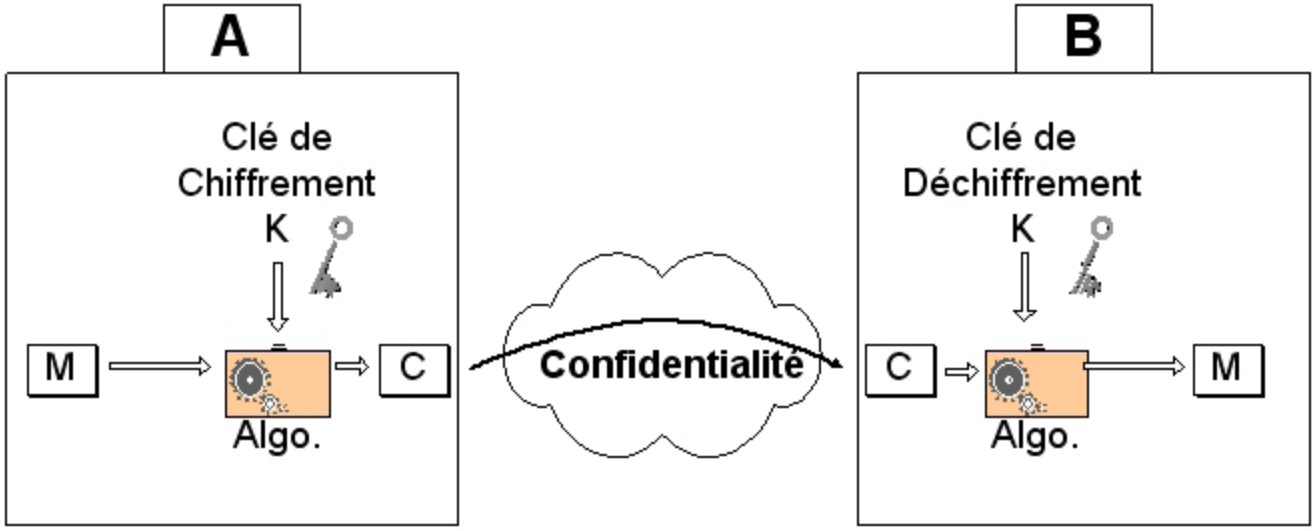
- plusieurs entités sont impliquées dans un échange de messages sécurisés.

- protocoles cryptographiques : Les règles qui déterminent l'ensemble des opérations cryptographiques à réaliser, leur séquence, afin de sécuriser la communication.

- Sécuriser un échange : 3 services :

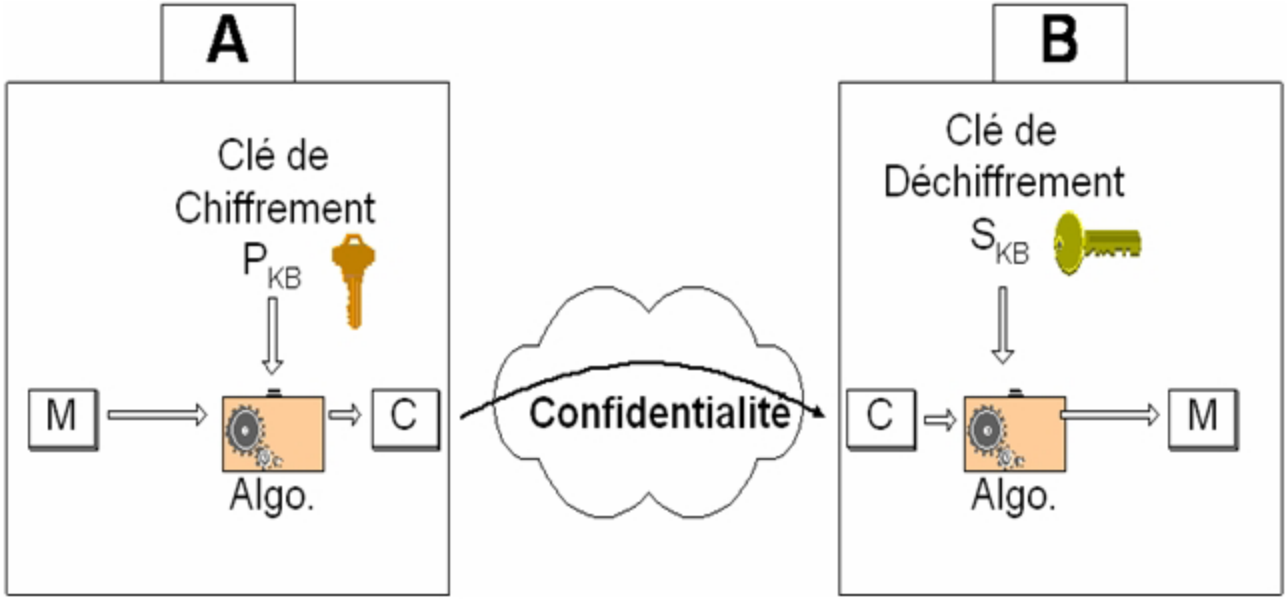
- la confidentialité
- l'intégrité
- l'authentification

Confidentialité



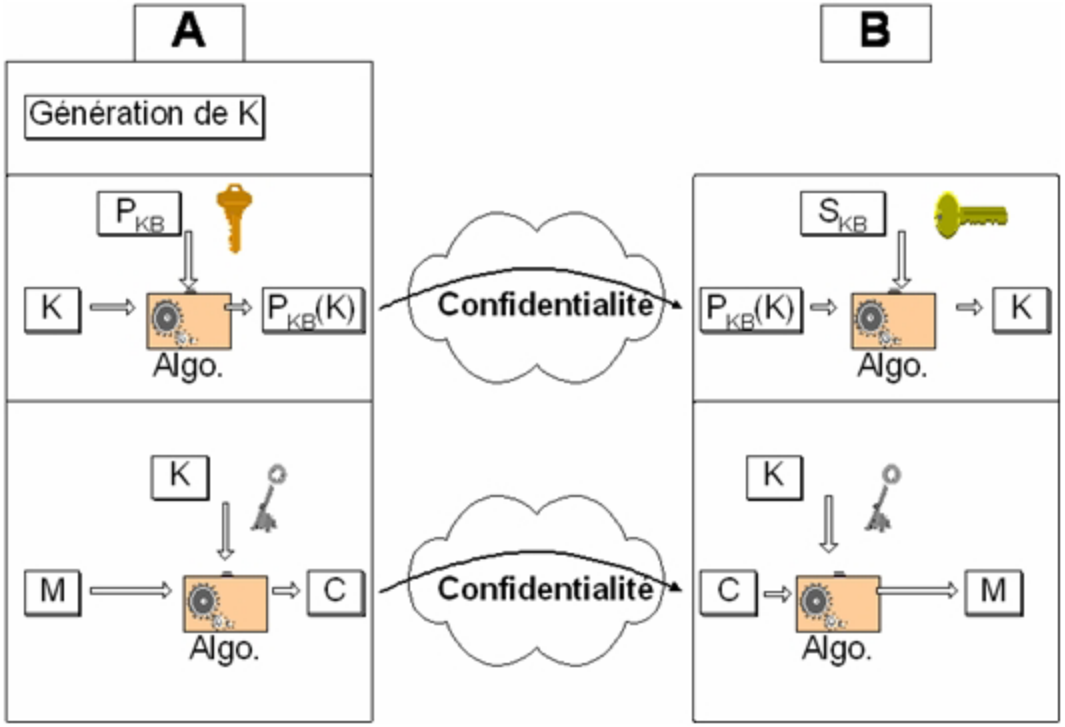
Confidentialité d'un système symétrique

Confidentialité



Confidentialité d'un système asymétrique

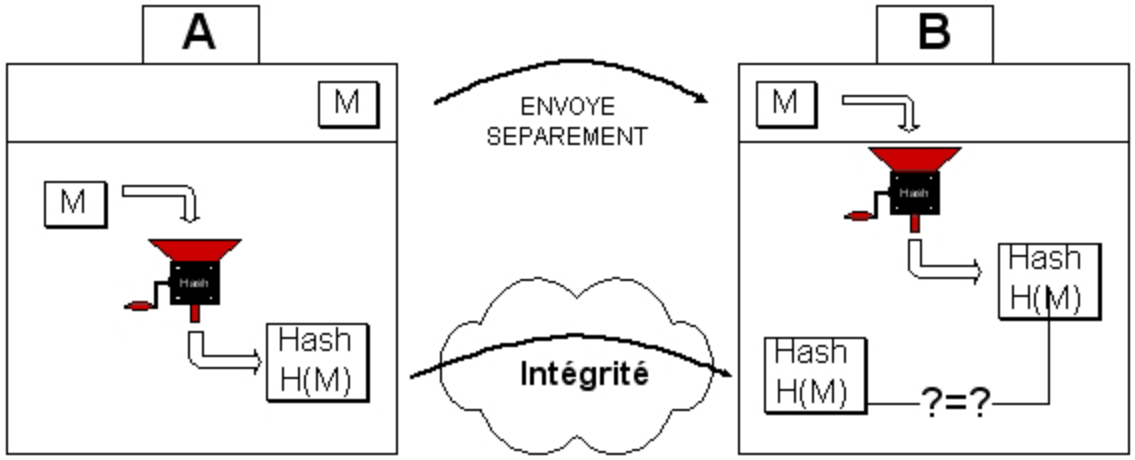
Confidentialité



Confidentialité d'un système hybride

Intégrité

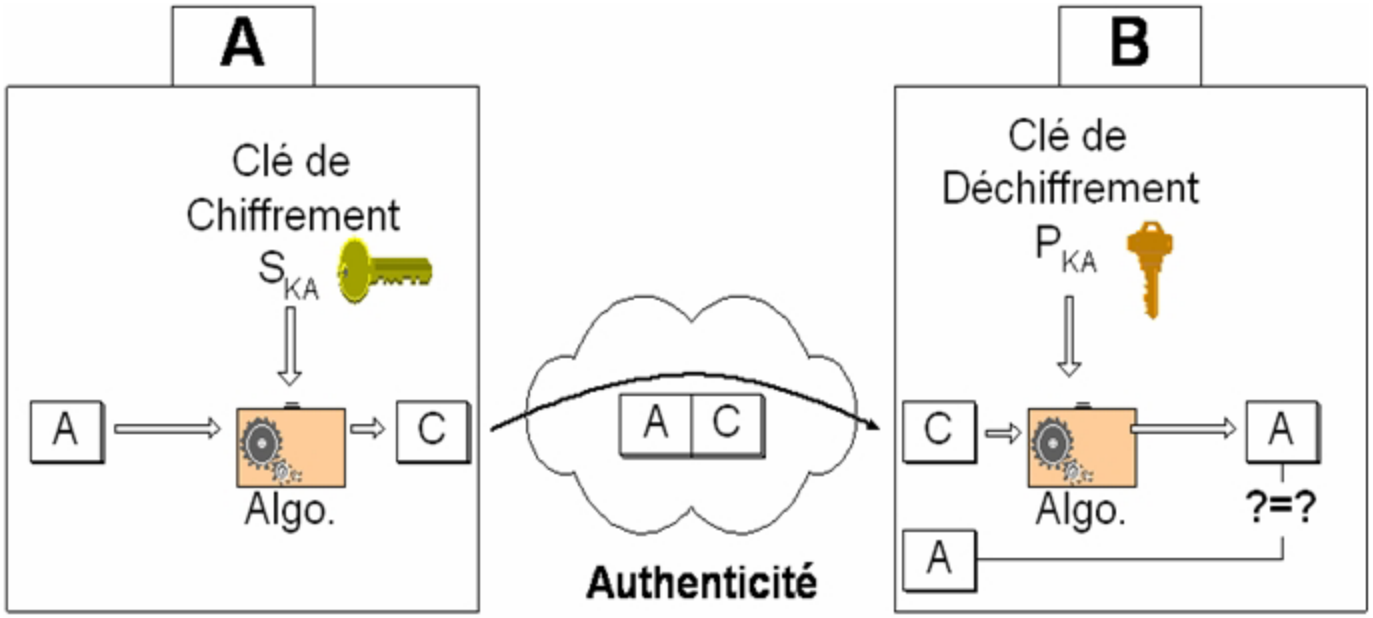
- Vérifier si le message n'a pas subi de modification durant la communication. C'est ici qu'interviennent les fonctions de hachage.



Vérification de l'intégrité par fonction de hachage

Authentification

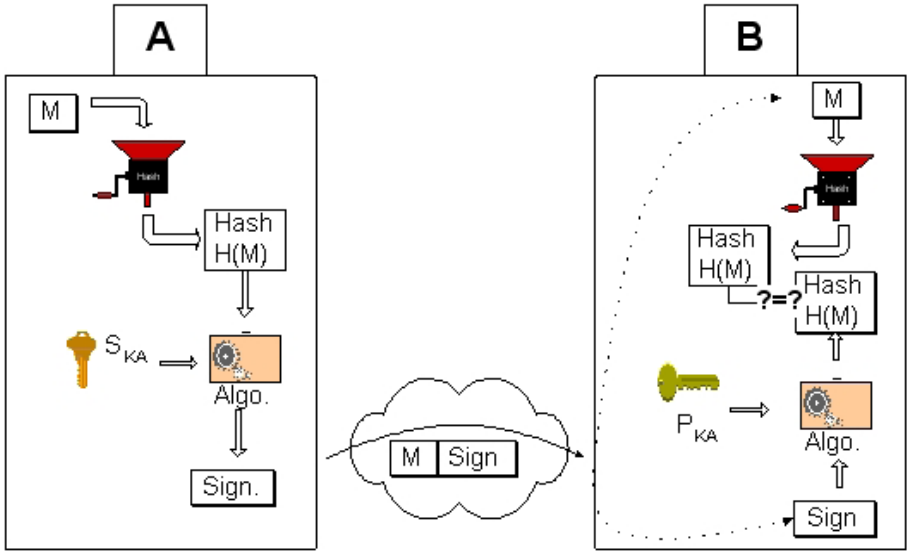
- Au niveau des parties communicantes, dans le cas d'un système asymétrique



Authentification

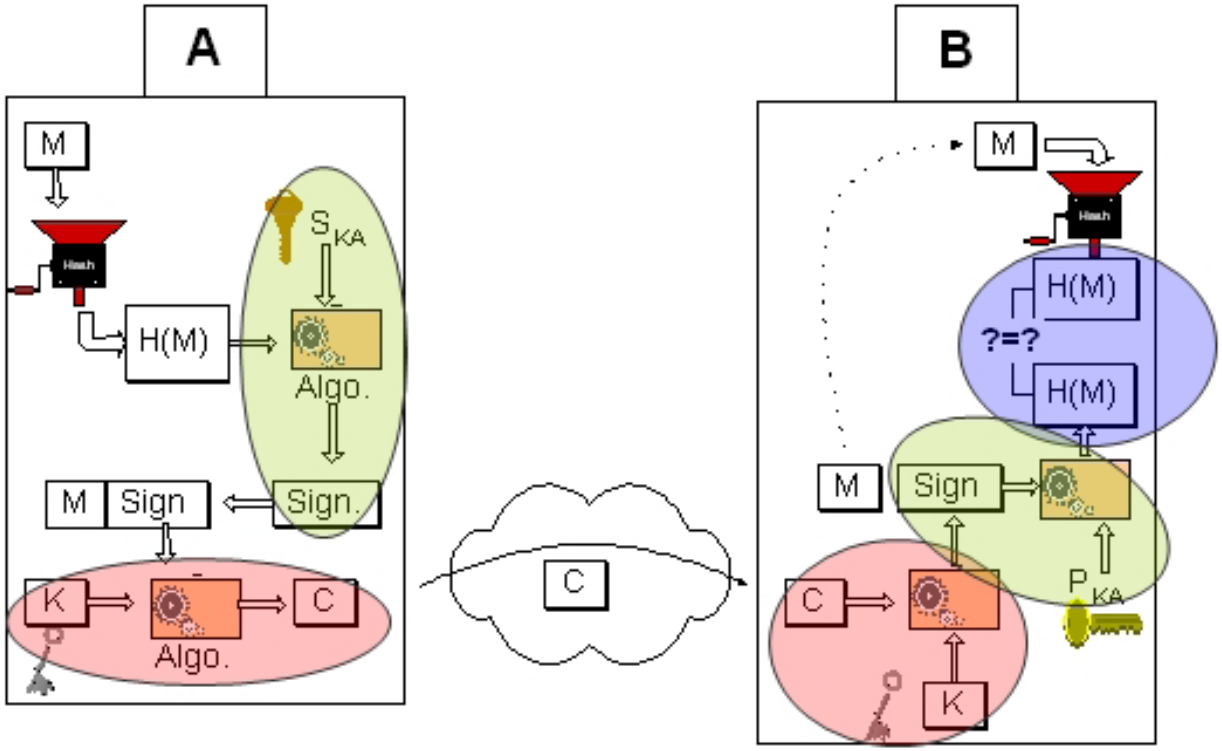
- Par l'utilisation d'une signature digitale

  propriétés des signatures: authentiques, infalsifiables, non-réutilisables, non-répudiables, et inaltérables.



Authentification par signature (technique asymétrique)

Synthèse



Confidentialité(Rouge), Intégrité(Violet), Authentification(Vert)

Institut Supérieur des Mathématique Appliquées et d'Informatique

Chapitre II

La cryptographie classique

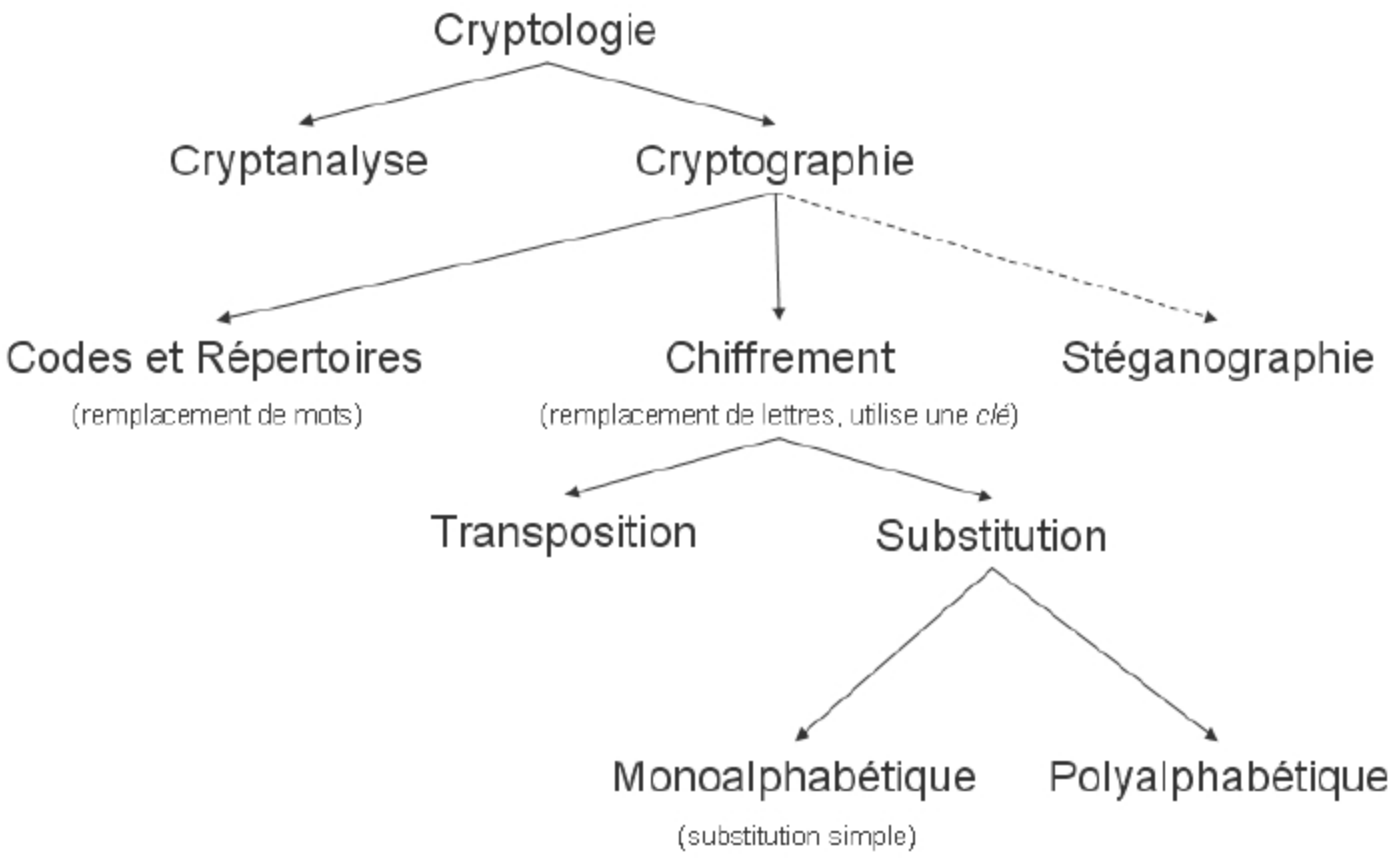
Enseignante : Dhikra Saffar Amira

1ere année mastère ASSIR

PLAN

- Substitution monoalphabétique
- Chiffrement polygraphique
- Substitutions polyalphabétiques
- Transpositions
- Machines à rotor

les différentes branches de la cryptographie classique



Substitution monoalphabétique

- Chaque lettre est remplacée par une autre lettre ou symbole
- Les plus connus, le chiffre de César, le chiffre affine.
- Tous ces chiffres sont sensibles à l'analyse de fréquence d'apparition des lettres.
- De nos jours, ces chiffres sont utilisés pour le grand public, pour les énigmes de revues ou de journaux

Chiffre de César

- Il s'agit d'un des plus simples et les plus populaires des chiffres classiques.
- Son principe est un décalage des lettres de l'alphabet.
- Pour le chiffrement

$$C = E(p) = (p + k) \bmod 26$$

- Pour le déchiffrement

$$p = D(C) = (C - k) \bmod 26$$

- p est l'indice de la lettre de l'alphabet,
- k est le décalage.

- Si on connait l'algorithme utilisé (ici César), la cryptanalyse par force brute est très facile ➔ seules 25 (!) clés sont possibles

Chiffre de César

Correspondance : A → 0, B → 1, C → 3, …, Z → 25

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

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25
9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	0	1	2	3	4	5	6	7	8

On additionne 9 à chaque nombre m de la première ligne

Si m + 9 > 25, on lui retranche 26.

La clé est le nombre 9

Arithmétique modulo n

Etant donné un nombre entier m, on peut lui fait correspondre un nombre m' (unique) compris entre 0 et n-1 en lui retranchant un multiple de n

On dit que m est égal à m' modulo n

On note

$$m = m'(\text{mod } n)$$

Arithmétique modulo 26

Etant donné un nombre entier, on peut lui faire correspondre un nombre (unique) entre 0 et 25 en lui retranchant 26 ou un certain nombre de fois 26.

Exemples :

$$29 - 26 = 3$$

On dit que « 29 est égal à 3 modulo 26 »

On écrit $29 = 3 \pmod{26}$

$$26647 - 1024 * 26 = 26647 - 26624 = 23$$

On dit que « 26647 est égal à 23 modulo 26 »

On écrit $26647 = 23 \pmod{26}$

Chiffrement affine

- Le chiffrement affine est une technique de chiffrement par substitution simple qui consiste à substituer à chaque symbole m_i du message clair, le symbole chiffré c_i calculé par :

$$c_i=(a\times m_i+b)(mod\ 26)$$

Où a et b sont deux entiers compris entre 0 et 25, a devant être premier avec 26.

- Le déchiffrement s'effectue en calculant :

$$m_i=a^{-1}\times(c_i-b)\ (mod\ 26)$$

Où a^{-1} désigne l'inverse de a modulo 26, c'est–à–dire l'unique entier compris entre 0 et 25 tel que :

$$a \times a^{-1}(mod\ 26) = 1$$

Chiffrement affine

a	a^{-1}
1	1
3	9
5	21
7	15
9	3
11	19
15	7
17	23
19	11
21	5
23	17
25	25

- Il y'a 12*26=312 clefs possibles pour ce type de chiffrement

Exemple

- Pour clef=(3,11) donner le chiffrement de la suite de lettres: "NSA"

- Essayer de déchiffrer le résultat.

Chiffrement affine

- **Correction exemple**

- Transformation de chiffrement :

$$c_i = f(m_i) = 3\ \ m_i + 11 \bmod 26$$

- Transformation de déchiffrement :

$$k^{-1} = 3^{-1} \bmod 26 = 9 \text{ [car } 3 * 9 \bmod 26 = 1]$$

- $m_i = f^{-1}(c_i) = 9\ \ (c_i - 11) \bmod 26$

- ’NSA’ ➔13 18 0 ➔24 13 11 ➔’YNL’

Chiffrement polygraphique

- Il s'agit ici de chiffrer un groupe de n lettres par un autre groupe de n symboles.
- Exemple : le chiffre de Playfair et le chiffre de Hill.
- Ce type de chiffrement porte le nom de substitutions polygamiques.

Chiffrement polygraphique

- **Chiffre de Playfair (1854)**

- On chiffre 2 lettres par 2 autres. On procède donc par digramme.

- On dispose les 25 lettres de l'alphabet (W exclu car inutile à l'époque, on utilise V à la place) dans une grille de 5x5, ce qui donne la clef.

- 4 règles à appliquer selon les deux lettres à chiffrer lors de l'étape de substitution.

- Pour le déchiffrement, on procède dans l'ordre inverse.

Chiffrement polygraphique

- **Chiffre de Playfair**

1) Si les lettres sont sur des "coins", les lettres chiffrées sont les 2 autres coins.

Exemple : OK devient VA, RE devient XI ...

2) Si les lettres sont sur la même ligne, il faut prendre les deux lettres qui les suivent immédiatement à leur droite.

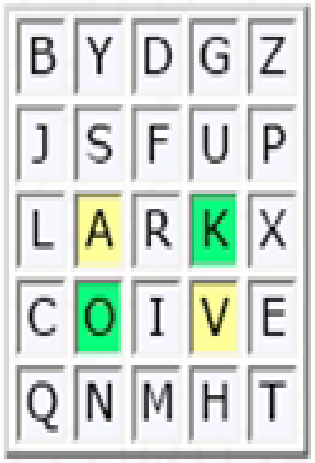
3) Si les lettres sont sur la même colonne, il faut prendre les deux lettres qui les suivent immédiatement en dessous.

4) Si elles sont identiques, il faut insérer une nulle (habituellement le X) entre les deux pour éliminer ce doublon.

Exemple : "balloon" devient "ba" "lx" "lo" "on".

Chiffrement polygraphique

- **Exemple du chiffre de Playfair**



Règle 1

Règle 2

Règle 3

Chiffrement polygraphique

- **Chiffre de Hill**
- Les lettres sont d'abord remplacées par leurs rangs dans l'alphabet. Les lettres P_k et P_{k+1} deviennent C_k et C_{k+1}

$$\begin{pmatrix} C_k \\ C_{k+1} \end{pmatrix} = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} P_k \\ P_{k+1} \end{pmatrix} (\mathrm{mod} 26)$$

- Les composantes de cette matrice doivent être des entiers positifs. De plus la matrice doit être inversible dans Z26.
- sa taille n'est pas fixée à 2. Elle grandira selon le nombre de lettres à chiffrer simultanément.
- Chaque digramme clair (P_1 et P_2) sera chiffré (C_1 et C_2) selon

$$C_1 \equiv aP_1 + bP_2 (\mathrm{mod} 26)$$

$$C_2 \equiv cP_1 + dP_2 (\mathrm{mod} 26)$$

Chiffrement polygraphique

- **Chiffre de Hill**
- Exemple de chiffrement : A prend comme clef de cryptage la matrice

$$\begin{pmatrix} 9 & 4 \\ 5 & 7 \end{pmatrix}$$

- Pour chiffrer le message "je vous aime" qu'elle enverra à B. Après avoir remplacé les lettres par leur rang dans l'alphabet (a=1, b=2, etc.), elle obtiendra

$$C1 = 9 * 10 + 4 * 5 (mod 26) = 110 (mod 26) = 6$$
$$C2 = 5 * 10 + 7 * 5 (mod 26) = 85 (mod 26) = 7$$

- Elle fera de même avec les 3e et 4e lettres, 5e et 6e, etc. Elle obtiendra finalement le résultat suivant :

Chiffrement polygraphique

- **Chiffre de Hill**

Lettres	j	e	v	o	u	s	a	i	m	e
Rangs (P_k)	10	5	22	15	21	19	1	9	13	5
Rangs chiffrés (C_k)	6	7	24	7	5	4	19	16	7	22
Lettres chiffrées	F	G	X	G	E	D	S	P	G	V

- Pour déchiffrer, le principe est le même que pour le chiffrement : on prend les lettres deux par deux, puis on les multiplie par une matrice

$$\begin{pmatrix} P_1 \\ P_2 \end{pmatrix} = \begin{pmatrix} a & b \\ c & d \end{pmatrix}^{-1} \begin{pmatrix} C_1 \\ C_2 \end{pmatrix} (\mathrm{mod} 26)$$

Chiffrement polygraphique

- **Exemple de déchiffrement de Hill**

$$\begin{pmatrix} 9 & 4 \\ 5 & 7 \end{pmatrix}^{-1} = \frac{1}{43}\begin{pmatrix} 7 & -4 \\ -5 & 9 \end{pmatrix} (\mathrm{mod} 26) = (43)^{-1}\begin{pmatrix} 7 & -4 \\ -5 & 9 \end{pmatrix} (\mathrm{mod} 26)$$

Comme pgcd(43, 26) = 1, $(43)^{-1}$ existe dans Z26 et $(43)^{-1}$ = 23. B a la matrice de déchiffrement :

$$\begin{pmatrix} 9 & 4 \\ 5 & 7 \end{pmatrix}^{-1} = 23\begin{pmatrix} 7 & -4 \\ -5 & 9 \end{pmatrix} (\mathrm{mod} 26) = \begin{pmatrix} 161 & -92 \\ -115 & 207 \end{pmatrix} (\mathrm{mod} 26) = \begin{pmatrix} 5 & 12 \\ 15 & 25 \end{pmatrix} (\mathrm{mod} 26)$$

B prend donc cette matrice pour déchiffrer le message "FGXGE DSPGV". Après avoir remplacé les lettres par leur rang dans l'alphabet (A=1, B=2, etc.), il obtiendra :

P1 = 5 * 6 + 12 * 7(mod26) = 114(mod26) = 10
P2= 15 * 6 + 25* 7(mod26) = 265(mod26) = 5

Chiffrement polygraphique

- **Chiffre de Hill**

  Il fera de même avec les 3e et 4e lettres, 5e et 6e, etc. Il obtiendra finalement le résultat suivant

Lettres chiffrées	F	G	X	G	E	D	S	P	G	V
Rangs chiffrés (C_k)	6	7	24	7	5	4	19	16	7	22
Rangs (P_k)	10	5	22	15	21	19	1	9	13	5
Lettres	j	e	v	o	u	s	a	i	m	e

Table de multiplication modulo 26

	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
×	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25
A	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
B	1	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25
C	2	0	2	4	6	8	10	12	14	16	18	20	22	24	0	2	4	6	8	10	12	14	16	18	20	22	24
D	3	0	3	6	9	12	15	18	21	24	1	4	7	10	13	16	19	22	25	2	5	8	11	14	17	20	23
E	4	0	4	8	12	16	20	24	2	6	10	14	18	22	0	4	8	12	16	20	24	2	6	10	14	18	22
F	5	0	5	10	15	20	25	4	9	14	19	24	3	8	13	18	23	2	7	12	17	22	1	6	11	16	21
G	6	0	6	12	18	24	4	10	16	22	2	8	14	20	0	6	12	18	24	4	10	16	22	2	8	14	20
H	7	0	7	14	21	2	9	16	23	4	11	18	25	6	13	20	1	8	15	22	3	10	17	24	5	12	19
I	8	0	8	16	24	6	14	22	4	12	20	2	10	18	0	8	16	24	6	14	22	4	12	20	2	10	18
J	9	0	9	18	1	10	19	2	11	20	3	12	21	4	13	22	5	14	23	6	15	24	7	16	25	8	17
K	10	0	10	20	4	14	24	8	18	2	12	22	6	16	0	10	20	4	14	24	8	18	2	12	22	6	16
L	11	0	11	22	7	18	3	14	25	10	21	6	17	2	13	24	9	20	5	16	1	12	23	8	19	4	15
M	12	0	12	24	10	22	8	20	6	18	4	16	2	14	0	12	24	10	22	8	20	6	18	4	16	2	14
N	13	0	13	0	13	0	13	0	13	0	13	0	13	0	13	0	13	0	13	0	13	0	13	0	13	0	13
O	14	0	14	2	16	4	18	6	20	8	22	10	24	12	0	14	2	16	4	18	6	20	8	22	10	24	12
P	15	0	15	4	19	8	23	12	1	16	5	20	9	24	13	2	17	6	21	10	25	14	3	18	7	22	11
Q	16	0	16	6	22	12	2	18	8	24	14	4	20	10	0	16	6	22	12	2	18	8	24	14	4	20	10
R	17	0	17	8	25	16	7	24	15	6	23	14	5	22	13	4	21	12	3	20	11	2	19	10	1	18	9
S	18	0	18	10	2	20	12	4	22	14	6	24	16	8	0	18	10	2	20	12	4	22	14	6	24	16	8
T	19	0	19	12	5	24	17	10	3	22	15	8	1	20	13	6	25	18	11	4	23	16	9	2	21	14	7
U	20	0	20	14	8	2	22	16	10	4	24	18	12	6	0	20	14	8	2	22	16	10	4	24	18	12	6
V	21	0	21	16	11	6	1	22	17	12	7	2	23	18	13	8	3	24	19	14	9	4	25	20	15	10	5
W	22	0	22	18	14	10	6	2	24	20	16	12	8	4	0	22	18	14	10	6	2	24	20	16	12	8	4
X	23	0	23	20	17	14	11	8	5	2	25	22	19	16	13	10	7	4	1	24	21	18	15	12	9	6	3
Y	24	0	24	22	20	18	16	14	12	10	8	6	4	2	0	24	22	20	18	16	14	12	10	8	6	4	2
Z	25	0	25	24	23	22	21	20	19	18	17	16	15	14	13	12	11	10	9	8	7	6	5	4	3	2	1

Substitutions polyalphabétiques

- Chiffre de Vigenère
- Chiffre de Verman
- Transpositions
- Machines à rotor
- Machine Enigma

Substitutions polyalphabétiques

- **Chiffre de Vigenère**

- C'est une amélioration décisive du chiffre de César.
- Sa force réside dans l'utilisation non pas d'un, mais de 26 alphabets décalés pour chiffrer un message.
- On parle du carré de Vigenère.
- Ce chiffre utilise une clef qui définit le décalage pour chaque lettre du message
- La grande force du chiffre de Vigenère est que la même lettre sera chiffrée de différentes manières ➔ perte de la fréquence des lettres ➔l'analyse de fréquence classique devient inutilisable

Substitutions polyalphabétiques

- **Chiffre de Vigenère**

Exemple

Chiffrer le texte "CHIFFRE DE VIGENERE" avec la clef "BACHELIER" (cette clef est éventuellement répétée plusieurs fois pour être aussi longue que le texte clair)

Clair	C	H	I	F	F	R	E	D	E	V	I	G	E	N	E	R	E
Clef	B	A	C	H	E	L	I	E	R	B	A	C	H	E	L	I	E
Décalage	1	0	2	7	4	11	8	4	17	1	0	2	7	4	11	8	4
Chiffré	D	H	K	M	J	C	M	H	V	W	I	I	L	R	P	Z	I

Carré de Vigenère

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

Substitutions polyalphabétiques

- **Chiffre de Verman** One Time Pad
- Le masque jetable est défini comme un chiffre de Vigenère avec la caractéristique que la clef de chiffrement a la même longueur que le message clair.

Clair	M	A	S	Q	U	E	J	E	T	A	B	L	E
Clef	X	C	A	A	T	E	L	P	R	V	G	Z	C
Décalage	23	2	0	0	19	4	11	15	17	21	6	25	2
Chiffré	J	C	S	Q	N	I	U	T	K	V	H	K	G

Substitutions polyalphabétiques

- **Chiffre de Verman**
- Pour utiliser ce chiffrement, il faut respecter plusieurs propriétés :

– choisir une clef aussi longue que le texte à chiffrer,

– utiliser une clef formée d'une suite de caractères aléatoires,

– protéger votre clef,

Substitutions polyalphabétiques

- **Exemple illustrant l'inviolabilité (Chiffre de Verman) :**

- Soit le texte chiffré : cuskqxwmfwituk

- Soit le masque jetable possible : bgfbcdfbfdecdg

➔ Résultat : BONJOURLATERRE-

- Soit un autre masque jetable : quauwtedbdisjg

➔ Résultat : MASQUESJETABLE

Il est donc impossible de déterminer le bon masque !

Chiffrement par transposition

- Elles consistent, par définition, à changer l'ordre des lettres.

- C'est un système simple, mais peu sûre pour de très brefs messages car il y a peu de variantes.

Exemple : un mot de trois lettres ne pourra être transposé que dans 6 (=3!) positions différentes.

"col" ne peut se transformer qu'en "clo", "ocl", "olc", "lco" et "loc".

- Lorsque le nombre de lettres croît, il devient de plus en plus difficile de retrouver le texte original sans connaître le procédé de transposition.

Chiffrement par transposition

- Ecrire le message dans une grille rectangulaire
- Arranger les colonnes de cette grille selon un mot de passe donné (le rang des lettres dans l'alphabet donne l'agencement des colonnes).
- **Exemple :** clef : GRAIN, message : SALUT LES PETITS POTS.

G	R	A	I	N
2	5	1	3	4
S	A	L	U	T
L	E	S	P	E
T	I	T	S	P
O	T	S	(A)	(B)

A	G	I	N	R
1	2	3	4	5
L	S	U	T	A
S	L	P	E	E
T	T	S	P	I
S	O	(A)	(B)	T

Machines à Rotors

- Entre les deux guerres : le début de la mécanisation de la cryptographie
- Des outils mécaniques, comme les cylindres chiffrant et et des machines électromécaniques sont mises au point.
- Ces machines fonctionnent sur le principe des rotors et des contacts électriques, afin de réaliser des formes de substitution polyalphabétique
- la clef a une longueur gigantesque de l'ordre de centaines de millions de lettres, au lieu de quelques dizaines dans les méthodes artisanales, comme le chiffre de vigenère.

Machines à Rotors

La machine Enigma

- Enigma est la machine à chiffrer et déchiffrer qu'utilisèrent les armées allemandes du début des années trente jusqu'à la fin de la seconde guerre mondiale.

- Elle automatise le chiffrement par substitution.

- Cette machine ressemble à une machine à écrire. Quand on presse sur une touche, deux choses se passent :

Machines à Rotors

La machine Enigma (Suite)

- Premièrement, une lettre s'allume sur un panneau lumineux : c'est la lettre chiffrée

- Deuxièmement, un mécanisme fait tourner le rotor de droite d'un cran ; toutes les 26 frappes, le deuxième rotor tourne d'un cran, toutes les 676 frappes (26 au carré), c'est le troisième rotor qui tourne d'un cran.

- Ces rotors tournants modifient les connexions électriques dans la machine, ce qui fait que la touche "A" allumera peut-être le "B" la première fois, mais le "X" la deuxième, le "E" la troisième, etc.

Machines à Rotors