Cryptographie

Réaliser par Mr: Chouha Adel

Chapitre01: Notions de base

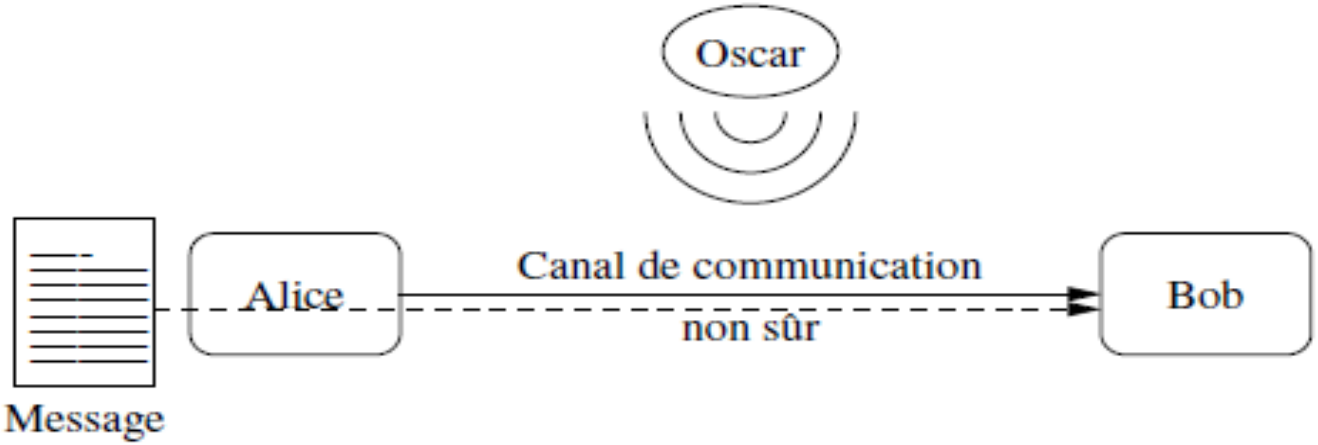
Plan:

- ***Introduction***
- ***Rôle de la cryptographie***
- ***Vocabulaire de base***
- ***Cryptographie /stéganographie***
- ***Crypto systèmes symétriques/asymétrique***

Introduction

- L'objectif fondamental de la cryptographie est de permettre à deux personnes, traditionnellement appelées ***A*** et ***B***, de communiquer utilisant un canal peu sûr de telle sorte qu'un opposant ***O***, ne puisse comprendre ce qui est échangé.
- Le canal peut être par exemple une ligne de téléphone, Internet, ou autre.
- L'information qu'***A*** souhaite transmettre à ***B***, que l'on appelle **texte** (ou message) **clair**, peut être un texte écrit en français ou encore des données numériques.
- ***A*** transforme le **texte clair** par un procédé de **chiffrement**, en utilisant une **clef** prédéterminée, et envoie le **texte** (ou message) **chiffré** (ou encore **cryptogramme**).
- ***O***, qui espionne éventuellement le canal, ne peut retrouver le **texte clair**, mais ***B***, qui connaît la clef pour **déchiffrer**, peut récupéré le **message clair** à partir du **cryptogramme**.

Réaliser par : Chouha Adel



- ✓ Alice et Bob veulent communiquer
- ✓ Oscar (opposant ou espion) veut savoir ce que s'échangent Alice et Bob

Objectif principal de la cryptographie

- ✓ Permettre à Alice et Bob de communiquer sur un canal peu sûr sans que Oscar comprenne ce qui est échangé

Définition

Science mathématique permettant d’effectuer des opérations sur un texte clair afin d’assurer une ou plusieurs propriétés de la sécurité de l’information.

Rôle de la cryptographie

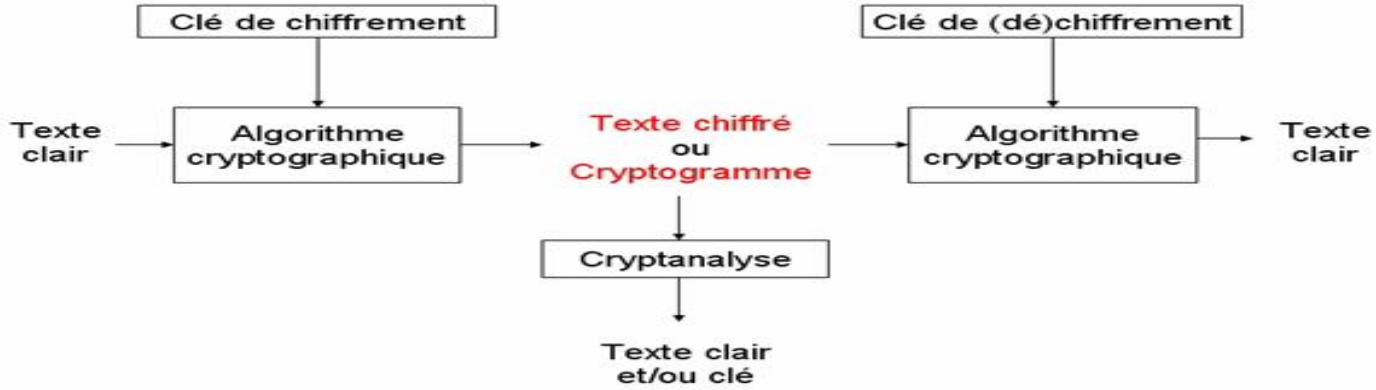
La cryptographie protège l'information de différentes manières :

- **confidentialité** : pour s'assurer que l'information ne soit seulement accessible qu' à ceux dont l'accès est autorisé ;
- **authenticité** : vérifier l'identité d'une personne ou d'un matériel informatique ;
- **intégrité** : pouvoir affirmer que les données n'ont pas été modifiées ;

Ces moyens doivent reposer sur des secrets

- clé secrète : cryptographie symétrique ;
- clé publique/secrète : cryptographie asymétrique

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.

Vocabulaire de base

- **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 le destinataire.
- La fonction permettant de retrouver le texte clair à partir du texte chiffré porte le nom de **déchiffrement**.
- **Texte chiffré** : Appelé également **cryptogramme**, le texte chiffré est le résultat de l'application d'un chiffrement sur un texte clair.
- **Clef** : Il s'agit du paramètre impliqué et autorisant des opérations de chiffrement et/ou déchiffrement. Dans le cas d'un algorithme symétrique, la clef est identique lors des deux opérations. Dans le cas d'algorithmes asymétriques, elle diffère pour les deux opérations.

Vocabulaire de base

- **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.

L'algorithme est en réalité un triplet d'algorithmes :

– l'un générant les clés K,

– un autre pour chiffrer M, et

– un troisième pour déchiffrer C.

Notations

En cryptographie, la propriété de base est que

$$M = D(E(M))$$

où

– **M** représente le texte clair,

– **C** est le texte chiffré,

– **K** est la clé (dans le cas d'un algorithme à clé symétrique), $\mathbf{E_k}$ et $\mathbf{D_k}$ dans le cas d'algorithmes asymétriques,

– **E(x)** est la fonction de chiffrement, et

– **D(x)** est la fonction de déchiffrement.

Ainsi, avec un algorithme à clef symétrique,

$$\mathbf{M = D(C) \text{ si } C = E(M)}$$

Cryptographie /stéganographie

Il faut distinguer la cryptographie de la stéganographie.

- La **cryptographie** vise à transformer un message clair en un cryptogramme (message chiffré) de sorte que le message originel soit complètement incompréhensible. Un observateur voit qu'il y a un message, mais ne le comprend pas.
- La **stéganographie** vise à dissimuler l'existence même de l'information secrète. Un observateur ne voit pas de message.

Principe de Kerckhoff

La sécurité du chiffre ne doit pas dépendre de ce qui ne peut pas être facilement changé.

En d'autres termes, aucun secret ne doit résider dans l'algorithme mais plutôt dans la clé. Sans celle-ci, il doit être impossible de retrouver le texte clair à partir du texte chiffré. Par contre, si on connaît K, le déchiffrement est immédiat.

On parle aussi de la **Maxime de Shannon**, dérivée du principe énoncé ci-dessus :

L'adversaire connait le système.

Suivant la nature des clés et de l'algo, on distingue deux grandes familles de crypto systèmes:

- Crypto systèmes à clés symétriques
- Crypto systèmes à clés publiques

Crypto systèmes à clés symétriques

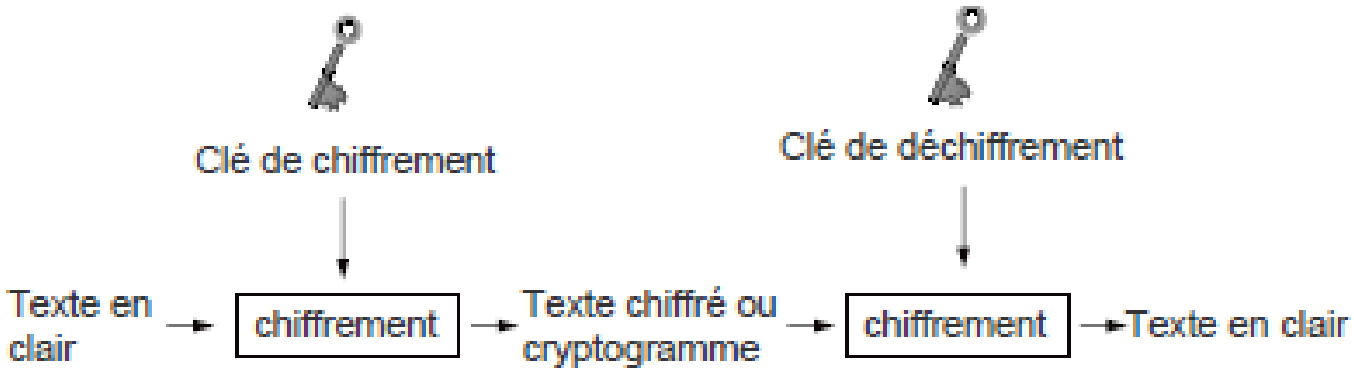
Caractéristiques:

- Clés identiques: Ke=Kd=K
- Clé secrète!

Principe: Algorithmes basés sur des opérations de transposition et de substitution des bits du texte clair, en fonction de la clé.

Distribution des clés:

- Opération critique.
- Doit s'effectuer de manière sécurisée (voir manuellement).



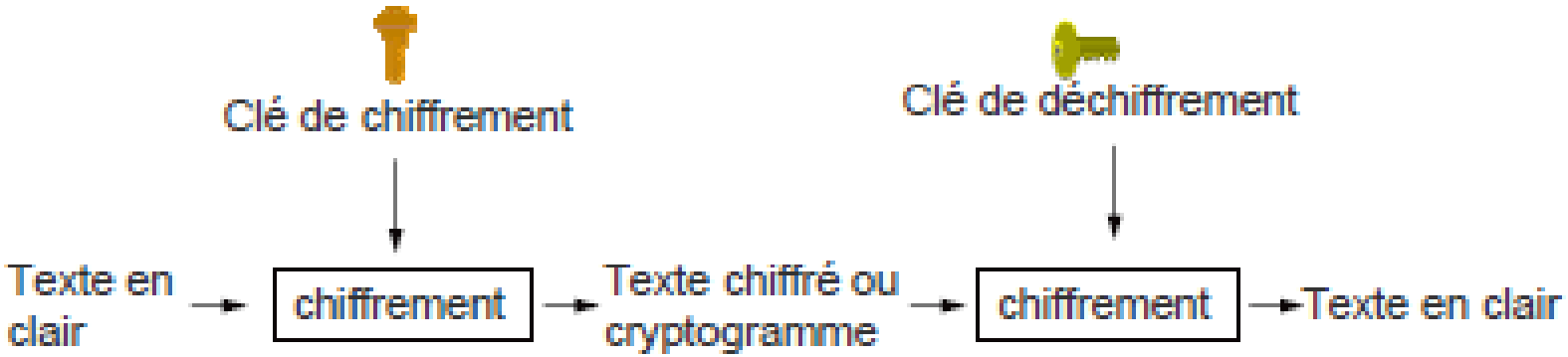
Crypto systèmes à clés publiques

Caractéristiques:

- 1 Clé publique: P_k
- 1 Clé privée: S_K (secrète)

Propriétés:

- La connaissance de P_k ne permet pas de déduire S_K.



Chapitre02: Chiffrement Classique

Plan :

- **Scytale**
- **Chiffrement par substitution**
- **Chiffrement par décalage ou de César**
- **Chiffrement de Vigenère**
- **Chiffrement de Hill**

Réaliser par : Chouha Adel

Chiffrement Classique

Chiffrement par transposition (permutation)

On considère le message

ton secret est ton prisonnier; s'il fuit tu deviendras son prisonnier.

On le réécrit sur deux lignes

T N E R T : : :

O S C E : : :

On le lit ligne à ligne, et on obtient le message chiffre.

TNERTSTNRSNIRFITDVEADSNRSNIROSCEET : : :

Autrement dit on a réécrit les lettre du message dans un ordre diffèrent.

Scytale

La technique consistait à:

- enrouler une bande de papyrus sur un cylindre appelé **scytale**
- écrire le texte sur la bandelette ainsi enroulée (le message dans l'exemple ci-dessus est "comment ça marche")
- Le message une fois déroulé n'est plus compréhensible ("cecaeonar mt c m mh "). Il suffit au destinataire d'avoir un cylindre de même rayon pour pouvoir déchiffrer le message.

Remarque: en réalité un casseur peut déchiffrer le message en essayant des cylindres de diamètre successifs différents.

Chiffrement par substitution

- ✓ On associant à chaque lettre de l'alphabet une seconde
- ✓ Pour crypter un message on substitue la lettre de l'alphabet avec celle qui correspondant.

a	b	c	d	e	f	g	h	i	j	k	l	m
↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓
B	N	S	U	H	Z	J	R	Y	E	A	Q	V

n	o	p	q	r	s	t	u	v	w	x	y	z
↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓
X	D	I	T	W	M	C	O	F	K	R	P	G

j	a	i		c	a	c	h	e	...
E	B	Y		S	B	S	R	H	

Chiffrement par substitution

Autre formulation

- On se donne une fonction S

  S : {a,b,.....,z}→{A,B,.....,Z}

  - **Chiffrement** : on substitue chaque lettre x du message clair par $S(x)$.
  - **Déchiffrement** : on substitue chaque lettre y du message chiffré par $S^{-1}(y)$.

Exercice

Soit la clef suivante :

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

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

- Chiffrer le message suivant “On ne peut rien apprendre aux gens. On peut seulement les aider à découvrir qu’ils possèdent déjà en eux tout ce qui est à apprendre” (Galilée).
- Déchiffrer le message suivant

  MGZVYZLGHCMHJMYXSSFMNHAHYCDLMHA.
- Quel est le nombre total de clefs possibles dans le chiffrement par substitution ?

Chiffrement par décalage ou de César

- C'est un exemple simple de chiffrement par substitution.
- Décalage de k rangs : chaque lettre est substituée par une lettre se trouvant **k** rang après.

Par exemple pour k = 4

a	b	c	d	e	f	g	h	i	j	k	l	m
↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓
E	F	G	H	I	J	K	L	M	N	O	P	Q

n	o	p	q	r	s	t	u	v	w	x	y	z
↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓
R	S	T	U	V	W	X	Y	Z	A	B	C	D

Chiffrement par décalage ou de César

On peut utiliser le chiffrement par décalage pour chiffrer un texte ordinaire en décidant d'une correspondance entre les caractères alphabétiques et les résidus modulo 26 comme donné dans la table suivante :

A	B	C	D	E	F	G	H	I	J	K	L	M
0	1	2	3	4	5	6	7	8	9	10	11	12

N	O	P	Q	R	S	T	U	V	W	X	Y	Z
13	14	15	16	17	18	19	20	21	22	23	24	25

Pour $0 \leq K \leq 25$ et $0 \leq x \leq 25$, on définit

$$E(x,K) = x + K \bmod 26 \quad et$$

$$D(x,K) = y - K \bmod 26$$

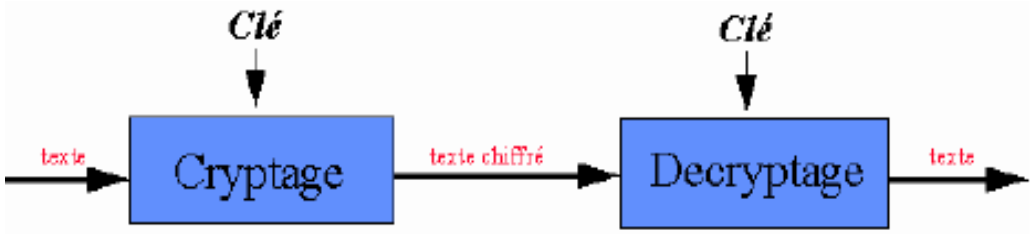
Lorsque **K** = **3**, le système par décalage s'appelle le chiffrement de **César**

Exercice

Déchiffrer le message suivant en utilisant la clef K = 11.

HPHTWWXPPELEXTOYTRSE

Le schéma général d'un envoie de message



- ✓ Si l'ennemi intercepte le message et qu'il connait la méthode de chiffrement
  - ➢ Si c'est un décalage : il pourra essayer les 25 décalages possible.
  - ➢ Si c'est une substitution plus générale il devra essayer:

    26! = 400000000000000000000000000 substitutions possibles, Ce qui est impossible même avec les ordinateurs d'aujourd'hui.

Utilisation de mot/phrase clef

Problème pratique :

- Si l'alphabet substitue est aléatoire, il est difficile de le mémoriser. Par exemple

  BNSUHZJRYEAQVXDITWMCOFKRPG

Solution:

- Un moyen pratique couramment utilisé est d'utiliser une **phrase clef**.

  Par exemple : TOUT CADENASSER

  - Pour fabriquer l'alphabet substitué on enlève les doublons

    TOUCADENSR

  - Et on complète par les lettre manquante (s'il y en a) a la fin

    TOUCADENSRBFGHIJKLMPQVWXYZ

  - Deux personnes peuvent alors facilement retenir la phrase clef.

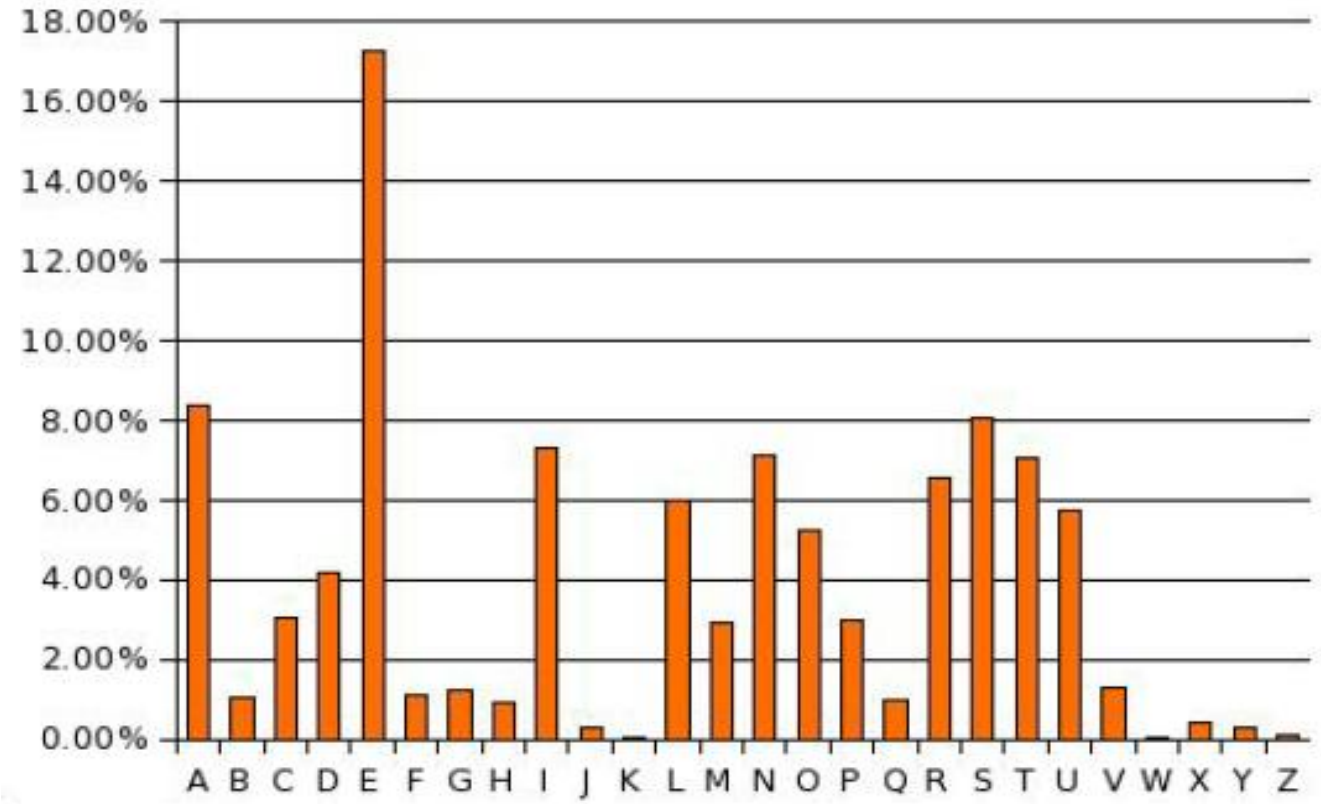
Substitution par des symboles

Consiste à substituer les lettres de l‘ alphabet par symbole autre qu‘ alphabétique.

Par exemple:

Cryptanalyse: Analyse de fréquence dans la langue française

- Dans la langue française chaque lettre n’apparait pas avec la même fréquence .



Cryptanalyse: Analyse de fréquence dans la langue française

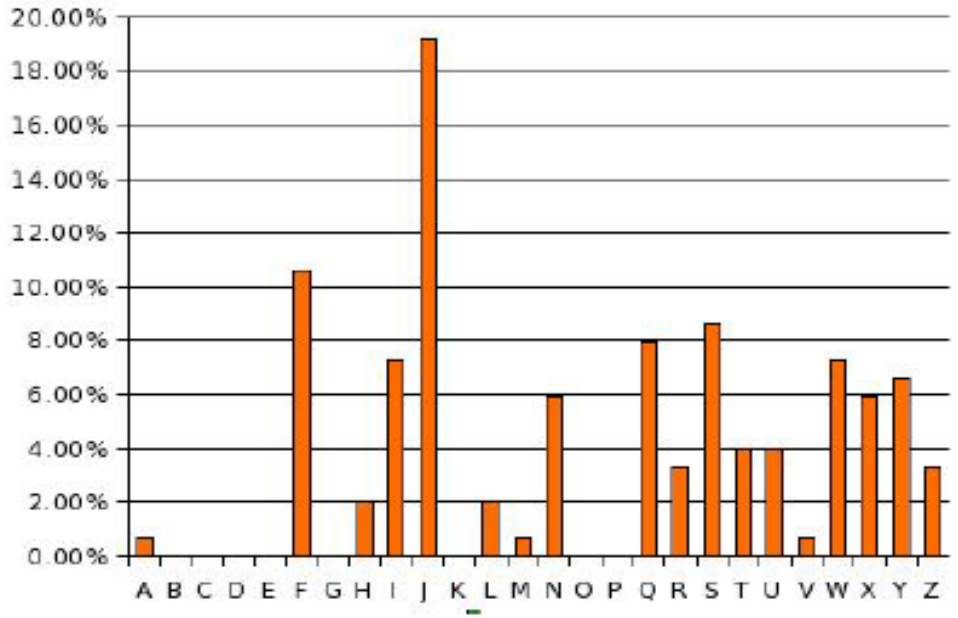
- Dans un message chiffre par substitution, une lettre **x** apparaitra dans le message clair avec la même fréquence que **S(x)** dans le message chiffré.
- En étudiant la fréquence d'apparition des lettre d'un message chiffré, on peut les ranger dans l'un des groupe ci-dessous.

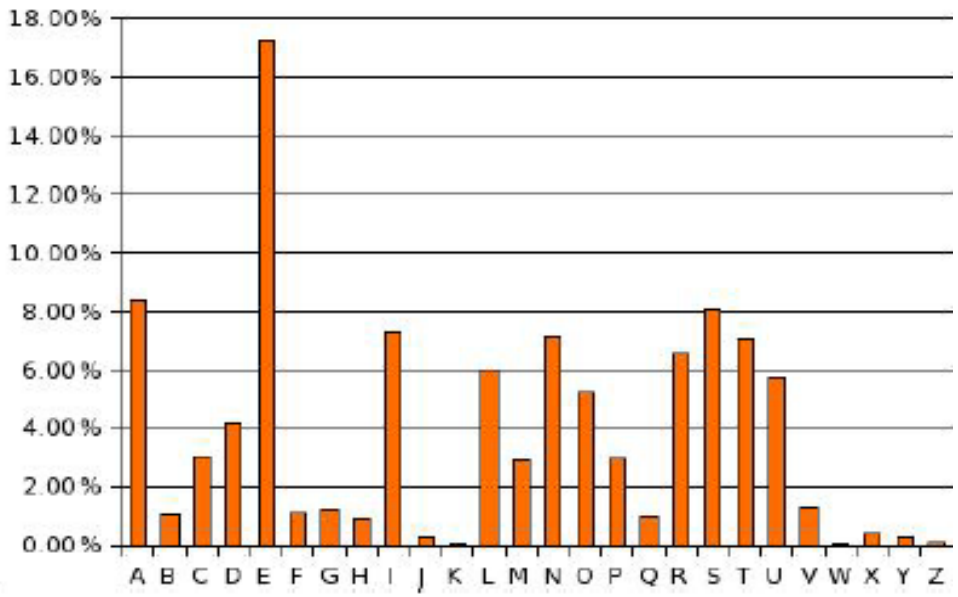
$$
\begin{array}{lcl}
17\% & \rightarrow & e \\
6\% - 8\% & \rightarrow & a, i, l, n, r, s, t, u, o \\
3\% - 4\% & \rightarrow & c, d, m, p \\
0\% - 1\% & \rightarrow & b, f, g, h, j, k, q, v, w, x, y, z
\end{array}
$$

- Ensuite en étudiant les fréquences d'apparition de paire de lettre on peut affiner l'étude et découvrir la clef de chiffrement.

Soit un message chiffre par decalage

IJAFS YQFQT NXJIW JXXJQ
JLFWI NJSIJ QFUTW YJZSM
TRRJI JQFHF RUFLS JXJUW
JXJSY JJYIJ RFSIJ FJSYW JWIFS
XQFQT NRFNX QJLFW INJSI
NYVZJ UTZWQ NSXYF SYNQS
JUJZY UFXQZ NFHHT WIJWQ
JSYWJ J





DEVANT LA LOI SE DRESSE LE GARDIEN DE LA PORTE. UN HOMME DE LA CAMPAGNE SE PRESENTE ET DEMANDE A ENTRER DANS LA LOI. MAIS LE GARDIEN DIT QUE POUR L INSTANT IL NE PEUT PAS LUI ACCORDER L ENTREE.

Exemple

BQPSNRSJXJNJXLDPCLDLPQBE_QRKJXHNKPKSJPJIKSPUN
BDKIQRBKPQPBQPZITEJQDQBTSKPELNIUNPHNKPBKPCKSS
QWKPSLXJPSNVVXSQCCKDJPBLDWPXBPSNVVXJPGKPJKDXI
PZLCEJKPGKSPSJQJXSJXHNKSPGPLZZNIIKDZKPGKSPGXV
VKIKDJKSPBKJJIKS

déchiffrer ce message en utilisant le tableau de fréquence des lettres suivant?

_	19.3	L	4.7	H	0.8
E	13.9	O	4.1	G	0.8
A	6.7	D	2.9	B	0.6
S	6.3	P	2.5	X	0.4
I	6.1	C	2.4	Y	0.3
T	6.1	M	2.1	J	0.3
N	5.6	V	1.3	Z	0.1
R	5.3	Q	1.3	K	0.0
U	5.2	F	0.9	W	0.0

Occurrence des lettres

En français

_	19.3	L	4.7	H	0.8
E	13.9	O	4.1	G	0.8
A	6.7	D	2.9	B	0.6
S	6.3	P	2.5	X	0.4
I	6.1	C	2.4	Y	0.3
T	6.1	M	2.1	J	0.3
N	5.6	V	1.3	Z	0.1
R	5.3	Q	1.3	K	0.0
U	5.2	F	0.9	W	0.0

Dans le cryptogramme

P	14.3	D	4.6	W	1.0
K	12.8	L	4.1	U	1.0
S	9.2	V	3.1	T	1.0
J	9.2	Z	2.6	_	0.5
X	5.6	G	2.6	O	0.0
Q	5.6	C	2.6	M	0.0
N	5.6	E	2.0	F	0.0
B	5.1	R	1.5	A	0.0
I	4.6	H	1.5	Y	0.0

Réaliser par : Chouha Adel

Remplaçons **P** par _ et **K** par E

BQ_SNRSJXJNJXLD_CLDL_QBE_QRE**JXHN**E_E**SJ_JI**E**S_UN**
BDE**IQRB**E_**Q_BQ_ZITEJQDQBTS**E_**ELNIUN_HN**E_**B**E_**C**E**SS**
QWE_**SLXJ_SNVVXSQCC**E**DJ_BLDW_XB_SNVVXJ_G**E_**J**E**DXI**
ZLCEJE**GES_SJQJXSJXHNES_G_LZZNII**E**DZ**E_**GES_GXV**
VE**I**E**DJES_B**E**JJIES**

Remplaçons Q par A et B par L

LA_SNRSJXJNJXLD_CLDL_ALE_AREJXHNE_ESJ_JIES_UN
LDEIARLE_A_LA_ZITEJADALTSE_ELNIUN_HNE_LE_CESS
AWE_SLXJ_SNVVXSACCEDJ_LLDW_XL_SNVVXJ_GE_JEDXI
_ZLCEJE_GES_SJAJXSJXHNES_G_LZZNIIEDZE_GES_GXV
VEIEDJES_LEJJIES

Remplaçons S par S et G par D

LA_SNRSJXJNJXLD_CLDL_ALE_AREJXHNE_ESJ_JIES_UN
LDEIARLE_A_LA_ZITEJADALTSE_ELNIUN_HNE_LE_CESS
AWE_SLXJ_SNVVXSACCEDJ_LLDW_XL_SNVVXJ_DE_JEDXI
_ZLCEJE_DES_SJAJXSJXHNES_D_LZZNIIEDZE_DES_DXV
VEIEDJES_LEJJIES

Remplaçons J par T et I par R

LA_SNRSTXTNTXLD_CLDL_ALE_ARETXHNE_EST_TRES_UN
LDERARLE_A_LA_ZRTETADALTSE_ELNRUN_HNE_LE_CESS
AWE_SLXT_SNVVXSACCEDT_LLDW_XL_SNVVXT_DE_TEDXR
_ZLCETE_DES_STATXSTXHNES_D_LZZNRREDZE_DES_DXV
VEREDTES_LETTRES

Remplaçons **X** par I, **H** par Q et **N** par U

LA_SU**R**STITUTI**LD**_**CLDL**_AL**E**_A**R**ETIQUE_EST_TRES_**U**U
L**D**ERA**R**LE_A_LA_**Z**R**TE**TA**D**AL**T**SE_**EL**UR**U**U_QUE_LE_**C**ESS
A**W**E_S**L**IT_SU**VV**ISA**CC**E**D**T_L**LDW**_IL_SU**VV**IT_DE_TE**D**IR
_**ZLCE**TE_DES_STATISTIQUES_D_**LZZ**URRE**DZ**E_DES_DI**V**
VERE**D**TES_LETTRES

Remplaçons V par F et D par N

LA_SURSTITUTILN_CLNL_ALE_ARETIQUE_EST_TRES_UU
LNERARLE_A_LA_ZRTETANALTSE_ELURUU_QUE_LE_CESS
AWE_SLIT_SUFFISACCENT_LLNW_IL_SUFFIT_DE_TENIR
_ZLCETE_DES_STATISTIQUES_D_LZZURRENZE_DES_DIF
FERENTES_LETTRES

Remplaçons R par B et L par O

LA_SUBSTITUTION_CONO_ALE_ARETIQUE_EST_TRES_UU
LNERABLE_A_LA_ZRTETANALTSE_EOURUU_QUE_LE_CESS
AWE_SOIT_SUFFISACCENT_LONW_IL_SUFFIT_DE_TENIR
_ZOCETE_DES_STATISTIQUES_D_OZZURRENZE_DES_DIF
FERENTES_LETTRES

Finalement

LA_SUBSTITUTION_MONO_ALPHABETIQUE_EST_TRES_VU
LNERABLE_A_LA_CRYPTANALYSE_POURVU_QUE_LE_MESS
AGE_SOIT_SUFFISAMMENT_LONG_IL_SUFFIT_DE_TENIR
_COMPTE_DES_STATISTIQUES_D_OCCURRENCE_DES_DIF
FERENTES_LETTRES

Chiffrement de Vigenère

- Dans le cas du chiffrement par décalage ou par substitution, dès qu'une clef est fixée, chaque caractère alphabétique, partout où il apparaît dans le texte est transformé en un même caractère. Autrement dit, pour toute lettre , chaque occurrence de **x** dans le texte clair est transformée en **E(x , K)**. Pour cette raison, le procédé est dit **mono alphabétique**.
- On présente maintenant un chiffrement qui n'est pas mono alphabétique : le **chiffrement de Vigenère**.
  - En utilisant la correspondance 0 ↔ a, 1 ↔ b, ..., 25 ↔ z,
  - on décrit chaque clef **K** du chiffrement de **Vigenère** par une chaîne de caractères de longueur **m** appelée mot-clef.
  - Le chiffrement de Vigenère traite **m** caractères alphabétiques à la fois :

    chaque bloc du texte clair est équivalent à **m** caractères alphabétiques.

Chiffrement de Vigenère

- Soit **m** un entier strictement positif. Soit $\mathbf{P = C = K = (Z/26Z)^m}$. Pour toute clef $\mathbf{K = (k_1,\ldots, k_m)}$ (où $k_i \in Z/26Z$ pour chaque i = 1,…,m),

on définit:

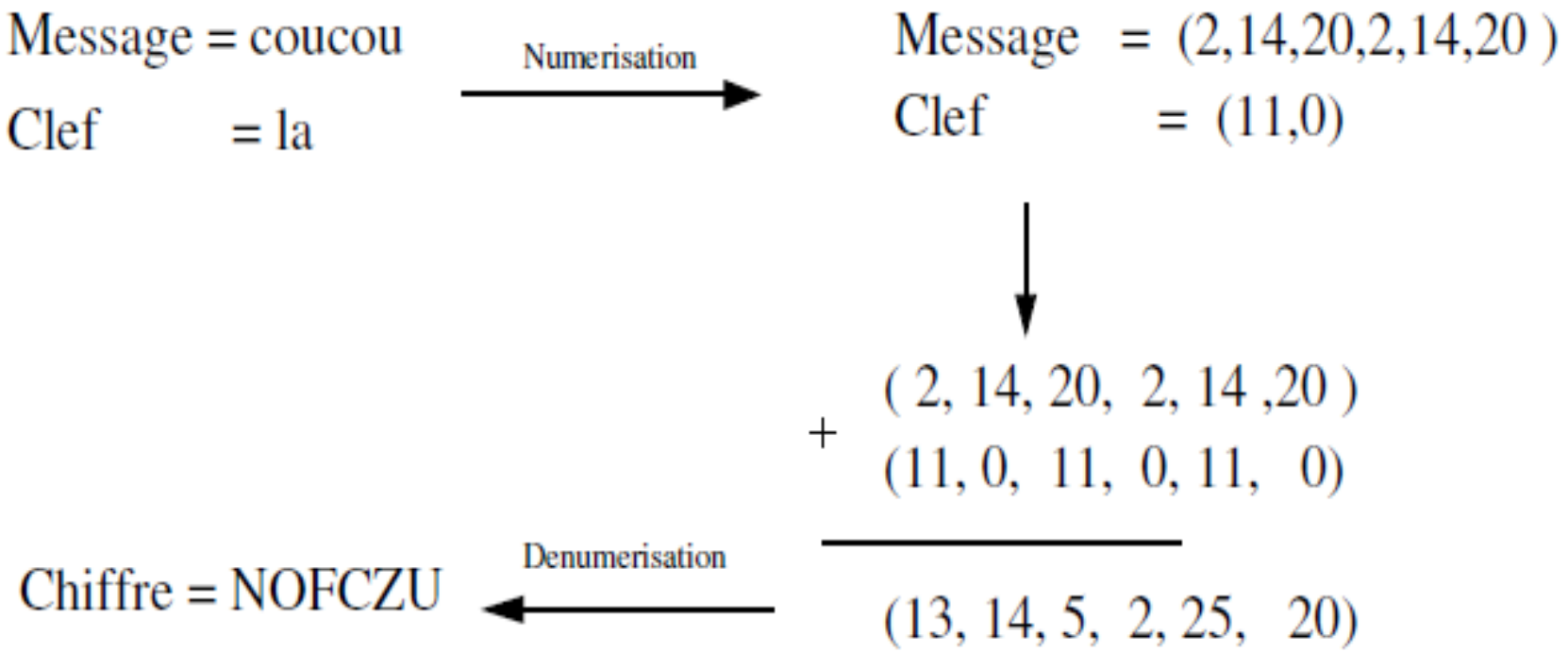
$$E(x_1,x_2,\ldots,x_m;K) = (x_1 + k_1, x_2 + k_2,\ldots,x_m + k_m)$$

et

$$D(y_1, y_2,\ldots,y_m ;K) = (y_1 - k_1, y_2 - k_2,\ldots,y_m - k_m)$$

où les opérations sont effectuées dans **Z/26Z**.

Exemple


Message = coucou
Clef = la
Numerisation
Message = (2,14,20,2,14,20)
Clef = (11,0)
(2, 14, 20, 2, 14 ,20)
+
(11, 0, 11, 0, 11, 0)
(13, 14, 5, 2, 25, 20)
Denumerisation
Chiffre = NOFCZU

Exercice

Déchiffrer le texte suivant (chiffré avec la méthode de Vigenère et le mot-clef “CIPHER") :

VPXZGIAXIVWPUBTTMJPWIZITWZT.

Solution :

La clef correspondant au mot-clef est (2; 8; 15; 7; 4; 17). Et le texte déchiffré est:

THISCRYPTOSYSTEMISNOTSECURE.

Chiffrement de Hill

- ✓ Ce crypto système généralise celui de Vigénère. Il a été publié par L. S. Hill en 1929.
- ✓ On choisit un alphabet de **n** lettres (on prendra dans nos exemples n = 26) et une taille **m** pour les blocs alors:

P = C = (Z/26Z)^{m}, (en général Z/nZ).

La clef de codage est une matrice inversible **K**, si m = 2

$$\mathbf{K} = \begin{pmatrix} \boldsymbol{a} & \boldsymbol{b} \\ \boldsymbol{c} & \boldsymbol{d} \end{pmatrix}$$

Chiffrement de Hill

Chiffrement :

- Les lettres sont d'abord remplacées par leur rang dans l'alphabet.

Si $(x_1, x_2) \in (Z/26Z)^2$ est le message clair alors le message chiffré sera

$$(y_1, y_2) = E_K((x_1, x_2)) = \begin{pmatrix} x_1 \\ x_2 \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix} = (ax_1 + bx_2 , cx_1 + dx_2)$$

(L'addition et la multiplication sont réalisées dans Z/26Z.)

Chiffrement de Hill

Déchiffrement :

- La clé de déchiffrement est la matrice inverse de **K** c.à.d :

$$(x_1, x_2) = D_K((y_1, y_2)) = \begin{pmatrix} y_1 \\ y_2 \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix}^{-1}$$

Cette matrice doit être l'inverse de matrice de chiffrement (modulo 26). Ordinairement, cet inverse est:

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}^{-1} = \frac{1}{ad - bc} \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}$$

Remarques:

- ✓ On ne peut pas prendre n'importe quoi comme matrice de chiffrement. Ses composantes doivent tout d'abord être des **nombres entiers positifs**.
- ✓ Il faut aussi qu'elle ait une matrice inverse dans Z_{26}.

  si **pgcd(det A,26)=1** alors, **A** a une matrice inverse A^{-1}

  sinon **A** n'a pas une matrice inverse.

Exemple

- Chiffrez le mot ***vous*** en prenant comme clef la matrice $\begin{pmatrix} \mathbf{9} & \mathbf{4} \\ \mathbf{5} & \mathbf{7} \end{pmatrix}$
- Après avoir remplacé les lettres par leur rang dans l'alphabet (a=1, b=2, etc.), on obtient pour la première et la deuxième lettre:
  - Y1= 9*22+4*15=24 , y2=5*22+7*15=7

  Et pour la troisième et quatrième lettre:

  - Y1= 9*21+4*19=5 , y2= 5*21+7*19=4

  Donc **vous** est chiffré par **xged**

Exercice

En utilisant le chiffrement du Hill avec la clef K = $\begin{pmatrix} \mathbf{11} & \mathbf{8} \\ \mathbf{3} & \mathbf{7} \end{pmatrix}$ chiffrer le mot suivant :

CRYPTOSYSTEMES

Attaque à texte clair connu du chiffrement de Hill

- Le chiffrement de Hill est plus difficile à casser par une attaque à texte chiffré connu, mais facilement par une attaque à texte clair choisi.
- Supposons tout d'abord que l'opposant ait trouvé la valeur m utilisée.
- Supposons ensuite qu'il dispose d'au moins m paires de lettres (clairs et chiffrés).on obtient :

  Y = XK, où **K** est la matrice (inconnue) définissant la clef.

  Si **X** est inversible, alors on peut calculer $\mathbf{X^{-1}}$ et obtenir $\mathbf{K = X^{-1}Y}$.

  Si **X** n'est pas inversible, alors il faut un autre ensemble de **m** paires de vecteurs.