Sécurité Informatique

3éme licence informatique

Université de Jijel

F.BOUDJERIDA

Chapitre 2

Objectifs de ce cours:

- Introduire les bases de la cryptographie classique.
- Introduire les bases de la cryptanalyse.
- Comprendre les principes de bases de la cryptographie.

Exemple de message crypté

- Déchiffer le message suivant :
  - « CPOKPVS MF NPOEF »
- Indice n°1 : les espaces restent des espaces
- Indice n°2 : l'alphabet a été décalé
- Clé : chaque lettre a été décalée d'un rang
  - Message clair: « BONJOUR LE MONDE »

Deuxième exemple

- Déchiffer le message suivant :
  - « FH WHAWH HVW FKLIIUH SDU FHVDU »
- Indice n°1 : les espaces restent des espaces
- Indice n°2 : l'alphabet a été décalé
- Clé : chaque lettre a été décalée de 3 rangs
  - Message clair: « CE TEXTE EST CHIFFRE PAR CESAR »

Cryptographie

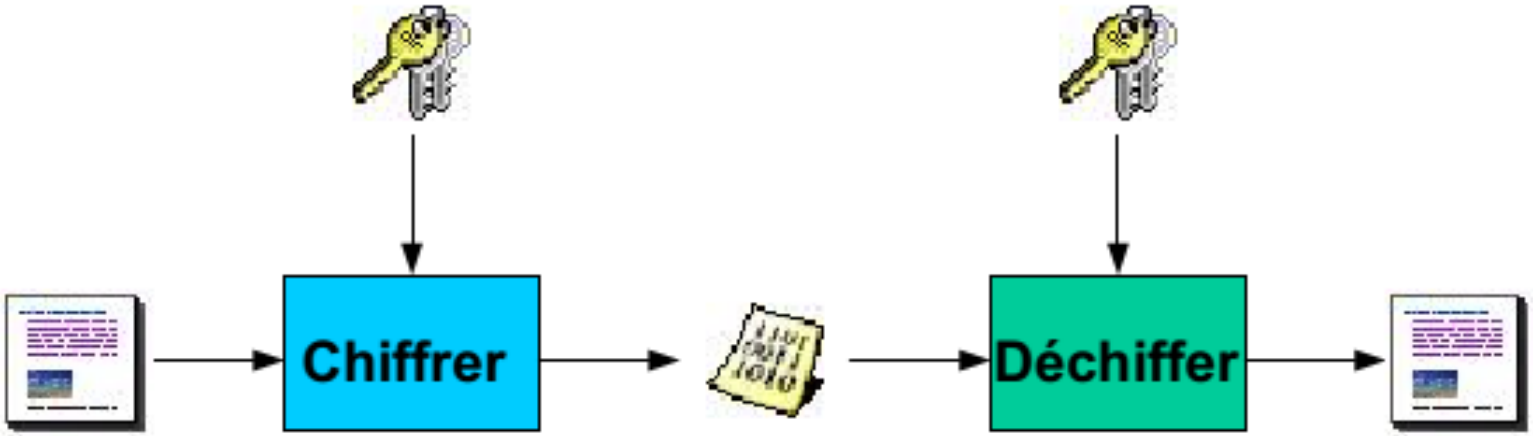
Information chiffrée

Connaissance de l'existence de l'information

≠

connaissance de l'information

systèmes cryptographies



systèmes cryptographies

- Un système cryptographique est un quintuplet `S={P,C,K,E,D}` avec:
  - `P` : ensemble fini de clairs (plain texts)
  - `C` : ensemble fini de chiffrés (cipher texts)
  - `K` : ensemble fini de clés (key space)
  - `E` : ensemble fini de règles de chiffrement (encryption rules)
  - `D` : ensemble fini de règles de déchiffrement (decryption rules)

$$\forall k \in K, \exists e_k \in E \text{ tel que } e_k : P \to C,$$
$$\exists d_k \in D \text{ tel que } d_k : C \to P \text{ et}$$
$$d_k \circ e_k = id_P \qquad (1)$$

systèmes cryptographies
protocole

1. Alice et Bob conviennent de S.

2. Ils choisissent leur(s) clé(s).

3. Alice chiffre le clair $x = x_1x_2...x_n$, $x_i \in P$ en $y = y_1y_2...y_n$, $y_i \in C$ avec $y_i = E_K(x_i)$ et l'envoie à Bob.

4. Bob calcule $\forall i$, $x_i = D_K(y_i)$ c'est à dire x et retrouve ainsi le clair à partir du chiffré.

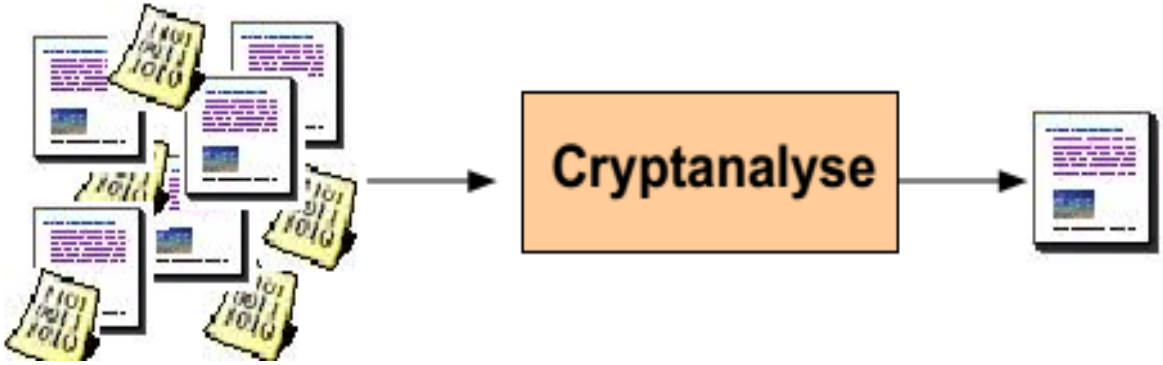
Remarque : x n'appartient pas à P, mais est un mot constitué d'éléments de l'alphabet P (les x_i ci-dessus).

Principes de la cryptographie et la cryptanalyse

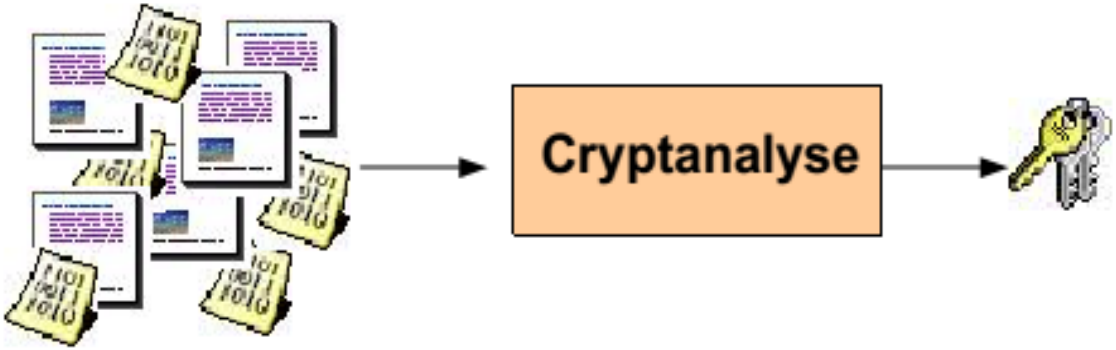
- Considérations pratiques
  - les fonctions e_k et d_k doivent pouvoir se calculer efficacement
  - un opposant observant les messages chiffrés ne peut déterminer *k* ou *x*
  - cryptanalyse : rechercher *k* à partir de *y*. Donnera aussi *x*
- Algorithme public, clé cachée : principe de Kerckhoffs (1883)
  - la sécurité d'un cryptosystème ne repose que sur le secret de la clé.
  - exprimé aussi par Shannon : l'adversaire connaît le système
  - chiffres civils suivent le principe de Kerckhoffs. Militaires utilisent des systèmes secrets.
- Le nombre de clés possibles doit être grand.

Cryptanalyse

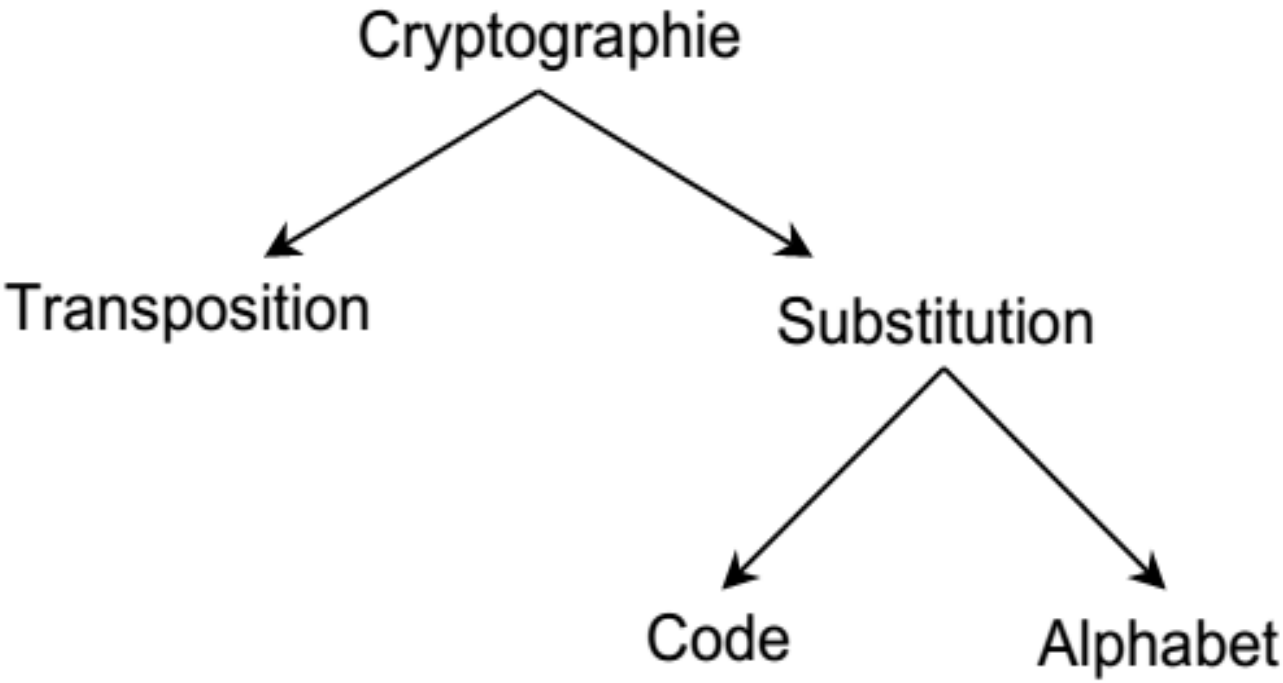
- Décrypter les messages sans connaître la clé.



- Découvrir la clé de chiffrement



La cryptographie classique



Cryptage par substitution

Dans un cryptage par substitution, chaque lettre ou groupe de lettre est remplacée par une autre lettre (ou un autre groupe de lettres) On distingue deux cryptages :

- monoalphabétique-seule une substitution/transposition est appliquée
- polyalphabétique- plusieurs substitutions/transpositions sont utilisées

Cryptage par substitution monoalphabétique

Le chiffrement de César (60-50 av JC)

la substitution est définie par un décalage de lettres.
Par exemple, si on remplace A par D, on remplace B par E, C par F, D par G, etc...

Texte clair	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
Texte codé	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

Définition (Cryptosytème par décalage)

Soient $P = C = K = \mathbb{Z}_{26}$. Pour $0 \leq k < 26$, on définit

$e_k(x) = x + k \bmod 26$, $d_k(y) = y - k \bmod 26$.

Nombre de clés possibles (espace de clés): $|K| = 26$

► Vérifier (1) ? $d_k \circ e_k = d_k(e_k(x)) = d_k(x+k) = y - k = (x+k) - k = x$

Cryptage par substitution monoalphabétique

Substitution arbitraire

Table de substitution (π)

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

TOUS_LES_CHEMINS_MENENT_A_ROME devient
FQLJRPAJRHCAE_ZJREAZAZFRDRNQEA

On prend un texte en clair et, pour chacune des lettres du texte, on utilise la lettre comme index dans une table de substitution (π) pour trouver l'équivalent chiffré

→ La table de substitution π représente la clé

→Le décodage devrait être plus difficile. Peut-on essayer tous les décodages possibles? on a 26 ! possibilités de permutations des lettres, soit environ 288 (hors de portée manuelle)

Cryptage par substitution **polyalphabétique**

Les substitutions polyalphabétiques (aussi appelées **à alphabets multiples**), utilisent plusieurs "alphabets", ce qui signifie qu'une même lettre peut être remplacée par plusieurs symboles.

L'exemple le plus connu de chiffre polyalphabétique est sans doute le chiffre de **Vigenère**, qui résista aux cryptanalystes pendant trois siècles.

Publié en 1586 par Blaise de Vigenère.

Le **cryptage de Vigenère** 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.

Ce système de chiffrement fût une petite révolution et resta "incassable" jusqu'en 1854, année où Charles Babbage en réussit la cryptannalyse.

Cryptage par substitution **polyalphabétique**

Cryptage de vigenère

Définition (Chiffrement de Vigenère)

Soit $m > 0$ *et* $P = C = (\mathbb{Z}_{26})^m$. Pour la *clé* $k = (k_1, k_2, \ldots, k_m)$, on définit

$$e_k(x_1, x_2, \ldots, x_m) = (x_1 + k_1, x_2 + k_2, \ldots, x_m + k_m)$$

$$d_k(y_1, y_2, \ldots, y_m) = (y_1 - k_1, y_2 - k_2, \ldots, y_m - k_m)$$

- Le message clair est découpé en bloc de m lettres. Les clés comme les messages sont traduits de l'alphabet a-z vers les nombres 0-25.
- Vérifier (1) ? **Espace de clés :** $|K| = 26^m$

$$\begin{aligned} d_k \circ e_k = d_k(e_k(x)) &= d_k(x_1 + k_1, x_2 + k_2, \ldots, x_m + k_m) \\ &= ((x_1 + k_1) - k_1, (x_2 + k_2) - k_2, \ldots, (x_m + k_m) - k_m) \\ &= (x_1, x_2, \ldots, x_m) = x \end{aligned}$$

Cryptage par substitution **polyalphabétique**

Matrice de chiffrement Vigenère

Clé:
JEPENSEDONCJESUIS

Message:
ATTAQUEZDEMAIN
JEPENSEDONCJES

Message chiffré:
JXIEDMICRROJMF

La clés utilisée

Texte claire

	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

Cryptage par substitution **polyalphabétique**

Matrice de chiffrement Vigenère

Clé:
JEPENSEDONCJESUIS

Message:
ATTAQUEZDEMAIN
JEPENSEDONCJES

Message chiffré:
JXIEDMICRROJMF

	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

Cryptage par substitution **polyalphabétique**

Matrice de chiffrement Vigenère

Clé:
JEPENSEDONCJESUIS

Message:
ATTAQUEZDEMAIN
JEPENSEDONCJES

Message chiffré:
JXIEDMICRROJMF

	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

Cryptage par substitution **polyalphabétique**

Matrice de chiffrement Vigenère

Clé:
JEPENSEDONCJESUIS

Message:
ATTAQUEZDEMAIN
JEPENSEDONCJES

Message chiffré:
JXIEDMICRROJMF

	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

Cryptage par substitution **polyalphabétique**

Cryptage de vigenère

Exemple: cryptons 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

L'avantage du chiffre de Vigenère est de pouvoir chiffrer une lettre par plusieurs manières différentes.
(par exemple la lettre « E » a été remplacée par M, V, L et I). Cela rend inutile l'analyse des fréquences qui est un système de cryptanalyse classique.

Cryptage par substitution **polyalphabétique**
masque jetable

- **Technique du masque jetable** (one–time pad, 1919): Seule méthode connue 100% sécure.

L'algorithme est simple: on ajoute le rang de la lettre à chiffrer au rang de la lettre correspondante du masque, le résultat mod 26 donne le rang de la lettre chiffrée.

• Le destinataire dispose d'un bloc identique et utilise le masque de la même manière pour déchiffrer chaque lettre du message chiffré.

• Le masque est utilisé une seule fois, pour un seul message.

Exemple texte en claire m asque jetable
avec le masque : t bfrgfarfmilkl
texte chiffré : G CYIBKKWZNKWQ

13
+20
7

Cryptage par substitution **polyalphabétique**
masque jetable

- Si on ne connait pas la clef TBFRGFARFMIKLAO alors il est impossible de retrouver le message original.

- Toutes les clef sont également probables et celle-ci aurait aussi bien pu être

  RXDCXFHVQBYRX

- Si on déchiffre GCYIBKKWZNKWQ avec cette clef on obtient:

  OEUFSDECAILLES

- Si on avait choisit la clef:

  RTFDAPUVHMGNX

  on aurait obtenu le texte en clair:

  OISEAUPARADIS

Cryptage par substitution **Polygrammique**

Polygrammique : Se dit d'un chiffre où un groupe de n lettres est codé par un groupe de n symboles.

Dans les substitutions polygrammiques (aussi appelées polygraphiques), les lettres ne sont pas chiffrées séparément, mais par groupes de plusieurs lettres.

Cryptage par substitution **Polygrammique**

Chiffre de Playfair

- Inventé en 1854 par wheatstone, utilisé en 1ère guerre mondiale.
- À base de l'alphabet et d'un mot clé, une matrice 5X5 est construite (I et J = 1 lettre).

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

Exemple: Mot clé est MONARCHY

Séparer les lettres doubles par x (ex de lettre addition.)

balloon →ba lx lo on

- Lettres même rangée remplacées par celles de droite

  ar →RM

- Lettres même colonne remplacées par celles d'au-dessous

  mu →CM

- Sinon, chaque digramme est chiffré selon leurs rangée et colonne

  hs →BP et ea →IM (ou JM)

•Le texte en clair est chiffré par 2 lettres à la fois, avec 26 lettres →26X26=676 digrammes→Identification difficile

Cryptage par substitution **Polygrammique**

Chiffre de Playfair

- Pour déchiffrer, il suffit de connaître le mot clef pour reconstituer la grille et procéder à l'envers.
- Malheureusement, on peut facilement casser ce code en regardant quels digrammes apparaissent le plus couramment et supposer qu'ils correspondent aux digrammes usuels de la langue.
- *Exemple* : en Français il s'agirait de : es, en, ou, de, nt, te, on.

Cryptage par substitution **Polygrammique**

Chiffre de Hill

Chiffrement

- **Les lettres sont d'abord remplacées par leur rang dans l'alphabet. Les lettres P_k et P_{k+1} du texte clair seront chiffrées C_k et C_{k+1} avec la formule ci-dessous:**

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

- **Ce qui signifie, pour fixer les idées, que les deux premières lettres du message clair (P_1 et P_2) seront chiffrées (C_1 et C_2) selon les deux équations suivantes:**

$$\begin{aligned} C_1 &\equiv aP_1 + bP_2 \pmod{26} \\ C_2 &\equiv cP_1 + dP_2 \pmod{26} \end{aligned}$$

Exemple de chiffrement

Alice prend comme clef de cryptage la matrice $\begin{pmatrix} 9 & 4 \\ 5 & 7 \end{pmatrix}$ pour chiffrer le message : je vous aime

Cryptage par substitution **Polygrammique**

Chiffre de Hill

- **Après avoir remplacé les lettres par leur rang dans l'alphabet (a=1, b=2, etc.), elle obtiendra:**

- **Ce qui signifie, pour fixer les idées, que les deux premières lettres du message clair (P_1 et P_2) seront chiffrées (C_1 et C_2) selon les deux équations suivantes:**

$$C_1 \equiv 9 \cdot 10 + 4 \cdot 5 \pmod{26} = 110 \pmod{26} = 6$$
$$C_2 \equiv 5 \cdot 10 + 7 \cdot 5 \pmod{26} = 85 \pmod{26} = 7$$

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

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

Certains auteurs posent "A"=1, "B"=2, ..., "Z"=0. On a utilisé ici cette convention. Cependant, d'autres auteurs posent "A"=0, "B"=1, ..., "Z"=25.

Cryptage par substitution **Polygrammique**

Chiffre de Hill

Remarques :

- le premier E de je vous aime est transformé en G,
- tandis que le second est transformé en V
- Le critère des chiffrements polyalphabétique est bien respecté : les analyses statistiques directes sur la fréquence des lettres sont impossibles.

Cryptage par substitution **Polygrammique**
Chiffre de Hill

Déchiffrement de Hill

- **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. :**

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

- Pour déchiffrer le message d'Alice, Bob doit calculer l'inverse de la matrice

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

Cryptage par substitution **Polygrammique**
Chiffre de Hill

Déchiffrement de Hill

Déchiffrement se fait par la matrice inverse K^{-1} tq $K.K^{-1} = I$

Bob prend donc la matrice $\begin{pmatrix} 5 & 12 \\ 15 & 25 \end{pmatrix}$ 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

Cryptage par substitution **Polygrammique**
Chiffre de Hill

Déchiffrement de Hill

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

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

Remarque

- De nombreux cryptosystemes sont (au moins en partie)bases sur l' **arithmétique modulaire** .

Définition

Si a, b et n sont des entiers, et si $n > 0$, on écrit $a = b \pmod{n}$ si, et seulement si, n divise $b - a$.

L'entier n est parfois appelé le **modulus**.

- On est maintenant en mesure de définir **l'arithmétique modulo *n***.
- Z_n symbolise l'ensemble $\{0, \ldots, n-1\}$. On définit sur Z_n deux opérations notées + et × .
- L'addition et la multiplication dans Z*n* fonctionnent exactement comme l'addition et la multiplication usuelles, excepte le fait que tous les résultats sont réduits modulo *n*.

- par exemple on veuille calculer 11×13 dans Z_{16}. En tant qu'entiers ordinaires,

  on a $11 \times 13 = 143$.

  Pour réduire 143 modulo 16, on réalise une division euclidienne : $143 = 8 \times 16 + 15$,

  donc $143 \pmod{16} = 15$,

  et par conséquent $11 \times 13 = 15$ dans Z_{16}.

Arithmétique modulo *n*.

- **Addition modulo** *n* : Pour *a* et *b* des entiers quelconques, l'addition modulo *n* de *a* et *b* est $(a + b) \pmod{n}$ soit le reste modulo *n* de $a + b$.
- Concrètement pour calculer cette somme, on commence par calculer $a + b$ de façon usuelle, puis on réduit le résultat modulo *n*.
- Le résultat de cette addition appartient a l'ensemble Z_n.

Exemples :

$3 + 7 \pmod{2} = 0$;
$3 + 7 \pmod{5} = 0$;
$3 + 7 \pmod{6} = 4$;
$3 + 7 \pmod{11} = 10$.

Arithmétique modulo *n*.

- **Opposé modulo** *n* : Soit $a \in Zn$, alors $n - a$ satisfait la propriété

  $a + (n - a) = 0 = (n - a) + a$ (additions modulo*n*).
- $n - a$ est l'**oppose modulo´** *n* **de** *a*, qui est note $-a$.
- Remarquons que si $a = 0$, alors $n - a = n = 0 \pmod{n}$.

- Exemples :
  $-3 \pmod 5 = 2$. On a donc $3 + 2 = 0 \pmod 5$;
  $-4 \pmod 8 = 4$. On a donc $4 + 4 = 0 \pmod 8$.

Arithmétique modulo *n*.

- **Multiplication modulo** *n* : Pour *a* et *b* des entiers quelconques, la multiplication modulo *n* de *a* par *b* est $(a \times b) \pmod{n}$ soit le reste modulo *n* de $a \times b$.
- Concrètement pour calculer ce produit, on commence par calculer $a \times b$ de façon usuelle, puis on réduit le résultat modulo *n*.
- La multiplication modulo *n* est également une opération interne à Z*n*.

Exemples :
$3 \times 2 \pmod{2} = 0$;
$3 \times 2 \pmod{5} = 1$;
$3 \times 2 \pmod{6} = 0$;
$3 \times 2 \pmod{4} = 2$.

Arithmétique modulo *n*.

- Pour déchiffrer le message d'Alice, Bob doit calculer :

$$\begin{pmatrix} 9 & 4 \\ 5 & 7 \end{pmatrix}^{-1} \pmod{26} = \frac{1}{9\cdot 7 - 4\cdot 5}\begin{pmatrix} 7 & -4 \\ -5 & 9 \end{pmatrix} \pmod{26} = 43^{-1}\begin{pmatrix} 7 & -4 \\ -5 & 9 \end{pmatrix} \pmod{26} = \ldots ?$$

- Le problème est maintenant de calculer l'inverse de 43 modulo 26. Il existe des algorithmes efficaces pour déterminer l'inverse de k (mod n), par exemple l'algorithme d'Euclide étendu.
- Mais quand n = 26, la méthode force brute est sans doute la manière la plus simple :

  Algorithme pour trouver k^{-1} modulo 26 (force brute)

  1. Multiplier successivement k par les entiers m de l'ensemble {1, 3, 5, 7, 9, 11, 15, 17, 19, 21, 23, 25}
  2. Stopper quand le produit k·m est égal à 1 (mod 26) ; k^{-1} modulo 26 =m.

- L'utilisation de cet algorithme nous dit que $43^{-1} \pmod{26} = 23$.

Arithmétique modulo *n*.

- **Soustraction modulo** *n* : Pour *a* et *b* des entiers tels que $a \geq b$, la soustraction modulo *n* de *a* et *b* est $(a - b) \pmod{n}$ soit le reste modulo *n* de $a - b$.
- Concrètement pour effectuer cette soustraction, on commence par calculer $a - b$ de façon usuelle, puis on réduit le résultat modulo *n*.

- **Exemples** :
  $7 - 3 \pmod{2} = 0$;
  $7 - 2 \pmod{3} = 2$.

Cryptage par Transposition

- Les méthodes de cryptage par substitution et les codages conservent l'ordre des caractères du texte en clair qu'ils se contentent de dissimuler.

- Les méthodes de cryptage par transposition, au contraire, changent l'ordre des caractères sans les dissimuler.

- Une substitution ne change pas l'**ordre** des lettres dans un message mais seulement les lettres elle- mêmes figurant dans le message. En d'autres termes, a partir d'un` message, **on remplace chaque lettre par un autre symbole mais en conservant l'ordre d'apparition des lettres**.

Par exemple

si une lettre "e" apparait en positions 3, 8, 25 d'un message

" . . . *e*. . . *e*. . . *e*. . . ", alors on la remplace, disons, par le symbole " @" exactement aux positions 3, 8 et 25 de telle sorte que l'on obtienne :
" . . . @ . . . @ . . . @. . . ". Pour changer l'ordre, on utilise les **transpositions**.

Cryptage par Transposition

Principe :

- Utilisation d'une clef qui est un mot ou une phrase ne contenant aucune lettre répétée. La clé sert à numéroter les colonnes. Dans le chiffrage on lit les colonnes par ordre alphabétique de la clé

Exemple :

Clé : briques

Texte en clair= transférez un milliard de francs à mon compte suise numéroté zéro zéro sept un

Cryptage par Transposition

Principe :

- Utilisation d'une clef qui est un mot ou une phrase ne contenant aucune lettre répétée. La clé sert à numéroter les colonnes.

Exemple :
Clé : briques
Texte en clair= transférez un milliard de francs à mon compte suise numéroté zéro zéro sept un

Texte crypté : trleàpetéu fmdcoiropa ziroeuzon uaansmésr elfmtnézn éidsmsozts nrncuére

b	r	i	q	u	e	s
1	5	3	4	7	2	6
t	r	a	n	s	f	é
r	e	z	u	n	m	i
l	l	i	a	r	d	d
e	f	r	a	n	c	s
à	M	o	n	c	o	m
p	t	e	s	u	i	s
e	n	u	m	é	r	o
t	é	z	é	r	o	z
é	z	o	s	e	p	t
u	n					

Cryptanalyse de la cryptographie classique

- ✓ Introduction
- ✓ Cryptanalyse par recherche des clés(Force brute, recherche exhaustive)
  - Cryptanalyse du chiffrement césar,
- ✓ Cryptanalyse par analyse de fréquences
  - Idée
  - Cryptanalyse du chiffrement arbitraire
  - Cryptanalyse du chiffrement de Vigenère

❑Cryptanalyse

- **Objectif** : Attaquer un système cryptographique. Un cryptosystème est dit **vulnérable** s'il est possible de :
  - décrypter des messages sans connaître la clé
  - encrypter des messages sans connaître la clé
  - trouver la clé

❑Classification des attaques

- **Attaques** : Elles peuvent être classifiées selon les informations disponibles aux cryptanalystes.

➢ **Attaque à texte chiffré**: l'analyste dispose de textes chiffrés *c1, … , cn* et cherche à trouver leurs correspondants en clair.

➢ **Attaque à texte clair**: l'analyste dispose de textes en clair *m1, ..., mn* et de leurs chiffrements *c1, ..., cn* respectifs et essaye de trouver la clé du cryptage ou de décrypter d'autres textes.

➢ **Attaque à texte clair choisi** : L'analyste peut choisir des textes clairs et obtenir leurs textes chiffrés correspondants.
En ayant ces connaissances, il essaye de trouver la clé du cryptage ou de décrypter d'autres textes.

➢ **Etc…**

❑Méthodologie de cryptanalyse

Techniques :

- Bien comprendre le système cryptographique en question
- Dégager ses propriétés
- Exploiter ses propriétés pour en déduire ses faiblesses

➢Recherche exhaustive de la clé (Brute force attack)

Idées :

- Un système cryptographique manipule un ensemble fini de clés (espace de clés)

- Si l'espace de clés est petit alors un adversaire peut les essayer une par une jusqu'à ce qu'il trouve la bonne

Recherche exhaustive de la clé

Exemple : Le chiffrement de César

Rappel : $e_k(x) = x + k \bmod 26$ *et* $d_k(x) = x - k \bmod 26$

Remarque : Il y'a 26 clés possibles == on peut rapidement les parcourir.

Exemple : Le message crypté est $C = JZCBM\ NWZKM$

$k = 0 \Rightarrow D_0(C) = JZCBM\ NWZKM$

$k = 1 \Rightarrow D_1(C) = IYBALMVYJL$

$k = 2 \Rightarrow D_2(C) = HXAZK\ LUXIK$

$k = 3 \Rightarrow D_3(C) = GWZYJ\ KTWHJ$

$k = 4 \Rightarrow D_4(C) = FVYXI\ JSVGI$

$k = 5 \Rightarrow D_5(C) = EUXWH\ IRUFH$

$k = 6 \Rightarrow D_6(C) = DTWVG\ HQTEG$

$k = 7 \Rightarrow D_7(C) = CSVUF\ GPSDF$

$k = 8 \Rightarrow D_8(C) = BRUTE\ FORCE$

Aha!!!··· j'ai trouvé la clé $k = 8$

Niveau de sécurité *théorique* :

– Alphabet à 26 lettres : 26! alphabets possibles.

Clairement, le chiffrement de César n'est pas sécuritaire.

➢Recherche exhaustive de la clé

Limites : Pour que cette technique soit réalisable, il faut que l'espace de clé ait une taille raisonnable.

Question : Peut-on appliquer cette technique, par exemple, sur le chiffrement du Vigenère avec une clé de taille 20 ?

Réponse : Non, il y a trop de clés à explorer 26^{20}

Question : C'est peut être trop pour un humain, mais est ce que c'est trop pour un ordinateur qui peut faire 2 milliard d'opérations par seconde (*2 GHz = 2X10^9* o.p.s.)?

NB: Pour le chiffrement arbitraire, le nombre de clés = 26**!**.
26**!** > 4X1026 (La recherche *exhaustive* est impossible).

➢Recherche exhaustive de la clé

Limites (suite) :

Réponse : Oui, c'est encore trop pour un ordinateur. En effet, avec un ordinateur de cette puissance (*2 GHz*), il faut :

$$\frac{26^{20}}{2\times10^{9}} \approx 9964074447604704576 \quad \text{sec}$$

$$\approx 166067907460078409 \quad \text{min}$$

$$\approx 2767798457667973 \quad \textit{heures}$$

$$\approx 115324935736165 \quad \textit{jours}$$

$$\approx 315095452831 \quad \textit{années}$$

$$\approx 315 \quad \textit{milliard d'années}$$

➢Cryptanalyse **par analyse de fréquence**

Origine : Approche introduite par Abu Youssif Al-Kindi (**9 ème siècle)**

Idée :

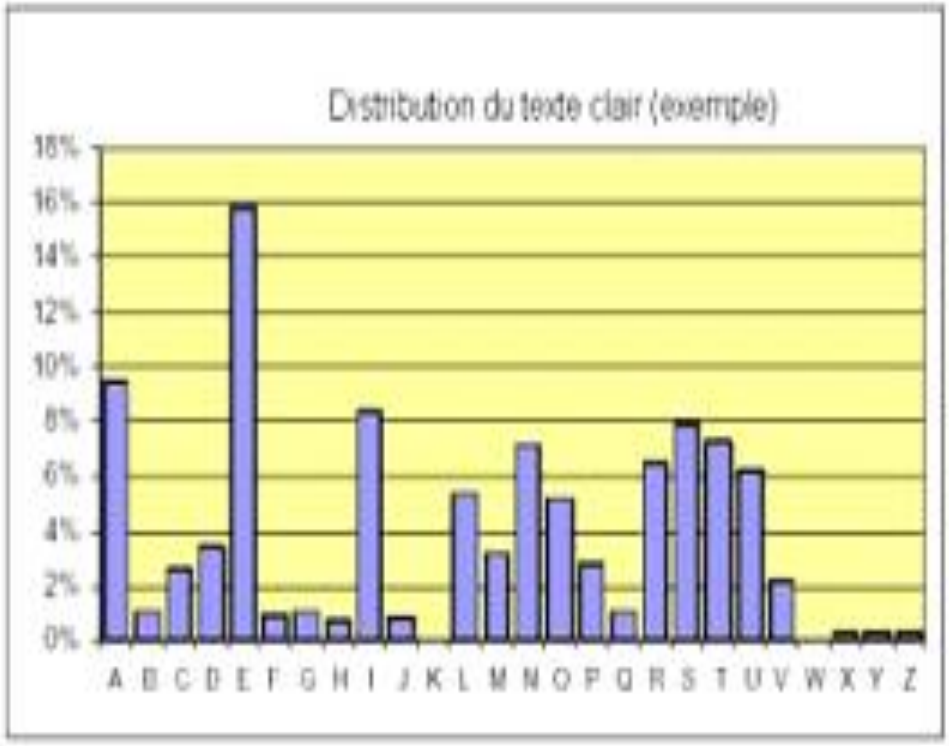
1. Établir la fréquence de chaque lettre de l'alphabet. En français la lettre la plus fréquente est « e » suivie par « a » puis par « i », etc
2. Examiner les fréquences des caractères dans le texte chiffré.
3. Remplacer les caractères les plus fréquents du texte chiffré par les caractères les plus fréquents du langage.
4. Si par exemple la lettre la plus fréquente du texte chiffré est « j », suivie par « m », suivi par « k », alors on fait un premier essai en remplaçant « j » par « e », « m » par « a » et « k » par « i ».

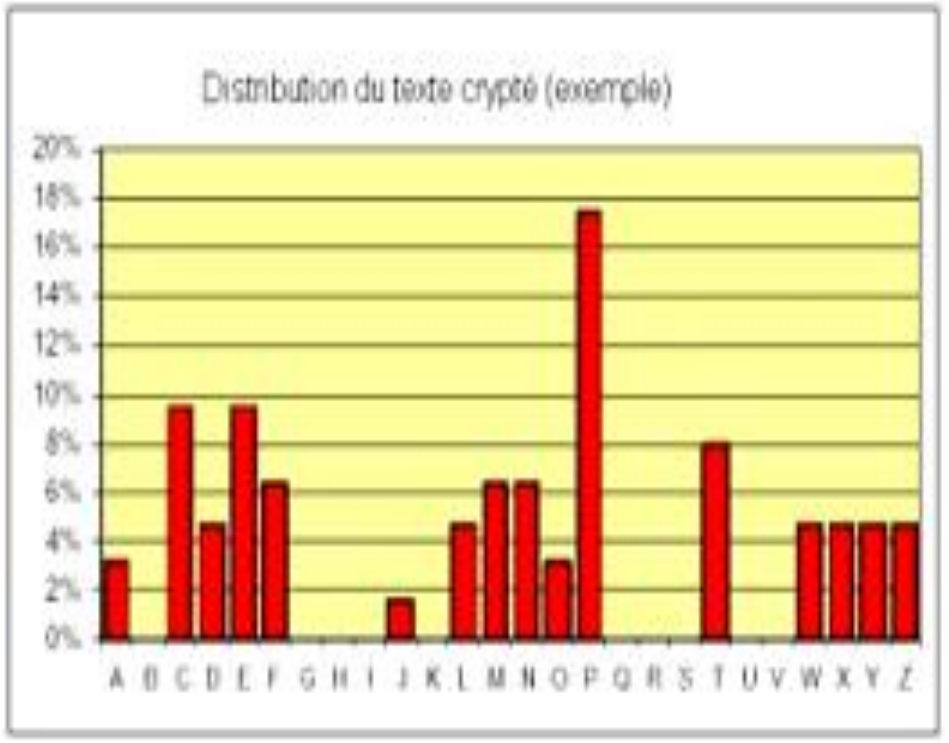
➢Cryptanalyse **par analyse de fréquence**

Remarques :

- Dans un texte quelconque chaque lettre a une fréquence d'apparition.
- Les probabilités de toutes les lettres définissent la distribution de ce texte.
- Soit D_C la distribution d'un texte clair.
- Soit D_E la distribution de son correspondant crypté.
- Le lien entre D_E et D_C dépend du cryptosystème.
- Un bon cryptosystème doit détruire le lien entre D_E et D_C.

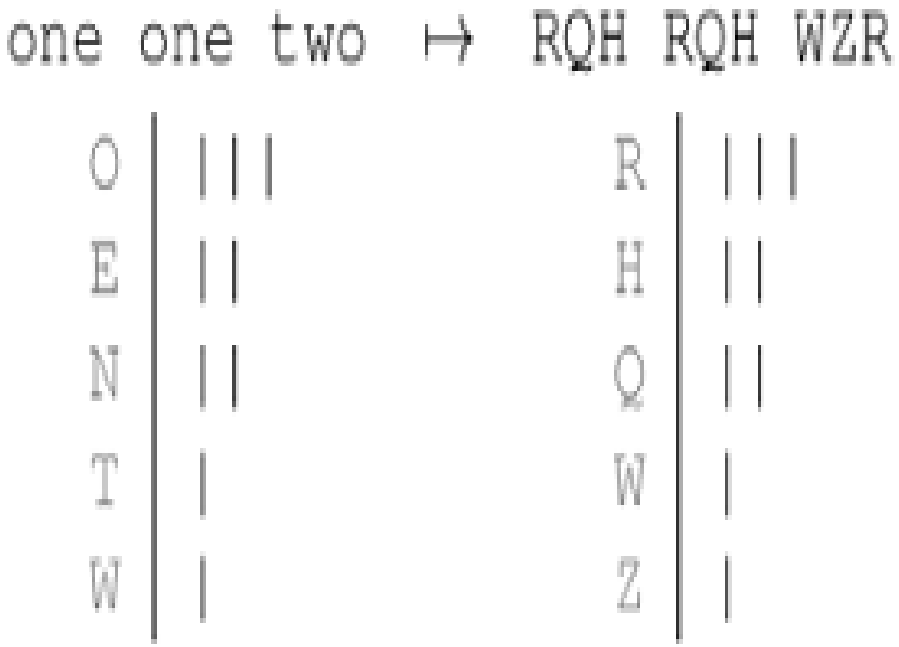
➢Cryptanalyse **par analyse de fréquence**





➢Cryptanalyse **par analyse de fréquence**

- Si le cryptosystème est une substitution monoalphabétique alors DE est une permutation de DC



➢Cryptanalyse **par analyse de fréquence**

Exemple: Substitution arbitraire

BQPSNRSJXJNJXLDPCLDLPQBE_QRKJXHNKPKSJPJIKSPUNBDKIQRB
KPQPBQPZITEJQDQBTSKPELNIUNPHNKPBKPCKSSQWKPSLXJPSNV
VXSQCCKDJPBLDWPXBPSNVVXJPGKPJKDXIPZLCEJKPGKSPSJQJXSJX
HNKSPGPLZZNIIKDZKPGKSPGXVVKIKDJKSPBKJJIKS

➢Cryptanalyse **par analyse de fréquence**

Exemple: Substitution arbitraire

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

➢Cryptanalyse **par analyse de fréquence**

Exemple: Substitution arbitraire

Remplaçons P par _ et K par E

BQ_SNRSJXJNJXLD_CLDL_QBE_QREJXHNE_ESJ_JIE
S_UNBDEIQRBE_Q_BQ_ZITEJQDQBTSE_ELNIUN_HN
E_BE_CESSQWE_SLXJ_SNVVXSQCCEDJ_BLDW_XB_
SNVVXJ_GE_JEDXI_ZLCEJE_GES_SJQJXSJXHNES_G
_LZZNIIEDZE_GES_GXVVEIEDJES_BEJJIES

Remplaçons Q par A et B par L

LA_SNRSJXJNJXLD_CLDL_ALE_AREJXHNE_ESJ_JIES
_UNLDEIARLE_A_LA_ZITEJADALTSE_ELNIUN_HNE_L
E_CESSAWE_SLXJ_SNVVXSACCEDJ_LLDW_XL_SNV
VXJ_GE_JEDXI_ZLCEJE_GES_SJAJXSJXHNES_G_LZ
ZNIIEDZE_GES_GXVVEIEDJES_LEJJIES

➢Cryptanalyse **par analyse de fréquence**

Exemple: Substitution arbitraire

Remplaçons S par S et G par D

LA_S**NR**S**JXJNJXLD_CLDL**_AL**E_AR**E**JXHN**E_ES**J_JI**ES
_UNLD**E**I**AR**LE_A_LA_**ZITEJ**A**D**AL**T**SE_**ELNIUN_HN**E_L
E_**C**ESSA**W**E_S**LXJ**_S**NVVX**SA**CC**E**DJ**_L**LDW_X**L_S**NV
VXJ_DE_J**E**D**XI_ZLCEJ**E_DES_SJA**JX**S**JXHN**ES_D_**LZZ
NIIE**DZ**E_DES_D**XVV**E**I**E**DJ**ES_LE**JJI**ES

Remplaçons J par T et I par R

LA_S**NR**ST**X**T**N**T**XLD_CLDL**_AL**E_AR**ET**XHN**E_EST_TR
ES_**UN**L**D**ER**AR**LE_A_LA_**Z**R**TE**TA**D**AL**T**SE_**ELN**R**UN_H
NE_LE_**C**ESSA**W**E_S**LX**T_S**NVVX**SA**CC**E**DT**_L**LDW_X**L_
S**NVVX**T_DE_TE**DX**R_**ZLCE**TE_DES_STAT**X**ST**XHN**ES_
D_**LZZN**RRE**DZ**E_DES_D**XVV**ERE**D**TES_LETTRES

➢Cryptanalyse **par analyse de fréquence**

Exemple: Substitution arbitraire

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**UL**D**ERA**R**LE_A_LA_**Z**R**TE**TA**D**AL**T**SE_**EL**UR**U**U_QUE
_LE_**C**ESSA**W**E_S**L**IT_SU**VV**ISA**CC**E**D**T_L**LDW**_IL_SU**V**
VIT_DE_TE**D**IR_**ZLCE**TE_DES_STATISTIQUES_D_**LZZ**U
RRE**DZ**E_DES_DI**VV**ERE**D**TES_LETTRES

Remplaçons V par F et D par N

LA_SU**RS**TITUTI**LN**_**CLNL**_AL**E**_A**R**ETIQUE_EST_TRES
_**U**ULNERA**R**LE_A_LA_**Z**R**TE**TANAL**T**SE_**EL**UR**U**U_QUE
_LE_**C**ESSA**W**E_S**L**IT_SUFFISA**CC**ENT_L**L**N**W**_IL_SUFF
IT_DE_TENIR_**ZLCE**TE_DES_STATISTIQUES_D_**LZZ**UR
REN**Z**E_DES_DIFFERENTES_LETTRES

➢Cryptanalyse **par analyse de fréquence**

Exemple: Substitution arbitraire

Remplaçons R par B et L par O

LA_SUBSTITUTION_**C**ONO_AL**E**_A**R**ETIQUE_EST_TRE
S_**U**ULNERABLE_A_LA_**Z**R**TE**TANAL**T**SE_**E**OUR**U**U_QU
E_LE_**C**ESSA**W**E_SOIT_SUFFISA**CC**ENT_LON**W**_IL_SU
FFIT_DE_TENIR_**Z**O**CE**TE_DES_STATISTIQUES_D_O**Z**
ZURREN**Z**E_DES_DIFFERENTES_LETTRES

Finalement

LA_SUBSTITUTION_MONO_ALPHABETIQUE_EST_TRE
S_VULNERABLE_A_LA_CRYPTANALYSE_POURVU_QU
E_LE_MESSAGE_SOIT_SUFFISAMMENT_LONG_IL_SU
FFIT_DE_TENIR_COMPTE_DES_STATISTIQUES_D_OC
CURRENCE_DES_DIFFERENTES_LETTRES

Cryptanalyse **par analyse de fréquence**

- Si le cryptosystème est une substitution polyalphabétique alors D_E est différent de D_C

```
clueclueclueclueclue
teleconference ↦  VPFIEZHJGCYREP
```

E	4
C	2
N	2
F	1
L	1
O	1
T	1

E	2
P	2
C	2
F	1
G	1
H	1
I	1
J	1
R	1
V	1
Y	1
Z	1

➢Cryptanalyse d'un chiffre de Vigenère

KQOWE FVJPU JUUNU KGLME KJINM WUXFQ MKJBG WRLFN FGHUD
WUUMB SVLPS NCMUE KQCTE SWREE KOYSS IWCTU AXYOT APXPL
WPNTC GOJBG FQHTD WXIZA YGFFN SXCSE YNCTS SPNTU JNYTG
GWZGR WUUNE JUUQE APYME KQHUI DUXFP GUYTS MTFFS HNUOC
ZGMRU WEYTR GKMEE DCTVR ECFBD JQCUS WVBPN LGOYL SKMTE
FVJJT WWMFM WPNME MTMHR SPXFS SKFFS TNUOC ZGMDO EOYEE
KCPJR GPMUR SKHFR SEIUE VGOYC WXIZA YGOSA ANYDO EOYJL WUNHA
MEBFE LXYVL WNOJN SIOFR WUCCE SWKVI DGMUC GOCRU WGNMA
AFFVN SIUDE KQHCE UCPFC MPVSU DGAVE MNYMA MVLFM AOYFN
TQCUA FVFJN XKLNE IWCWO DCCUL WRIFT WGMUS WOVMA TNYBU
HTCOC WFYTN MGYTQ MKBBN LGFBT WOJFT WGNTE JKNEE DCLDH
WTVBU VGFBI JG

➢Cryptanalyse d'un chiffre de Vigenère

Phase 1 : Trouver la longueur de la clé

Étape 1 : Soulignez les répétitions de 3 caractères ou plus :

KQOWE FVJPU JUUNU KGLME KJINM WUXFQ MKJBG WRLFN FGHUD
WUUMB SVLPS NCMUE KQCTE SWREE KOYSS IWCTU AXYOT APXPL
WPNTC GOJBG FQHTD WXIZA YGFFN SXCSE YNCTS SPNTU JNYTG
GWZGR WUUNE JUUQE APYME KQHUI DUXFP GUYTS MTFFS HNUOC
ZGMRU WEYTR GKMEE DCTVR ECFBD JQCUS WVBPN LGOYL SKMTE
FVJJT WWMFM WPNME MTMHR SPXFS SKFFS TNUOC ZGMDO EOYEE
KCPJR GPMUR SKHFR SEIUE VGOYC WXIZA YGOSA ANYDO EOYJL
WUNHA MEBFE LXYVL WNOJN SIOFR WUCCE SWKVI DGMUC GOCRU
WGNMA AFFVN SIUDE KQHCE UCPFC MPVSU DGAVE MNYMA MVLFM
AOYFN TQCUA FVFJN XKLNE IWCWO DCCUL WRIFT WGMUS WOVMA
TNYBU HTCOC WFYTN MGYTQ MKBBN LGFBT WOJFT WGNTE JKNEE
DCLDH WTVBU VGFBI JG

➢Cryptanalyse d'un chiffre de Vigenère

Étape 2 : Pour chaque répétition, mesurer la période

Séquence répétée	Distance
WUU	95
EEK	200
WXIZAYG	190
NUOCZGM	80
DOEOY	45
GMU	90

➢Cryptanalyse d'un chiffre de Vigenère

Étape 3 : Pour chaque période, décomposer en facteurs premiers et regarder quel facteur est commun à tous :

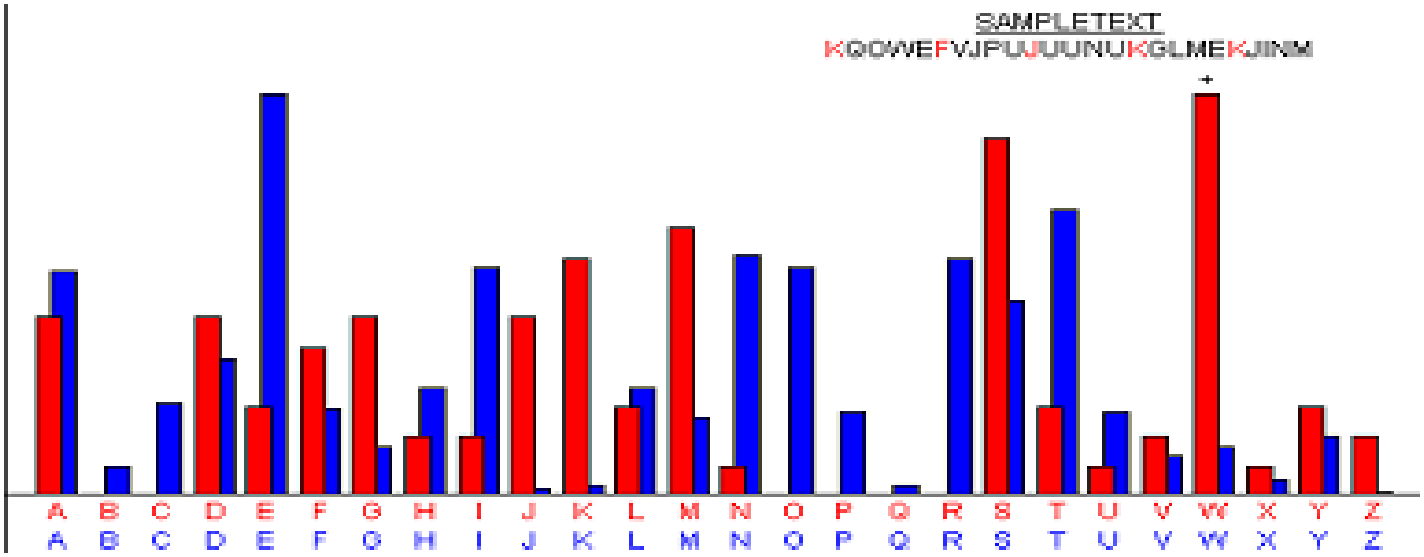
La clé est ici longue de 5 caractères.

		Longueurs de clef possibles			
Séquence répétée	Espace de répétition	2	3	5	19
WUU	95			x	x
EEK	200	x		x	
WXIZAYG	190	x		x	x
NUOCZGM	80	x		x	
DOEOY	45		x	x	
GMU	90	x	x	x	

➢Cryptanalyse d'un chiffre de Vigenère

Phase 2 : Trouver la 1er lettre du mot clé

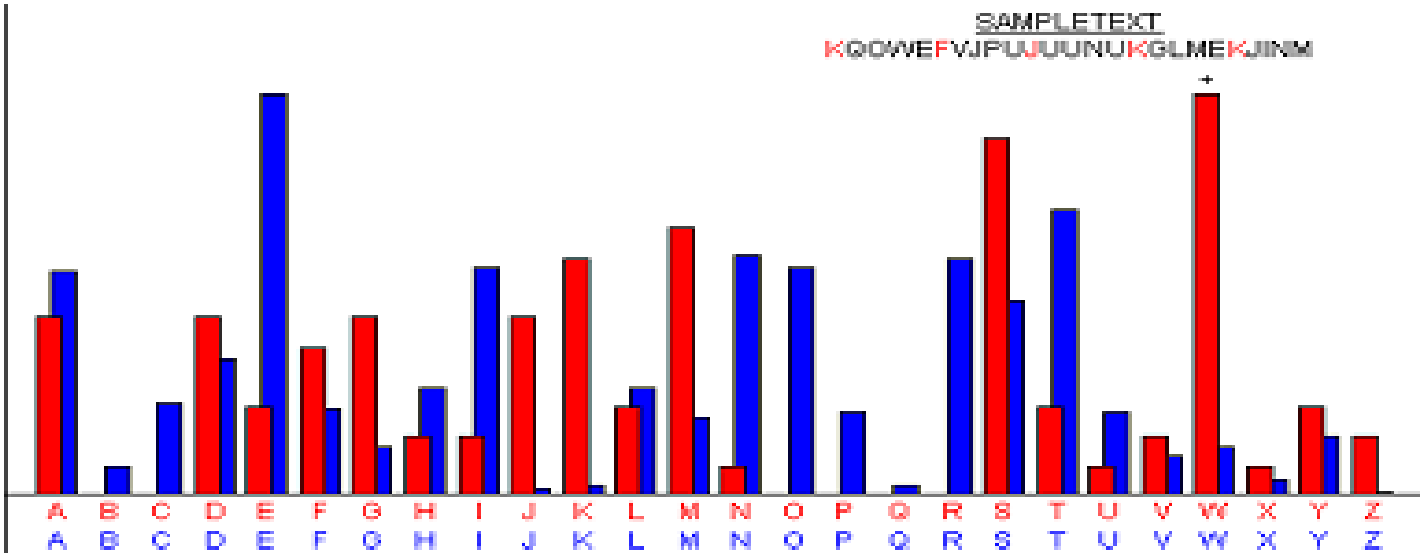
Étape 1 : Faire une analyse de fréquence
seulement sur les caractères 1, 6, 11, ...
On obtient ici :



➢Cryptanalyse d'un chiffre de Vigenère

En rouge, l'analyse de fréquence « modulo 5 »
En bleu le diagramme de fréquence des lettres en français.

Étape 2 : On décale pour faire correspondre
On décale les diagrammes pour mettre le pic du W sur le E
... L'ensemble correspond à peut prés : On à la première lettre de la clé.

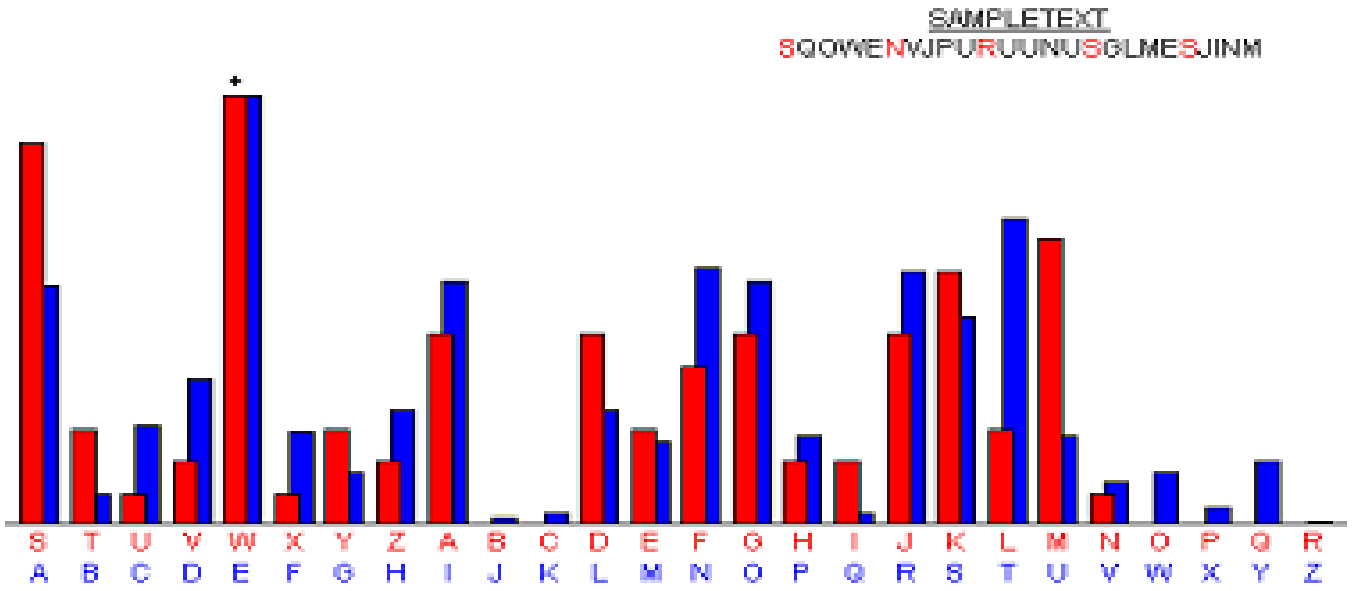


➢Cryptanalyse d'un chiffre de Vigenère

Avec W = 23 et E = 5, c'est la (23 – 5 + 1= 19_{eme}) soit S

Phase 3, 4, 5 et 6 : On recommence pour avoir les 5 lettres du mot clé.

Le mot clé est SCUBA



➢Cryptanalyse d'un chiffre de Vigenère

On peut déchiffrer le cryptogramme :
Soit encore :
Souvent pour s'amuser les hommes d'équipage prennent des albatros, vastes oiseaux des mers, qui suivent, indolents compagnons de voyage, le navire glissant sur les gouffres amers.
A peine les ont-ils déposés sur les planches que ces rois de l'azur, maladroits et honteux, laissent piteusement leurs grandes ailes blanches, comme des avirons, traîner à côté d'eux.
Ce voyageur ailé, comme il est gauche et veule, lui naguère si beau, qu'il est comique et laid. L'un agace son bec avec un brûle-gueule, l'autre mime en boitant l'infirme qui volait.
Le poète est semblable au prince des nuées, qui hante la tempête et se rit de l'archer.
Charles Baudelaire

➢Limites de l'analyse de fréquences

Échantillon représentatif

- On a besoin d'un texte assez long pour que les statistiques soient représentatives.
- Certains textes n'obéissent pas aux lois des fréquences.

- Dans le texte suivant la lettre Z, généralement la moins utilisée dans les textes en français, est la plus utilisée.

«*De Zanzibar à la Zambie et au Zaïre, des zones d'ozone font courir les zèbres en zigzags zinzins* »

- Georges Perec a écrit tout un livre *La dispariation* sans utiliser la lettre **e**