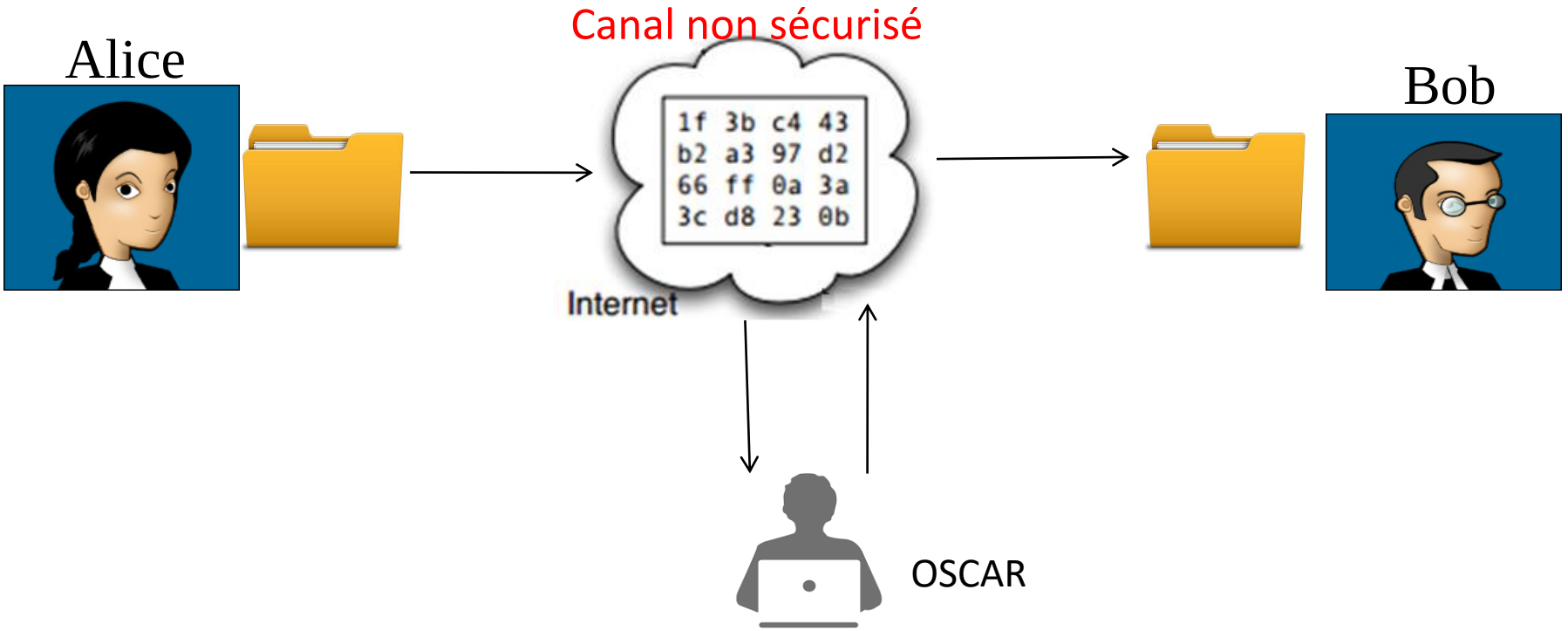
Cryptographie et Sécurité

Pr. D. AIT OMAR
Faculté des Sciences et Techniques
-Beni Mellal-

plan

- Cryptographie classique
  - Substitution monoalphabétique
  - Substitution polyalphabétique
  - Substitution polygramme
  - Chiffrement par transposition
- Cryptographie moderne
  - Cryptographie symétrique
    - Par flot
    - Par bloc
      - DES
      - AES
  - Cryptographie asymétrique
    - RSA
    - El Gamal
- Signature
- Fonctions de Hashage
- MAC: Message authentification code

Introduction



- Problème de confidentialité, d'intégrité et d'authentification

Les buts de la cryptographie

Elle doit satisfaire plusieurs fonctions :

- La confidentialité
- L'authentification
- L'intégrité
- La non répudiation

Les buts de la cryptographie

La confidentialité

- Il s'agit de garantir le secret de l'information transmise ou archivée.
- Seuls les utilisateurs autorisés doivent y avoir accès.

Les buts de la cryptographie

L'authentification:

- l'émetteur est sûr de l'identité du destinataire c'est à dire que seul le destinataire pourra prendre connaissance du message car il est le seul à disposer de la clef de déchiffrement.

- le destinataire est sûr de l'identité de l'émetteur

- L'authentification Consiste à vérifier qu'une personne possède bien l'identité, ou les droits, qu'elle affirme avoir.

Les buts de la cryptographie

L’intégrité

- Il s’agit de préserver les informations contre les modifications.
- "L’intégrité est la prévention d’une modification non autorisée de l’information "
- Avec les techniques actuelles, cette fonction est réalisée par la signature numérique.

Les buts de la cryptographie

La non répudiation

- Impossibilité, pour une personne ou pour toute autre entité engagée dans une communication par voie informatique, de nier avoir reçu ou émis un message.

- Les algorithmes asymétriques assurent la non-répudiation d'un message signé dans la mesure où seul l'expéditeur possède la clé secrète utilisée pour cette signature.

Terminologie

- La cryptologie est la science du secret. Elle se divise en deux disciplines :
  - La cryptographie qui est l'étude des algorithmes permettant de protéger de l'information. Ces algorithmes sont appelés cryptosystèmes ;
  - la cryptanalyse qui est l'étude du niveau de sécurité des cryptosystèmes fournis par les cryptographes.

Terminologie

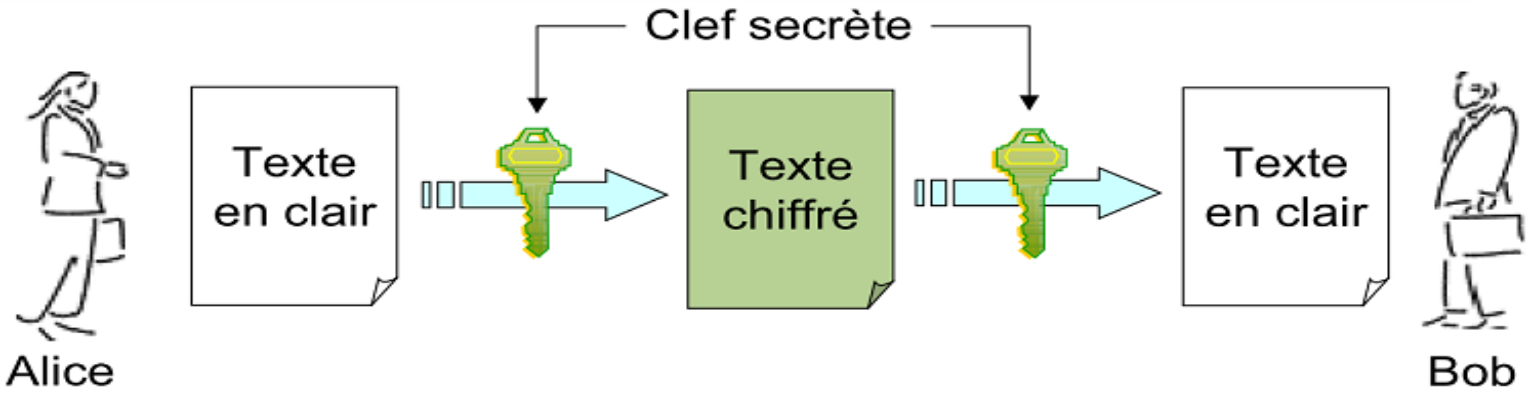
- Chiffrer : l'action de rendre un message en clair M (plaintext) en un message illisible C appelé (ciphertext) cryptogramme ou message chiffré.
- Déchiffrer : Action inverse du chiffrement.
- Cryptosystème : L'algorithme (ou le dispositif physique) permettant de chiffrer des données.
- Attaquer, Casser : Mettre à mal la sécurité d'un cryptosystème (retrouver M à partir de C sans connaitre la clé, retrouver la clé).

Terminologie

- Message en clair/ message chiffré(cryptogramme)
- Chiffrer /déchiffrer: avec une clé= action autorisée,
- Décrypter: sans la clé= action illégale!
- Algorithme: description non-ambiguë d'une méthode de résolution d'un problème.
- Protocole: description non-ambiguë d'une suite d'interactions entre plusieurs participants.

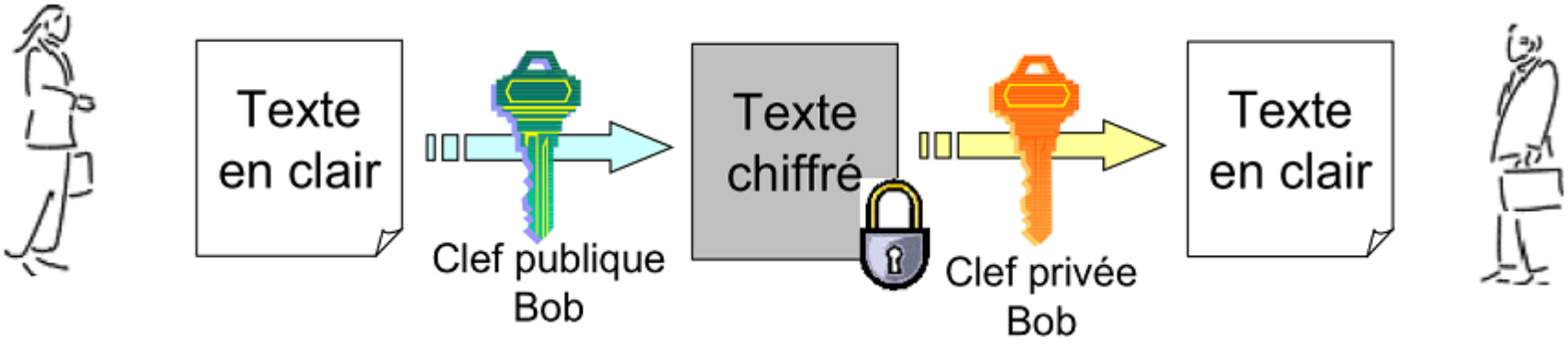
Terminologie

- Il existe 2 types de chiffrement:
  - Le chiffrement symétrique (ou chiffrement à clé privée) consiste à utiliser la même clé pour le chiffrement et le déchiffrement.



Terminologie

– Le chiffrement asymétrique (ou chiffrement à clés publiques) consiste à utiliser une clé publique pour le chiffrement et une clé privée pour le déchiffrement.



Cryptographie classique

Quelques cryptosystèmes classiques

- Chiffrement par substitution
  - Substitution monoalphabétique
    - Chiffre de César
    - Chiffre affine
  - Substitution polyalphabétique
    - Chiffre de Vigenère
    - Chiffre de Vernam
  - Substitution polygrammes
    - Chiffre de Playfair
- Chiffrement par transposition
  - Transposition simple par colonnes
  - Transposition complexe par colonnes

Chiffrement par substitution

Définition:

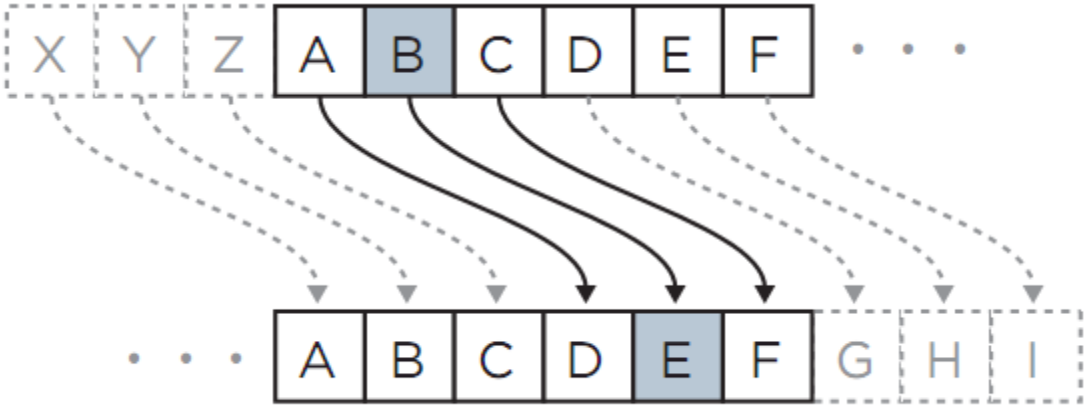
- Le chiffrement par substitution consiste à remplacer dans un message une ou plusieurs entités (généralement des lettres) par une ou plusieurs autres entités.

- Toutes les substitutions simples sont vulnérables à une analyse des fréquences d'apparition des lettres.

Chiffrement par substitution

Chiffre de César:

- Substituer chaque lettre du message en clair par une autre située à distance fixe dans l'alphabet. Cette distance devait être connue de l'expéditeur comme du destinataire.
- décalage de trois lettres :



Chiffrement par substitution

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

Chiffrement de César:

- Principe :
  - Soit p (c, respec.) l'indice de la lettre du message en clair(chiffré,respec.) et k le décalage (la clé: k=3):
  - Chiffrement : $c = E_k(p) = (p + k) \bmod 26$
  - Déchiffrement : $p = D_k(c) = (c - k) \bmod 26$

Chiffrement par substitution

Chiffrement de César:

- Exemple :
  - Chiffrez le message « bonjour tout le monde » en utilisant le cryptosystème de César(k=3).
  - ERQMR XUWRX WOHPR QGH
  - Déchiffrez le message : «FKLII UHGHF HVDU »
  - Chiffre de Cesar
  - Décryptez le message chiffré suivant:
  - c= HMNKK WJIJH JXFW
  - CHIFFRE DE CESAR
  - Donnez la clef de chiffrement

    k=5

Chiffrement par substitution

Chiffrement de César:

- L'espace de clés est:|K|=26.

- Cette méthode est vulnérable aux attaques de type:
  - Force brute (26 clés possibles !)

  - Analyse de fréquences :

  Le principe de cette cryptanalyse consiste à deviner les lettres d'un texte clair sur la base de leur fréquence d'apparition

Chiffrement par substitution

Analyse fréquentielle:

- Fréquences d'apparition des lettres(français)

E	A	S	I	T	N	R	U	L	O	D	C	P
17,1%	8,1%	7,9%	7,5%	7,2%	7,1%	6,6%	6,3%	5,5%	5,4%	3,7%	3,2%	3%

M	V	Q	F	B	G	H	J	X	Y	Z	W
3%	1,6%	1,4%	1,1%	0,9%	0,9%	0,7%	0,5%	0,4%	0,3%	0,1%	0,1%

- Analyse des fréquences des lettres : A et E sont les plus fréquentes en français, le moins fréquent est W.

- Cette technique ne fonctionne bien que si le message chiffré est suffisamment long pour avoir des moyennes significatives.

Chiffrement par substitution

Analyse fréquentielle(di/tri-grammes):

- Digrammes les plus utilisés en langue française : ES, LE, EN …
- Trigrammes : ENT, LES, EDE…

Digrammes	Pourcentages
ES	3,15 %
LE	2,46 %
EN	2,42 %
DE	2,15 %
RE	2,09 %
NT	1,97 %
ON	1,64 %
TE	1,63 %
ER	1,63 %
SE	1,55 %

Chiffrement par substitution

Le chiffrement affine:

- L'idée est d'utiliser comme fonction de chiffrement une fonction affine du type $y=(k_1.x + k_2) \bmod 26$, où k_1 et k_2 sont des constantes, et où x et y sont des nombres correspondant aux lettres de l'alphabet (A=0,B=1,…,Z=25).

- On peut remarquer que si $k_1=1$, alors on retrouve le chiffre de César et k_2 est le décalage.

Chiffrement par substitution

Le chiffrement affine : fonctionnement

- **Message**

$$M=m_1m_2\ldots m_{n-1}m_n$$

- **Clé** :

$$(k_1, k_2) \in \{0,25\} \text{ et } \mathbf{pgcd(k_1,26)=1}$$

- **Chiffrement**:

$$c_i= f(m_i) = (k_1*m_i + k_2) \bmod 26$$

- **Déchiffrement** :

$$m_i= f^{-1}(c_i) = (u*(c_i–k_2)) \bmod 26$$

Où u est l'inverse de k_1 mod 26 (càd $k_1 *u=1 \bmod 26$)

- **Nombres de clés possibles** :

Il n'existe que 12 entiers compris entre 0 et 26 et premiers avec 26 [1, 3, 5, 7, 9, 11, 15, 17, 19, 21, 23 et 25]. Il n'existe donc que 12 × 26 = 312 clés de chiffrement possible. Cette méthode est vulnérable par force brute.

Chiffrement par substitution

Le chiffrement affine:

Identité de Bézout :

Soient a et b deux entiers relatifs. Si d est le PGCD de a et b, alors il existe deux entiers relatifs x et y tels que ax + by = d.

- On a pgcd(k_1,26)=1, alors il existe x et y tels que :

$$k_1.x+26.y=1$$

- Si On prend cette équation mod 26, on trouve que:

$$k_1.x=1 \bmod 26 \text{ (car } 26 = 0 \bmod 26)$$

D'où u=x

Chiffrement par substitution

Le chiffrement affine:

- Exemple:
  - Clé = $(k_1, k_2) = (17,3)$
  - Message : C O D E → 2 ; 14 ; 3 ; 4
  - Chiffrement :

$$c_i = f(m_i) = (17 * m_i + 3) \bmod 26$$

C= L H C T

  - Déchiffrement :

17.x+26.y=1 → u=-3 et y=2, donc u=-3 mod 26 = 23

$$m_i = f^{-1}(c_i) = 23 * (c_i - 3) \bmod 26$$

On trouve 2 ; 14 ; 3 ; 4 - > M = C O D E

Chiffrement par substitution

Le chiffrement affine : Recherche de l'inverse

- **Algorithme d'Euclide étendu:**

```
 Entrée : a, b entiers (naturels)
Sortie : r entier (naturel) et  u, v entiers relatifs tels que r = pgcd(a, b) et r = a*u+b*v

Initialisation : r := a, r' := b, u := 1, v := 0, u' := 0, v' := 1
                 q  quotient entier
                 rs, us, vs  variables de stockage intermédiaires

les égalités r = a*u+b*v et r' = a*u'+b*v' sont des invariants de boucle

tant que (r' ≠ 0) faire
    q := r÷r'
    rs := r, us := u, vs := v,
    r := r', u := u', v := v',
    r' := rs - q*r', u' = us - q*u', v' = vs - q*v'
   fait
renvoyer (r, u, v)
```

Chiffrement par substitution

Cryptanalyse: chiffre affine

- message chiffré : HGAHY RAEFT GAGRH DGAGM OEHIY RAAOT ZGAGJ GKFDG AZGSB INNTG KGRHE NNIRG
- Sachant que le message a été chiffré par le chiffre affine, trouvez le message en clair (utiliser une analyse de fréquence).

- Solution:
  - ✓ On remarque que G apparait 13 fois et A 8 fois.
  - ✓ E, S, A, I sont les lettres les plus fréquentes, donc

E → G et S → A

Indice 4

Indice 18

Chiffrement par substitution

Cryptanalyse: chiffre affine

Trouver $(k_1; k_2)$??

On a

$$E_{k1;\,k2}(E)=G \quad \text{et} \quad E_{k1;\,k2}(S)=A$$

$$4k_1 + k_2 = 6 \bmod 26 \quad \text{et} \quad 18k_1 + k_2 = 0 \bmod 26$$

Alors

$$14k_1=-6 \bmod 26 \rightarrow 7k_1=20 \bmod 26 \rightarrow 7k_1=10 \bmod 13.$$

D'où

$$\mathbf{k_1=7 \text{ et } k_2=4.}$$

Le message déchiffré est:

TESTONS A PRESENT LES EQUATIONS SUR DES EXEMPLES DE CHIFFREMENT AFFINE

Chiffrement par substitution

Subst. polyalphabétique: chiffre de Vigenère

- Le **chiffre de Vigenère** est une amélioration décisive du chiffre de César.
- Sa force réside dans le fait que ce chiffre utilise une **clef** qui définit le décalage pour chaque lettre du message.

Chiffrement par substitution

Exemple: Chiffrement de Vigenère

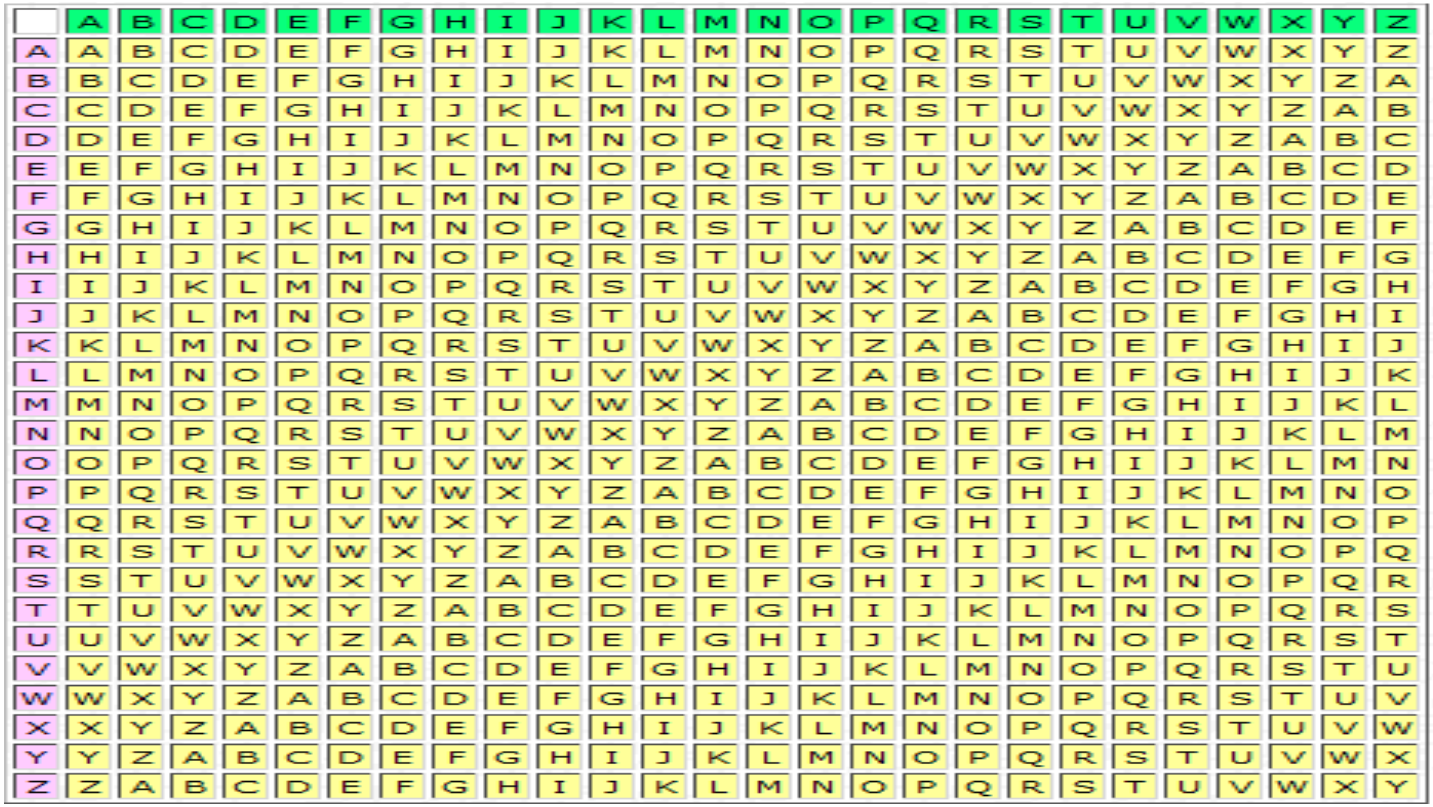
chiffrons le texte "CHIFFRE DE VIGENERE" avec la clef « IDBM"

(cette clef est éventuellement répétée plusieurs fois pour être aussi longue que le texte en clair).

clair	c	h	i	f	f	r	e	d	e	v	i	g	e	n	e	r	e
clef	i	d	b	m	i	d	b	m	i	d	b	m	i	d	b	m	i
décalage	8	3	1	12	8	3	1	12	8	3	1	12	8	3	1	12	8
chiffré	k	g	j	r	n	u	f	p	m	x	j	s	m	q	f	d	M

Chiffrement par substitution

Carré de Vigenère

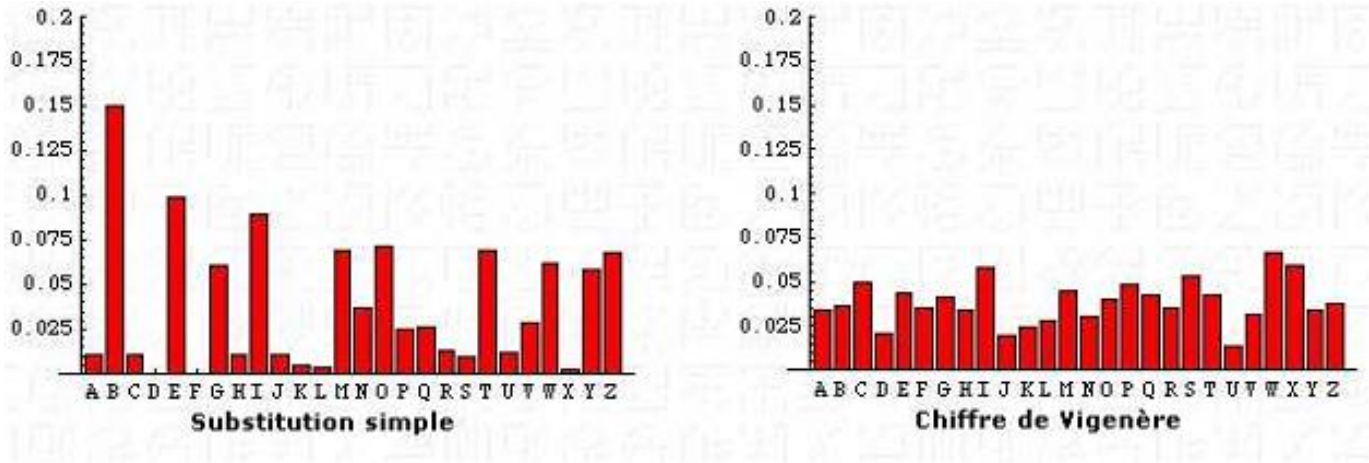


	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
C	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T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

- ✓ La lettre de la clef est dans la colonne la plus à gauche,
- ✓ la lettre du message clair est dans la ligne tout en haut.
- ✓ La lettre chiffrée est à l'intersection des deux.

Chiffrement par substitution

La grande force du chiffre de Vigenère est que la même lettre sera chiffrée de différentes manières d'où perte de la fréquence des lettres, ce qui rend inutilisable l'analyse de fréquence classique.



Perte de la fréquence des lettres

Chiffrement par substitution

Chiffre Playfair:

- Le chiffre de Playfair utilise un tableau de 5×5 lettres, contenant un mot clé.
- La mémorisation du mot clé et de 4 règles à suivre pour utiliser ce chiffrement.
- Remplir le tableau avec les lettres du mot clé (en ignorant les doublons), puis le compléter avec les autres lettres de l'alphabet dans l'ordre.
- **W exclu** car inutile, on utilise **V à la place**
- La variante anglaise consiste à garder le W et à fusionner I et J.

Chiffrement par substitution

Chiffre Playfair:

Exemple

- Soit le mot clé = GALOIS, Donner le carré Playfair correspondant :

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

Chiffrement par substitution

- Chiffre Playfair **:** Chiffrement :

Pour chiffrer un message, il faut prendre les lettres 2 par 2 et appliquer les règles suivantes en fonction de la position des lettres dans la table :

1. Si les **2 lettres sont identiques** (ou s'il n'en **reste qu'une**) **mettre un 'X' après la première lettre**. Chiffrer la nouvelle paire ainsi constituée et continuer avec la suivante. Par exemple pour chiffrer le message **'OR'.**
2. Si les lettres se trouvent sur **la même ligne de la table**, il faut les remplacer par celles se trouvant immédiatement à leur droite (en bouclant sur la gauche si le bord est atteint),

sur la même ligne

OR → YZ

YR → RZ

Chiffrement par substitution

- Chiffre Playfair : Chiffrement :

3. Si les lettres apparaissent sur la **même colonne**, les **remplacer** par celles qui sont juste **en dessous** (en bouclant par le haut si le bas de la table est atteint),

sur la même colonne

OR → BY

RY → YO

4. **Sinon**, **remplacer** les lettres par celles se trouvant **sur la même ligne**, mais dans le **coin opposé** du **rectangle** défini par la paire originale.

forment un rectangle

OR → ZX

Chiffrement par substitution

- Chiffre Playfair : Déchiffrement :
- Utiliser la **méthode inverse** en prenant les **lettres à gauche** dans le cas d'une même **ligne**, vers le **haut** dans le cas d'une même **colonne**, et toujours les **coins opposés** dans le cas d'un rectangle.
- Ignorer les 'X' qui n'ont pas leur place dans le message final.

Chiffrement par substitution

Exercice :

1) Soit la clé « exemple playfair », remplissez le tableau et chiffrez le message M=« Cache l'or dans la souche de l'arbre » :

CA CH EL OR DA NS LA SO UC HE DE LA RB RE

BY DB XE QI BF JU ER VJ TD BL BM ER AH AL

2) Déchiffrer le message « **AE SC PX**» :

AE SC PX

ES TB ME

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

Chiffrement par substitution

Chiffre de Vernam (One-Time Pad)

- Masque jetable = chiffre de Vigenère avec comme caractéristique que la clef de chiffrement a la même longueur que le message en clair.
- Exemple :
  - Message clair: Masque jetable
  - Clef : xcaatelprvgzc

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

Chiffrement par substitution

Chiffrement de Vernam (One-Time Pad)

- Méthode du masque jetable, Il faut :
  1. Choisir une clef aussi longue que le texte à chiffrer,
  2. Utiliser une clef formée d'une suite de caractères aléatoires,
  3. Protéger votre clef,
  4. Ne jamais réutiliser une clef,
  5. Écrire des textes clairs ne contenant que les lettres (sans ponctuation et sans espaces).

Chiffrement par substitution

Difficultés du chiffrement de Vernam:

- Le problème de ce système est de communiquer les clefs de chiffrement ou de trouver un algorithme de génération de clef commun aux deux partenaires :
  1. La création de grandes quantités des clefs aléatoires : n'importe quel système fortement utilisé pourrait exiger des millions de caractères aléatoires de façon régulière.
  2. La distribution des clés : une clé de longueur égale est nécessaire pour l'expéditeur et pour le récepteur. Nécessite une bonne organisation.

Chiffrement par substitution

Chiffre polygrammique: Le chiffre Playfair:

- Le chiffre de Playfair utilise un tableau de 5×5 lettres, contenant un mot clé.
- La mémorisation du mot clé et de 4 règles à suivre suffisent pour utiliser ce chiffrement.
- Remplir le tableau avec les lettres du mot clé (en ignorant les doublons), puis le compléter avec les autres lettres de l'alphabet dans l'ordre.
- W exclu car inutile, on utilise V à la place
- La variante anglaise consiste à garder le W et à fusionner I et J.

Chiffrement par substitution

- Pour chiffrer un message, il faut prendre les lettres 2 par 2 et appliquer les règles suivantes en fonction de la position des lettres dans la table :
  1. si les 2 lettres sont identiques (ou s'il n'en reste qu'une) mettre un 'X' après la première lettre. Chiffrer la nouvelle paire ainsi constituée et continuer avec la suivante.
  2. si les lettres se trouvent sur la même ligne de la table, il faut les remplacer par celles se trouvant immédiatement à leur droite (en bouclant sur la gauche si le bord est atteint),
  3. si les lettres apparaissent sur la même colonne, les remplacer par celles qui sont juste en dessous (en bouclant par le haut si le bas de la table est atteint),
  4. sinon, remplacer les lettres par celles se trouvant sur la même ligne, mais dans le coin opposé du rectangle défini par la paire originale.

Chiffrement par substitution

- Pour chiffrer le digramme 'OR' par exemple, trois configurations peuvent se présenter dans le tableau :

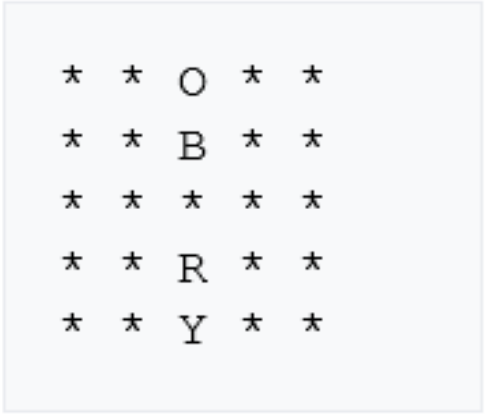
1)

sur la même ligne

alors, OR → YZ

2)

sur la même colonne



alors, OR → BY

3)

forment un rectangle

alors, OR → ZX

Chiffrement par substitution

Pour déchiffrer:

- utiliser la méthode inverse en prenant les lettres à gauche dans le cas d'une même ligne, vers le haut dans le cas d'une même colonne, et toujours les coins opposés dans le cas d'un rectangle.
- Ignorer les 'X' qui n'ont pas leur place dans le message final.

Chiffrement par substitution

- **Exemple**
- En supposant que la clé soit « exemple playfair », remplissez le tableau:

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

- Chiffrez le message « Cache l'or dans la souche de l'arbre » :
- soit

  BY DB XE QI BF JU ER VJ TD BL BM ER AH AL

Chiffrement par substitution

- Ce chiffrement est significativement plus dur à casser car les attaques par analyse fréquentielle habituellement utilisées sur les chiffrements par substitutions simples sont peu efficaces sur lui.
- L'analyse de fréquence des digrammes reste toujours possible, mais appliquée à $25^2 = 625$ digrammes possibles au lieu des 26 lettres de l'alphabet, elle est considérablement plus difficile et exige un texte chiffré beaucoup plus long pour espérer être efficace.

Chiffrement par transposition

Définition:

- Les méthodes de chiffrement par transposition consistent à réarranger les données à chiffrer de telle façon à les rendre incompréhensibles.

- Transposition simple par colonnes :
  - On écrit le message horizontalement dans une matrice prédéfinie, et on trouve le texte à chiffrer en lisant la grille verticalement .
  - Le destinataire légal pour déchiffrer le message réalise le procédé inverse.

Chiffrement par transposition

Transposition simple par colonnes :

- Exemple:
  - texte à chiffrer= «faculte polydisciplinaire de beni mellal» en utilisant une matrice 5x6.

f	a	c	u	l	t
e	d	e	s	s	c
i	e	n	c	e	s
e	t	t	e	c	h
n	i	q	u	e	s

  - **Soit**

    Feien adeti centq usceu lsece tcshs

Chiffrement par transposition

Transposition complexe par colonnes :

- Une clé secrète (avec uniquement des caractères) est utilisé pour dériver une séquence de chiffres commençant à 1 et finissant au nombre de lettres de la clé.

- Cette séquence est obtenue en numérotant les lettres de la clé en partant de la gauche vers la droite et en donnant l'ordre d'apparition dans l'alphabet.

- On chiffre en écrivant d'abord le message par lignes dans un rectangle , puis on lit le texte par colonnes en suivant l'ordre déterminé par la séquence(clef).

Chiffrement par transposition

Transposition complexe par colonnes :

- Exemple:
- Prenons l'exemple la clef : **DELIVRANCE**

D	E	L	I	V	R	A	N	C	E
|	|	|	|	|	|	|	|	|	|
3	4	7	6	10	9	1	8	2	5

- on souhaite chiffrer : "VENEZ NOUS AIDER AU PORT DE BREST" :

3	4	7	6	10	9	1	8	2	5
V	E	N	E	Z	N	O	U	S	A
I	D	E	R	A	U	P	O	R	T
D	E	B	R	E	S	T	X	Y	Z

- OPT SRY VID EDE ATZ ERR NEB UOX NUS ZAE

Chiffrement par transposition

Transposition complexe par colonnes :

- Exemple:
  - voici un message déjà chiffré, VTGURX SDEAEM SCYRRS UCEOEE ZPAEYS par la clef **DELIVRANCE**.
  - Déchiffrez le message ci-dessus.

3	4	7	6	10	9	1	8	2	5
S	A	U	R	E	Z	V	O	U	S
D	E	C	R	Y	P	T	E	R	C
E	M	E	S	S	A	G	E	X	Y

  - Solution: Saurez vous décrypter ce message

Cryptanalyse

- Deux grands types d'attaques en cryptographie:
  - Attaques passives
  - Attaques actives

- Dans une attaque passive, l'opposant (Oscar) se contente d'écouter les messages qui transitent sur le canal de communication.
  - Menace sur la confidentialité

- Dans une attaque active, l'opposant modifie le contenu des messages échangés sur le canal de communication.
  - Menace sur l'intégrité et l'authentification

Cryptanalyse

les attaques potentielles les plus connues :

- Attaque à texte chiffré connu
- Attaque à texte clair connu
- Attaque à texte clair choisi
- Attaque à texte chiffré choisi
- Attaque par recherche exhaustive
- Etc.

Cryptanalyse

- **L'attaque à texte chiffré connu**
  - Le cryptanalyste dispose du texte chiffré de plusieurs messages, tous ayant été chiffrés avec le même algorithme.
  - Sa tâche est de retrouver le plus grand nombre de messages clairs possibles, ou mieux encore de retrouver la ou les clefs qui ont été utilisées, ce qui permettrait de déchiffrer d'autres messages chiffrés avec ces mêmes clefs

Cryptanalyse

- **L'attaque à texte clair connu**
  - Le cryptanalyste a non seulement accès aux textes chiffrés de plusieurs messages, mais aussi aux textes clairs correspondants.
  - La tâche est de retrouver la ou les clefs qui ont été utilisées pour chiffrer ces messages ou un algorithme qui permet de déchiffrer d'autres messages chiffrés avec ces mêmes clefs.

Cryptanalyse

- **L'attaque à texte clair choisi**
  - Le cryptanalyste a non seulement accès aux textes chiffrés et aux textes clairs correspondants, mais de plus il peut choisir les textes en clair.
  - Cette attaque est plus efficace que l'attaque à texte clair connu, car le cryptanalyste peut choisir des textes en clair spécifiques qui donneront plus d'informations sur la clef.

Cryptanalyse

- **L'attaque à texte chiffré choisi**
  - Le cryptanalyste peut choisir différents textes chiffrés à déchiffrer.
  - Les textes déchiffrés lui sont alors fournis.
  - Par exemple, le cryptanalyste a un dispositif qui ne peut être désassemblé et qui fait du déchiffrement automatique. Sa tâche est de retrouver la clef.

Cryptanalyse

Substitutions polyalphabétique

- Si on connaît la longueur de la clé n
  - On réarrange le cryptogramme en n groupes de lettres
  - On applique l'analyse statistique classique sur chaque groupe
- Si on ne connaît pas la longueur de la clé
  - On cherche à la découvrir!
  - On applique l'analyse statistique classique sur chaque groupe

Cryptanalyse

Indice de coïncidence :

- est utilisé pour déterminer la longueur de la clé dans un chiffrement de Vigenère.

- Ce concept fut mis au point par le cryptologue américain W. Friedman qui le publia en 1920,

Principe:

- Dans un texte quelconque de n lettres, on compte le nombre de répétition de chaque lettre :
  - N_A= nombre de A dans le texte
  - N_B = nombre de B dans le texte
  - …….
  - N_Z = nombre de Z dans le texte
- On calcul l'Indice de coïncidence simplement par la formule:

$$IC = \frac{N_A(N_A-1)+N_B(N_B-1)+\ldots+N_Z(N_Z-1)}{N(N-1)}$$

Cryptanalyse

Indice de coïncidence:

- Exemple:
  - calculons l'indice de coïncidence du texte : *Un enfant n'a pas d'aversion pour la laideur de sa mère*
  - le nombre de lettres dans cette phrase est n=43, le nombre de a est 7, le nombre de b et de c est 0, le nombre de d est 3, etc. L'indice de coïncidence est donc

$$\mathrm{IC} = \frac{(7\times 6)+0+0+(3\times 2)+\ldots}{43\times 42} = 0,070$$

Cryptanalyse

- Indice de coïncidence
  - Exemples d'indices calculés sur des textes dans différentes langues:

Langue	allemand	anglais	français	italien	norvégien	suédois
IC	0.072	0.065	0.074	0.075	0.073	0.071

  - l'indice de coïncidence moyen d'un texte aléatoire IC_a=0,038.

  - Pour tout chiffre mono-alphabétique, l'indice de coïncidence est le même pour le texte chiffré que pour le texte clair.

Cryptanalyse

Indice de coïncidence:

- Test de Friedman
  - On peut utiliser l'indice de coïncidence pour déterminer la longueur de la clé dans un texte chiffré selon le chiffre de Vigenère.
  - on calcule l'indice de coïncidence de chacun des sous-ensembles de lettres suivants du texte chiffré:
    1. l'ensemble de toutes les lettres du texte
    2. l'ensemble des lettres en position 1,3, 5, . . ., dans le texte
    3. l'ensemble des lettres en position 1,4, 7, . . ., dans le texte

    …

    k. l'ensemble des lettres en position 1,k + 1, 2k + 1, . . ., dans le texte

    …

Cryptanalyse

Indice de coïncidence:

- Test de Friedman
  - Si l'ensemble, considéré à la k-ième étape, est celui pour lequel l'indice de coïncidence est le plus élevé, alors on choisit k comme longueur de la clé.
- trouver la longueur du mot-clé du texte:

  YTTFT CTMUG FEJCU XFRSK UIBZF AZEJH VDQTD TNUGD JBFZY SFHNV OQWT

- on calcule les indices de coïncidence pour les différents sous-ensembles correspondant à chaque étapes:

Cryptanalyse

Indice de coïncidence:

- Intervalle de 1: YTTFT CTMUG FEJCU XFRSK UIBZF AZEJH VDQTD TNUGD JBFZY SFHNV OQWT

- Intervalle de 2: YTTTU FJUFS UBFZJ VQDNG JFYFN OW et TFCMG ECXRK IZAEH DTTUD BZSHV QT

- Intervalle de 3: YFTGJ XSIFE VTNDF SNQ, TTMFC FKBAJ DDUJZ FVW et TCUEU RUZZH QTGBY HOT

- Intervalle de 4: YTUJF UFJQN JYNW , TCGCR IAHTU BSVT, TTFUS BZVDG FFO et FMEXK ZEDTD ZHQ.

- Intervalle de 5: YCFXU AVTJS O, TTEFI ZDNBF Q, …

Cryptanalyse

Indice de coïncidence:

Intervalle	Indice de coïncidence				
1	0.04263				
2	0.05983	0.03134			
3	0.03922	0.03922	0.05229		
4	0.07692	0.04396	0.05128	0.03846	
5	0.00000	0.03636,	0.00000	0.03636,	0.02222

- La clé est donc probablement de longueur 4.
- Pour décrypter le message, on applique l'analyse statistique classique sur chaque groupe.

La Cryptographie moderne

La Cryptographie moderne