Module: Cryptographie

3ème année licence en Informatique

Par : Prof. Cherif Foudil

Chapitre 3

Principe de la cryptographie

Partie 1: Cryptographie Classique

2. Cryptographie

1) Introduction

- La **cryptographie traditionnelle** ou classique inclut tous les mécanismes et algorithmes basés sur des fonctions mathématiques ou logiques.
- Elle comprend tous les systèmes de chiffrement utilisés depuis l'Egypte ancienne jusqu'aux principaux systèmes de chiffrement actuellement en vigueur.
- Elle se devise en deux classes de systèmes de chiffrement :

  - les **chiffrement symétrique**

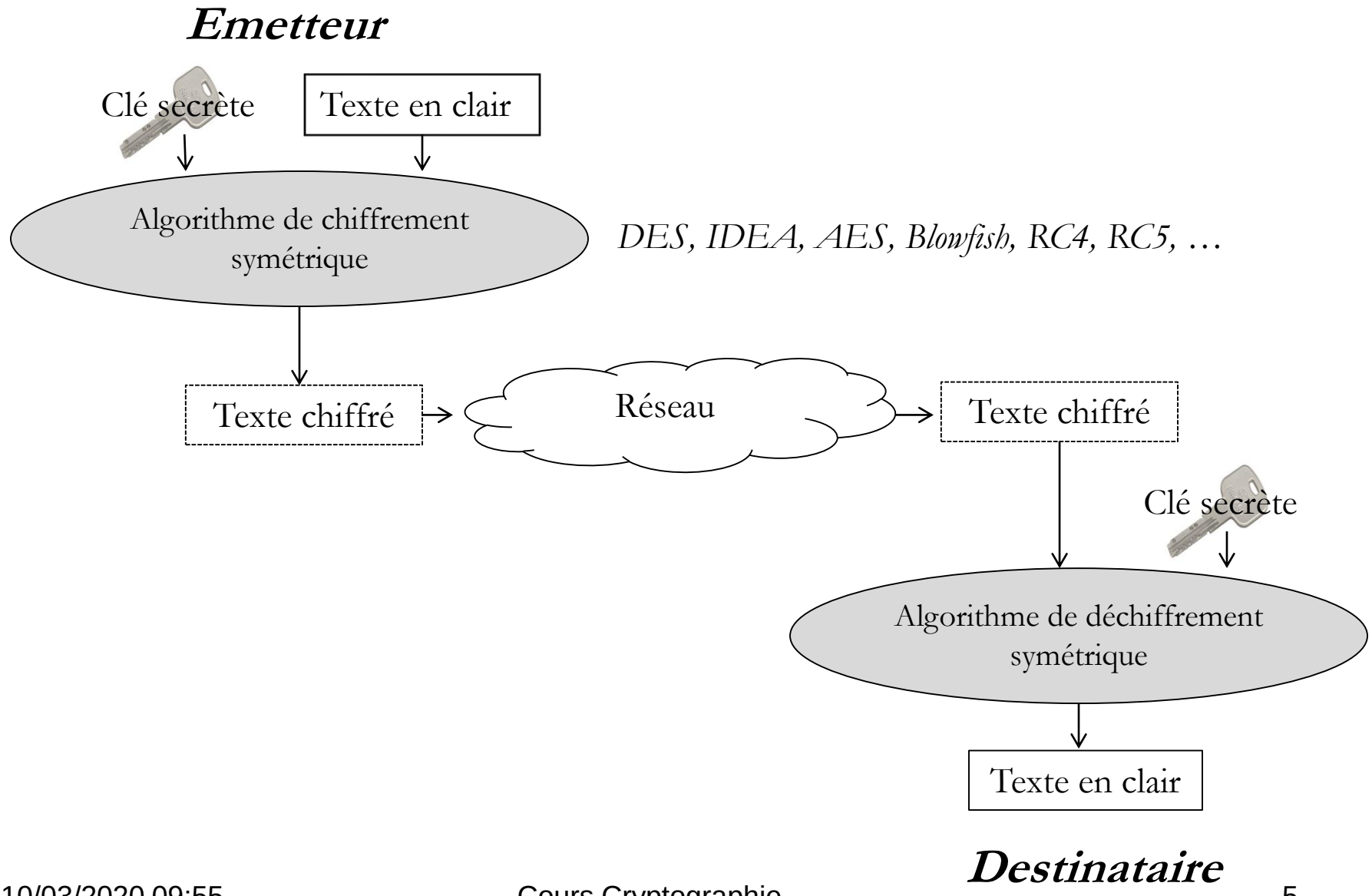
  - et les **systèmes de chiffrement asymétrique**

2) Systèmes de chiffrement symétrique

Mode opératoire

- Pour crypter ou décrypter un texte, il faut détenir **une clé** et **un algorithme de chiffrement**. S'il s'agit de la même clé pour effectuer ces deux opérations, le système de chiffrement est dit **symétrique**.
- L' émetteur et le récepteur doivent posséder **la même clé secrète** pour rendre confidentielle des données et pouvoir les comprendre (chiffrer et déchiffrer).

2. Cryptographie



2. Cryptographie

Un exemple : "chiffrement de César"

- Pour crypter un message, il faut **décaler de trois lettres** dans l'alphabet chaque lettre du message à transmettre.
- Pour décrypter un message chiffré, il suffit de décaler chacune des lettres de 3 positions dans **le sens inverse** de l'alphabet.

Exemple numérique:

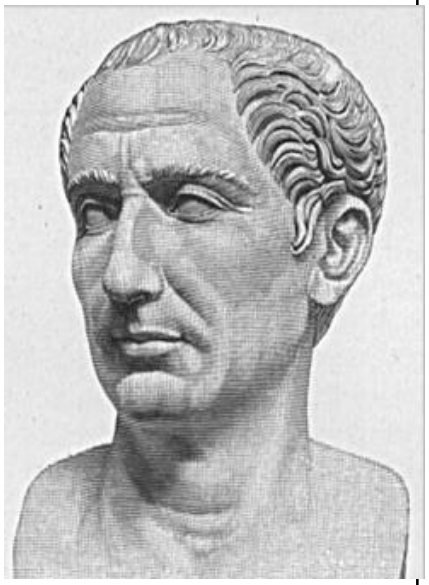
- La clé : 3

- Texte en clair : **salam**

- Texte chiffré : **vdodp** (décaler en arrière de trois lettres dans l'alphabet)

Appelé aussi chiffrement de César (50 avant. J-C)

Il s'agit du plus simple et plus ancien chiffre classique ayant existé. Son principe est un décalage des lettres de l'alphabet.



Dans les formules ci-dessous, x est l'indice de la lettre de l'alphabet,

k est le décalage.

Pour le chiffrement, on aura la formule:

$$e_k(x) = x + k \bmod 26$$

Pour le déchiffrement, on aura la formule:

$$d_k(y) = y - k \bmod 26$$

Exemples

On utilise le tableau suivant:

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

Exemple:

X= CRYPTOGRAPHIECLASSIQUE

K= 3

$E_k(x)$= FUBSWRJUDSKLHFODVVLTXH

K = 13 (*ROT13*)

$E_k(x)$= PELCGBTENCUVRPYNFFVDHR

2- **Chiffrement de César**

_ ABCDEFGHIGKLMNOPQRSTUVWXYZ

Par exemple, avec un décalage de **trois**, le nom devient

ALAIN TAPP = DODLQCWDSS

(On décale aussi les espaces…)

Cette technique de chiffrement est-elle sécuritaire?

2. **Chiffrement de César**

ABCDEFGHIGKLMNOPQRSTUVWXYZ

On intercepte le message suivant:

FAGEMYREMPURZV_EMZR_R FMNMDAZR

Essayons différents décalages…(L'attaquant)

1: **E_FDLXQDLOTQYUZDLYQZQZELMLC_YQ**

2: **DZECKWPCKNSPXTYCKXPYPYDKLKBZXP**

3… 4… 5… 6… 7… 8… 9… 10… 11… 12…

13: **TOUS_LES_CHEMINS_MENENT_A_ROME**
(message compréhensible)

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

Nombre de possibilités: ?????

3. Substitution mono-alphabétique

Essayons autre chose.

_	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

Le décodage devrait être plus difficile. Peut-on essayer tous les décodages possibles?

Il y a 27!=**10 888 869 450 418 352 160 768 000 000 possibilités(permutations)**

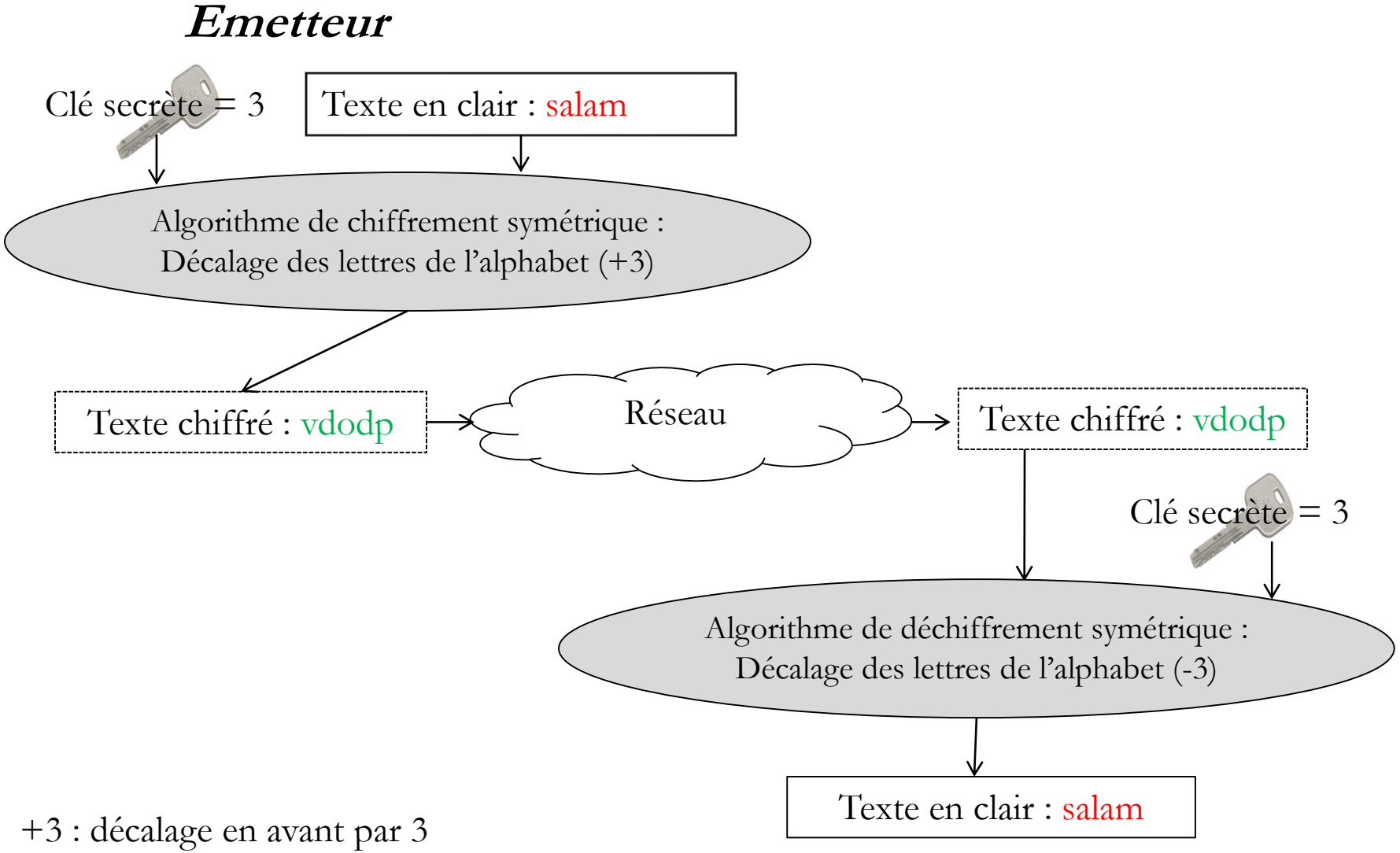
Cryptanalyse des substitutions mono-alphabétique

- Nombre de possibilités (alphabet de 26 lettres) ?
  - chiffrement de A : 26 possibilités
  - chiffrement de B : 25 possibilités
  - ... $\longrightarrow 26! \approx 4 \times 10^{26}$ possibilités
  - Ordre de grandeur de comparaison : plier 50 fois sur elle-même une feuille de papier (épaisseur : 1 dixième de mm)
    $\longrightarrow$ épaisseur de la feuille :
    2^{50} dixième de millimètre $\approx 1,1 \times 10^{8}$ km
    (110 millions de km $\approx$ 300 fois distance Terre/Lune)

2- Il y a plus de clés différentes que de grains de sable sur Terre !

3- Si un ordinateur pouvait tester 1 000 000 de clés par seconde, il lui faudrait alors 12 millions d'années pour tout énumérer.

Exemple (César K=3)



+3 : décalage en avant par 3

- 3 : décalage en arrière par 3

3. Substitution mono-alphabétique(cryptanalyse)

La substitution mono-alphabétique fut la technique de chiffrement la plus utilisée durant le premier millénaire. Nombreux savants de l'antiquité tenaient cette technique pour inviolable.

Ce sont les Arabes qui ont réussi à briser ce code et qui ont inventé la cryptanalyse au 9ième siècle.

Comment déchiffrer ce message?

BQPSNRSJXJNJXLDPCLDLPQBE_QRKJXHNKPKSJPJIKSP
UNBDKIQRBKPQPBQPZITEJQDQBTSKPELNIUNPHNKPBKP
CKSSQWKPSLXJPSNVVXSQCCKDJPBLDWPXBPSNVVXJPGK
PJKDXIPZLCEJKPGKSPSJQJXSJXHNKSPGPLZZNIIKDZK
PGKSPGXVVKIKDJKSPBKJJIKS

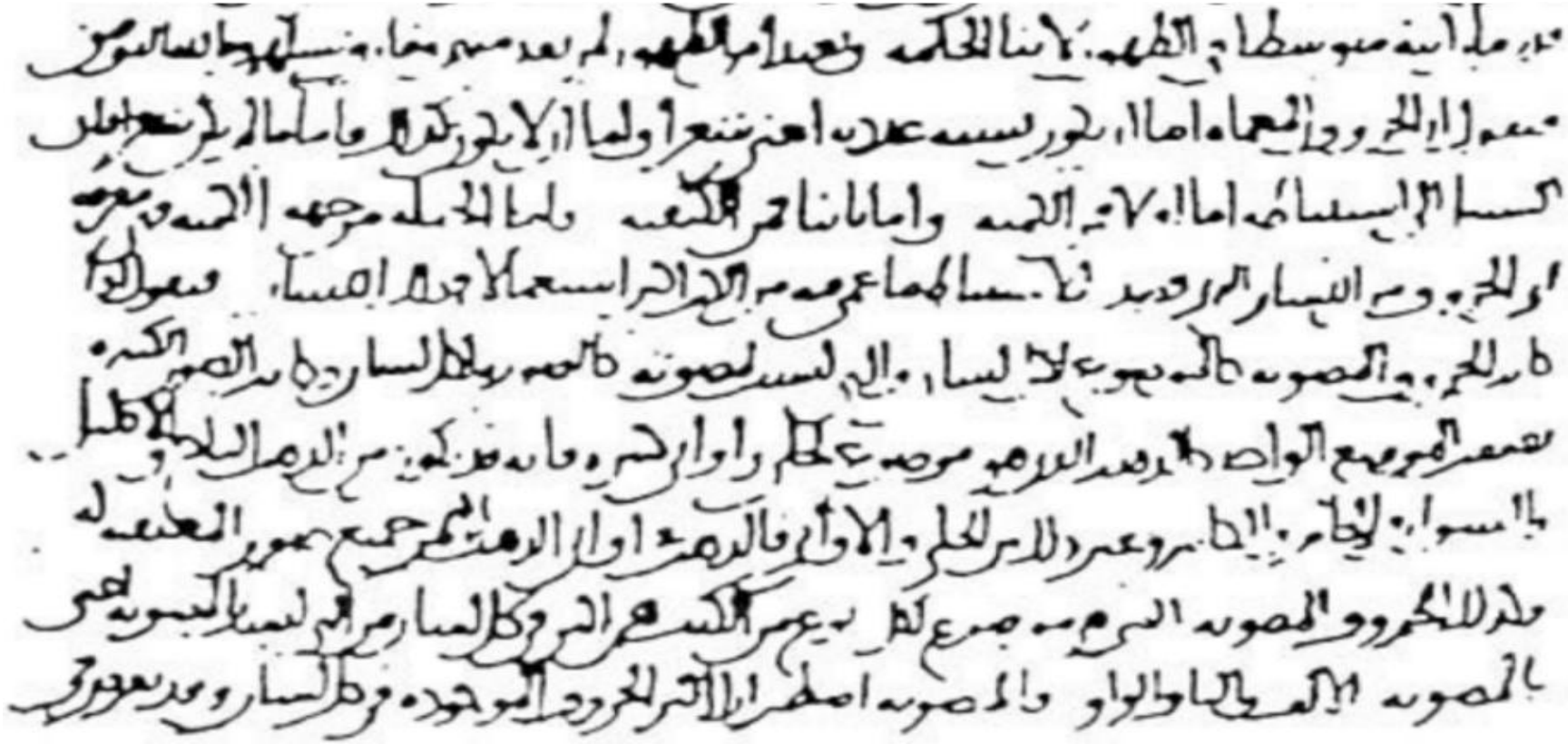
L'idée est que:

1-Chaque lettre est chiffrée de la même façon ?

2-Certaines lettres sont utilisées plus souvent ?

Par l’analyse fréquentielle

Al-Kindi (801-873) rédige le plus ancien texte connu décrivant la technique de décryptement appelée analyse des fréquences.



Analyse fréquentielle: Principe

«On génère un graphique sur la fréquence d'apparition de chaque lettre dans le texte crypté et un autre avec un texte de référence, dans la langue du message d'origine, et on explore par décalages successifs toutes les possibilités. En les comparant, un humain peut facilement voir la valeur du décalage entre ces deux graphiques, et trouver la clé de chiffrement ».

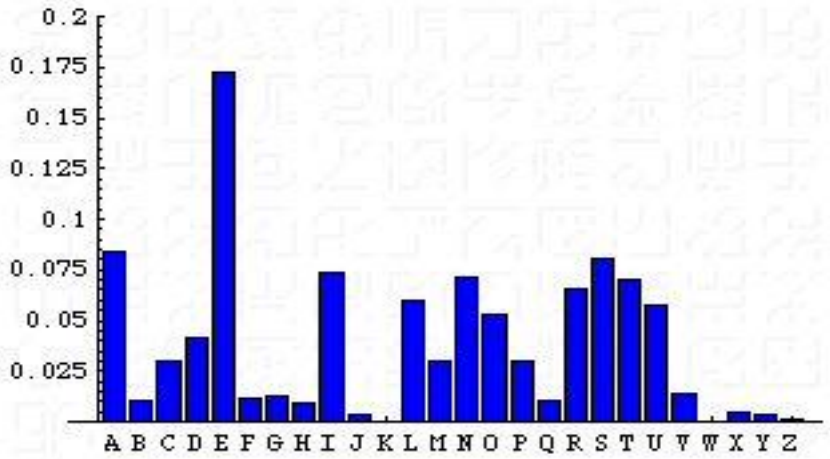
Analyse fréquentielle: Principe

Cette technique ne fonctionne bien que si le cryptogramme est **suffisamment long** pour avoir des moyennes significatives.

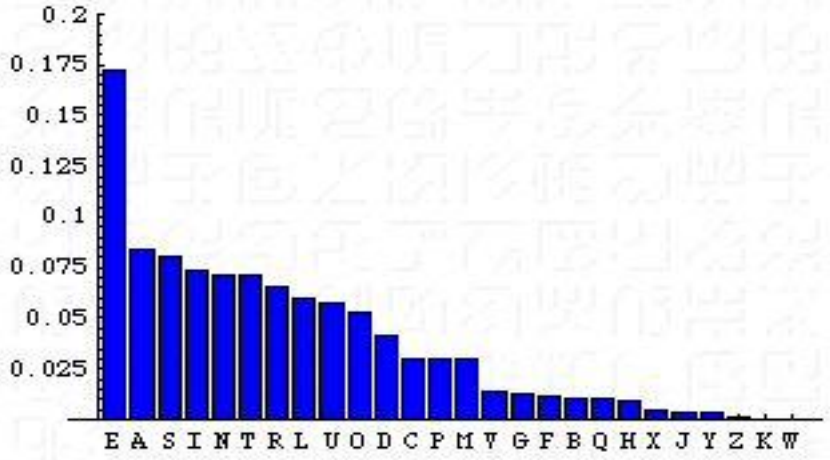
Fréquences d'apparition des lettres

Lettre	Fréquence	Lettre	Fréquence
A	8.40 %	N	7.13 %
B	1.06 %	O	5.26 %
C	3.03 %	P	3.01 %
D	4.18 %	Q	0.99 %
E	17.26 %	R	6.55 %
F	1.12 %	S	8.08 %
G	1.27 %	T	7.07 %
H	0.92 %	U	5.74 %
I	7.34 %	V	1.32 %
J	0.31 %	W	0.04 %
K	0.05 %	X	0.45 %
L	6.01 %	Y	0.30 %
M	2.96 %	Z	0.12 %

Histogramme par ordre alphabétique



Histogramme par ordre décroissant des fréquences



Analyse fréquentielle: principe

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

Cryptographie 161

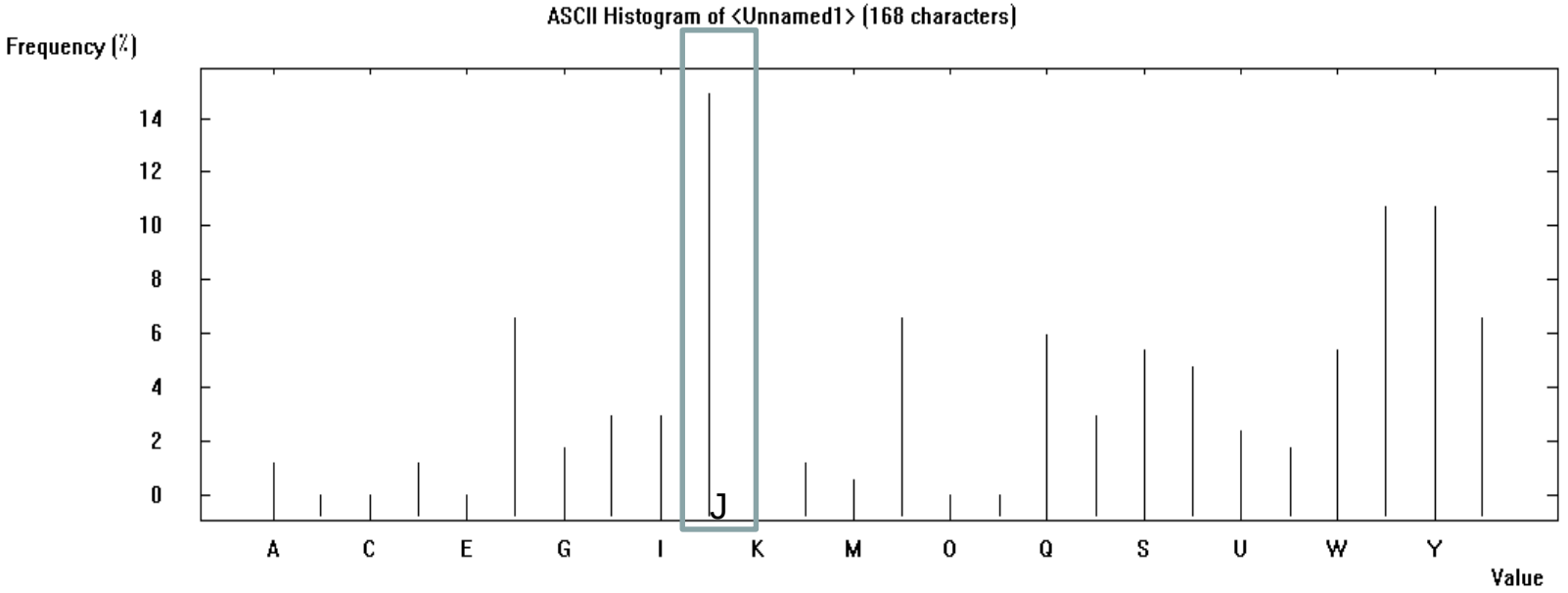
Analyse fréquentielle: Exemple

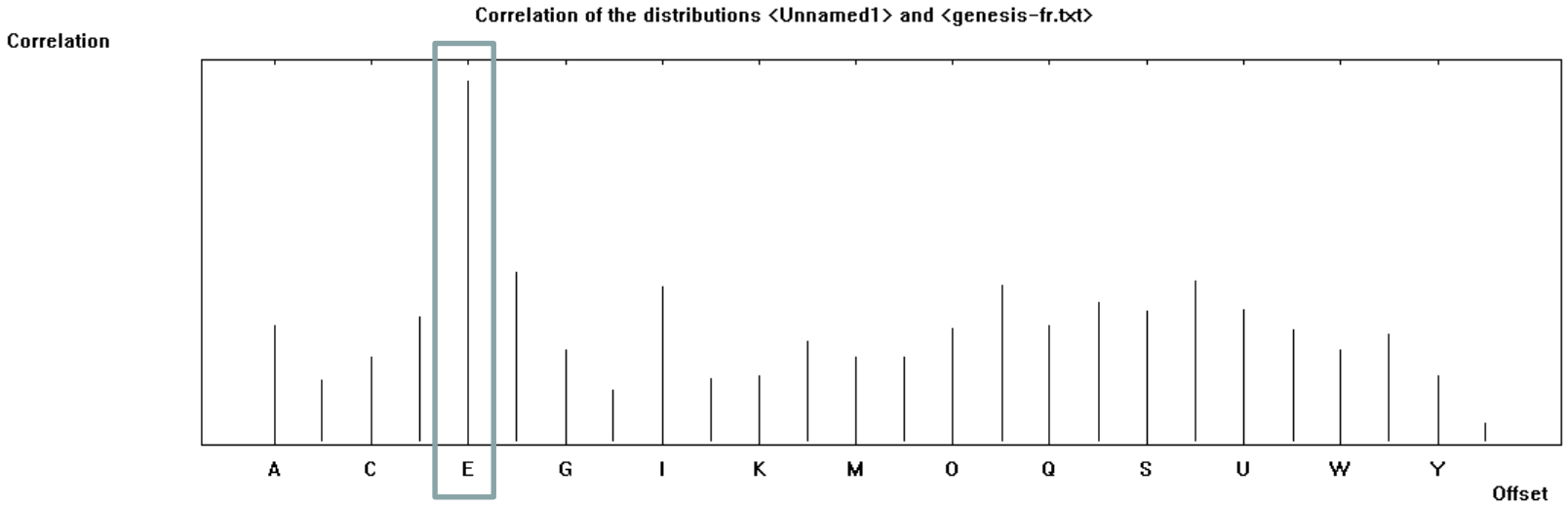
Analyse fréquentielle :On utilise le principe de l'analyse fréquentielle.

Exemple:

QFXZG XYNYZ YNTSR TSTFQ UMFGJ YNVZJ JXYYW JXAZQ SJWFG QJFQF HWDUY FSFQD XJUTZ WAZVZ JQJRJ XXFLJ XTNYX ZKKNX FRRJS YQTSL NQXZK KNYIJ YJSNW HTRUY JIJXX YFYNX YNVZJ XITHH ZWWJS HJIJX INKKJ WJSYJ XQJYY WJX

Analyse fréquentielle Exemple





Analyse fréquentielle: Exemple

- Donc J = E
- ➔ K = 5 (F).
- Le texte clair est:

LASUBSTITUTIONMONOALPHABETIQUEESTTRESVULNERABLE ALACRYPTANALYSEPOURVUQUELEMESSAGESOITSUFFISAMM ENTLONGILSUFFITDETENIRCOMPTEDESSTATISTIQUESDOC CURRENCEDESDIFFERENTESLETTRES

On ajoutant les espaces on obtient le message plus clair:

LA_SUBSTITUTION_MONO_ALPHABETIQUE_EST_TRES_VULN ERABLE_A_LA_CRYPTANALYSE_POURVU_QUE_LE_MESSAGE _SOIT_SUFFISAMMENT_LONG_IL_SUFFIT_DE_TENIR_COMP TE_DES_STATISTIQUES_D_OCCURRENCE_DES_DIFFERENTE S_LETTRES

4-Chiffrement de Vigenère(polyalphabétique)

Élaboré par **Blaise de Vigenère**(1523, 1596).

Chiffrement de Vigenère de type polyalphabétique.

Ce chiffrement introduit **la notion de clé**. Une clé se présente généralement sous la forme **d'un mot ou d'une phrase**.

Pour pouvoir chiffrer notre texte, à chaque caractère nous utilisons une lettre de la clé pour effectuer la substitution.

4-Chiffrement de Vigenère

L'espace des clés du chiffrement mono-alphabétique est immense, mais le fait qu'une lettre soit toujours cryptée de la même façon représente une trop **grande faiblesse**.
Le chiffrement de Vigenère remédie à ce problème. On regroupe les lettres de notre texte par blocs, par exemple ici par blocs de longueur 4 :

CETTE PHRASE NE VEUT RIEN DIRE

devient

CETT EPHR ASEN EVEU TRIE NDIR E

(les espaces sont purement indicatifs)

Si k est la longueur d'un bloc, alors on choisit une clé constituée de k nombres de 0 à 25 : $(n_1, n_2, \ldots, n_k)$. Le chiffrement consiste à effectuer un chiffrement de César, dont le décalage dépend du rang de la lettre dans le bloc :

5-Chiffrement de Vigenère

- un décalage de n_1 pour la première lettre de chaque bloc,
– un décalage de n_2 pour la deuxième lettre de chaque bloc,
– ...
– un décalage de n_k pour la k-ème et dernière lettre de chaque bloc

Pour notre exemple, si on choisit comme clé (3,1,5,2) alors pour le premier bloc "CETT" :
– un décalage de 3 pour C donne F,
– un décalage de 1 pour E donne F,
– un décalage de 5 pour le premier T donne Y,
– un décalage de 2 pour le deuxième T donne V.
Ainsi "CETT" de vient "FFYV".
Vous remarquez que les deux lettres T ne sont pas cryptées par la même lettre et que les deux F ne cryptent pas la même lettre.
On continue ensuite avec le deuxième bloc...

4-Chiffrement de Vigenère

Il y a (26 puissance k)choix possibles de clés, lorsque les blocs sont de longueur k.
Pour des blocs de longueur k=4 cela en donne 456 976, et même si un ordinateur teste toutes les combinaisons possibles sans problème, il n'est pas question de parcourir cette liste pour trouver le message en clair,

une faiblesse du même ordre que celle rencontrée dans le chiffrement mono-alphabétique : la lettre A n'est pas toujours cryptée par la même lettre, mais si deux lettres A sont situées à la même position dans deux blocs différents (comme par exemple "ALPH ABET") alors elles seront cryptées par la même lettre.

Une attaque possible: on découpe notre message en plusieurs listes, les premières lettres de chaque bloc, les deuxièmes lettres de chaque bloc... et on fait une attaque statistique sur chacun de ces regroupements.
Ce type d'attaque n'est possible que **si la taille des blocs est petite** devant la longueur du texte.

5-Les clés secrètes

L'inconvénient des chiffrements précédents est qu'une **même lettre** est régulièrement chiffrée de la **même façon**, car la correspondance d'un alphabet à un ou plusieurs autres est fixée une fois pour toutes, ce qui fait qu'une attaque **statistique est toujours possible**.

Nous allons voir qu'en changeant la correspondance à chaque lettre, il est possible de créer un chiffrement **parfait** !

6-Les clés secrètes

Principe du chiffrement:

le message secret M à envoyer suivant **: ATTAQUE LE CHÂTEAU**

On choisi une clé secrète C: Cette clé secrète est de la même longueur que le message (les espaces ne comptent pas) et composée d'entiers de 0 à 25, tirés au hasard. Par exemple C:

[4, 18, 2, 0, 21, 12, 18, 13, 7, 11, 23, 22, 19, 2, 16, 9]

On crypte la première lettre par un décalage de César donné par le premier entier :A est décalé de 4 lettres et devient donc E. La seconde lettre est décalée du second entier : le premier T devient L. Le second T est lui décalé de 2 lettres, il devient V. Le A suivant est décalé de 0 lettre, il reste A...

6-Les clés secrètes

Le message chiffré X transmit: ELVALGW YL NEWMGQD

Pour le décrypter, si on connaît la clé, on n'a qu'à faire le décalage dans l'autre sens.

Notez que deux lettres identiques (par exemples les T) n'ont aucune raison d'être cryptées de la même façon. Par exemple, les T du message initial sont cryptés dans l'ordre par un L, un V et un M,

Formalisons cette opération. On identifie A avec 0, B avec 1, ...,Z avec 25. Alors le message crypté X est juste la "somme" du message M avec la clé secrète C, la somme s'effectuant lettre à lettre, terme à terme, modulo 26.

Notons cette opération M © C=X. (+)

6-Les clés secrètes

	A	T	T	A	Q	U	E	L	E	C	H	A	T	E	A	U
	0	19	19	0	16	20	4	11	4	2	7	0	19	4	0	20
⊕																
	4	18	2	0	21	12	18	13	7	11	23	22	19	2	16	9
=	4	11	21	0	11	6	22	24	11	13	4	22	12	6	16	3
	E	L	V	A	L	G	W	Y	L	N	E	W	M	G	Q	D

6-Les clés secrètes

On reçoit X et connaît C, on effectue donc X - C = M.

Il y a trois principes à respecter pour que ce système reste **inviolable** :

1. La longueur de la clé est égale à la longueur du message.
2. La clé est choisie au hasard.
3. La clé ne sert qu'une seule fois.

6-Les clés secrètes

Ce système appelé "**masque jetable**" ou chiffrement de **Vernam** est parfait en théorie, mais sa mise en œuvre n'est pas pratique du tout !

Tout d'abord il faut que la clé soit aussi longue que le message.
Pour un message court cela ne pose pas de problème, mais pour envoyer une image par exemple cela devient très lourd. Ensuite, il faut trouver un moyen sûr d'envoyer la clé secrète à son interlocuteur avant de lui faire parvenir le message.
Et il faut recommencer cette opération à chaque message, ou bien se mettre d'accord dès le départ sur un carnet de clés: une longue liste de clés secrètes.

7- Chiffrement Affine

- Chiffrement Affine (monoalphabétique):

L'idée est d'utiliser comme fonction de chiffrement une fonction affine du type **$y = (a.x + b) \bmod 26$**,

Où a et b sont des constantes, et où x et y sont des nombres correspondant aux lettres de l'alphabet.

- $K = (a,b)$
- $e_k(x) = a.x + b \bmod 26$
- $d_k(x) = a^{-1}.(y-b) \bmod 26$

a^{-1} est multiplicatif inverse de modulo 26, i.e,

$a.\ a^{-1} \equiv 1 \pmod{26}$

Pour que le chiffrement soit **valide** (unique), il faut que la fonction de chiffrement ait une **solution unique** (injective).

La fonction $e_k(x)$ a une solution unique (pour toute valeur de b) ssi: pgcd(a,26)=1

7- Chiffrement Affine – Exemple

K = (17,9)=(a,b)

Vérification: PGCD(17,26) = 1

➔ **cryptage valide**

17^{-1} mod 26 = 23 [17*23 = 391 = 1 mod 26]

➔ **a. $a^{-1} \equiv 1 \pmod{26}$ vérifié**

$e_k(x) = 17.x + 9 \bmod 26$

$d_k(x) = 17^{-1}. (y-9) \bmod 26 = 23 * (y-9) \bmod 26$

$= 23\ y - 25 \bmod 26$

On peut vérifier que $d_k(e_k(x)) = x$

…….. Validez !!!!

Chiffrement de Vigenère: cryptanalyse

- Clairement, une attaque statistique simple ne fonctionnera pas. Si le mot de code est suffisamment long (une phrase), essayer toutes les clefs est aussi impossible.
- Le chiffre de Vigenère est-il indéchiffrable?

Les cryptanalyses furent déjoués pendant près de 3 siècles par le chiffre de Vigenère.

Au 19ième siècle, Charles Babbage réussit à le casser.

La technique s'appelle « Attaque par indice de coïncidence ».

Chiffrement de Vigenère: Cryptanalyse

Phase 1: Trouver la longueur de la clé (n).

Etape 1: Souligner chaque répétition de 3 caractères ou plus.

Etape 2: Pour chaque répétition, mesurer la période.

Etape 3: pour chaque période, décomposer en facteurs premier et regarder quel facteur est commun à tous.

Chiffrement de Vigenère: cryptanalyse

Phase 2: Trouver la 1ére lettre du mot clé.

Etape 1: faire une analyse de fréquence seulement sur les caractéres 1, N+1, 2N+1,3N+1,...

Etape 2: on décale pour faire correspondre. (on a la première lettre de la clé)

Phase 3,5..,i,.. (nombre des lettres de la clé restante):

On recommence pour les N lettres du mot clé.

i, N+i, 2N+i,3N+i,...

Le chiffre de Vigenère: exemple Phase 1

KQOWEFVJPUJUUNUKGLMEKJINMWUXFQMKJBGWRLFNFGHUDWUUMBSVLPSNCMUEKQCTES
WREEKOYSSIWCTUAXYOTAPXPLWPNTCGOJBGFQHTDWXIZAYGFFNSXCSEYNCTSSPNTUJN
YTGGWZGRWUUNEJUUQEAPYMEKQHUIDUXFPGUYTSMTFFSHNUOCZGMRUWEYTRGKMEED
CTVRECFBDJQCUSWVBPNLGOYLSKMTEFVJJTWWMFMWPNMEMTMHRSPXFSSKFFSTNUOCZ
GMDOEOYEEKCPJRGPMURSKHFRSEIUEVGOYCWXIZAYGOSAANYDOEOYJLWUNHAMEBFELX
YVLWNOJNSIOFRWUCCESWKVIDGMUCGOCRUWGNMAAFFVNSIUDEKQHCEUCPFCMPVSUDG
AVEMNYMAMVLFMAOYFNTQCUAFVFJNXKLNEIWCWODCCULWRIFTWGMUSWOVMATNYBUHT
COCWFYTNMGYTQMKBBNLGFBTWOJFTWGNTEJKNEEDCLDHWTVBUVGFBIJG

KQOWEFVJPUJUUNUKGLMEKJINMWUXFQMKJBGWRLFNFGHUDWUUMBS
VLPSNCMUEKQCTESWREEKOYSSIWCTUAXYOTAPXPLWPNTCGOJBGFQ
HTDWXIZAYGFFNSXCSEYNCTSSPNTUJNYTGGWZGRWUUNEJUUQEAPY
MEKQHUIDUXFPGUYTSMTFFSHNUOCZGMRUWEYTRGKMEEDCTVRECF
BDJQCUSWVBPNLGOYLSKMTEFVJJTWWMFMWPNMEMTMHRSPXFSSKF
FSTNUOCZGMDOEOYEEKCPJRGPMURSKHFRSEIUEVGOYCWXIZAYGOS
AANYDOEOYJLWUNHAMEBFELXYVLWNOJNSIOFRWUCCESWKVIDGMUC
GOCRUWGNMAAFFVNSIUDEKQHCEUCPFCMPVSUDGAVEMNYMAMVLFM
AOYFNTQCUAFVFJNXKLNEIWCWODCCULWRIFTWGMUSWOVMATNYBU
HTCOCWFYTNMGYTQMKBBNLGFBTWOJFTWGNTEJKNEEDCLDHWTVBU
VGFBIJG

1
1

Le chiffre de Vigenère: Exemple Phase 1

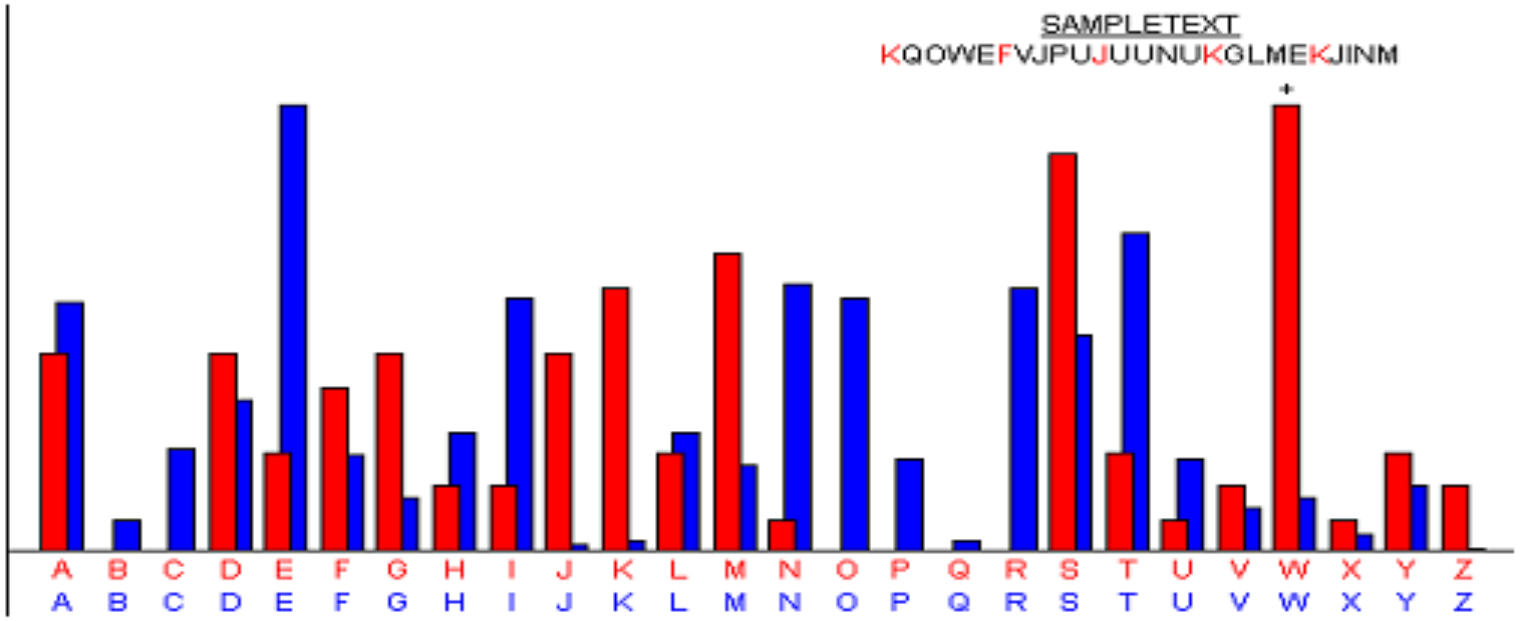
Etape 2

		Longueurs de clef possibles (diviseurs de la distance)			
Séquence répétée	**Distance entre les répétitions**	**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**	

Etape 3

- Il apparaît dans le tableau que toutes les périodes sont divisibles par **5**

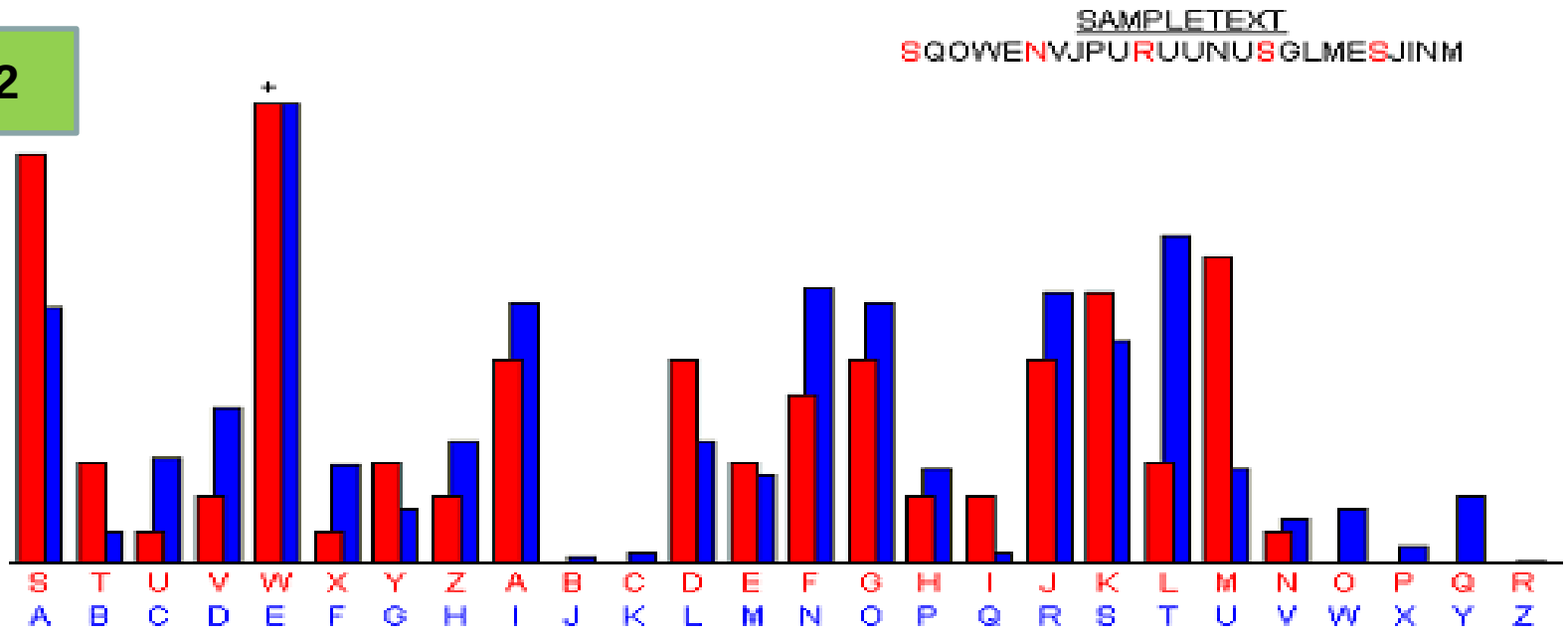
Le chiffre de Vigenère: Exemple Phase 2



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

Le chiffre de Vigenère: Exemple Phase 2

Etape 2



- On décale les diagrammes pour mettre le pic du **W** sur le **E.**
- W= 22 et E = 4 ➔ c'est la (22-4= 18) soit **S**
- **La première lettre de la clé est S**

Le chiffre de Vigenère: Exemple Phase 3,4,5,6

- On répète pour la deuxième lettre de la clé, la lettre 2, 7, 13,
- Le mot clé est: **SCUBA**
- On peut déchiffrer le cryptogramme:

```
SOUVE NTPOU RSAMU SERLE SHOMM ESDEQ UIPAG EPREN NENTD ESALB ATROS VASTE SOISE AUXDE SMERS
QUISU IVENT INDOL ENTSC OMPAG NONSD EVOYA GELEN AVIRE GLISS ANTSU RLESG OUFFR ESAME RSAPE
INELE SONTI LSDEP OSESS URLES PLANC HESQU ECESR OISDE LAZUR MALAD ROITS ETHON TEUXL AISSE
NTPIT EUSEM ENTLE URSGR ANDES AILES BLANC HESCO MMEDE SAVIR ONSTR AINER ACOTE DEUXC EVOYA
GEURA ILECO MMEIL ESTGA UCHEE TVEUL ELUIN AGUER ESIBE AUQUI LESTC OMIQU EETLA IDLUN AGACE
SONBE CAVEC UNBRU LEGUE ULELA UTREM IMEEN BOITA NTLIN FIRME QUIVO LAITL EPOET EESTS EMBLA
BLEAU PRINC EDESN UEESQ UIHAN TELAT EMPET EETSE RITDE LARCH ERBAU DELAI RE
```

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

Synthèse sur la Cryptographie Classique

Il existe des **centaines** de façon de chiffrer des données représentées par l'alphabet classique, tout en gardant les opérations réalisées secrètes. Nous avons deux classes:

a) Substitution : La substitution consiste effectuer des dérivations pour que chaque caractère du message chiffré soit différent des caractères du message en clair

- **Substitution simple ou substitution monoalphabétique**: Un caractère du message clair est substitué par un caractère unique du message chiffré
- **Substitution homophonique**: Un caractère du message clair correspond à plusieurs caractères du message chiffré
- **Substitution polyalphabétique**: : Il s'agit d'un ensemble de substitutions simples.
- **Substitution par polygrammes** : le principe est de substituer des blocs de caractères, au lieu d'un seul caractère.

b) **Transposition**: Toutes les lettres du message sont présentes, mais dans un ordre différent. Il utilise le principe mathématique des permutations

- Transposition simple par colonnes
- Transposition complexe par colonne
- Transposition par carré polybique

Interrogation écrite

1-quelle est la différence entre la cryptographie symétrique et asymétrique

2- calculer pgcd(105,35)

3- quelle méthode de cryptanalyse pour casser la méthode mono alphabétique