

Techniques cryptographiques classiques

Dr. Nouredine Chikouche

nouredine.chikouche@univ-msila.dz

<https://sites.google.com/view/chikouchenouredine>

Plan du cours

- Les catégories de chiffrement classique
- Analyse fréquentielle
- Chiffrement par décalage
- Chiffrement de Vigenère
- Chiffrement de Affine
- Chiffrement par transposition rectangulaire
- Chiffrement assyrien

► Cryptographie classique ...

Les catégories de chiffrement classique

Catégories de chiffrement classique

```
graph TD; A[Catégories de chiffrement classique] --- B[Par substitution de lettres]; A --- C[Par transposition de lettres];
```

Par substitution de lettres

Par transposition de lettres

Les catégories de chiffrement classique

▶ Chiffrement par substitution:

- ▶ Chaque caractère du texte clair est **remplacé** par un caractère dans un texte chiffré.
- Chiffrement mono-alphabétique: 1 lettre → 1 seule lettre.
- Chiffrement poly-alphabétique: 1 lettre → 1 lettre parmi plusieurs.
- Chiffrement polygraphique: n lettre → n autre lettre.
- Exemples: par décalage, Vigenère, affine, Hill, ...

Les catégories de chiffrement classique

▶ Chiffrement par transposition:

- ▶ On crypte message en **permutant l'ordre des lettres** du texte clair suivant des règles bien définies.
- ▶ Consiste à changer les positions des lettres.
- ▶ **Exemples:** technique assyrienne, transposition rectangulaire.

Analyse fréquentielle

L'**analyse fréquentielle** est une technique de cryptanalyse découverte par Al-Kindi. **Al-Kindi** (801-873).

في مادة آية عن سطران الطهمة. لأننا للحكمة ونعدنا من الطهمة لم يعد من غيرنا. وسيلها في السطور
معها في الخور والمعجم. أما في الخور فليس من غيرنا. أما في المعجم فليس من غيرنا. وأما في الخور فليس من غيرنا.
كسب الإستهانة أما في الخور فليس من غيرنا. أما في المعجم فليس من غيرنا. وأما في الخور فليس من غيرنا.
أو الخور من السطور فليس من غيرنا. أما في المعجم فليس من غيرنا. وأما في الخور فليس من غيرنا.
في الخور من السطور فليس من غيرنا. أما في المعجم فليس من غيرنا. وأما في الخور فليس من غيرنا.
تصغير المعجم مع الواو والهمزة والراء في الخور فليس من غيرنا. أما في المعجم فليس من غيرنا.
بالسوا: الخور والمعجم. أما في الخور فليس من غيرنا. أما في المعجم فليس من غيرنا. وأما في الخور فليس من غيرنا.
وتدلل الخور والمعجم من غيرنا. أما في الخور فليس من غيرنا. أما في المعجم فليس من غيرنا. وأما في الخور فليس من غيرنا.
بالمصونة الألف والياء والواو والمصونة أصح من الخور والمعجم. أما في الخور فليس من غيرنا. أما في المعجم فليس من غيرنا.

Analyse fréquentielle

- ▶ Elle consiste à examiner la fréquence des lettres utilisées dans un texte chiffré.
- ▶ Elle est l'étude de la répartition des lettres dans un texte.
- ▶ Cette technique ne fonctionne bien que si:
 - ▶ le texte chiffré est **suffisamment long** pour avoir des moyennes significatives.
 - ▶ on connaît la **langue** utilisée.

Analyse fréquentielle: Principe

- ▶ Exemple: les fréquences d'apparition des lettres en langue française:

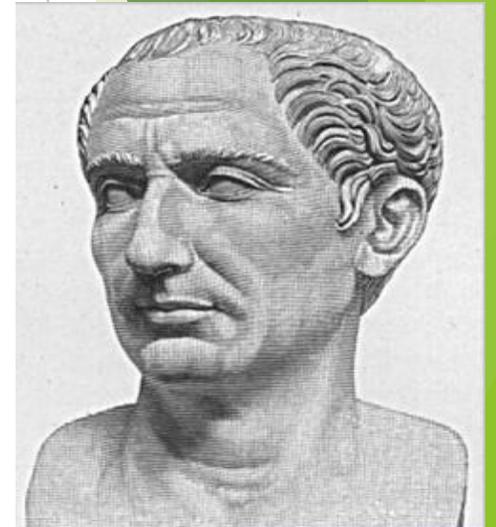
Lettre	Fréquence %
E	17.76
S	8.23
A	7.68
N	7.61
T	7.30
I	7.23
.	
.	
.	

Analyse fréquentielle

- ▶ L'analyse fréquentielle consiste:
 - ▶ À relever les occurrences d'apparition des lettres dans le message.
 - ▶ Ensuite il suffit de procéder par **correspondance**, on va associer **la lettre la plus fréquente dans le texte chiffré** à celle **la plus fréquente dans la langue du texte de référence**.

Chiffrement par décalage

- ▶ Appelé aussi chiffrement de César (50 av. 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.
 - $k \in \mathbb{Z}/26\mathbb{Z}$ (est un entier statique)
- ▶ Pour le chiffrement, on aura la formule:
 - ▶ $y = E_k(x) = x + k \bmod 26$
- ▶ Pour le déchiffrement, on aura la formule:
 - ▶ $x = D_k(y) = y - k \bmod 26$



Chiffrement par décalage

- ▶ On numérote les 26 lettres de l'alphabet de 0 pour A à 25 pour 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	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

X= CRYPTOGRAPHIE

K= D = 3

Chiffrement par décalage

Texte clair	C	R	Y	P	T	O
Indice. Clair	2	17	24	15	19	14
Clé	D	D	D	D	D	D
Indice. Clé	3	3	3	3	3	3
Ind. Chiff	5	20	1	18	22	17
Texte chiffré	F	U	B	S	W	R

► Exemple:

► $E(2)_k = 2 + 3 \% 26 = 5$

► $D(5)_k = 5 - 3 \% 26 = 2$

Chiffrement par décalage: Cryptanalyse

❶ Par recherche de la valeur du décalage:

- ▶ il suffit de tester tous les chiffrements possibles jusqu'à trouver le bon. C'est ce qu'on appelle une **attaque par force brute**, technique de test de toutes les combinaisons possibles, il y a **25 clés sont possibles**.

Chiffrement par décalage: Cryptanalyse

② Analyse fréquentielle :

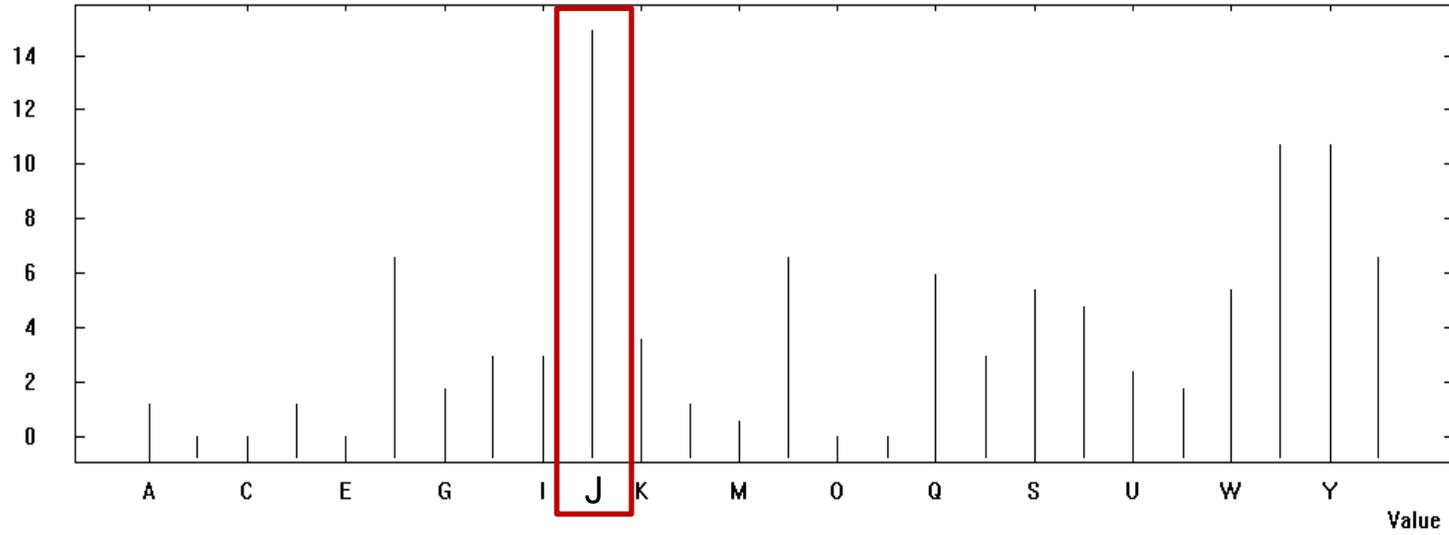
On utilise le principe de l'analyse fréquentielle.

► 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

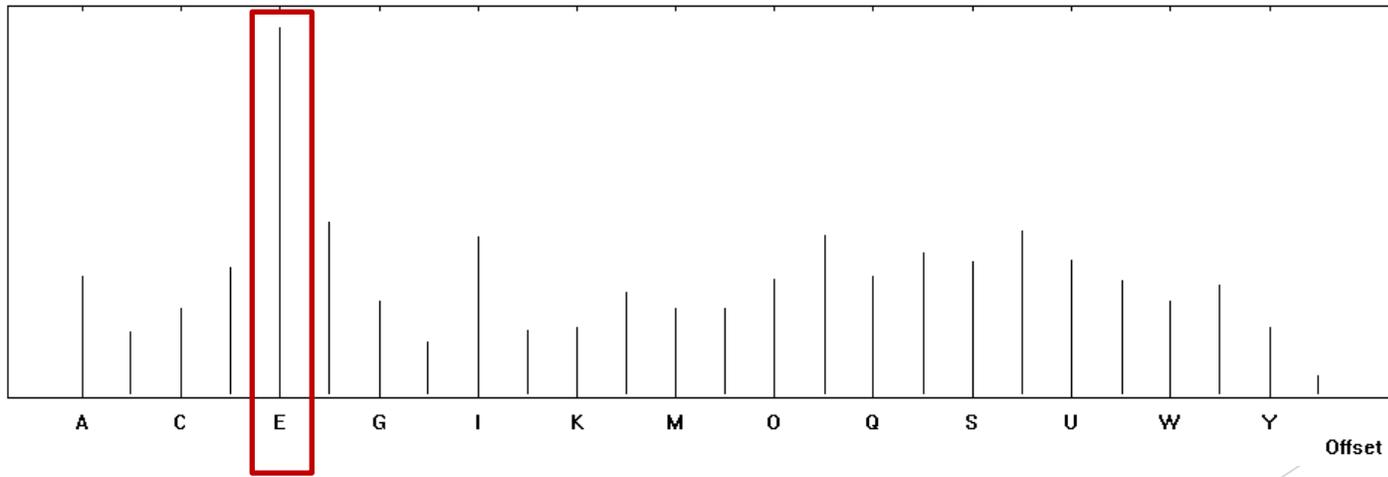
ASCII Histogram of <Unnamed1> (168 characters)

Frequency (%)



Correlation of the distributions <Unnamed1> and <genesis-fr.txt>

Correlation



Chiffrement par décalage: Cryptanalyse

- ▶ Donc J (texte chiffré) = E (texte clair)
- ▶ $E(x) = x + k \% 26 \Rightarrow k = E(x) - x \% 26$
- ▶ $k = 9 - 4 = 5$ (F).
- ▶ Le texte clair est:

LASUBSTITUTIONMONOALPHABETIQUEESTTRESVULNERABLEALACRYPTANALYSEPOURVUQUELEMESSAGESOITSUFFISAMMENTLONGILSUFFITDETENIRCOMPTEDESSTATISTIQUESDOCCURRENCEDESDIFFERENTESLETTRES

LA_SUBSTITUTION_MONO_ALPHABETIQUE_EST_TRES_VULNERABLE_A_LA_CRYPTANALYSE_POURVU_QUÉ_LE_MESSAGE_SOIT_SUFFISAMMENT_LONG_IL_SUFFIT_DE_TENIR_COMPTE_DES_STATISTIQUES_D_OCCURRENCE_DES_DIFFERENTES_LETTRES

Chiffrement de Vigenère

- ▶ 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 un texte, à chaque caractère nous utilisons une lettre de la clé pour effectuer la substitution.



Chiffrement de Vigenère

- ▶ $k = (k_1, k_2, \dots, k_n)$, $k_i \in \mathbb{Z}/26\mathbb{Z}$, k est un ensemble des entiers
- ▶ Pour le chiffrement, on aura la formule:
 - ▶ $y = E_k(x_1, x_2, \dots, x_n) = (x_1 + k_1, x_2 + k_2, \dots, x_n + k_n)$
- ▶ Pour le déchiffrement, on aura la formule:
 - ▶ $x = D_k(y_1, y_2, \dots, y_n) = (y_1 - k_1, y_2 - k_2, \dots, y_n - k_n)$
- ▶ Les opérations sont effectuées dans $\mathbb{Z}/26\mathbb{Z}$

Chiffrement de Vigenère

- ▶ Texte en clair: **CHIFFREMENT**
- ▶ Clé: **SECRET = (18, 4, 2, 17, 4, 19)**

Texte clair	C	H	I	F	F	R	E	M	E	N	T
Indice. Clair	2	7	8	5	5	17	4	12	4	13	19
Clé	S	E	C	R	E	T	S	E	C	R	E
Indice. Clé	18	4	2	17	4	19	18	4	2	17	4
Ind. Chiff	20	11	10	22	9	10	22	16	6	4	23
Texte chiffré	U	L	K	W	J	K	W	Q	G	E	X

Chiffrement de Vigenère: Cryptanalyse

- ▶ Au 19^{ième} siècle, Charles Babbage réussit à casser la cryptographie de Vigenère.
- ▶ Il a utilisé une 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 premiers et regarder quel facteur est commun à tous.

Chiffrement de Vigenère : Cryptanalyse

- ▶ **Phase 2:** trouver la 1^{ère} lettre ($i=1$) du mot clé. 
- ▶ **Etape 1:** faire une analyse de fréquence seulement sur les caractériser $i, N+i, 2N+i, 3N+i, \dots$
- ▶ **Etape 2:** on décale pour faire correspondre. (on à première ($j^{\text{ème}}$) lettre de la clé)
- ▶ **Phase 3,4...,i,..** (nombre des lettres de la clé restante): On recommence pour les N lettres du mot clé. 

Cryptanalyse de Vigenère: Exemple

Phase 1

► KQOWEFVJPUJUUNUKGLMEKJINMWUXFQMKJBGWRLFNFGHUDWUUMBSVLPNSCMUEKQCTESWREEKOYSSIW
CTUAXYOTAPXPLWPNTCGOJBGFQHTDWXIZAYGFFNSXCSEYNCTSSPNTUJNYTGGWZGRWUUNEJUJUEAPYME
KQHUIDUXFPGUYTSMFFSHNUOCZGMRUWEYTRGKMEEDCTVRECFBDJQCUSWVBNLGOYLSKMTEFVJTTWW
MFMWPNMEMTMHRSPXFSSKFFSTNUOCZGMDOEOYEKCPJRGPMURSKHFRSEIUEVGOYCWIZAYGOSAANYDO
EOYJLWUNHAMEBFELXYVLWNOJNSIOFRWUCCEWVKVIDGMUCGOCRUWGNMAAFFVNSIUDEKQHCEUCPFCMP
VSUDGAVEMNYMAMVLFMAOYFNTQCUAFVFJNXKLNEIWCWODCCULWRIFTWGMUSWOVMATNYBUHTCOCWFY
TNMGYTQMKBBNLGFBTWOJFTWGNTEJKNEEDCLDHWTVBVUGFBIJG

► **Phase 1**
Etape 1

NUKGLMEKJINMWUXFQMKJBGWRLFNFGHUDWUUMBSVLPNSCMUEKQCTESWREEKOYSSIW
NTCGOJBGFQHTDWXIZAYGFFNSXCSEYNCTSSPNTUJNYTGGWZGRWUUNEJUJUEAPYME
SMTFFSHNUOCZGMRUWEYTRGKMEEDCTVRECFBDJQCUSWVBNLGOYLSKMTEFVJTTWW
MFMWPNMEMTMHRSPXFSSKFFSTNUOCZGMDOEOYEKCPJRGPMURSKHFRSEIUEVGOYCWIZAYGOSAANYDO
EOYJLWUNHAMEBFELXYVLWNOJNSIOFRWUCCEWVKVIDGMUCGOCRUWGNMAAFFVNSIUDEKQHCEUCPFCMP
VSUDGAVEMNYMAMVLFMAOYFNTQCUAFVFJNXKLNEIWCWODCCULWRIFTWGMUSWOVMATNYBUHTCOCWFY
TNMGYTQMKBBNLGFBTWOJFTWGNTEJKNEEDCLDHWTVBVUGFBIJG

Source: <https://www.apprendre-en-ligne.net/crypto/vigenere/decodevig.html>

Cryptanalyse 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	

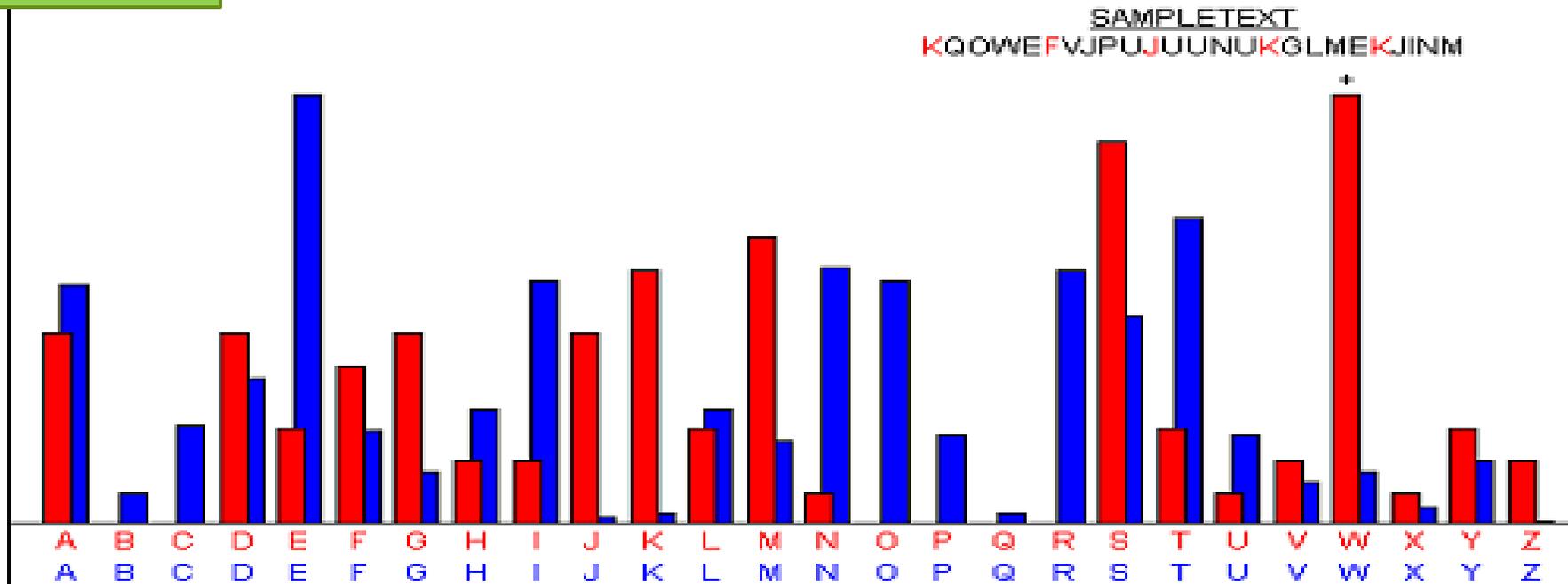
Etape
3

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

Cryptanalyse de Vigenère: Exemple

Phase 2

Etape 1



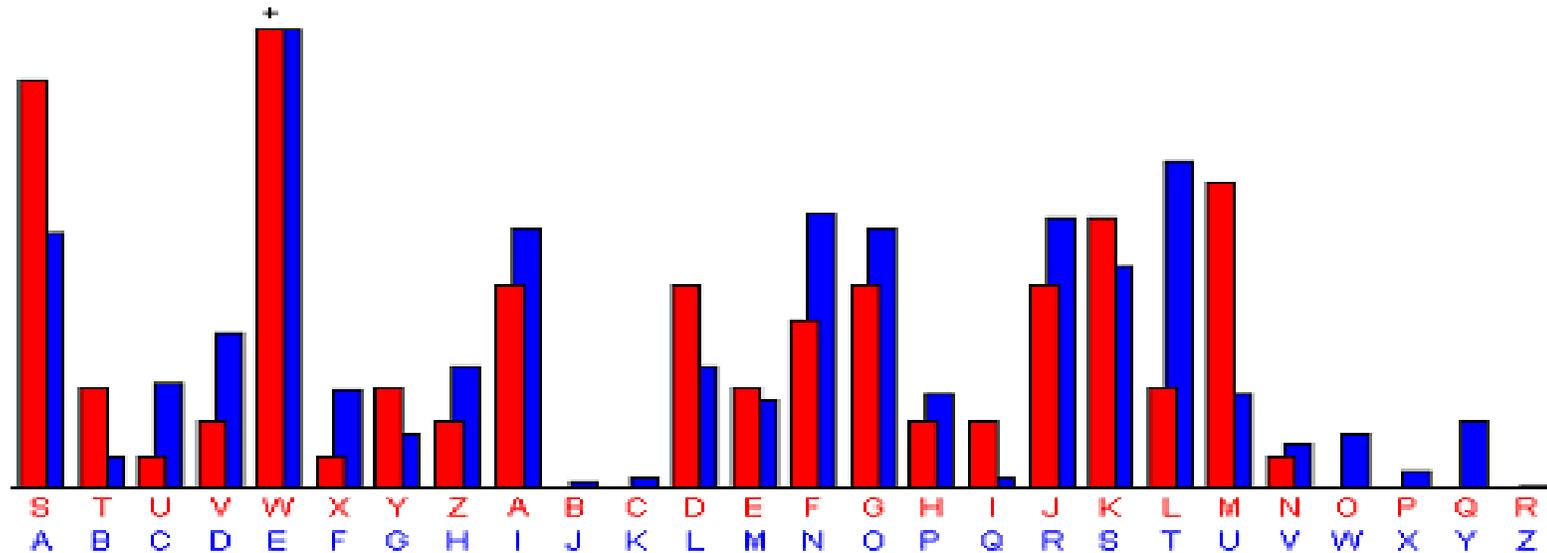
- En rouge, l'analyse de fréquence « modulo 5 »
- En bleu le diagramme de fréquence des lettres en français.

Cryptanalyse de Vigenère: Exemple

Phase 2

Etape 2

SAMPLETEXT
 SQOWENWJIPURUUNUSGLMESJINM



- On décale les diagrammes pour mettre le pic du **W** sur le **E**.
- $W = 22$ et $E = 4 \rightarrow$ c'est la $(22 - 4 = 18)$ soit **S**

Cryptanalyse de Vigenère: Exemple

Phase 3,4,5,6

- Le mot clé est: **SCUBA**
- On peut déchiffrer le cryptogramme:

Soit:

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

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.

À 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

Chiffrement Affine

- ▶ C'est un chiffrement mono-alphabétique.
- ▶ L'idée est d'utiliser comme fonction de chiffrement une **fonction affine** du type **$y = (a.x + b) \bmod 26$** ,
 - ▶ **a** et **b** sont des constantes,
 - ▶ **x** et **y** sont des nombres correspondant aux lettres de l'alphabet.

Chiffrement Affine

- ▶ $K = (a, b)$
- ▶ $E_k(x) = a \cdot x + b \pmod{26}$
- ▶ $D_k(y) = a^{-1} \cdot (y - b) \pmod{26}$
- ▶ a^{-1} est multiplicatif inverse de modulo 26, i.e, $a \cdot a^{-1} \equiv 1 \pmod{26}$

Chiffrement Affine

- ▶ 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:
$$\text{pgcd}(a, 26) = 1$$

Chiffrement Affine: cryptanalyse

- ▶ Le nombre de clés possibles est 26 fois le nombre d'éléments premiers avec 26.
- ▶ Il y a 12 valeurs qui sont premiers avec 26 :
1 3 5 7 9 11 15 17 19 21 23 et 25.
- ▶ Le nombre de clés possibles est $26 \cdot 12 = 312$.

Chiffrement Affine - Exemple 1

$K = (17, 3)$, $a=17$ et $b=3$

Vérification: $\text{PGCD}(17, 26) = 1$

→ **cryptage valide**

$17^{-1} \text{ mod } 26 = 23$ [$17 \cdot 23 = 391 = 1 \text{ mod } 26$]

→ **a. $a^{-1} \equiv 1 \text{ (mod } 26)$ vérifié**

▶ $E_k(x) = 17 \cdot x + 3 \text{ mod } 26$

▶ $D_k(x) = 17^{-1} \cdot (y-3) \text{ mod } 26 = 23 \cdot (y-3) \text{ mod } 26$
 $= 23y - 17 \text{ mod } 26$

Chiffrement Affine - Exemple 2

- ▶ Soit $K = (17, 3)$
- ▶ Chiffrer le texte **CODE**

Texte clair	C	O	D	E
Ind. Clair	2	14	3	4
Ind. Chiffré	11	7	2	19
Texte chiffré	L	H	C	T

- ▶ Exemple:
 - ▶ $E(2)_k = 17 * 2 + 3 \% 26 = 37 \% 26 = 11$
 - ▶ $D(11)_k = 23 * 11 - 17 \text{ mod } 26 = 2$

Chiffrement Affine: cryptanalyse

- ▶ Les hypothèses réalisées lors de la correspondance sont variables: si on pense que le chiffre de r_1 est s_1 et que le chiffre de r_2 est s_2 , en résolvant le système composé par
 - ▶ $r_1 \cdot a + b = s_1$
 - ▶ $r_2 \cdot a + b = s_2$
- ▶ nous trouvons une solution unique pour a et b dans Z_{26} .
- ▶ Si le $\text{pgcd}(a, 26) \neq 1$, on sait que la correspondance est mauvaise,
- ▶ et on essaie une autre correspondance (toujours sur base de la table de fréquence des lettres) .

Cryptanalyse Affine: Exemple

- ▶ Texte chiffré:
- ▶ GHUYI DEGRS YTG^OHKEIA AOTD^G SBINRGSG^H HGNYI ASIR RYOV^G
EOHGA N TGKGR HENNI

Cryptanalyse Affine: Exemple

- ▶ Fréquence des lettres: **G = 10** **H=6**
- ▶ Hypothèse : **E** et **T** sont les lettres les plus fréquentes en anglais
- ▶ Equations correspondantes :

$$\begin{cases} \mathbf{E \rightarrow G : E_k(E) = G} \\ \mathbf{T \rightarrow H : E_k(T) = H} \end{cases}$$

$$\begin{cases} \mathbf{4 \rightarrow 6 : E_k(4) = 6} \\ \mathbf{19 \rightarrow 7 : E_k(19) = 7} \end{cases}$$

Cryptanalyse Affine: Exemple (3)

► Résoudre les équations pour a et b inconnus:

$$\begin{cases} E_k(4) = 6 \\ E_k(19) = 7 \end{cases}$$

$$\begin{cases} 4a + b = 6 \pmod{26} \\ 19a + b = 7 \pmod{26} \end{cases}$$

$$15a = 1 \pmod{26}$$

Alors: **$a = 7 \pmod{26}$**

Chiffrement par transposition rectangulaire

- ▶ Une transposition rectangulaire consiste:
 - ▶ écrire le message dans une grille rectangulaire,
 - ▶ arranger les colonnes de cette grille selon un **mot de passe donné** (le rang des lettres dans l'alphabet donne l'agencement des colonnes).

Chiffrement par transposition rectangulaire

► Exemple:

► Texte clair: SALAM MES ETUDIANTS.

► La clé SALUT

S	A	L	U	T
3	1	2	5	4
S	A	L	A	M
M	E	S	E	T
U	D	I	A	N
T	S			



A	L	S	T	U
1	2	3	4	5
A	L	S	M	A
E	S	M	T	E
D	I	U	N	A
S		T		

► Texte chiffré: ALSMAESMTEDIUNAS T

Autres techniques de chiffrement

- ▶ Vernam
- ▶ Playfair,
- ▶ ADFGVX
- ▶ La machine Enigma
- ▶ . . .

Quiz

- ▶ La technique «Attaque par indice de coïncidence» utilisée pour casser:
 - ▶ le chiffrement par décalage.
 - ▶ le chiffrement de Vigenère
 - ▶ le chiffrement par transposition rectangulaire
 - ▶ le chiffrement Affine
- ▶ **Nombre de clés possibles du chiffrement Affine est :**
 - ▶ 26
 - ▶ 144
 - ▶ 312
 - ▶ 676

Questions ?

Moodle:

<https://elearning.univ-msila.dz/moodle/course/view.php?id=698>