

# Introduction à la cryptographie

## “L'époque artisanale”

**Christina Boura**

christina.boura@uvsq.fr

26 janvier 2018



# Organisation du module

- Cours : vendredi 9h40-11h10  
(Amphi D)
- TD :
  - mardi 9h40-12h50  
(Salle G003) DLBI-INF Gr 1, avec Édouard Rousseau
  - jeudi 13h40-16h50  
(Salle G103) INF Gr 2, avec Ilaria Chillotti

Les TDs se feront sans ordinateur.

# Contenu du cours

- Chiffrements **historiques** (César, Vigenère, ...), machine ENIGMA (2 semaines)
- Cryptographie **symétrique** (3 semaines)
  - Chiffrements à flot
  - Chiffrements par blocs
- Cryptographie **asymétrique** (6 semaines)
  - Protocole d'échange de clés Diffie-Hellman
  - Chiffrements RSA, Elgamal
  - Tests de primalité
  - Signatures numériques
- Certificats numériques, openssl (1 semaine)
- Fonctions de hachage (1 semaine)

# Agenda du jour

Stéganographie et cryptographie

Chiffrements historiques

L'analyse des fréquences

Le chiffre de Vigenère

# Agenda du jour

Stéganographie et cryptographie

Chiffrements historiques

L'analyse des fréquences

Le chiffre de Vigenère

# La stéganographie

**Définition :** La stéganographie est l'art de cacher un message dans un autre message (art de la dissimulation).

### Examples :

- L'encre invisible
- Écrire le message sur la tête d'un esclave
- Les micropoints



# La lettre de George Sand à Alfred de Musset

Je suis très émue de vous dire que j'ai bien compris l'autre soir que vous aviez toujours une envie folle de me faire danser. Je garde le souvenir de votre baiser et je voudrais bien que ce soit là une preuve que je puisse être aimée par vous. Je suis prête à vous montrer mon affection toute désintéressée et sans calcul, et si vous voulez me voir aussi vous dévoiler sans artifice mon âme toute nue, venez me faire une visite. Nous causerons en amis, franchement. Je vous prouverai que je suis la femme sincère, capable de vous offrir l'affection la plus profonde comme la plus étroite en amitié, en un mot la meilleure preuve dont vous puissiez rêver, puisque votre âme est libre. Pensez que la solitude où j'habite est bien longue, bien dure et souvent difficile. Ainsi en y songeant j'ai l'âme grosse. Accourez donc vite et venez me la faire oublier par l'amour où je veux me mettre.

# La lettre de George Sand à Alfred de Musset

Je suis très émue de vous dire que j'ai  
bien compris l'autre soir que vous aviez  
toujours une envie folle de me faire  
danser. Je garde le souvenir de votre  
baiser et je voudrais bien que ce soit  
là une preuve que je puisse être aimée  
par vous. Je suis prête à vous montrer mon  
affection toute désintéressée et sans cal-  
cul, et si vous voulez me voir aussi  
vous dévoiler sans artifice mon âme  
toute nue, venez me faire une visite.  
Nous causerons en amis, franchement.  
Je vous prouverai que je suis la femme  
sincère, capable de vous offrir l'affection  
la plus profonde comme la plus étroite  
en amitié, en un mot la meilleure preuve  
dont vous puissiez rêver, puisque votre  
âme est libre. Pensez que la solitude où j'ha-  
bite est bien longue, bien dure et souvent  
difficile. Ainsi en y songeant j'ai l'âme  
grosse. Accourez donc vite et venez me la  
faire oublier par l'amour où je veux me  
mettre.



# Le problème de la stéganographie

## Problème fondamental :

Si le message est **découvert**, le contenu de la communication secrète est **révélé**.

Développement en parallèle de la stéganographie d'un autre art, appelé "*l'art du secret*" :

la **cryptographie**.

# La cryptographie

*“La cryptographie est la pratique et étude des techniques pour assurer des communications sûres en présence d’adversaires.”*

Ron Rivest

Assurer plusieurs services de sécurité :

- **Confidentialité** : personne ne doit pouvoir lire le message.
- **Authenticité** : personne ne doit pouvoir contrefaire l'origine du message.
- **Intégrité** : personne ne doit pouvoir modifier le message.

# Confidentialité

Protéger le contenu des informations sauvegardées ou transmises sur un réseau.

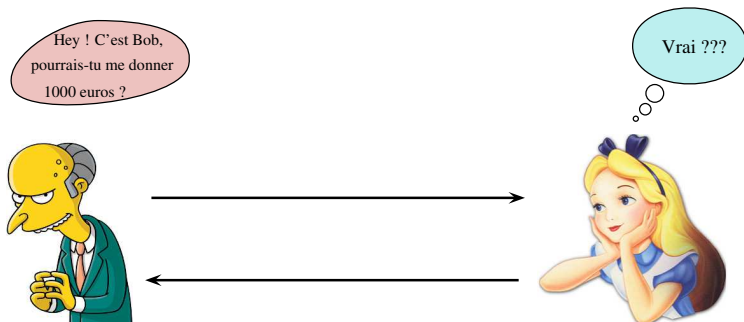
Échanger des messages en présence d'un espion.



Stocker des messages de façon sécurisée.

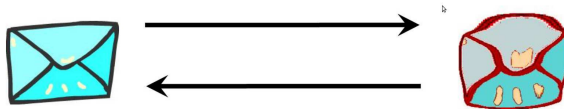
# Authenticité

S'assurer de la **provenance** d'un message et de l'**authenticité** de son émetteur.





# Intégrité

S'assurer de la **non-modification** d'un message,  
accidentelle ou intentionnelle.



# Vérifier l'intégrité d'un logiciel

HOMELINUX DISTRIBUTIONSLINUX TUTORIALSNEWSFREQUENTLY ASKED QUESTIONSOPENSOURCEUNIX

ASK/UNIXMEN

Link: <http://www.ubuntu.com/download/alternative-downloads>

3. Once you have downloaded the ISO image, lets check its md5sum (or any other Hash Checksum). Matched hash checksum will ensure two things. First that our download was complete and not interrupted. Second We Downloaded the correct Image. The Checksum of current Ubuntu release can be found here.

link: <ftp://ftp.free.fr/mirrors/ftp.ubuntu.com/releases/16.04/MD5SUMS>


To check md5sum of the downloaded ISO, run the below command from terminal.

```
$ md5sum ubuntu-16.04-desktop-amd64.iso
```

Sample Output

```
c94d54942a2954cf852884d656224186  ubuntu-16.04-desktop-amd64.iso
```

```
avi@deb:~/Downloads$ md5sum ubuntu-16.04-desktop-amd64.iso
c94d54942a2954cf852884d656224186  ubuntu-16.04-desktop-amd64.iso
avi@deb:~/Downloads$
```

 Follow @unixmen

Contact UnixMen

13 / 57

# Agenda du jour

Stéganographie et cryptographie

Chiffrements historiques

L'analyse des fréquences

Le chiffre de Vigenère

# Chiffrements par transposition

## Définition :

Un **chiffrement par transposition** est un mécanisme qui consiste à **changer l'ordre des lettres** du message.

Message **clair**

MESSAGE

Message **chiffré**

SEESMGA



# La scytale

Sparte 400 avant J.-C.

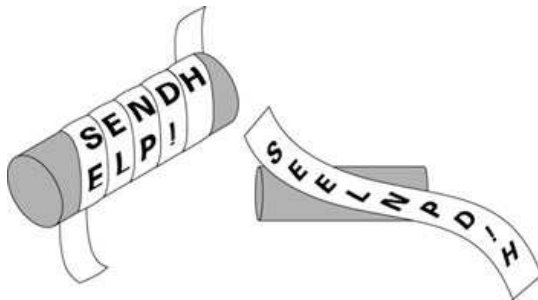
Chiffrer :

- Enrouler la ceinture sur la scytale.
- Écrire le message en plaçant une lettre sur chaque circonvolution.



Déchiffrer :

Posséder d'un bâton d'un  
diamètre identique.



# Sécurité d'un chiffrement par transposition

Nombre de façons de permuter  $n$  lettres :  $n!$

**Exemple** : Mot “CLE”

CLE CEL LEC LCE ELC ECL

$3! = 6$  façons de transposer les lettres.

Pour un mot de 20 lettres :

$$20! = 2432902008176640000 \approx 2^{61}.$$

Une transposition **au hasard** des lettres semble offrir un très haut niveau de sécurité.

# Recherche exhaustive

**Temps estimé** pour retrouver une clé de  $k$  bits :  $2^{k-1}$  opérations.

$k$ (bits)	Complexité en temps (operations)	Sécurité
40	$2^{40}$	facile à casser
64	$2^{64}$	possible à casser
80	$2^{80}$	pas encore possible
128	$2^{128}$	sécurité forte
256	$2^{256}$	sécurité très très forte

Table de [Knudsen, Robshaw, "The Block Cipher Companion", 2011.]

- La vie de l'univers est inférieure à  $2^{80}$  microsecondes !
- Le nombre de protons dans l'univers est  $\approx 2^{265}$ .

## Mais il y a un inconvénient ...

### En pratique :

L'ordonnancement des lettres doit suivre un **système rigoureux** sur lequel l'expéditeur et le récepteur se sont préalablement entendus.

### Exemple : Le chiffre Rail Fence

Message = "CRYPTOGRAPHIE"

C	Y	T	G	A	H	E
	R	P	O	R	P	I

Chiffré = "CYTGAHERPORPI"

# Transpositions rectangulaires

Message :

“Cela semble toujours impossible, jusqu'à ce qu'on le fasse.”

Mot clé : “CRYPTO”

C	R	Y	P	T	O
---	---	---	---	---	---

# Transpositions rectangulaires

Message :

“Cela semble toujours impossible, jusqu'à ce qu'on le fasse.”

Mot clé : “CRYPTO”

C	R	Y	P	T	O
1	4	6	3	5	2
C	E	L	A	S	E
M	B	L	E	T	O
U	J	O	U	R	S
I	M	P	O	S	S
I	B	L	E	J	U
S	Q	U	A	C	E
Q	U	O	N	L	E
F	A	S	S	E	

# Transpositions rectangulaires

Message :

“Cela semble toujours impossible, jusqu'à ce qu'on le fasse.”

Mot clé : “CRYPTO”

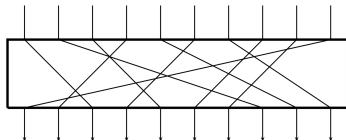
C	R	Y	P	T	O
1	4	6	3	5	2
C	E	L	A	S	E
M	B	L	E	T	O
U	J	O	U	R	S
I	M	P	O	S	S
I	B	L	E	J	U
S	Q	U	A	C	E
Q	U	O	N	L	E
F	A	S	S	E	

Texte chiffré : CMUIISQF EOSSUEE AEUOEANS EBJMBQUA  
STRSJCLE LLOPLUOS



## Conclusion : Chiffrements par transposition

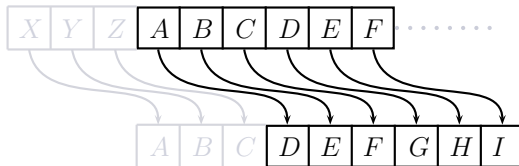
- L'algorithme utilisé est souvent **facile à deviner** (ainsi que la clé de la transposition).
- Algorithme cassé avec un seul couple "clair-chiffré".
- Les chiffrements par transposition font partie des **chiffrements modernes** (ex. chiffrements par blocs).



# Le chiffre de César

Jules César (100 - 44 avant J.-C.)

- César utilisait un chiffre pour protéger ces communications.
- $A \rightarrow D, B \rightarrow E, C \rightarrow F, \dots$



# Le chiffre de César – Chiffrement et déchiffrement

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
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

# Le chiffre de César – Chiffrement et déchiffrement

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
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

## 1. Chiffrement

ATTAQUONS CE SOIR

# Le chiffre de César – Chiffrement et déchiffrement

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
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

## 1. Chiffrement

ATTAQUONSCESOIR

# Le chiffre de César – Chiffrement et déchiffrement

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
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

## 1. Chiffrement

AT TAQUONSCESOIR  
DWWDTXRQVFHVRLU

# Le chiffre de César – Chiffrement et déchiffrement

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
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

## 1. Chiffrement

ATT AQUONSCESOIR  
DWWDTXRQVFHFR LU

## 2. Déchiffrement

DOHDMDFWDH VW

# Le chiffre de César – Chiffrement et déchiffrement

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
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

## 1. Chiffrement

ATT AQUONSCESOIR  
DWWDTXRQVFHRLU

## 2. Déchiffrement

DOHDMDFWDHVW  
ALEAJACTAEST



# Le chiffre de César – Chiffrement et déchiffrement

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
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

## 1. Chiffrement

ATT AQUONSCESOIR  
DWWDTXRQVFHFR LU

## 2. Déchiffrement

DOHDMDGWDH VW  
ALEA JACTA EST

“Les dés sont jetés”.

# Chiffrement par décalage

Décalage de l'alphabet par un entier  $k \in \{1, 2, \dots, 25\}$ .

- $k = 3$  (Chiffre de César)

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
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

- $k = 1$

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	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

# Chiffrement par décalage

Décalage de l'alphabet par un entier  $k \in \{1, 2, \dots, 25\}$ .

- $k = 3$  (Chiffre de César)

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
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

- $k = 1$

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	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



# Sécurité du chiffrement par décalage

Est-ce que ce chiffrement est sûr ?

**Nombre de clés possibles : 26**

- Aujourd'hui : Sécurité inexistante.
- Époque de César : Probablement sûr (analphabétisme, plusieurs langues étrangères, ...)
- Toujours utilisé pour des “secrets anodins”.

# Les chiffrements par substitution

**Substitution** : Remplacer chaque lettre de l'alphabet clair par une autre **lettre**, **chiffre** ou **symbole**.

**Substitution monoalphabétique** : Le **même alphabet** est conservé tout au long du chiffrement.

La **clé secrète** est la permutation entre les alphabets.

## Quelques Exemples :

- Chiffre par décalage (César)
- Carré de Polybe
- Chiffre des Templiers
- Chiffre de PigPen

# Le carré de Polybe

**Polybe**, historien grec ( $\approx$  200 - 125 av. J.-C.)

	1	2	3	4	5
1	A	B	C	D	E
2	F	G	H	I,J	K
3	L	M	N	O	P
4	Q	R	S	T	U
5	V	W	X	Y	Z

Texte clair : "CARRE DE POLYBE"

# Le carré de Polybe

**Polybe**, historien grec ( $\approx$  200 - 125 av. J.-C.)

	1	2	3	4	5
1	A	B	C	D	E
2	F	G	H	I,J	K
3	L	M	N	O	P
4	Q	R	S	T	U
5	V	W	X	Y	Z

Texte clair : "CARRE DE POLYBE"

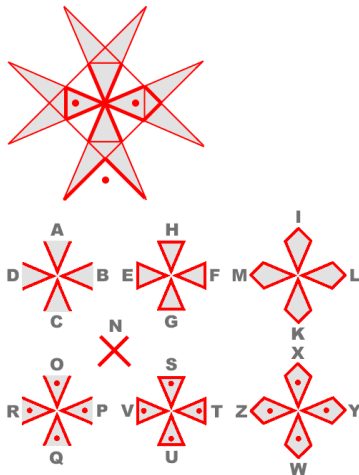
Texte chiffré : "13 11 42 42 15 14 15 35 34 31 54 12 15"

# Le chiffre des Templiers

- **Ordre du Temple** : ordre religieux et militaire du Moyen Âge.
- Chiffre basé sur la *croix de huit béatitudes*.

Texte clair : CRYPTOGRAPHIE

Texte chiffré :  $\wedge > \diamond < \triangleleft \nabla \Delta > \vee < \triangledown \triangleright$





# Le point faible de la substitution monoalphabétique

Nombre de **permutations** pour un alphabet de 26 lettres :  $26!$

$$26! \approx 2^{88}$$

Les chiffrements par substitution monoalphabétique ont été employés jusqu'au **16<sup>ième</sup> siècle** !

Cryptanalysés par l'**analyse de la fréquence des lettres**.

# Agenda du jour

Stéganographie et cryptographie

Chiffrements historiques

L'analyse des fréquences

Le chiffre de Vigenère

# L'analyse des fréquences

- Méthode de **cryptanalyse** développée par les Arabes au 9<sup>e</sup> siècle.
- Exposée dans le “Manuscrit sur le déchiffrement des messages cryptographiques” de **Al Kindi**.

Dans chaque langue, certaines lettres ou combinaisons de lettres apparaissent avec une certaine **fréquence**.

- **Examiner la fréquence** des lettres employées dans un message chiffré.

# Fréquence des lettres en Français

Lettre	Fréquence	Lettre	Fréquence
A	9.42%	N	7.15%
B	1.02%	O	5.14%
C	2.64%	P	2.86%
D	3.39%	Q	1.06%
E	15.87%	R	6.46%
F	0.95%	S	7.90%
G	1.04%	T	7.26%
H	0.77%	U	6.24%
I	8.41%	V	2.15%
J	0.89%	W	0.04%
K	0.05%	X	0.30%
L	5.34%	Y	0.24%
M	3.24%	Z	0.32%

## Quelques exceptions

“De Zanzibar à la Zambie et au Zaïre, des zones d’ozone font courir les zèbres en zigzags zinzins!”

Plus un texte est **long**, plus il a de chances de **suivre** les fréquences moyennes.

Une **exception** notable : “*La Disparition*” de Georges Perec, 1969.

## Un texte chiffré

BAELXEJ JCKJ ZA JANBH HSXGXWXL  
XMXPJ LCEEA XK GCP JGCPH DPOH.  
FKXEL AOOA AKJ JAGNPEA O'SPHJCPGA  
LA NX'GKD OA HXMAJPAG, AOOA HA OAMX,  
YXPHX OA HCO LAMXEJ OA HCKMAGXPE  
AJ OKP LPJ : "IGXEL GCP, LABKPH  
NPOOA AJ KEA EKPJH RA J'XP GXZCEJA  
OAH GAZPJH LA O'XEZPAE JANBH AJ OAH  
OAIAELAH LAH GCPH BXHHAH BKPH-RA  
NA BAGNAJJGA LA HCOOPZPJAG KEA  
DXMAKG LA MCJGA NXRAHJA?"  
ABPOCIKA-ZCEJAH LAH NPOOA  
AJ KEA EKPJH

[*"Histoire des codes secrets"*, Simon Singh]

# Analyse des fréquences du texte chiffré

Lettre	Occur.	Fréquence	Lettre	Occur.	Fréquence
A	61	19.5%	N	9	2.9%
B	8	2.4%	O	23	7.3%
C	14	4.5%	P	26	8.3%
D	3	1.0%	Q	0	0%
E	19	6.1%	R	3	1.0%
F	1	0.3%	S	2	0.6%
G	18	5.7%	T	0	0%
H	28	8.9%	U	0	0%
I	3	1.0%	V	0	0%
J	28	8.9%	W	1	0.3%
K	16	5.1%	X	20	6.4%
L	15	4.8%	Y	3	1.0%
M	7	2.2%	Z	6	1.9%

# Analyse des fréquences du texte chiffré

Lettre	Occur.	Fréquence	Lettre	Occur.	Fréquence
A	61	19.5%	N	9	2.9%
B	8	2.4%	O	23	7.3%
C	14	4.5%	P	26	8.3%
D	3	1.0%	Q	0	0%
E	19	6.1%	R	3	1.0%
F	1	0.3%	S	2	0.6%
G	18	5.7%	T	0	0%
H	28	8.9%	U	0	0%
I	3	1.0%	V	0	0%
J	28	8.9%	W	1	0.3%
K	16	5.1%	X	20	6.4%
L	15	4.8%	Y	3	1.0%
M	7	2.2%	Z	6	1.9%



$A \leftrightarrow e$ 

BAELXEJ JCKJ ZA JANBH HSXGXWXL  
XMXPJ LCEEA XK GCP JGCPH DPOH.  
FKXEL AOOA AKJ JAGNPEA O'SPHJCPGA  
LA NX'GKD OA HXMAJPAG, AOOA HA OAMX,  
YXPHX OA HCO LAMXEJ OA HCKMAGXPE  
AJ OKP LPJ : "IGXEL GCP, LABKPH  
NPOOA AJ KEA EKPJH RA J'XP GXZCEJA  
OAH GAZPJH LA O'XEZPAE JANBH AJ OAH  
OAIANELAH LAH GCPH BXHHAH BKPH-RA  
NA BAGNAJJGA LA HCOOPZPJAG KEA  
DXMAKG LA MCJGA NXRAHJA?"  
ABPOCIKA-ZCEJAH LAH NPOOA  
AJ KEA EKPJH

$$A \leftrightarrow e$$

BeELXEJ JCKJ Ze JeNBH HSXGXWXL  
 XMXPJ LCEEe XK GCP JGCPH DPOH.  
 FKXEL eOOe eKJ JeGNPeE O'SPHJCPGe  
 Le NX'GKD Oe HXMeJPeG, eOOe He OeMX,  
 YXPHX Oe HCO LeMXEJ Oe HCKMeGXPE  
 eJ OKP LPJ : "IGXEL GCP, LeBKPH  
 NPOOe eJ KEe EKPJH Re J'XP GXZCEJe  
 OeH GeZPJH Le O'XEZPeE JeNBH eJ OeH  
 OeLeELeH LeH GCPH BXHHeH BKPH-Re  
 Ne BeGNeJJGe Le HCOOPZPJGe KEe  
 DXMeKG Le MCJGe NXReHJe?"  
 eBPOCIKe-ZCEJeH LeH NPOOe  
 eJ KEe EKPJH

## Quelques observations

- 'A' se trouve 13 fois à côté du 'O' (OA, AOOA, OAH, ...)

OA, AOOA, OAH  
- e, e - - e, - e -

## Quelques observations

- 'A' se trouve 13 fois à côté du 'O' (OA, AOOA, OAH, ...)

OA, AOOA, OAH  
l e, e l l e, l e -

## Quelques observations

- 'A' se trouve 13 fois à côté du 'O' (OA, AOOA, OAH, ...)
- 'H' se trouve plusieurs fois en fin de mot.

OA, AOOA, OAH  
l e, e l l e, l e s

O  $\leftrightarrow$  l

H  $\leftrightarrow$  s

## Quelques observations

- 'A' se trouve 13 fois à côté du 'O' (OA, AOOA, OAH, ...)
- 'H' se trouve plusieurs fois en fin de mot.

OA, AOOA, OAH  
l e, e l l e, l e s

O  $\leftrightarrow$  l

H  $\leftrightarrow$  s

- La lettre 'J' apparaît 12 fois à côté du A (AJ 4 fois).
- AJ  $\leftrightarrow$  'en' ou 'et' ?

## Quelques observations

- 'A' se trouve 13 fois à côté du 'O' (OA, AOOA, OAH, ...)
- 'H' se trouve plusieurs fois en fin de mot.

OA, AOOA, OAH  
l e, e l l e, l e s

O  $\leftrightarrow$  l

H  $\leftrightarrow$  s

- La lettre 'J' apparaît 12 fois à côté du A (AJ 4 fois).
- AJ  $\leftrightarrow$  'en' ou 'et' ?

J  $\leftrightarrow$  t

BeELXEJ JCKJ Ze JeNBH HSXGXWXL  
XMXPJ LCEEe XK GCP JGCPH DPOH.  
FKXEL eOOe eKJ JeGNPEe O'SPHJCPGe  
Le NX'GKD Oe HXMeJPeG, eOOe He OeMX,  
YXPHX Oe HCO LeMXEJ Oe HCKMeGXPE  
eJ OKP LPJ : "IGXEL GCP, LeBKPH  
NPOOe eJ KEe EKPJH Re J'XP GXZCEJe  
OeH GeZPJH Le O'XEZPeE JeNBH eJ OeH  
OeleELeH LeH GCPH BXHHeH BKPH-Re  
Ne BeGNeJJGe Le HCOOPZPJeG KEe  
DXMeKG Le MCJGe NXReHJe?"  
eBPOCIKe-ZCEJeH LeH NPOOe  
eJ KEe EKPJH



BeELXEt tCKt Ze teNBs sSXGXWXL  
 XMXPt LCEEe XK GCP tGCPs DPIs.  
 FKXEL elle eKt teGNPEe l'SPstCPGe  
 Le NX'GKD le sXMetPeG, elle se leMX,  
 YXP sX le sCl LeMXEt le sCKMeGXPE  
 et lKP LPt : "IGXEL GCP, LeBKPs  
 NPll e et KEe EKPs Re t'XP GXZCete  
 les GeZPs Le l'XEZPeE teNBs et les  
 leleELes Les GCPs BXsses BKPs-Re  
 Ne BeGNettGe Le sClIPZPteG KEe  
 DXMeKG Le MCtGe NXReste?"  
 eBPIClKe-ZCetes Les NPll e  
 et KEe EKPs

## Encore quelques observations

- 'C' voyelle ? (tCKt, sCl)

## Encore quelques observations

- 'C' voyelle ? (tCKt, sCl)
- C  $\leftrightarrow$  o ? (toKt, sol)

## Encore quelques observations

- 'C' voyelle ? (tCKt, sCl)
- C  $\leftrightarrow$  o ? (toKt, sol)
- K  $\leftrightarrow$  u ? (tout, eKt  $\leftrightarrow$  eut)

BeELXEt tCKt Ze teNBs sSXGXWXL  
XMXPt LCEEe XK GCP tGCPs DPIs.  
FKXEL elle eKt teGNPEe l'SPstCPGe  
Le NX'GKD le sXMetPeG, elle se leMX,  
YXP sX le sCl LeMXEt le sCKMeGXPE  
et lKP LPt : "IGXEL GCP, LeBKPs  
NPll e et KEe EKPs Re t'XP GXZCete  
les GeZPs Le l'XEZPeE teNBs et les  
leleELes Les GCPs BXsses BKPs-Re  
Ne BeGNettGe Le sClIPZPteG KEe  
DXMeKG Le MCtGe NXReste?"  
eBPIClKe-ZCetes Les NPll e  
et KEe EKPs

BeELXEt tout Ze teNBs sSXGXWXL  
XMXPt LoEEe Xu GoP tGoPs DPls.  
FuXEL elle eut teGNPEe l'SPstoPGe  
Le NX'GuD le sXMetPeG, elle se leMX,  
YXP sX le sol LeMXEt le souMeGXPE  
et luP LPt : "IGXEL GoP, LeBuPs  
NPll e et uEe EuPts Re t'XP GXZoEte  
les GeZPts Le l'XEZPeE teNBs et les  
leleELes Les GoPs BXsses BuPs-Re  
Ne BeGNettGe Le sollPZPteG uEe  
DXMeuG Le MotGe NXReste?"  
eBPlolue-ZoEtes Les NPll e  
et uEe EuPts

pendant tout ce temps sharazad  
avait donne au roi trois fils.  
quand elle eut termine l'histoire  
de ma'ruf le savetier, elle se leva,  
baisa le sol devant le souverain  
et lui dit : " grand roi, depuis  
mille et une nuits je t'ai raconte  
les recits de l'ancien temps et les  
legendes des rois passes puis-je  
me permettre de solliciter une  
faveur de votre majeste ?"  
epilogue-contes des mille  
et une nuits

# Agenda du jour

Stéganographie et cryptographie

Chiffrements historiques

L'analyse des fréquences

Le chiffre de Vigenère



## Après la substitution monoalphabétique ?

**Conclusion** : Le chiffrement par substitution monoalphabétique est très fragile.

Comment **resister** à l'analyse des fréquences ?

# Après la substitution monoalphabétique ?

**Conclusion** : Le chiffrement par substitution monoalphabétique est très **fragile**.

Comment **resister** à l'analyse des fréquences ?

**Quelques alternatives peu efficaces :**

- **Mal orthographier** le message clair (ex. "*Sessi ha kom eifai dêfassé lé fhrekans*")
- Remplacer chaque **mot** par un autre mot ou symbole.

**Exemple :**

assassinez = D                  roi = Ω                  cette nuit = 13

Message : assassinez le roi cette nuit

Chiffré : DΩ13

## Des solutions plus sérieuses

- Substitution **homophonique** (1500-1750).  
(Remplacer une lettre par un nombre de symboles proportionnel à la fréquence d'apparition de la lettre.)

**Exemple** : Remplacer 'E' par 15 symboles différentes.

E	13	●h ↓ ψueη ο πjc Λ κ
A	9	θτ⊙ ~ λ * aT⊥
I	8	vη† ~ † + u⊗
R	8	snC†χ† dα
S	7	kwll † ⊙ • ◇
N	7	→ < ziy × ∞
T	7	∞lm⊙ ∨ ν
O	6	∇ο = ●pp
L	5	⊖Λ ⊗ bθ
U	4	> gfo
C	4	VNe
M	3	Ξrh
D	2	θp
P	2	⊥ξ
H	2	∇x
G	2	μα
B	2	βφ
Y	1	q
V	1	≠
Z	1	—
W	1	ω
J	1	δ
X	1	△
Q	1	⊞
F	1	∃
K	1	t

- Chiffrements par substitution **polyalphabétique** (ex. Vigenère).

# Chiffre de Vigenère

Blaise de Vigenère (1523-1596) :  
diplomate, cryptographe et astrologue  
français.



- **1586** : Présente un chiffrement polyalphabétique qui porte depuis son nom.
- **Paternité** de ce système **contesté** (Giovan Batista Belaso avait proposé un système similaire en 1564).
- **Battista Alberti** avait proposé autour de 1460 un chiffre basé sur l'emploi de **deux alphabets différents**.

# Le chiffre d'Alberti

alphabet 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  
alphabet chiffré 1 F Z B V K I X A Y M E P L S D H J O R G N Q C U T W  
alphabet chiffré 2 G O X B F W T M Q I L A P Z J D E S V Y C R K U H N

Message : hello

Chiffré : A F P A D

# Le 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

# Chiffrement

- **Clé de chiffrement** : **Quels alphabets** seront utilisés et dans quel ordre.

**Exemple.** Mot-clé : CRYPTO

ATTAQUEENNEMIDEMA I N  
CRYPTOCRYPTOCRYPTOC  
CKRPJIGVLCXAKUCBTWP

# Chiffrement

- **Clé de chiffrement** : **Quels alphabets** seront utilisés et dans quel ordre.

**Exemple.** Mot-clé : CRYPTO

ATTAQUEENNEMIDEMA I N  
CRYPTOCRYPTOCRYPTOC  
CKRPJIGVLCXAKUCBTWP

## Avantage

- Une même lettre du texte clair sera chiffrée de plusieurs façons différentes. → l'analyse de fréquences échouera



# Cryptanalyse du chiffre de Vigenère

- Charles Babbage (1792- 1871)
- Friedrich Wilhelm Kasiski (1805-1881)

## Deux étapes :

- Déterminer la longueur de la clé.
- Effectuer une analyse de fréquences à chaque alphabet.

## Un exemple

K I L O K I L O K I L O K I L O K I L O K I L O K  
t h e r u s s e t h e j a s m i n t h e c h i n e  
D P P F E A D S D P P X K A X W X B S S M P T B O

- Les **mêmes séquences** de lettres sont chiffrées avec la **même partie** de la clef !

## Un exemple complet

XAUNMEESYIEDTLLFGSNBWQ  
UFXPQTYORUTYIINUMQIEUL  
SMFAFXGUTYBXXAGBHMIFII  
MUMQIDEKRIFRIRZQUHIENO  
OOIGRMLYETYOVQRYSIXEOK  
IYPYOIGRFBWPIYRBQURJIY  
EMJIGRYKXYACPPQSPBVESI  
RZQRUFREDYJIGRYKXBLOPJ  
ARNPUGEFBWMILXMZSMZYXP  
NBPUMYZMEEFBUGENLRDEPB  
JXONQEZTMBWOFIIPAHPPQ  
BFLGDEMFWFAHQ

## Un exemple complet

XAUNMEESYIEDTLLFGSNBWQ  
UFXPQTYORUTYIINUMQIEUL  
SMFAFXGUTYBXXAGBHMIFII  
MUMQIDEKRIFRIRZQUHIENO  
OOIGRMLYETYOVQRYSIXEOK  
IYPYOIGRFBWPIYRBQURJIY  
EMJIGRYKXYACPPQSPBVESI  
RZQRUFREDYJIGRYKXBLOPJ  
ARNPUGEFBWMILXMZSMZYXP  
NBPUMYZMEEFBUGENLRDEPB  
JXONQEZTMBWOFIIPAHPPQ  
BFLGDEMFWFAHQ

## Un exemple complet

XAUNMEESYIEDTLLFGSNBWQ  
UFXPQTYORUTYIINUMQIEUL  
SMFAFXGUTYBXXAGBHMIFII  
MUMQIDEKRIFRIRZQUHIENO  
OOIGRMPLYETYOVQRYSIXEOK  
IYPYOIGRFBWPYIRBQURJIY  
EMJIGRYKXYACPPQSPBVESI  
RZQRUFREDYJIGRYKXBLOPJ  
ARNPUGEFBWMILXMZSMZYXP  
NBPUMYZMEEFBUGENLRDEPB  
JXONQEZTMBWOFIIPAHPPQ  
BFLGDEMFWFAHQ

## Un exemple complet

XAUNMEESYIEDTLLFGSNBWQ  
UFXPQTYORUTYIINUMQIEUL  
SMFAFXGUTYBXXAGBHMIFII  
MUMQIDEKRIFRIRZQUHIENO  
OOIGRMLYETYOVQRYSIXEOK  
IYPYOIGRFBWPYIRBQURJIY  
EMJIGRYKXYACPPQSPBVESI  
RZQRUFREDYJIGRYKXBLOPJ  
ARNPUGEFBWMILXMZSMZYXP  
NBPUMYZMEEFBUGENLRDEPB  
JXONQEZTMBWOFIIPAHPPQ  
BFLGDEMFWFAHQ

Séquence répétée	Espace de répétition	Longueurs de clé possibles								
		2	3	4	5	6	7-9	10	11-14	15
UMQI	30	✓	✓		✓	✓		✓		✓
OIGR	25				✓					
JIGRY	30	✓	✓		✓	✓		✓		✓

Séquence répétée	Espace de répétition	Longueurs de clé possibles								
		2	3	4	5	6	7-9	10	11-14	15
UMQI	30	✓	✓		✓	✓		✓		✓
OIGR	25				✓					
JIGRY	30	✓	✓		✓	✓		✓		✓

Mot-clé de 5 lettres :  $L_1L_2L_3L_4L_5$

- chiffre polyalphabétique composé de 5 chiffres monoalphabétiques



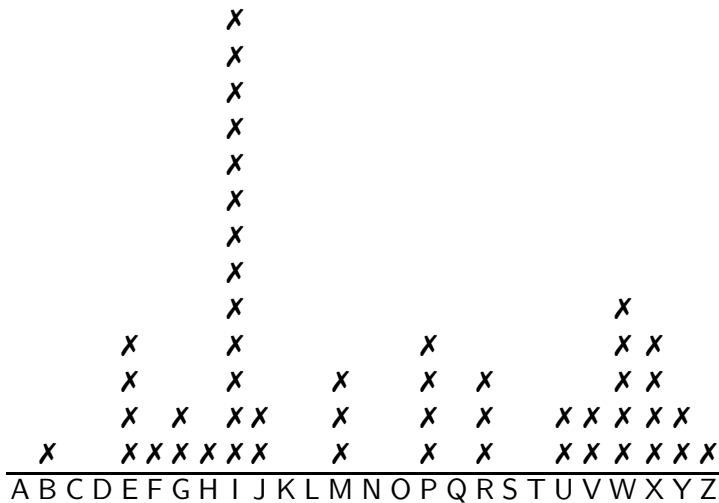
# Alphabet $L_1$

XAUNMEESYIEDTLLFGSNBWQ  
UFXPQTYORUTYIINUMQIEUL  
SMFAFXGUTYBXXAGBHMIFII  
MUMQIDEKRIFRIRZQUHIENO  
OOIGRMLYETYOVQRYSIXEOK  
IYPYOIGRFBWPIYRBQURJIY  
EMJIGRYKXYACPPQSPBVESI  
RZQRUFREDYJIGRYKXBLOPJ  
ARNPUGEFBWMILXMZSMZYXP  
NBPUMYZMEEFBUGENLRDEPB  
JXONQEZTMBWOFIIPAHPPQ  
BFLGDEMFWFAHQ

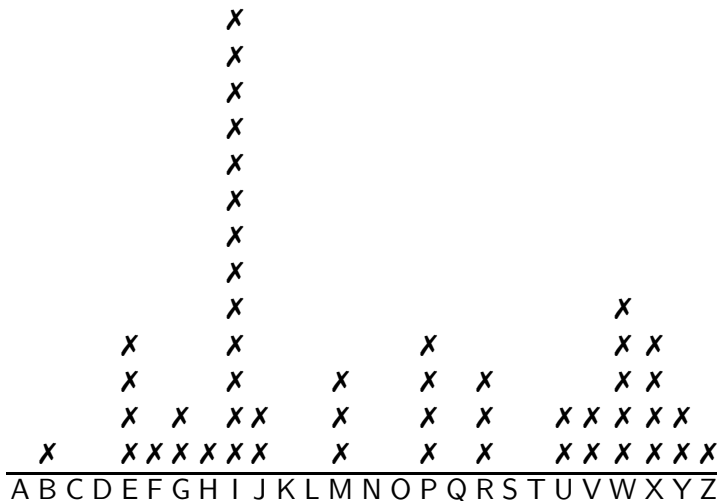
# Alphabet $L_1$

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

# Fréquences selon l'alphabet $L_1$



# Fréquences selon l'alphabet $L_1$



- $I \leftrightarrow e$
- $L_1 = e$

## Alphabet $L_2$

XAUNMEESYIEDTLLFGSNBWQ  
UFXPQTYORUTYIINUMQIEUL  
SMFAFXGUTYBXXAGBHMIFII  
MUMQIDEKRIFRIRZQUHIENO  
OOIGRMLYETYOVQRYSIXEOK  
IYPYOIGRFBWPIYRBQURJIY  
EMJIGRYKXYACPPQSPBVESI  
RZQRUFREDYJIGRYKXBLOPJ  
ARNPUGEFBWMILXMZSMZYXP  
NBPUMYZMEEFBUGENLRDEPB  
JXONQEZTMBWOFIIPAHPPQ  
BFLGDEMFWFAHQ

# Alphabet $L_2$

XAUNMEESYIEDTLLFGSNBWQ  
UFXPQTYORUTYIINUMQIEUL  
SMFAFXGUTYBXXAGBHMIFII  
MUMQIDEKRIFRIRZQUHIENO  
OOIGRMLYETYOVQRYSIXEOK  
IYPYOIGRFBWPIYRBQURJIY  
EMJIGRYKXYACPPQSPBVESI  
RZQRUFREDYJIGRYKXBLOPJ  
ARNPUGEFBWMLXMXZSMZYXP  
NBPUMYZMEEFBUGENLRDEPB  
JXONQEZTMBWOFIIPAHPPQ  
BFLGDEMFWFAHQ

## Le principe de Kerckhoffs (1883)

En 1883 **August Kerckhoffs** énonce 6 principes de conception pour des chiffrements à usage **militaire**. Le deuxième principe dit :

*La sécurité d'un cryptosystème ne doit reposer que sur le secret de la clé.*

Reformulé par **Claude Shannon** comme

**“L'adversaire connaît le système.”**

i.e., *“On doit concevoir des systèmes en supposant que l'ennemi trouvera les moyens de se familiariser immédiatement avec.”*

# Bibliographie

- "*L'histoire des codes secrets*", Simon Singh.
- "*Handbook of Applied Cryptography*", Alfred J. Menezes, Paul C. van Oorschot, Scott A. Vanstone (livre gratuit en version électronique) <http://cacr.uwaterloo.ca/hac/>
- "*Cryptographie : théorie et pratique*", D. Stinson (en ligne) [http://www.icst.pku.edu.cn/course/Cryptography/CryptographyTheoryandpractice\(3ed\).pdf](http://www.icst.pku.edu.cn/course/Cryptography/CryptographyTheoryandpractice(3ed).pdf)
- "*Introduction to Modern Cryptography*", J. Katz and Y. Lindell.
- "*Understanding Cryptography*", C. Paar and J. Pelzl.