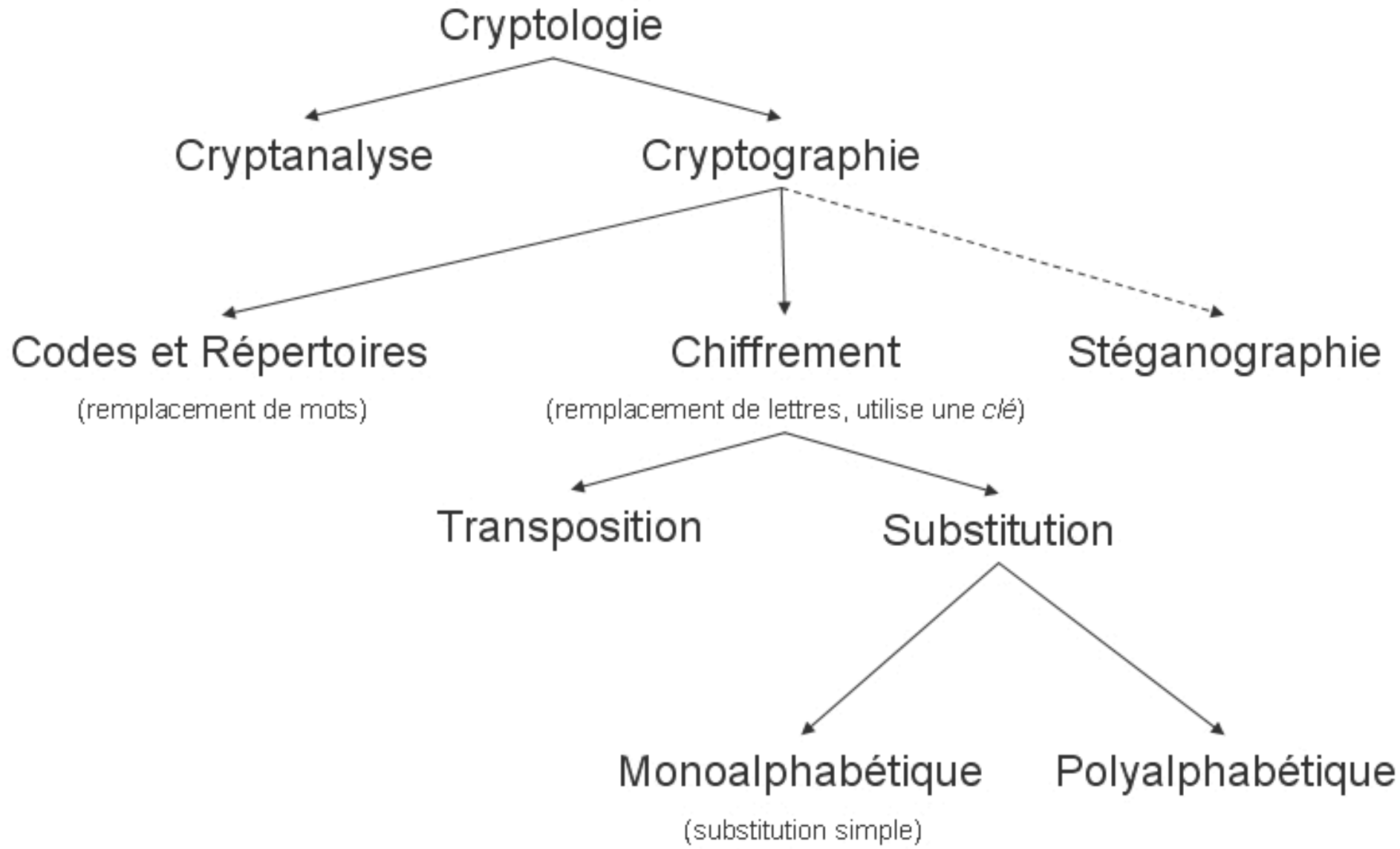
# Cryptographie Classique

A. ATLAS

**Génie Info**


Cryptologie
Cryptanalyse
Cryptographie
Codes et Répertoires
(remplacement de mots)
Chiffrement
(remplacement de lettres, utilise une *clé*)
Stéganographie
Transposition
Substitution
Monoalphabétique
(substitution simple)
Polyalphabétique

# Codes à répertoire

- Consistent en un dictionnaire qui permet de remplacer certains mots par des mots différents
- Très anciens et ont été utilisés intensivement jusqu'au début du 20-ème siècle
- Sévèrement critiqué par Kirckhoffs.
- usages commerciaux ou militaires au 19$^{e}$ siècle
- Tout changement du code nécessitait l'envoi de documents volumineux

# Codes à répertoire

- Exemple :

| | |
|---|---|
| rendez-vous ↔ **175** | demain ↔ **oiseaux** |
| midi ↔ **à vendre** | Villetaneuse ↔ **au marché** |

- Message Crypté

175 OISEAUX À VENDRE AU MARCHÉ

- Décrypter ???

# Codes de Permutation

# Scytale

- **Utilisé par les Sparte ( -450 AJ)**


**Message Crypté ??**

# Exercice 1 : La Scytale

Décrypter le texte suivant qui a été obtenu en appliquant un chiffrement par transposition par scytale sur un texte en langue française dans lequel les espaces ont été supprimées :

lelnracsrunanatuvllerrmcnjeeaeseiaetanctsagsgeemftqdnne
ntrarauenecilliianeredofaesntdneenignpcdaishdcaoaeenede

# Chiffrement par transp. de Col.

- Comme le chiffrement par Scytale, le message a crypter est écrit dans une grille rectangulaire et lu par colonne.
- Pour augmenter la sécurité, les deux interlocuteurs peuvent ajouter une clef.
- Le but est de pouvoir changer facilement le cryptage d'un message tout en gardant le même algorithme de codage

# Chiffrement par transp. de Col.

- Exemple : Si on choisit la clé « CAPTER »

# Exercice 2 : Cryptanalyse de T.C.

Décrypter le texte suivant qui a été obtenu en appliquant un chiffrement par transposition par colonnes sur un texte en langue française dans lequel les espaces ont été supprimées (en sachant que la clé utilisée est une permutation de longueur 8) :

```
ahcaaieqreeiecadapniieliuouuxiusnlbocoretcllia
uintsefesetdletvseeeedeauennsuuivntshnenlttvtl
ydsrtonsasrutonndiicneijttestjliiaeesaoleddrev
lriaimxrpserulnaereautvorqhidoeelutssglaneeslh
```

# Codes de Substitution

# Code de César ( 50 avJ)

- Jules César pendant la guerre des Gaules avait utilisé le code de substitution par flot suivant :

lettre codée=lettre claire +3 (mod 26)

- Q1:Chiffrer ce message : « Bonjour ensam »??
- Sachant que la clef utilisée est 7, décoder

« YLUKLG CVBZ KLTHPU TPKP CPSSLAHULBZLBZL »

# Chiffrement affine

- L'idée est d'utiliser comme fonction de chiffrement une fonction affine du type

$$y = ( k1x + k2) \bmod 26$$

- Chiffrer le message clair suivant en utilisant k1 = et k2 =

«rebonjour ensam »

# Cryptanalyse du Chiffre affine

- Question :

Décrypter le texte suivant qui a été obtenu en appliquant le chiffrement affine sur un texte en langue française dans lequel les espaces ont été supprimées :

ntjmpumgxpqtstgqpgtxpnchumtputgfsftgthnngxnchumwx
ootrtumhpyctgktjqtjchfooxujqhgztumxpotjxotfoqtohr
xumhzutwftgtopfmntjmpuatmfmshodpfrxpjjtqtghbxuj

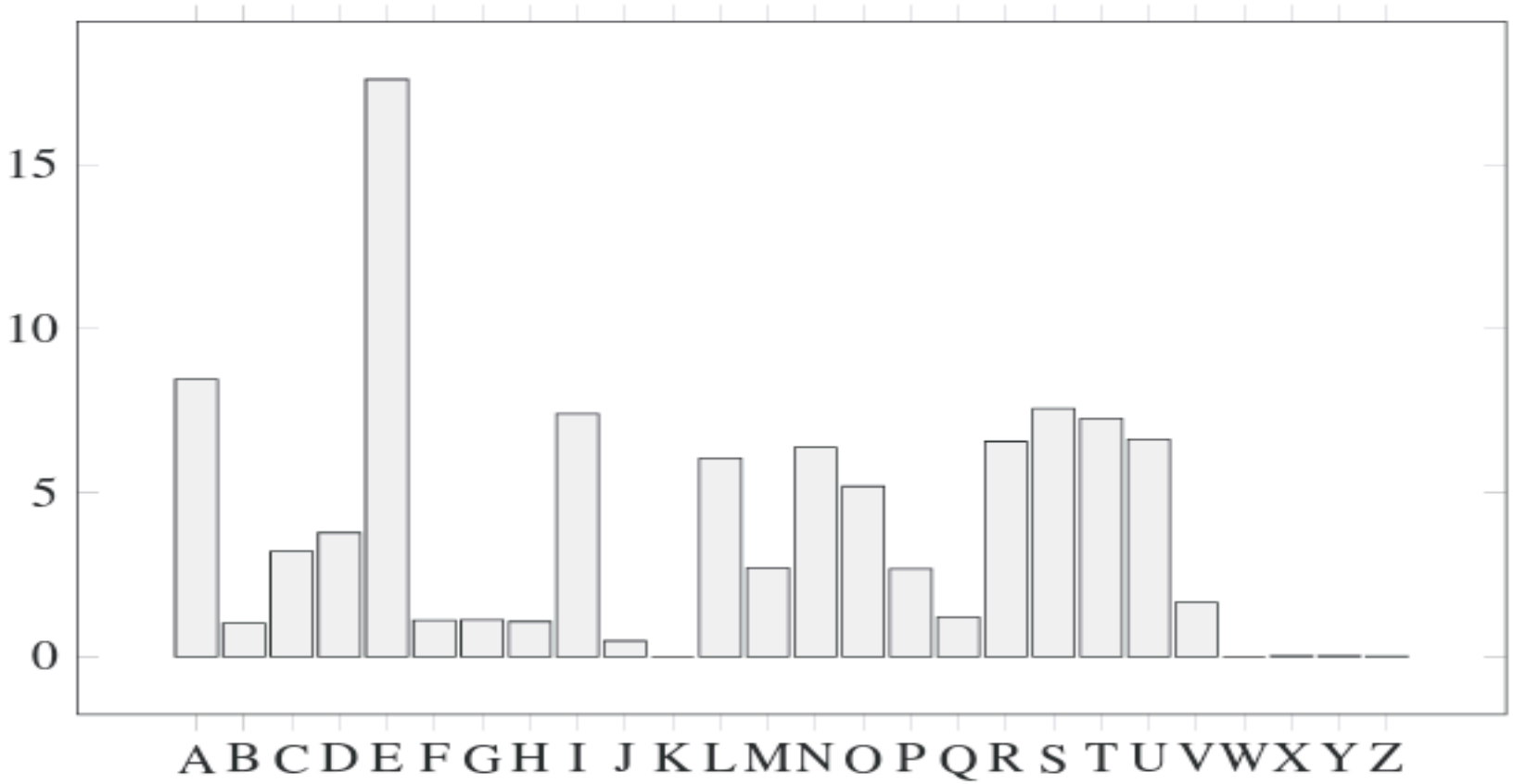
# Cryptanalyse du Chiffre affine

- Analyse de fréquence des lettres FR

| a | b | c | d | e | f | g | h | i | j | k | l | m |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 8,46 | 1,02 | 3,21 | 3,78 | 17,60 | 1,11 | 1,12 | 1,07 | 7,40 | 0,48 | 0 | 6,05 | 2,70 |
| n | o | p | q | r | s | t | u | v | w | x | y | z |
| 6,38 | 5,19 | 2,68 | 1,21 | 6,56 | 7,56 | 7,26 | 6,63 | 1,65 | 0 | 0,03 | 0,03 | 0,01 |

# Cryptanalyse du Chiffre affine

- Analyse de fréquence des lettres FR



# Chiffrement de Vigenere (1568)

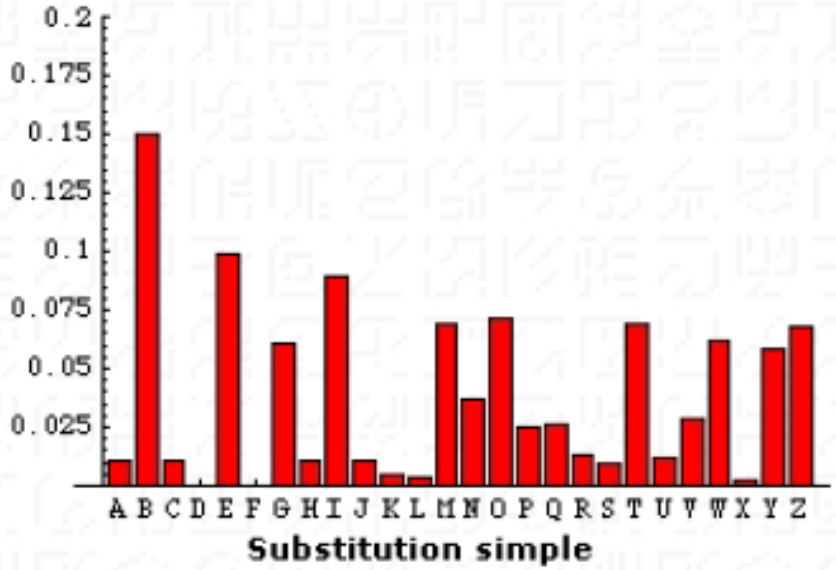
- C’est une amélioration décisive du chiffre de César.
- Rentre dans la catégorie de Substitutions polyalphabétiques ou bloc
- Ce chiffre utilise une clef.
- **Exemple :** chiffrer le texte "CHIFFRE DE VIGENERE " avec la clef « atlas »

# Carré de Vigenere

| | 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 |

# Cryptanalyse de Vigenere.

- la grande force de ce chiffrement est que la même lettre pourra être de différentes manières




# Cryptanalyse de Vigenere.

- Cryptanalyse de Kasiski

CS AZZMEQM, CO XRWF, CS DZRM GFMJECV. XTMOQJ JC LB NLFMK CC LBM WCCZBM
KFIMSZJSZ CS URQIUOU. CS ZLPIE ECZ RMWWTV, SB KCCJ QMJ FCSOVJ GCI ZI ICCKS, MK
QMLL YL'CV ECCJ OKTFWTVM JIZ CO XFWBIWVV, IV ACCI CC C'OCKFM, JINWWB
U'OBKSVUFM

| Séquence | Position | Distance | Décomposition |
|---|---|---|---|
| COX | 11-140 | 129 | 3.43 |
| FCS | 16-99 | 83 | 83 |
| ZRM | 20-83 | 63 | $3^2 7$ |
| FMJ | 24-162 | 138 | 2.3.23 |
| CLB | 37-46 | 9 | $3^2$ |
| KCC | 44-92 | 48 | $2^3 3$ |
| WTV | 87-133 | 46 | 2.23 |
| CCJ | 93-126 | 33 | 3.11 |
| ICC | 110-155 | 45 | $3^2.5$ |
| MJI | 136-163 | 27 | $3^3$ |

# Cryptanalyse de Vigenere.

- Exercice :

Le texte suivant a été obtenu en appliquant le chiffrement de Vigenère sur un texte en langue française dans lequel les espaces ont été supprimées :

```
zbpuevpuqsdlzgllksousvpasfpddggaqwptdgptzweemqzrdjtddefek
eferdprrcyndgluaowcnbptzzzrbvpssfpashpncotemhaeqrferdlrlw
wertlussfikgoeuswotfdgqsyasrlnrzppdhtticfrciwurhcezrpmhtp
uwiyenamrdbzyzwelzucamrptzqseqcfgdrfrhrpatsepzgfnaffisbpv
blisrplzgnemswaqoxpdseehbeeksdptdttqsdddgxurwnidbdddplncsd
```

Utiliser le test de Kasiski pour déterminer la longueur de la clé utilisée et décrypter ce texte.

# Cryptanalyse de Vigenere.

- **Cryptanalyse de Friedman** : utilise la notion de l'indice de coincidence (IC).
- Soient n le nombre de lettres dans le texte, n1 = nombre de A, ...,n26 = nombre de Z.

$$P(2\ fois\ A) = \frac{C_2^{n_1}}{C_2^n} = \frac{\frac{n_1(n_1-1)}{2}}{\frac{n(n-1)}{2}} = \frac{n_1(n_1-1)}{n(n-1)}$$

# Cryptanalyse de Vigenere.

- **Cryptanalyse de Friedman** : utilise la notion de l'indice de coincidence (IC).
- La probabilité de tirer 2 lettres identiques est donnée par

$$IC = \sum_{i=1}^{26} \frac{n_i(n_i - 1)}{n(n-1)}$$

| Langue | allemand | anglais | espagnol | esperanto | français | italien | norvégien | suédois |
|---|---|---|---|---|---|---|---|---|
| IC | 0.072 | 0.065 | 0.074 | 0.069 | 0.074 | 0.075 | 0.073 | 0.071 |

# Exemple de test de Friedman

- On calcule l'IC pour chaque sous chaine

| Intervalle | Indice de coïncidence |
|---|---|
| 1 | 0.0456107 |
| 2 | 0.0476954, 0.0443098 |
| 3 | 0.044249, 0.0494469, 0.0426771 |
| 4 | 0.0465839, 0.0453894, 0.0449116, 0.0425227 |
| 5 | 0.0799704, 0.0925583, 0.0836727, 0.0795282, 0.0684932 |
| 6 | 0.0512956, 0.0407192, 0.0371585, 0.0382514, 0.0661202, 0.0431694 |

# Exemple de test de Friedman

PERTQ UDCDJ XESCW MPNLV MIQDI ZTQFV XAKLR PICCP QSHZY DNCPW EAJWS ZGCLM QNRDE OHCGE ZTQZY HELEW AUQFR OICWH QMYRR UFGBY QSEPV NEQCS EEQWE EAGDS ZDCWE OHYDW QERLM FTCCQ UNCPP QSKPY FEQOI OHGPR EERWI EFSDM XSYGE UELEH USNLV GPMFV EIVXS USJPW HIEYS NLCDW MCRTZ MICYX MNMFZ QASLZ QCJPY DSTTK ZEPZR ECMYW OICYG UESIU GIRCE UTYTI ZTJPW HIEYI ETYYH USOFI XESCW HOGDM ZSNLV QSQPY JSCAV QSQLM QNRLP QSRLM XLCCG AMKPG QLYLY DAGEH GERCI RAGEI ZNMGI YBPP

- On considère les sous chaines en prenant les lettres en intervalle donné

Intervalle de 1 : PERTQ UDCDJ XESCW MPNLV ... (texte original)
Intervalle de 2 : PRQDD XSWPL ... et ETUCJ ECMNV ...
Intervalle de 3 : PTDJS MLIIQ ..., EQCXC PVQZF... et RUDEW NMDTV
...

# Cryptanalyse de Vigenere.

- Exercice :

Le texte suivant a été obtenu en appliquant le chiffrement de Vigenère sur un texte en langue française dans lequel les espaces ont été supprimées :

```
gmyxzoocxziancxktanmyolupjrztgxwshctzluibuic
yzwxyqtvqxzukibkotuxkagbknmimmzzyajvjzampqyz
loinoiqknaumbknknvkaiakgwtnilvvzvqydmvjcximr
vzkilxzqtomrgqmdjrzyazvzmmyjgkoaknkuiaivknvvy
```

Utiliser l'indice de coïncidence pour déterminer la longueur de la clé utilisée et décrypter ce texte.

# Chiffrement de Hill

$$\begin{pmatrix} C_k \\ C_{k+1} \end{pmatrix} = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} P_k \\ P_{k+1} \end{pmatrix} (\mathrm{mod}\, 26)$$

Chiffrer un message clair « rerebonjour ensam » en utilisant la clé suivante

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

# Chiffrement de Hill

- Exercice : attaque a clair connu

Décrypter le texte suivant qui a été obtenu en appliquant le chiffrement de Hill sur des blocs de taille 2 sur un mot de la langue française :

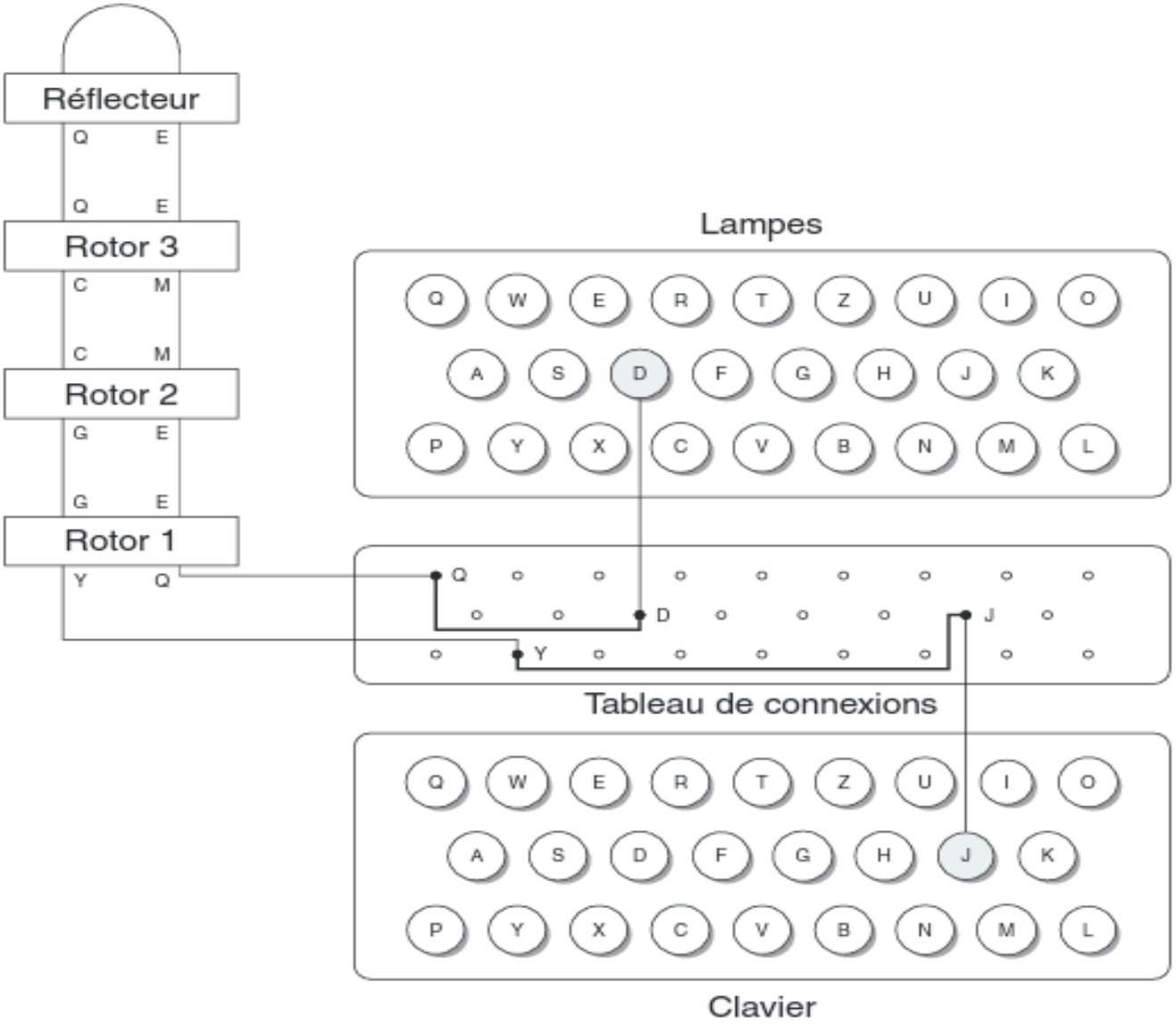
`gzatzxjihvbreosu`

sachant que le chiffrement du mot `chiffrer` avec la même clé donne le chiffré `jvfrtqnb`.

# Enigma

- Après la première guerre mondiale, Arthur Scherbius a présenté en 1918 une machine de chiffrement.
- Après avoir semblé jouer un rôle déterminant dans la victoire nazie, elle contribua à la chute d'Hitler.

# Enigma


Réflecteur
Q E
Q E
Rotor 3
C M
C M
Rotor 2
G E
G E
Rotor 1
Y Q
Lampes
Q W E R T Z U I O
A S D F G H J K
P Y X C V B N M L
Q
D
J
Y
Tableau de connexions
Q W E R T Z U I O
A S D F G H J K
P Y X C V B N M L
Clavier

# Vernam (One Time Pad – 1917)

- Egalement appelé chiffrement par masque jetable.
- Le message chiffré est obtenu comme dans le chiffrement de Vigenere avec le long de la clef soit aussi long que le message.
- Couramment utilisé de nos jours par les États. En effet, ceux-ci peuvent communiquer les clefs à leurs ambassades de manière sûre via la valise diplomatique. **( la crise de cuba )**
- Le risque que fait courir la réutilisation de la clef est facile montré.

# Exercice

*Mauvaise utilisation du chiffrement jetable*

Un utilisateur a chiffré deux mots (non accentués) de la langue française de sept lettres avec le chiffrement de Vernam mais il a été imprudent et a utilisé deux fois la même clé pour chiffrer ces deux messages. Sachant que les chiffrés obtenus sont les mots `hqdtmap` et `onooiup`, faire une recherche informatique dans un *corpus* de la langue française et trouver tous les couples de textes clairs susceptibles de produire ces chiffrés.

# Sténographie

- Message envoyé par un espion allemand pendant la seconde guerre mondiale:

« Apparently neutral's protest is thoroughly discounted and ignored. Isman hard it. Blockade issue affects pretext for embargo on byproducts, ejecting suets and vegetable oils»

# Sténographie

- Google célèbre les 50 ans **des Pierrafeu (30/9/2010)**