Idriss KOUROUMA
NI: 537 025 540

# Vigenère

## Exercice 5 : Briser Vigenère

Le chiffrement de Vigenère est un cryptosystème poly alphabétique. Il permet de crypter un message, à l'aide d'une clé, de la manière suivante :

- texte clair : hello
- clé : abc
- on décale chaque lettre en fonction de la clé, c'est-à-dire, que h est décalé de 0 positions (valeur de a), e est décalé de de 1 position (valeur de b), l est décalé de 2 (valeur de c), l est décalé de a, etc.
- On répète la clé autant de fois que nécessaire.

### Question 1 :

Dans le but d'estimer la taille de la clé, on utilise le Test de Friedman. Pour ce faire, on procède en trois étapes :

- On suppose que m=1,2,3,…
- Pour chaque valeur de m, on calcule les indices de coïncidence des $Y_i$.
- On retient la valeur de m qui donne des indices de coïncidence proches de celui de la langue d'origine.

Les indices de coïncidence sont calculés de la manière suivante :

- $n_0, ..., n_25$ sont respectivement les nombres d'occurrences des lettres $a, b, ..., z$ dans la chaîne *x*.

$$I_c(x) = \frac{\sum_{i=0}^{25} n_i(n_i-1)}{n(n-1)} \longrightarrow_{n\to\infty} \approx \sum_{i=0}^{25} p_i^2$$

Dans cet exercice, l'indice de coïncidence a été calculé à partir du fichier *Vigenere.jar,* comme montré sur la capture d'écran suivante :

Idriss KOUROUMA
NI: 537 025 540


Etant donné que l'indice de coïncidence de la langue d'origine (anglais) est de 0,066 alors on trouve une valeur cohérente pour m=6. On suppose donc que la taille de la clé est 6.

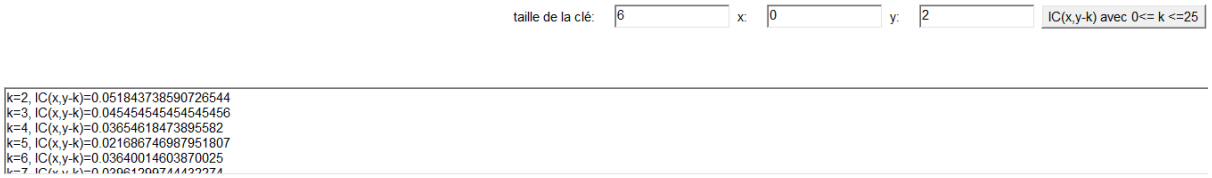
## Question 2 :

L'indice de coïncidence mutuel correspond à la probabilité de prendre un caractère au hasard dans $Y_0$ et un autre au hasard dans $Yi$ et que ces deux caractères soient identiques.

Il nous permet de trouver le décalage des colonnes par rapport à la colonne 0 en calculant : $Ic(Y_0, Y_i - k)$ avec *k* allant de 0 à 25 et *i* allant de 1 à m (taille de la clé).

Le $max(Ic(Y_0, Y_i - k))$, noté $maxic_i$, représente le décalage le plus probable entre la colonne 0 et la colonne *i* et nous permet de noter :
$k_i = k0 + maxic_i$

On calcule ces valeurs à l'aide du fichier *Vigenere.jar*, comme par exemple pour la valeur i=2 ci-dessous:



Au final, on trouve :

$k_1 = k_0 + 16$

$k_2 = k_0 + 13$

$k_3 = k_0 + 0$

$k_4 = k_0 + 6$

$k_5 = k_0 + 22$

Par la suite, on recherche la lettre la plus fréquente dans la colonne 0 (les lettres qui ont la position 6*i, i≥0). On trouve :

| Lettre | Occurrences |
|---|---|
| a | 0 |
| b | 2 |
| c | 8 |
| d | 0 |
| e | 11 |
| f | 2 |
| g | 12 |
| h | 10 |
| i | 19 |
| j | 2 |
| k | 4 |
| l | 4 |
| m | 15 |

| Lettre | Occurrences |
|---|---|
| n | 0 |
| o | 2 |
| p | 7 |
| q | 3 |
| r | 7 |
| s | 11 |
| t | 3 |
| u | 0 |
| v | 9 |
| w | 16 |
| x | 15 |
| y | 4 |
| z | 0 |

On a ‘i’ comme lettre avec le plus d’occurrences dans notre texte $Y_0$. Or la lettre la plus fréquente de la langue anglaise est le ‘e’.

D’où on déduit que $e_k(e) = i$, c’est-à-dire, que si on chiffre ‘e’ dans $Y_0$ alors on obtient ‘i’.

On peut raisonner comme cela car on a découpé le texte en plusieurs textes : $Y_i$, $i$ allant de 0 à 5, qui regroupe toutes les lettres en position $6i + i$. La taille de la clé étant de 6, cela nous donne des textes chiffrés par la simple technique de décalage.

On peut donc associé ‘e’ et ‘i’ de la manière suivant : $4 + k_0 = 8 \Rightarrow k_0 = 4$

Par conséquent on obtient :

📌 On trouve les clés à partir des décalages définis précédemment :

$k_0 = 4(e)$

$k_1 = 20(u)$

$k_2 = 17(r)$

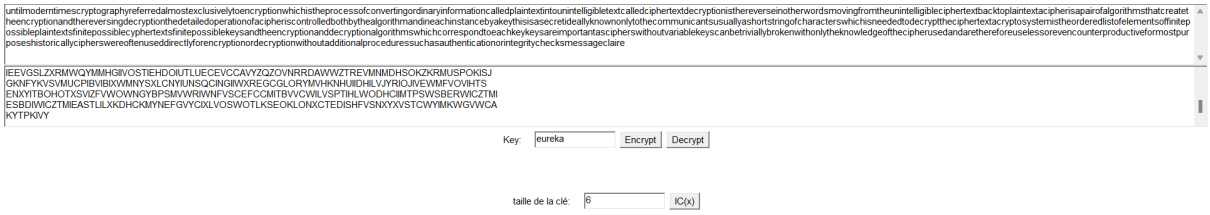
$k_3 = 4(e)$

$k_4 = 10(k)$

$k_5 = 0(a)$

Si ‘e’ à bien été codé avec ‘i’ alors la clé est ‘eureka’, vérifions cela.

On essaye maintenant de déchiffrer le message à l’aide de notre clé ‘eureka’, et on obtient :



📌 ***Le texte en clair en ajoutant les espaces :*** until modern times cryptography referred almost exclusively to encryption which is the process of converting ordinary information called plain text in to un intelligible text called cipher text decryption is the reverse in other words moving from the unintelligible cipher text back to plain text a cipher is a pair of algorithms that create the encryption and there versing decryption the detailed operation of a cipher is controlled both by the algorithm and in each instance by a key this is a secret ideally known only to the communicants usually a short string of characters which is needed to decrypt the cipher text a cryptosystem is the ordered list of elements of finite possible plain texts finite possible cypher texts finite possible keys and the encryption and decryption algorithms which correspond to each key keys are important as ciphers without variable keys can be trivially broken with only the knowledge of the cipher used and are there for euseless or even counter productive formost purposes historically ciphers were often used directly for encryption or decryption without additional procedures such as authentication or integrity checks message claire

Ce texte est un texte en anglais sur la cryptographie. La clé ‘eureka’ nous a permis de déchiffrer le texte en un texte qui a du sens c’est donc la bonne clé.