CHIFFREMENT DE VIGENÈRE

SUBSTITUTION POLY-ALPHABÉTIQUE

Chiffrement de Vigénère

Dans les chiffrements **poly-alphabétiques**, une lettre du message initial, peut être remplacée par des symboles différents selon sa position dans le texte.

Dans le **Chiffrement de Vigénère,** Il s'agit toujours de décaler les lettres du message, comme dans le chiffrement de César, mais le décalage dépend de la position de la lettre dans le message.

Ce décalage peut être donné par une clé pouvant s'exprimer par un mot.
Prenons, par exemple, le mot (clé) 'bec', dans lequel chaque lettre peut être associée à un rang : 'b' à 1, 'e' à 4, 'c' à 2.

Chiffrement de Vigénère

- La 1ère lettre sera décalée de 1 lettre
- *La 2ème de 4 lettres*
- La 3ème de 2 lettres
- La 4ème de 1 lettre
- *La 5ème de 4 lettres*
- La 6ème de 2 lettres
- La 7ème de 1 lettre
- …

Ce décalage peut être donné par une clé pouvant s'exprimer par un mot. Prenons, par exemple, le mot (clé) '**bec**', dans lequel chaque lettre peut être associée à un rang : 'b' à 1, 'e' à 4, 'c' à 2.

Travail sous Python

Programmer les fonctions suivantes

`chiffrevigenere(message,cle)` prenant en entrée le message et la clé et renvoyant le cryptogramme

`dechiffrevigenere(cryptogramme,cle)` prenant en entrée le cryptogramme et la clé, et renvoyant le message

CRYPTANALYSE VIGENÈRE

CAS SIMPLIFIÉ : LONGUEUR DE CLÉ CONNUE

Cryptanalyse Vigénère – longueur de clé connue

Décoder le cryptogramme suivant sachant qu'il a été obtenu par un chiffrement de Vigenère utilisant une clé de trois caractères :

'snzsmmifkcgusivsniwnasotshnohbzizgkcsfmgulifbsmizfiwyvhybjyvocmbnxfcaruvgx
mguntuqfyaeoqgyupfiwyvhcudizhuvhyasnkchawxmfujzyadoqgkcsfmgazohlsmxslach
vsmijuqshbzuqfnzsmwqwcdymgybduzqyyiivbykcgxfyvocbfcmbutsozgamgnmgfwfm
yiivguxslkccbihjsucxicfkcsfmilacwkijihcwbmachbdcmhlmgfmilusnqslnwamsnyictghw
bnxzoarytwyvopmqfijcmdicfkcccvsjigwwbnqbomfnmzovshnohbojwfnmffiryagoazyu
sgmfyoolleomgozqyyicmgnmhlibamfliwhmfgifcifctyytsnbfyaoovxycbyxcybs'

Indications ?

Cryptanalyse Vigénère – longueur de clé connue

Indication : si une clé de trois caractères a été utilisée, cela signifie que pour tous les caractères de rang multiple de 3, le même décalage a été utilisé, de même pour tous les caractères de rang congru à 1 modulo 3, et pour tous les caractères de rang congru à 2 modulo 3.

Cryptanalyse Vigénère – longueur de clé connue

Indication : si une clé de trois caractères a été utilisée, cela signifie que pour tous les caractères de rang multiple de 3, le même décalage a été utilisé, de même pour tous les caractères de rang congru à 1 modulo 3, et pour tous les caractères de rang congru à 2 modulo 3.

Créer une fonction **`scindermod(texte,longueur)`** prenant en entrée, **`texte`**, une chaine de caractère et un entier **`longueur`** (qui correspond à la longueur de la clé) et renvoyant une liste de **`longueur`** chaînes extraites de **`texte`** correspondant à la suite des caractères de texte d'indices congrus à 0,1…,l-1 modulo longueur

Par exemple :
texte='lavielemalheurlisolementlabandonlapauvretesontdeschampsdebataillequiontleursherosvictorhugo'

`scindermod(texte,3)` doit renvoyer la liste :

```
['lieluilelaoauestsasbalunesrvtho',
'aemhrsenannpvtodcmdaieituhoiou',
'vlaelomtbdlarenehpetlqolrescrg']
```

Créer une fonction **`scindermod(texte,longueur)`** prenant en entrée, **`texte`**, une chaine de caractère et un entier **`longueur`** (qui correspond à la longueur de la clé) et renvoyant une liste de longueur chaînes extraites de texte correspondant à la suite des caractères de texte d'indices congrus à 0,1…,l-1 modulo longueur

Cryptanalyse Vigénère – longueur de clé connue

Après avoir utilisé la fonction **`scindermod`** sur le cryptogramme, procédez à une analyse fréquentielle des chaînes obtenues et en déduire le décalage effectué sur chacune d'entre elles (avec un peu de chance cela peut aller assez vite). Décoder le message.

Finalement, quelle est la clé qui avait été utilisée dans le codage de Vigenère ?