TP I43

Chiffrement Affine

Exercice 1

Ecrire la fonction **enumere_keys(n)** qui renvoie la liste de toutes les clés possibles pour le chiffrement affine lorsque l'on travaille sur un alphabet à *n* symboles. On rappelle que chaque clé est de la forme *[a, b, c]* avec $1 < a < n$ et premier avec n, $b < n$ et c est l'inverse de a modulo n . Votre fonction renvoie donc une liste de listes.

Exercice 2

Ecrire une fonction ***brute_force(fic,n,eps)*** qui lit le texte se trouvant dans le fichier **fic** contenant un cryptogramme obtenu à partir d'un texte clair conçu sur un alphabet de *n* symboles. Votre fonction doit essayer toutes les clés de déchiffrement possible jusqu'à trouver la bonne clé. Pour cela, à chaque fois que vous avez appliqué une clé de déchiffrement, vous devez vérifier si le texte obtenu respecte l'analyse de fréquence d'un texte écrit en français. Le paramètre **eps** permet de régler l'écart que vous acceptez par rapport à la table ci-dessous. Vous testerez votre programme avec les fichiers **crypto1.txt, crypto2.txt, crypto3.txt, crypto4.txt et crypto5.txt** fournis. Pour la lecture dans un fichier voici un exemple de code permettant d'afficher le contenu d'un fichier, inspirez vous-en pour lire et traitre le contenu des fichiers crypto*.txt.

```
nomfic = "mettre le nom du fichier ici"
# ouverture du fichier en mode lecture
fic = open(nomfic,'r')
#on parcourt les lignes du fichier
for ligne in fic:
    # pour chaque ligne on parcourt les caracteres de la ligne
    for car in ligne:
        print(car)
# ne pas oublier de fermer les fichiers
fic.close()
```

Fréquences d'apparition des lettres

Lettre	Fréquence	Lettre	Fréquence
A	8.15 %	N	7.12 %
B	0.97%	O	5.28 %
C	3.15 %	P	2.80 %
D	3.73 %	Q	1.21 %
E	17.39 %	R	6.64 %
F	1.12 %	S	8.14 %
G	0.97 %	T	7.22 %
H	0.85 %	U	6.38 %
I	7.31 %	V	1.64 %
J	0.45 %	W	0.03 %
K	0.02 %	X	0.41 %
L	5.69 %	Y	0.28 %
M	2.87 %	Z	0.15 %

Statistiques obtenues à partir d'un corpus de 10'525'096 lettres.

Exercice 3 En utilisant les fonctions que vous avez écrites dans le précédent TP, écrire une fonction **cryptanalyse(fic)** qui lit le texte chiffré dans le fichier fic et en déduit la clé (λ,μ) qui a été utilisée pour effectuer le chiffrement. Votre fonction affichera la valeur de la clé ainsi que le texte déchiffré.
Testez votre fonction sur le fichier **crypto6.txt** qui correspond à un fichier dont le texte a été construit à partir d'un alphabet de 29 lettres {a ;b ;… ;z ;, ;' ;.} (les minuscules, la virgule, l'apostrophe et le caractère point.

Exercice 4 Ecrire la fonction **chiffre(fic, cle)** qui lit le fichier fic et affiche le cryptogramme correspondant en appliquant le chiffrement affine avec la clé **cle**, pour un alphabet de 29 lettres identique à celui de l'exercice précédent. Testez votre programme avec le texte clair et la clé que vous avez obtenus précédemment , vous devriez retomber sur le contenu de **crypto6.txt**.