

WLODARCZYK Mathurine

PINARD Mathilde

1^{ère} 3

Code César : Chiffrage et Décryptage

Nous souhaitons créer plusieurs fonctions nous permettant de chiffrer un texte par la méthode du code César et également de pouvoir décrypter un texte déjà chiffré. Le code César consiste au décalage des lettres de l'alphabet. Ce projet pourra être étendu à un code plus complexe : on pourra par exemple développer la fonction chiffage pour qu'elle permette de chiffrer grâce au code César ou au code par substitution. Le code par substitution consiste à remplacer une lettre par une autre lettre choisie aléatoirement, ce qui rend le texte plus compliqué à décrypter.

Nous allons créer trois fonctions : une première fonction permettant de décaler les lettres de l'alphabet en fonction d'un nombre entré par l'utilisateur ; une deuxième fonction permettant de remplacer dans un texte chaque lettre par le nouveau caractère y correspondant ; et une troisième fonction permettant de décrypter le texte grâce aux probabilités de récurrence de certaines lettres dans la langue française.

Commençons par expliquer le fonctionnement de notre première fonction « décalage ». Nous utiliserons une liste constituée de toutes les lettres de l'alphabet. La fonction décalage prend en compte le nombre X choisi par l'utilisateur. X correspondra au décalage souhaité. Si ce nombre est négatif, on calculera simplement $26 + X$, qui sera la nouvelle valeur de X. Si X est strictement supérieur à 26, on divisera X par 26 et le reste de cette division euclidienne sera la nouvelle valeur de X. On décalera alors tous les éléments de la liste alphabet grâce à ces instructions (pour une liste a par exemple):

```
a = [1, 2, 3, 4]
X = 8
for i in range (X) :
    a.insert(0,a.pop())
```

Nous obtenons ainsi la liste décalée que l'on appellera alphabet_chiffré.

Nous pouvons maintenant décrire notre deuxième fonction « chiffage ». Pour commencer, l'utilisateur doit entrer son texte. On utilisera alors deux listes : une liste alphabet_normal et la liste alphabet_chiffré de la fonction décalage. On utilise ensuite une boucle nous permettant de changer dans le texte toutes les récurrences de la lettre de position a dans la liste alphabet_normal par la lettre à la même position dans la liste alphabet_chiffré.

Enfin, expliquons notre troisième fonction « décryptage ». L'utilisateur doit d'abord rentrer son texte chiffré. On utilise alors la liste alphabet_normal et une boucle pour calculer la

réurrence dans le texte des lettres de la liste `alphabet_normal`. On met cette réurrence sous forme de pourcentage et on rajoute cette valeur à une liste `recurrence_lettres`. On crée alors les variables `recurrence_e`, `recurrence_a`, `recurrence_i`, `recurrence_l` et `recurrence_o` auxquelles on attribue des intervalles de probabilités correspondant pour la langue française. Nous ferons en sorte que ces intervalles ne se chevauchent pas. A l'aide d'une boucle, on teste pour chaque élément de la liste `recurrence_lettres` leur appartenance à ces intervalles de probabilités. Si une valeur est comprise dans un intervalle, on remplace dans la liste `recurrence_lettre` la probabilité par la lettre qui y serait associé. A l'aide d'une boucle, on remplace ensuite toutes les éléments de la liste par la lettre correspond à l'intervalle de probabilités auxquels ils appartiennent. On calcule ensuite la différence entre la position de la lettre e dans la liste `alphabet_normal` et sa position dans la liste `recurrence_lettre`. On donne cette valeur à la variable « clé ». On utilise alors notre première fonction décalage avec $X = \text{clé}$. On utilise alors une boucle permettant de changer dans le texte toutes les réurrences de la lettre de position a dans la liste `alphabet_chiffré` obtenue avec la fonction décalage, par la lettre de la même position dans la liste `alphabet_normal`. On obtient alors le texte décrypté.