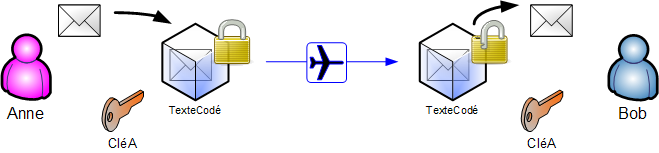
Université Ibn Tofail

ENSA de Kénitra

A.U : 2020/2021

Cycle ingénieur S8

**Rapport de TP1 : La cryptographie**

****

**Réalise par : Ahmed Mahmoud Ebou El hassani**

**Encadre par : Pr. K. Chougdali**

Objectif :

Le but de ce TP est de :

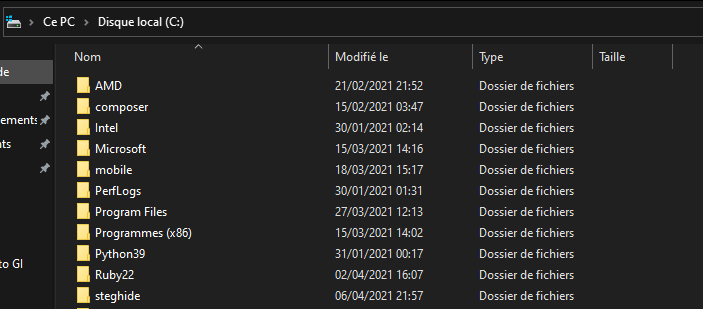
• Tester la stéganographie comme moyen de sécurité

• Comprendre le mécanisme de cryptanalyse par analyse fréquentielle

**Partie 1 : La stéganographie**

1. **Exercice 1 : Cacher un fichier dans une image**

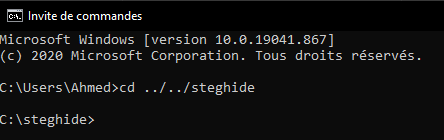
On décompresse le fichier steghide-0.5.1-win32 .zip dans le dossier "c:\Steghide".



Dans cet exercice nous allons cacher un fichier nommé "ensak.txt", contenant la phrase « Salut tout le monde », dans l'image "test.jpg" que nous avons placé préalablement dans le même répertoire de travail.

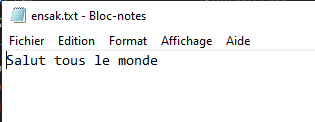
On ouvre cmd et on se positionne dans c:/steghide

Commande : **cd c:/steghide**

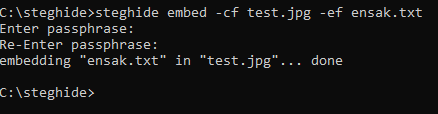


Pour cacher le fichier «ensak.txt» dans «test.jpg» on exécute la commande : **steghide embed -cf test.jpg -ef ensak.txt**

Voici le contenue du fichier « ensak.txt »



Voici l’exécution de la commande :

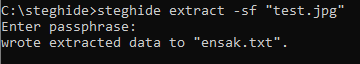


Maintenant je vais envoyer l’image « test.jpg » par email et je vais le récupère

Ensuite et après le téléchargement de l’image je le renomme pour la lecture « test.jpg » et on le met dans le dossier c:/steghide

Avant tous je supprime le fichier « ensak.txt »

Maintenant on veut extraire le texte cache dans l’image voici la commande : **steghide extract -sf "test.jpg"**



Cette commande va nous générer de nouveau un fichier « ensak.txt » dont le contenue est : « Salut tout le monde »

1. **Exercice 2 : Cacher un fichier texte dans un fichier audio**

On décompresse le fichier MP3stego.zip dans le dossier "c:\MP3stego".

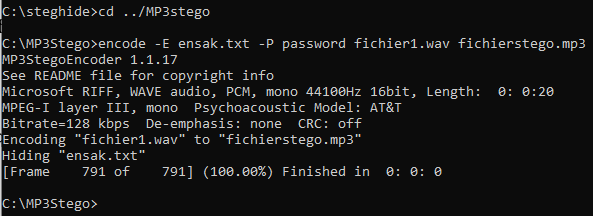
Dans ce répertoire on copie le fichier audio fichier1.wav qui va servir à cacher le texte.

On ouvre le cmd et on se positionne dans c:/MP3stego

Pour cacher le fichier ensak.txt contenue dans le dossier c:/MP3stego

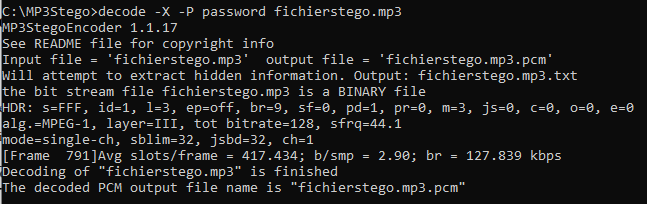
On exécute la commande :

**encode -E ensak.txt -P password fichier1.wav fichierstego.mp3**



Pour extraire le fichier texte de fichier audio voici la commande :

**decode -X -P password fichierstego.mp3**



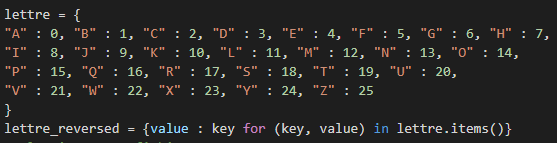
Cette commande nous génère un fichier« fichierstego.mp3.txt » contenant le texte cache.

**Partie 2 : Cryptanalyse des chiffrements par substitution mono alphabétique**

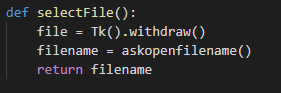
1. **Présentation des méthodes et structures :**



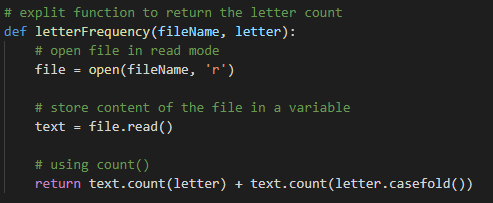
On a utilisé la bibliothèque tkinter pour mieux sélectionner le fichier à crypter ou à décrypter



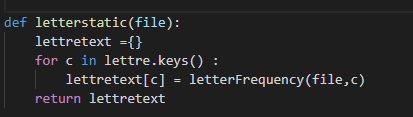
Ces deux dictionnaires sont indispensables dans notre programme l’est que l’inverse de l’autre



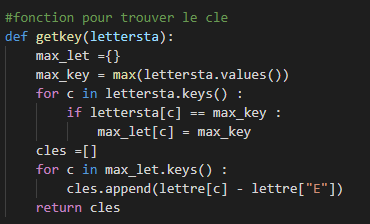
Cette fonction consiste à sélectionner un fichier et retourne son chemin absolu



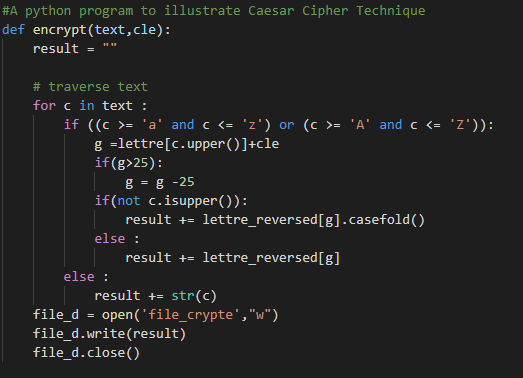
Cette fonction consiste à retourner l’occurrence d’une lettre dans un fichier.



Cette fonction retourne l’occurrence de chaque lettre dans un dictionnaire



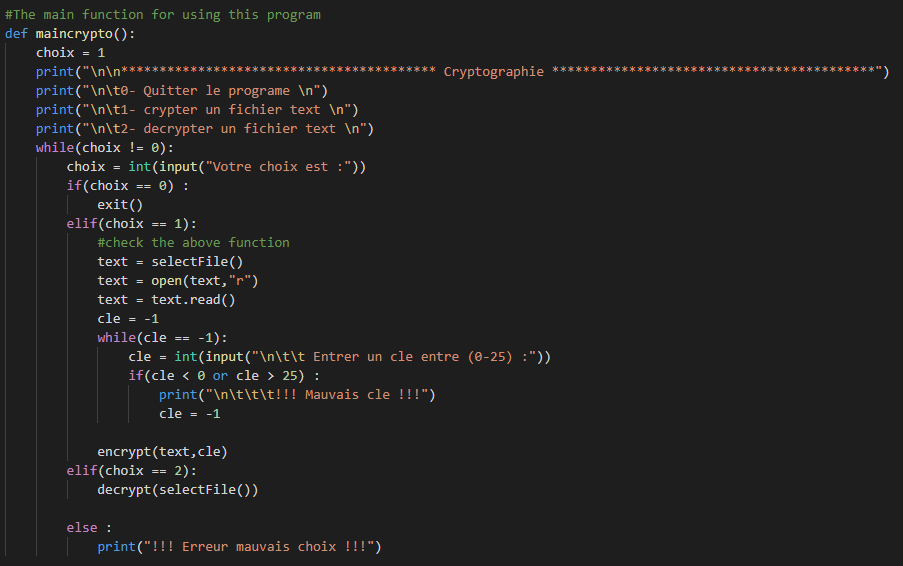
Cette fonction retourne les clés candidats selon les lettres les plus occurrents et dont le nombre d’occurrence sont égaux



Cette fonction consiste à crypter le texte d’un fichier dans un autre fichier selon le clé choisis



Cette fonction pour décrypter un fichier dans des fichiers selon le nombre de clés candidats

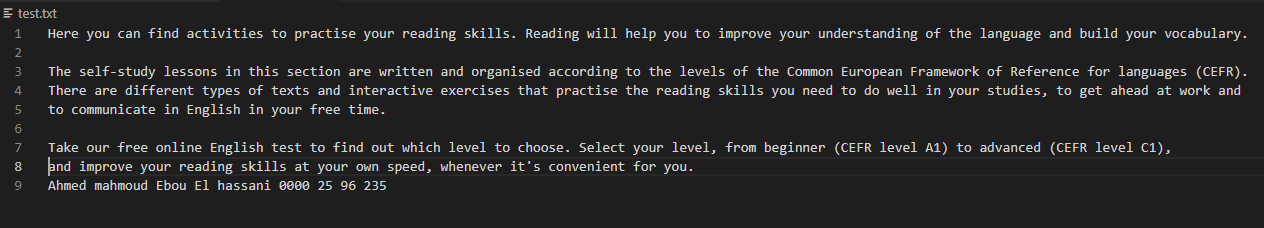


Cette fonction est la fonction principale de notre programme elle affiche un menue de choix

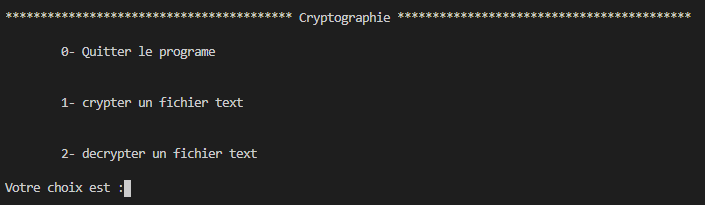


On appelle juste la fonction principale.

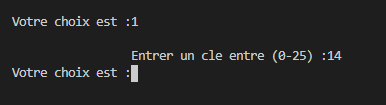
1. **Exécution du programme :**



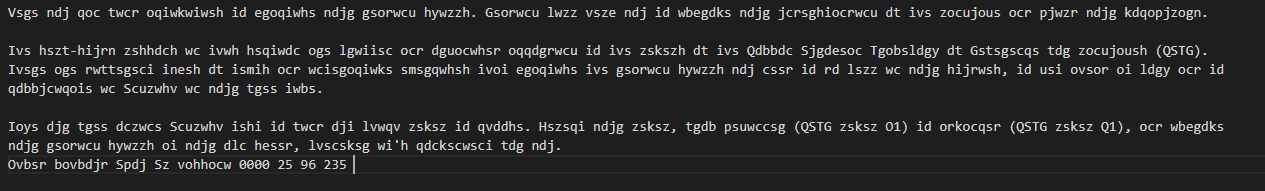
Ce fichier test.txt contenant un texte à crypter



Voici dessus le menue de choix



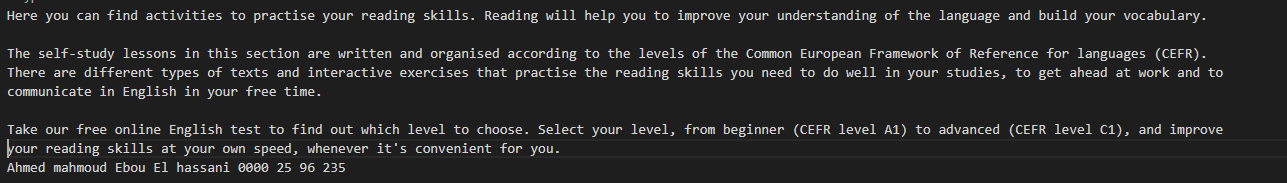
On a choisi le fichier et la clé de césar



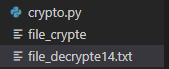
Voici le texte crypte avec la clé 14



On a choisi le fichier dessus crypte pour voir est ce que le résultat est le même que le fichier original



Elle a retourne le même texte que l’originale



Dans le cryptage il a créé un fichier nomme file\_crypte

Dans le décryptage il a créé un fichier nomme file\_decrypte14.txt selon les clés candidats si on par exemples deux clés candidats il va créer deux fichiers de décryptage.



On a choisi 0 pour sortir.