TP Sécurité - Semestre 6 Licence Informatique

Université de Franche-Comté – UFR-ST

L'objectif du TP est de réaliser un logiciel pour aider à déchiffrer un texte qui a été chiffré par substitution : il existe une permutation (la clé que l'on ne connaît pas) qui à chaque lettre associe bijectivement une lettre.

Pour simplifier, on étudiera des textes :

— Écrits en majuscules,
— Sans accents,
— en gardant espace et ponctuation.

L'objectif n'est pas nécessairement d'avoir un outil qui déchiffre automatiquement tout seul, mais permettant suffisament de manipulation pour y arriver.

Le TP (sur deux séances) peut être réaliser dans le langage de votre choix.

Les méthodes pouvant être utilisées :

1. Utilisation de la fréquence des lettres, [1]
2. Utilisation des lettres doublées (on n'a par exemple jamais deux q à la suite en français),
3. Les seuls mots de une lettres en Français sont $\grave{a}$ et y.
4. Liste des mots fréquents [2],
5. Lettres précédant une apostrophe,
6. ...

Vous pourrez aussi utilise une approche par mot connus pour les textes sur Napoléon.

Des fichiers chiffrés sont disponibles pour tester vos programmes.

1. `https://www.apprendre-en-ligne.net/crypto/stat/francais.html`
2. `https://eduscol.education.fr/document/15655/download`