TP 3 de Sécurité – Chiffrement par substitution

2013

Ce TP doit être fini avant la prochaine séance de TP, éventuellement sur votre temps de travail personnel.

Vous devez rendre ce TP avant 23h30 la veille de votre prochain TP. Pour cela, vous devez déposer une archive .zip contenant le fichier source et le fichier texte demandés dans la dernière section sur Moodle. Votre code source doit être commenté et les commentaires doivent être en français.

---

1 Chiffrement par substitution

1.1 Chiffrement et déchiffrement

Pour créer la table de substitution, on utilisera la méthode de construction de la clef à partir d'un mot-clef vue en cours.

Écrire une fonction `chiffre` qui prend en paramètre un nom de fichier, le mot-clef et un nom de fichier de sortie et qui réalise un chiffrement par substitution.

Écrire une fonction `dechiffre` qui prend également en paramètre un nom de fichier, le mot-clef et un nom de fichier de sortie et qui réalise le déchiffrement par substitution.

1.2 Décryptage

Écrire un programme `decrypte` qui décrypte un texte chiffré à l'aide d'un chiffrement par substitution. Pour cela, on pourra s'appuyer sur les heuristiques suivantes :

- Analyse fréquentielle des lettres
- Les lettres les plus souvent doubles en français sont `E`, `M`, `L`, `N`, `F`, `T` et `C`
- Les seuls mots de une lettre (sauf avant une apostrophe) sont le `A` et le `Y`
- Un mot d'une lettre devant une apostrophe est `T`, `S`, `D`, `J`, `L`, `M`, `C` ou `N`
- Analyse fréquentielle des séquences de taille 2
- Utilisation d'un mot probable apparaissant dans le texte
- Assistance humaine

Il est très difficile (long) de faire un programme qui décrypte très bien tout seul. Il est très facile de faire un programme qui décrypte à peu près. L'objectif de cette séance de TP est de faire un programme qui marche le mieux possible. Pour vous aider, vous avez à votre disposition un ensemble de paires de texte clair/chiffré.

2 Programme et document à rendre

Vous devez écrire un programme dont l'exécutable `substitution` qui aide l'utilisateur décrypter un texte. Vous devez également dans un document texte expliquer comment votre programme vous permet de décrypter le texte contenu dans l'archive .zip `adecrypter.txt.zip`

L'archive .zip doit être déposé sur Moodle avant 23h30 la veille de votre prochain TP.