TP Sécurité - Cryptanalyse statisitque

Le chiffrement par substitution est un chiffrement à clé symétrique qui a été longuement utilisé. Il s'agit simplement d'établir une correpondance d'une lettre avec une autre. Par exemple, on code le A en D, le B en Z, etc. Il y a donc 26! clés possible, ce qui rend un attaque par force brute impossible.

L'objectif du TP est de programmer un outils de cryptanalyse (retruver un texte initial) en s'appuyant essentiellement sur une approche statitique (fréquence des lettres). Différentes approches peuvent être utilisées en complément, comme l'utilisation d'un dictionnaire. On peut en trouver sur le site
http://www.freelang.com/dictionnaire/dic-francais.php ou si on travaille en majuscule au près de l'enseignant.