Initiation à la cryptographie

TP 1 : Cryptographie classique - César

Chiffrement de César

Le chiffre de César ou le code de César est un chiffrement par décalage. C' est une méthode de chiffrement très simple utilisée par Jules César dans ses correspondances secrètes. Le texte chiffré s'obtient en remplaçant chaque lettre du texte clair original par une lettre à distance fixe, toujours du même côté, dans l'ordre de l'alphabet. Pour les dernières lettres, on reprend au début. Par exemple avec un décalage de 3 vers la droite, A est remplacé par D, B devient E, et ainsi jusqu'à W qui devient Z, puis X devient A etc. La longueur du décalage, 3 dans l'exemple évoqué, constitue la clé du chiffrement qu'il suffit de transmettre au destinataire pour que celui-ci puisse déchiffrer le message.

Chiffrement

Ecrire l'algorithme de César. Le choix du langage est laissé libre. La clé et le texte à chiffrer seront passés en paramètres. Le résultat du chiffrement sera écrit dans un fichier "texteChiffre.txt".

Déchiffrement

Ecrire l'algorithme permettant le déchiffrement. La clé et le texte à déchiffrer seront passés en paramètres. Le résultat sera écrit dans un fichier texteClair.txt. Vous pouvez utiliser les options -c/-d en paramètre de votre programme pour les chiffrements et déchiffrements.

Cryptanalyse de cet algorithme

Le but de cette partie est de décrypter un message chiffré.

Attaque par force brute

Une première méthode est appelée une attaque par force brute. Comme il n'y a qu'un nombre limité de décalages (vingt-six dont un inutile), il suffit de tester tous les chiffrements possibles jusqu'à trouver le bon. Une méthode simple pour mener l'attaque est de prendre un fragment du texte chiffré et d'écrire dans un tableau tous les décalages possibles. Par conséquent, il est demandé d'écrire un programme pour décrypter le message suivant :

$<< RdcvgpijapixdcndjhjrrthhujaanqgtpzRtphtgrxewtg >>$

Attaque par Analyse de fréquences

Une deuxième méthode pour déterminer la clé k du chiffre de César est la suivante. On calcule, pour chaque valeur de k, la fréquence d'apparition de chacune des lettres dans le message cheffré. À l'aide d'un texte de référence, on détermine la fréquence d'apparition de chacune des lettres en français. On choisit la clé qui permet d'obtenir une liste de fréquences aussi proche que possible de la liste de référence. Pour cela, si $f = (f_0, ..., f_{25})$et $g = (g_0, ..., g_{25})$ sont deux listes de fréquences, on détermine leur distance via la fonction

$$d(f, g) = \sum_{i=0}^{25} |f_i - g_i| \tag{1}$$

Par conséquent, il est demandé d'écrire un programme pour décrypter le message ce trouvantt dans le fichier "TextChiffe.txt".

N'hésitez pas à me demander si vous avez des questions.

Bonne chance !