OS01-- TP 1+2

Exercice 1 : le chiffrement de Vigenère

Utilisez votre langage de programmation préféré pour implémenter la méthode de chiffrement de Vigenère. Votre programme prendra en entrée deux chaines de caractères de longueur variable : la première entrée sera le texte clair, la deuxième, la clé. La sortie sera une chaine de caractère : le chiffré.

Votre programme devrait fonctionner pour toute longueur de clé et de texte clair.

On demandera (sur la console) un texte clair et une clé. Avec ces données on affichera sur la console le texte chiffré obtenu.

Exercice 2 : le déchiffrement avec Vigenère

Dans le même langage de programmation que l'exercice 1, implémentez le déchiffrement d'un chiffré obtenu par la méthode de Vigenère. Votre programme prendra en entrée deux chaines de caractères : un chiffré et une clé. Votre programme rendra en sortie une chaine de caractère : le texte clair.

Exercice 3 : Kasiski et la taille de la clé en Vigenère

Pour le chiffrement de Vigenère, implémentez la méthode de Kasiski pour estimer la taille de la clé (inconnue) qui a été utilisée pour chiffrer un chiffré donné de Vigenère.

Le texte chiffré est donné en entrée.

Vous allez premièrement trouver des sous-chaines de caractères qui se répètent dans le texte chiffré et mesurer la distance entre les répétitions. Ensuite, vous devez les ordonner en fonction de leur taille, du fragment le plus long qui se répète au plus court. Affichez les répétitions en ordre, en donnant : la taille du fragment qui se répète, le nombre de fois qu'il se répète et la distance entre les répétitions.

En utilisant le PGCD entre des valeurs successives, faites votre algorithme estimer la taille de la clé.

Pouvez vous trouver la taille de la clé du fragment vu en TD ?