MISSION 4 "programme crypto"

DEFINITION DU BESOIN

La M2L désire sécuriser ses échanges informatisés. Pour cela elle vous charge d'une mission pour tester deux algorithmes de cryptage.

MISSION

Vous devez créer un programme qui permette de crypter un message textuel. L'objectif est de donner à l'utilisateur la possibilité de saisir un message puis de lui en afficher la version cryptée. Pour contrôler que tout a bien marché, le message crypté sera ensuite décrypté et réaffiché.

RECEPTION

Le programme est installé en local sur une machine.

Cahier des charges de la mission :

Un des plus anciens systèmes de cryptographie (aisément déchiffrable) consiste à décaler les lettres d'un message pour le rendre illisible. Ainsi, les A deviennent des B, les B des C, etc.

Une amélioration (relative) du principe précédent consiste à opérer avec un décalage non de 1, mais d'un nombre quelconque de lettres. Ainsi, par exemple, si l'on choisit un décalage de 12, les A deviennent des M, les B des N, etc.

1- Ecrivez un algorithme puis un programme en langage C qui demande une phrase sans ponctuation de 26 lettres au plus, à l'utilisateur (elle sera stockée dans un tableau de caractères, un espace sera exprimé par le caractère %), mais qui demande en plus quel est le décalage à utiliser et qui la code selon ce principe. Le codage doit s'effectuer au niveau de la variable stockant la phrase, et pas seulement à l'écran.

2- Décrypter ensuite la phrase codée pour l'afficher en clair et vérifier votre algorithme de la question 1.

Une technique ultérieure de cryptographie consiste à opérer non avec un décalage systématique, mais par une substitution aléatoire. Pour cela, on utilise un alphabet-clé, dans lequel les lettres se succèdent de manière désordonnée, par exemple :

HYLUJPVREAKBNDOFSQZCWMGITX

C'est cette clé qui va servir ensuite à coder le message. Selon notre exemple, les A deviendront des H, les B des Y, les C des L, etc.

3- Ecrire un algorithme et un programme en langage C qui effectue ce cryptage (soit l'alphabet-clé est saisi par l'utilisateur, et on suppose qu'il effectue une saisie correcte, soit il est défini en constante).

4- Décrypter ensuite la phrase codée pour l'afficher en clair et vérifier votre algorithme de la question 3.