TD – Chaînes de caractères

ING1 – Programmation C

Génie Informatique

Préambule

Dans ce TP, nous allons crypter des messages avec trois chiffrement symétriques différents:

— le code de César ;

— le code de Vigenère ;

— le codage de Scytale.

Le type de cryptage sera donné en argument au programme. Si aucun argument n'est donné (ou trop d'arguments), un message d'aide sera affiché pour expliquer à l'utilisateur comment utiliser le programme.

Les arguments d'un programme sont récupérés dans les paramètres de la fonction main. Le paramètre `argc` correspond au nombre d'arguments donnés, et le paramètre `argv` correspond à la valeur de chacun d'entre eux. Par défaut, `argv[0]` correspond au nom du programme. Pour appeler un programme avec des arguments, il suffit de les ajouter à la ligne de commande. Par exemple, pour lancer le programme TP avec un argument "vigenere" :

```
./TP vigenere
```

1 Code de César

Le code de César, ou encore le chiffrement par décalage, est une méthode de cryptage qui consiste à décaler les lettres vers la droite ou vers la gauche d'un même pas. César utilisait ce codage en décalant de 3 lettres vers la gauche. Donc A devient D, B devient E, C devient F, ... , X devient A, Y devient B et Z devient C. Les autres caractères (espace, ponctualtion, ...) restent inchangés.

Exemple : "Veni, vidi, vici" avec un décalage de 3 devient "Yhql, ylgl, ylfl".

(1) En se basant sur le principe du chiffrement par décalage, écrire la fonction qui permet de crypter un message (sous forme de phrase) en précisant le décalage. Le message retourné sera crypté. □

2 Code de Vigenère

Le code de Vigenère est un chiffrement par substitution. Contrairement au code de César où toutes les lettres sont décalées du même pas, le décalage du code de Vigenère se fait à partir d'un mot clé. Pour pouvoir chiffrer le message, à chaque caractère nous utilisons une lettre de la clé pour effectuer la substitution. La lettre de la clé est à prendre dans l'ordre dans laquelle elle se présente et on répète la clé en boucle autant que nécessaire. Si le mot clé est "FINTZ" et le message est "HELLO WORLD", la lettre H sera décalée de 5, la lettre E sera décalée de 8, etc. Ce qui donnera le message codé "MMYEN BWEEC".

(2) En se basant sur le principe du code de Vigenère, écrire la fonction qui permet de crypter un message (sous forme de phrase) en précisant le mot clé utilisé. Le message retourné sera crypté. □

3 Codage de scytale

Dans ce code de permutation, on garde le même alphabet mais on change la place des lettres à l'intérieur d'un bloc. La méthode de la grille est basée sur le principe de la Scytale, utilisée par les spartiates vers -400.

Pour plus de simplicité, on travaillera sur un système de codage symétrique et par blocs. Le message initial est placé dans une grille carrée. Par exemple, le message "RENDEZ VOUS DEMAIN SOIR A LA TIREUSE" s'écrirait dans la grille :

R	E	N	D	E	Z
	V	O	U	S	
D	E	M	A	I	N
	S	O	I	R	
A		L	A		T
I	R	E	U	S	E

Crypter le message correspond à lire la grille colonne par colonne. Le message chiffré est donc : "R D AIEVES RNOMOLEDUAIAUESIR SZ N TE".

Dans le cas où la taille du message n'est pas le carré d'un nombre, on ajoutera à la fin du message des espaces afin de compléter entièrement la grille.

(3) En se basant sur le principe du codage de Scytale, écrire la fonction qui permet de crypter un message (sous forme de phrase). La dimension de la grille sera calculée en fonction de la taille du message. Le message retourné sera crypté. □