ESIEE Paris

IN3R12 - Programmation C

Projet Vigenere
Documentation Utilisateur

Auteurs :
M. Kévin Ta
M. Antoine Mathis

Professeur :
M. Damien Masson

20 juin 2016

ESIEE
PARIS

Table des matières

1 Présentation

1.0.1 L'algorithme de calcul

Le Chiffre de Vigenère est un système de chiffrement par substitution poly-alphabétique, élaboré par Blaise de Vigenère. Utilisant généralement une clé et un tableau à double entrée, il permet de remplacer une lettre par une autre qui n'est pas toujours la même.

Le chiffrement utilise une clé et un alphabet. A chaque lettre, on fait correspondre la valeur de son rang dans l'alphabet en partant de 0=A, 1=B, ..., 25=Z.

Le chiffrement consiste à additionner la clé au texte clair. Le calcul s'effectue lettre après lettre en additionnant leur valeur dans l'alphabet. Le résultat est donné modulo 26, si le résultat est supérieur ou égal à 26, on soustrait 26 au résultat (où 26 est la longueur de l'alphabet). La clé est répétée aussi souvent que nécessaire pour correspondre à la longueur du texte.

On prend les premières lettres du message et de la clé et on additionne leur valeur. On note la nouvelle valeur et on continue avec la lettre suivante du message et la lettre suivante de la clé. Si on arrive à la fin de la clé, on recommence au début de celle-ci. Pour chaque nombre obtenu (qui doit avoir une valeur entre 0 et 25), on fait correspondre la lettre ayant le même rang dans l'alphabet.

Pour déchiffrer, prendre la première lettre du message et la première lettre de la clé, et soustraire leurs valeurs. Si le résultat est négatif, ajouter 26 au résultat (où 26 est le nombre de lettres dans l'alphabet), le résultat correspond au rang dans l'alphabet de la lettre claire.

On prend les premières lettres du message et de la clé et on les soustrait. On continue avec la lettre suivante du message et la lettre suivante de la clé, arrivé à la fin de la clé, on recommence au début de celle ci.

1.0.2 Exemple de chiffrement puis déchiffrement

D. C. O. D. E (message clair)
3. 2.14. 3. 4 (valeurs des lettres du message)
C. L. E. C. L (clé de chiffrement répétée)
2.11. 4. 2.11 (valeurs des lettres de la clé)
5.13.18. 5.15 (résultat de l'addition modulo 26)
F. N. S. F. P (message chiffré)

F. N. S. F. P (message chiffré)
5.13.18. 5.15 (valeurs des lettres du message)
C. L. E. C. L (clé de chiffrement répétée)
2.11. 4. 2.11 (valeurs des lettres de la clé)
3. 2.14. 3. 4 (résultat de la soustraction modulo 26)
D. C. O. D. E (message clair)

2 Structure du projet

Le projet se présente sous la forme de 3 dossiers :
- bin : Les fichiers exécutable vont se placer dans ce répertoire
- src : Code source du programme
- doc : Documentation utilisateur et développeur

A cela s'ajoute un fichier Makefile afin de rendre la compilation plus aisée.
Les options disponibles sont les suivantes :
- make (all) : Compile les sources seulement si un changement a été détecté
- make force : Force la compilation des sources
- make clean : Supprime le contenu du dossier bin
- make zip : Crée une archive du projet pour l'exportation

3 Compilation et lancement du programme

$ tar zxvf tak_mathisa.tar.gz
$ cd tak_mathisa
$ make
$ ./bin/code ou ./bin/decode
Le programme code encode un texte en utilisant le code Vigenère tandis que le programme decode décode un texte en utilisant le code Vigenère.

4 Options du programme

code [options] [fichier...]Options : [sh] [help] [skip] [-a alphabet] [- k clé] [– alphabet=alphabet] [– key=clé]

decode [options] [fichier...] Options : [sh] [help] [skip] [-a alphabet] [-k clé] [– alphabet=alphabet] [– key=clé]

L'option -s (skip), lorsqu'elle est présente, indique que les lettres du texte à encoder non présentes dans l'alphabet sont supprimées. Lorsqu'elle est absente, ces lettres restent en clair dans le message codé.

Les options a (alphabet) et k (key) permettent de spécifier les fichiers contenant respectivement l'alphabet et la clé. Si elles sont absentes, l'alphabet est l'alphabet latin non accentué composé uniquement de lettres minuscules (abcdefghijklmnopqrstuvwxyz) et la clé est notaverysmartkey.

L'option h (help) affiche ce manuel.

Lorsqu'aucun fichier n'est fourni, l'encodage se fait depuis l'entrée standard vers la sortie standard, ligne par ligne. Lorsqu'un seul fichier est fourni, l'encodage se fait depuis le fichier vers la sortie standard. Lorsque deux fichiers sont fournis, l'encodage se fait depuis le premier vers le deuxième.