Architecture des ordinateurs

Octobre 2015

Polytech' Montpellier

Projet : chiffre de Vigenère

1 Présentation

Le chiffre de Vigenère est un système de chiffrement polyalphabétique, c'est un chiffrement par substitution, mais une même lettre du message clair peut, suivant sa position dans celui-ci, être remplacée par des lettres différentes, contrairement à un système de chiffrement monoalphabétique comme le chiffre de César (qu'il utilise cependant comme composant). Cette méthode résiste ainsi à l'analyse de fréquences, ce qui est un avantage décisif sur les chiffrements monoalphabétiques. Cependant le chiffre de Vigenère a été cassé par le major prussien Friedrich Kasiski qui a publié sa méthode en 1863. Ainsi, depuis cette époque, il n'est plus considéré comme une méthode robuste de chiffrement.

Il est nommé ainsi au XIXème siècle en référence au diplomate du XVIème siècle Blaise de Vigenère, qui le décrit (intégré à un chiffrement plus complexe) dans son traité des chiffres paru en 1586. On trouve en fait déjà une méthode de chiffrement analogue dans un court traité de Giovan Battista Bellaso paru en 1533.

Ce chiffrement introduit la notion de clé. Une clé se présente généralement sous la forme d'un mot ou d'une phrase. Pour pouvoir chiffrer notre texte, à chaque caractère nous utilisons une lettre de la clé pour effectuer la substitution. Évidemment, plus la clé sera longue et variée et mieux le texte sera chiffré. L'outil indispensable du chiffrement de Vigenère est la « table de Vigenère » (voir table 1). Pour chaque lettre en clair, on sélectionne la colonne correspondante et pour une lettre de la clé on sélectionne la ligne adéquate, puis au croisement de la ligne et de la colonne on trouve la lettre chiffrée. 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. Par exemple :

Texte en clair : « BEWARE OF BUGS IN THE ABOVE CODE ».
Clé : « MARVIN ».

```
BEWARE OF BUGS IN THE ABOVE CODE
MARVIN MA RVIN MA RVI NMARV INMA
|
Colonne B et ligne M : on obtient N.
```

Le texte chiffré est alors : « NENVZR AF SPOF UN KCM NNOMZ KBPE ».

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
C	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
F	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
G	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
H	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
I	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
J	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
K	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
L	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
M	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
N	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
O	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
P	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
Q	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
R	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
S	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
T	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
U	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
V	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
W	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
X	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
Y	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
Z	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y

TABLE 1 – Table de Vigenère

Si on veut déchiffrer ce texte, on regarde pour chaque lettre de la clé répétée la ligne correspondante et on y cherche la lettre chiffrée. La première lettre de la colonne que l'on trouve ainsi est la lettre déchiffrée. Ainsi :

```
NENVZR AF SPOF UN KCM NNOMZ KBPE
MARVIN MA RVIN MA RVI NMARV INMA
|
Ligne M, on cherche N : on trouve la colonne B.
```

2 Travail à faire

Vous devrez réaliser en assembleur MIPS le système de chiffrement de Vigenère. En particulier, votre programme devra comporter :

1. Une routine pour encoder une chaîne de caractères en utilisant une clé donnée (le résultat devra être stockée dans une nouvelle chaîne de caractères) ;
2. Une routine pour décoder une chaîne de caractères en utilisant une clé donnée (le résultat devra être stockée dans une nouvelle chaîne de caractères) ;
3. Une routine pour encoder un fichier texte en utilisant une clé donnée (le résultat devra être stocké dans un nouveau fichier) ;
4. Une routine pour décoder un fichier texte en utilisant une clé donnée (le résultat devra être stocké dans un nouveau fichier) ;
5. Un menu permettant d'appeler les routines précédemment écrites ; ce menu devra boucler et donc comporter une entrée permettant de sortir du programme.

Vous pourrez vous limiter aux caractères majuscules dans un premier temps. Un point de bonus sera accordé si vous traitez les caractères minuscules et encore un autre point si vous traitez les caractères accentués et les caractères spéciaux.

3 Critères d'évaluation

Le projet doit être un programme assemblé et testé qui réalise la tâche demandée. Mais il doit également être écrit de façon satisfaisante.

Le code source du projet sera bien présenté, au moyen d'une indentation correcte. Il devra être convenablement commenté. En particulier, il devra être indiqué clairement quels sont les paramètres et résultats de chaque routine. Des commentaires justifiant vos structures de données seront également les bienvenus.

Le programme devra être divisé en routines de taille raisonnable (maximum une page d'écran). Cela vaut aussi pour la routine main qui ne doit pas être trop longue. Il pourra y avoir plusieurs fichiers, mais ce n'est pas obligatoire. Le code devra être clair et concis.

4 Consignes

Le projet est individuel : chaque élève doit le réaliser et doit en écrire seul chacune des lignes de code. Tous programmes identiques ou présentant trop de similitudes ne seront pas évalués et auront la note de 0.

Pendant la période de préparation du projet, vous pouvez demander l'aide à votre enseignant. Vous pouvez lui poser toutes les questions et lui soumettre tous vos problèmes. Sur le site du cours, un forum sera mis en place, où vous pourrez poser également vos questions et échanger avec votre enseignant et les autres élèves.

5 Remise du projet

Le projet terminé devra être rendu le 30 novembre 2015 au plus tard. Il devra être rendu directement sur le site du cours à l'adresse (ne pas l'envoyer par mail à votre enseignant) :

`https://moodle.umontpellier.fr/course/view.php?id=1027`