Projet 2015: chiffre de Vigenère

David Delahaye

David.Delahaye@lirmm.fr

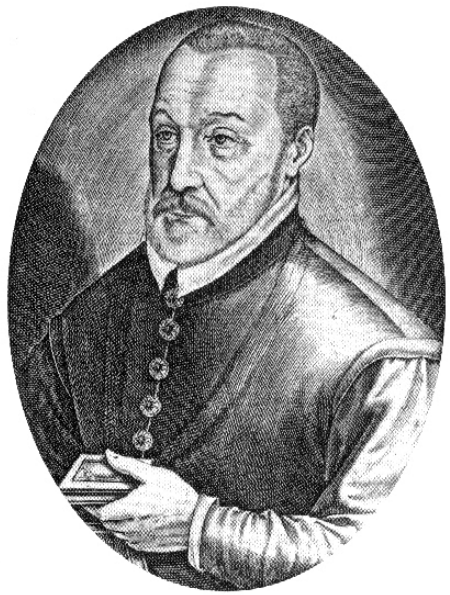
Polytech' Montpellier

IG3 2015-2016

Chiffre de Vigenère

Présentation

- Système de chiffrement polyalphabétique par substitution (une même lettre du message peut suivant sa position être remplacée par des lettres différentes ;
- Nommé ainsi en référence au diplomate du XVIème siècle Blaise de Vigenère, qui le décrit dans son traité des chiffres de 1586 ;
- Résiste à l'analyse de fréquences, mais a été cassé par le major prussien Friedrich Kasiski en 1863.



Principe

Encodage

- Utilisation d'une clé ;
- Clé : mot ou phrase ;
- Repose sur la table de Vigenère ;
- 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.

Principe

Grille de Vigenère

	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

Principe

Encodage

- 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.
```

- Résultat : « NENVZR AF SPOF UN KCM NNOMZ KBPE ».

Principe

Décodage

- Texte codé : « NENVZR AF SPOF UN KCM NNOMZ KBPE » ;
- Clé : « MARVIN ».

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

- Résultat : « BEWARE OF BUGS IN THE ABOVE CODE ».

Travail à faire

Programme assembleur MIPS comportant

- Une routine pour encoder une chaîne de caractères en utilisant une clé donnée (résultat dans une nouvelle chaîne de caractères) ;
- Une routine pour décoder une chaîne de caractères en utilisant une clé donnée (résultat dans une nouvelle chaîne de caractères) ;
- Une routine pour encoder un fichier texte en utilisant une clé donnée (le résultat devra être stocké dans un nouveau fichier) ;
- Une routine pour décoder un fichier texte en utilisant une clé donnée (le résultat devra être stocké dans un nouveau fichier) ;
- Un menu permettant d'appeler les routines précédentes ; ce menu devra boucler et comporter une entrée permettant de sortir.

Limité aux majuscules (bonus : minuscules et caractères spéciaux).

Évaluation, consignes, et remise

Évaluation

- Programme assemblé et testé ;
- Programme documenté ;
- Modularité (plusieurs routines).

Consignes

- Projet individuel ;
- Séances de TP ;
- Forum.

Remise

- Le 30 novembre 2015 au plus tard ;
- Sur le site du cours (ne pas envoyer de mail) :
  https://moodle.umontpellier.fr/course/view.php?id=1027