

VCRYPT : Codage d'un texte par le chiffre de Vigenère

Ce programme est une simple application du chiffre de Vigenère. J'ai conçu ce programme pour qu'il respecte le plus fidèlement possible ce cryptage sans chercher à en faire mon propre chiffre (à vous de le modifier si ça vous intéresse !).

I. Caractéristiques

Ce programme a été écrit sur TI-83+ en basic. Il fonctionnera donc sur TI-84+ sans problème. Il reste à tester su TI-82.

Mémoire requise : 522 octets

Variables utilisées : A, B, C, I, N, M, R, X, Z, Ø, Str1, Str0, Str2, Str3 , _MSG, _CLE

II. Le chiffre de Vigenère

Le chiffre mono-alphabétique de Vigenère a été créé par le cryptographe, alchimiste, diplomate et astrologue français Blaise de Vigenère au XVI^{ème} siècle.

Ce chiffre est basé sur celui de César, qui consiste à décaler les lettres dans l'alphabet d'un certain rang. Par exemple au rang 4 :

```
Alphabet original : ABCDEFGHIJJLMNOPQRSTUVWXYZ
Alphabet modifié  : EFGHIJKLMNOPQRSTUVWXYZABCD

Le texte suivant  : CECI EST UN EXEMPLE
donnera           : GIGM IWX YR IBIQTPI
```

Ce cryptage est très facile à percer en utilisant les statistiques d'apparition de chaque lettre. En effet, la lettre E apparaît plus souvent que les autres dans la langue française. Sachant que chaque lettre est toujours codée de la même manière, nous n'avons plus qu'à définir son rang dans l'alphabet modifié et décrypter le message.

Vigenère utilise le chiffre de César, mais avec une clé.

La clé contient l'écart du chiffre de César : A correspond à 0, Z à 25.

Par exemple, « CECI EST UNE APPLICATION DU CHIFFRE DE VIGENERE » codé avec la clé « SECRET » :

```
Texte à coder      : CECI EST UNE APPLICATION DU CHIFFRE DE VIGENERE
Clé répétée       : SECR ETS ECR ETSECRETSEC RE TSECRET SE CRETSECR
Texte résultant    : UIEZ ILL YPV EIHPKTEMASP UY VZMHWVX VI XZKXFITV
```

Grâce à la clé, la même lettre n'est pas codée deux fois de la même façon.

III. A propos du programme

Le programme VCRYPT.8xp est un application simple du chiffre de Vigenère. Il ne prend pas en compte les caractères autres que les lettres. Si un autre caractère qu'une lettre majuscule est entré, il est supprimé lors du chiffage.

```
MESSAGE ? ->Str0
J'AI MIS UNE APOCEAFBWMGXEHHLXJH
STROPHE ET DES EILWXMHWLXWHTVIK
SPACES
CLE:TEST0
```

Le résultat est disponible à la fin du cryptage dans la variable Str0 accessible par [VARS][7][0].

Enfin, je rappelle que vous êtes libre de modifier ce programme comme bon vous semble, mais mon nom devra être cité dans toute publication l'utilisant.

IV. Annexe : le carré 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
Le Carré de Vigenère																										