Le chiffrement de Vigenère

On se propose d'étudier le chiffrement de Vigenère qui constitue une amélioration du code de César. Voici son principe.

- À chaque lettre à coder de l'alphabet français, on fait correspondre son rang x compris entre 0 et 25.
- On choisit une clé sous la forme d'un mot (ici PLANETE). On écrit cette clé sous le mot à coder en répétant éventuellement la clé (ou une partie).
- Pour chaque lettre du mot à coder, on calcule le reste y de la division euclidienne de $x + z$ (où z est le rang dans l'alphabet de la lettre de la clé) par 26.
- On note la lettre de l'alphabet qui correspond au reste y que l'on vient d'obtenir.

Exemple

Le texte à coder :	J	E	S	E	R	A	I	B	A	C	H	E	L	I	E	R
La clé à répéter :	P	L	A	N	E	T	E	P	L	A	N	E	T	E	P	L

Pour la 1ère lettre : J est associé à 9 ; P est associé à 15.
Ainsi, $y \equiv 9+15$ [26], donc $y = 24$ et J est codé par Y.

1°) **Coder avec le chiffrement de Vigenère**

Reproduire et compléter le tableau suivant pour crypter : JESERAIBACHELIER.

Lettre en clair	J	E	…
Lettre de la clé	P	L	…
Calcul de y	24	15	…
Lettre codée	Y	P	…

2°) **Crypter avec le carré de Vigenère**

Pour éviter un travail de cryptage trop fastidieux, Blaise de Vigenère propose d'utiliser la table ci-après.
Expliquer comment utiliser cette table pour crypter un message.
Vérifier avec le message de la question 1°).

Clé utilisée \ Lettre en clair	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

Lettre chiffrée

3°) **Décrypter un message**

Décoder le message KTGRRXVTPSGENZTCGAEM qui a été crypté, selon le chiffrement de Vigenère, avec la clé PLANETE.
On pourra utiliser le carré de Vigenère ou un tableur.

Note historique :

Blaise de Vigenère (1523-1596) est un diplomate français. Il est né à Saint-Pourçain sur Sioule en Auvergne. Il a publié le *Traité des chiffres*, manuel de cryptographie diplomatique.

Information :

Ce chiffrement a résisté trois siècles aux cryptanalystes. En effet, on ne peut pas utiliser la fréquence des lettres (tant que l'on ne connaît pas la longueur du mot clé). Mais Babagge et Kasiski ont réussi à le casser au milieu du XIXe siècle.

Solution

1°)

Lettre en clair	J	E	S	E	R	A	I	B	A	C	H	E	L	I	E	R
Lettre de la clé	P	L	A	N	E	T	E	P	L	A	N	E	T	E	P	L
Calcul de *y*	24	15	18	17	21	19	12	16	11	2	20	8	4	12	19	2
Lettre codée	Y	P	S	R	V	T	M	Q	L	C	U	I	E	M	T	C

La phrase « Je serai bachelier » donne donc « yp srvtm qlcuiemtc ».

3°) Vigenère est auvergnat.