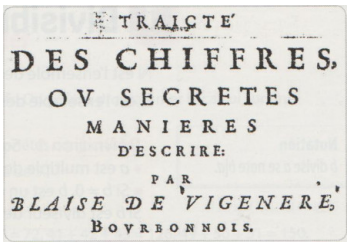
Le chiffrement Vigénère


TRAICTE'
DES CHIFFRES,
OV SECRETES
MANIERES
D'ESCRIRE:
PAR
BLAISE DE VIGENERE,
BOVRBONNOIS.

Blaise de Vigénère (1523-1596), traducteur, diplomate et cryptographe, expose dans son "traité des chiffres" une méthode de chiffrement qui repose sur une clé constituée d'un ou plusieurs mots. On répète les lettres de cette clé sous le texte à chiffrer, écrit sans accent ni ponctuation, ni espace. Pour chiffrer une lettre du texte, on décale dans l'alphabet d'autant de lettres que le rang - entre 0 et 25 - de la lettre correspondante de la clé.

Prenons comme clé : **VICTORHUGO**, la méthode donne :

Texte clair	E	T	S	I	L	N	E	N	R	E	S	T	E	Q	U	U	N	J	E	...
Clé	V	I	C	T	O	R	H	U	G	O	V	I	C	T	O	R	H	U	G	...
Décalage	21	8	2	19	14	17	7	20	6	14	21	8	2	19	14	17	7	20	6	...
Texte crypté	Z	B	U	B	Z	E	L	H	X	S	N	B	G	J	I	L	U	D	K	...

1) Quelles sont les lettres chiffrées par un Z ? un B ? Comment sont chiffrés les E du texte ? Les N ? Quels sont les avantages de ce chiffrement ? Que doit-on connaître pour le déchiffrer ?

2) Soit x le rang dans l'alphabet d'une lettre du message en clair, y le rang dans l'alphabet de la lettre correspondante de la clé et z le rang dans l'alphabet de la lettre dans le message chiffré.
Écrire la relation qui lie z à x et y.

3) Écriture en Python lorsque le texte a la même longueur que la clé.
On considère le mot "ALTERNATIF" qui a la même longueur que la clé "VICTORHUGO".
Écrire dans ce cas le programme vigeneresimple.py dont le script débutera comme ci-dessous.

```
alphabet="ABCDEFGHIJKLMNOPQRSTUVWXYZ"
message="ALTERNATIF"
cle="VICTORHUGO"
chiffre=""
for i in range(len(message)):
        ...
print(chiffre)
```

Le chiffrement donne "VTVXFEHNOT"

4) Adaptation de la clé à la longueur du message

Pour un texte de longueur quelconque, on construit une clé auxiliaire, de même longueur que le message. Pour cela, on recopie autant de fois que nécessaire la clé puis, on complète avec autant de lettres de la clé que nécessaire.

Exemple : Lorsque le message a pour longueur 52 et la clé a pour longueur 9, déterminer le nombre d'occurrences de la clé et le nombre de lettres pour compléter la clé auxiliaire.

Écrire le programme cleauxiliaire.py dont le script débutera comme ci-dessous.

```
alphabet="ABCDEFGHIJKLMNOPQRSTUVWXYZ"
message="ETSILNENRESTEQUUNJESERAISCELUILA"
cle="VICTORHUGO"
cleaux=""
q=...
r=...
for i in range(q):
        cleaux=cleaux+cle
for i in range(r):
        cleaux=cleaux+cle[i]
```

5) Écrire maintenant en Python le programme vigenere.py qui s'adapte à tout message et toute clé.

6) Déchiffrement.
   Écrire le programme decryptvigenere.py permettant de déchiffrer un message chiffré à l'aide de la méthode vigénère si l'on connait la clé d'encryptage.