Le chiffrement affine

On souhaite chiffrer un message. Chaque lettre, en majuscule, est remplacée par son rang entre 0 et 25 dans l'alphabet, les autres signes (espaces, traits d'union,...) sont supprimés.

A	B	C	D	E	F	G	H	I	J	K	L	M
0	1	2	3	4	5	6	7	8	9	10	11	12
N	O	P	Q	R	S	T	U	V	W	X	Y	Z
13	14	15	16	17	18	19	20	21	22	23	24	25

On nomme x le rang de la lettre, $0 \leqslant x \leqslant 25$ et on choisit deux entiers a et b.

Le rang y de la lettre chiffrée est alors le reste de la division euclidienne de $ax + b$ par 26.

Le couple d'entiers $(a\,;b)$ s'appelle la clé de chiffrement.

1) Écriture en Python.

   On choisit la clé $(7\,;17)$. Écrire le programme affine.py permettant de chiffrer, par la méthode affine, n'importe quel message.

```
alphabet="ABCDEFGHIJKLMNOPQRSTUVWXYZ"
message="ETSILNENRESTEQUUNJESERAISCELUILA"
a=7
b=17
chiffre=""
for i in range(len(message)):
        ...
print(chiffre)
```

   Le chiffrement donne "TUNVQETEGTNUTZBBECTNTGRVNFTQBVQR"

2) Avec d'autres clés de chiffrement.

   a) Observer le chiffrement du message si l'on prend :

      - $a = 5$ et $b = 11$;
      - $a = 31$ et $b = 11$;
      - $a = 265$ et $b = 37$.

   b) Soit a, a', b et b' des entiers. Démontrer que si $a - a'$ et $b - b'$ sont divisibles par 26, les cryptages avec les clés $(a\,;b)$ et $(a'\,;b')$ sont identiques.

   c) De combien de clés dispose-t-on en prenant $0 \leqslant a \leqslant 25$ et $0 \leqslant b \leqslant 25$?

3) cas $a = 13$

   a) Tester ce cas avec le programme Python. Que remarque-t-on ?

   b) Soit x et x' les rangs de deux lettres de l'alphabet et y et y' les rangs des lettres qui leur sont associées par le chiffrage affine.

      Démontrer que $y - y'$ est divisible par 13.

      Quelle en est la conséquence sur le codage du texte ?

   c) Pour quelle autre valeur de a peut-on rencontrer un problème similaire ?

      Tester votre réponse avec le programme.