## Et s'il n'en reste qu'un...

Savez-vous comment se termine ce célèbre vers de Victor Hugo, titre de l'activité ?

La réponse est WRFRENVPRYHVYN

Cette réponse est bien sûr cryptée ! Le chiffrement a été effectué en ROT 13, système souvent employé sur Internet pour donner la fin d'un film ou la réponse à une énigme. Très simple à déchiffrer, il évite qu'un lecteur puisse connaître la réponse par inadvertance.

Nous allons voir le principe de ce chiffrement et apprendre à l'automatiser.

### Partie A : Le chiffrement de César

Dans le chiffrement de Jules César, chaque lettre est remplacée par la lettre qui la suit trois rangs plus loin dans l'alphabet. Les trois dernières lettres sont remplacées, par permutation circulaire, par les trois premières lettres de l'alphabet.

1) Que devient le mot EGYPTE une fois crypté ?

2) Automatisation du codage.

   À chaque lettre on associe son rang dans l'alphabet :

| 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 |

   Soit $x$ le rang dans l'alphabet d'une lettre du message en clair et $y$ le rang dans l'alphabet de la lettre correspondante dans le message crypté. Écrire la relation qui lie $y$ à $x$.

3) Écriture en Python.

   Écrire le programme alphabet.py et vérifier que l'on obtient l'encodage de l'alphabet souhaité.

```
alphabet="ABCDEFGHIJKLMNOPQRSTUVWXYZ"
print(alphabet[3])
print(alphabet[0])
print(alphabet[25])
```

   Écrire le programme index.py et vérifier qu'il permet de retrouver le rang dans l'alphabet de toute lettre du mot EGYPTE.

```
message="EGYPTE"
alphabet="ABCDEFGHIJKLMNOPQRSTUVWXYZ"
print(message[3])
print(alphabet.index(message[3]))
```

4) En déduire le programme cesar.py permettant de chiffrer, par la méthode César, n'importe quel message. On pourra utiliser les commandes suivantes après les avoir testées.

```
message="EGYPTE"
print(len(message))
print(message+message[3])
```

5) Déchiffrage

   Écrire le programme dechiffrecesar.py permettant de déchiffrer n'importe quel message chiffré à l'aide de la méthode César.

**Partie B : Le ROT 13**

1) Le ROT 13 consiste en un décalage de 13 rangs (ROTation de 13 caractères).

   Écrire le programme decryptrot13.py afin de retrouver la fin du vers de Victor Hugo.

2) Vérifier, à l'aide de ce programme que, dans le cas du ROT 13, chiffrer un message ou le déchiffrer revient au même. Expliquer ce résultat.