Page 364. Exercice 2.4. Cryptographie de César.

On appelle cryptographie les méthodes pour coder les messages. Les premiers écrits stipulant l'utilisation de cryptographie datent de l'époque romaine avec l'apparition du « chiffrement de César ». On l'utilisait pour donner des ordres aux troupes afin que les ennemis ne puissent pas déchiffrer les messages et anticiper les mouvements des armées.

Un message crypté par cette méthode débutait par un nombre puis le message dont les lettres avaient été décalées de ce nombre de rang dans l'ordre alphabétique.

Par exemple, le message :

« 3 M'DLPH OHV PDWKV » signifie « J'AIME LES MATHS »

(le 3 signifie que l'on a décalé de trois rangs et donc un A est transformé en D, un B en E, etc).

Pour la programmation, on utilise deux fonctions :

* Lettre-nombre() qui, quand on lui donne une lettre, rend le numéro de cette lettre dans l'alphabet.
* Nombre-lettre() qui, quand on lui donne un nombre entre 1 et 26, rend la lettre de l'alphabet correspondante.

Voici des extraits de ces deux fonctions :

|  |
| --- |
| Lettre-nombre(lettre)if lettre=='a' : return(1)if lettre=='b' : return(2),,,,,,,, |
| Nombre-lettre(nombre)if nombre==1 : return(a)if nombre==2 : return(b),,,,,,,, |

**Imagine une autre façon de remplacer lettre par lettre par simple décalage et crée un algorithme correspondant.**