



## Un masque cohérent

Tirée de la finale du concours Alkindi, cette énigme est publiée par **jaudi**

Alice et Bob utilisent une méthode de chiffrement efficace. Le message à transmettre est écrit sur une ligne, et chaque lettre en français est remplacée comme suit : A=00, B=01, C=02, ... . Puis, sur une 2e ligne, on écrit une séquence de nombres, appelée masque, et on somme lettre par lettre.

Exemple: Pour chiffrer "ALKINDI" avec le masque "12 05 20 21 10 00 97" on obtient :

```
A L K I N D I  donne 00 11 10 08 13 03 08  +
12 05 20 21 10 00 97      12 05 20 21 10 00 97
-----
                        12 16 30 29 23 3  105
```

Plutôt que d'apprendre par cœur le masque, Alice et Bob le calculent facilement : le premier nombre du masque est appris par cœur et les autres sont obtenus l'un de l'autre. Si on note  $m_1, m_2, m_3$ , etc les nombres du masque, alors :

$m_2$  consiste en les 2 derniers chiffres de  $(m_1)^2+1$

$m_3$  consiste en les 2 derniers chiffres de  $(m_2)^2+1$

etc.

```
Exemple : m1=11
11*11+1=122 donc m2=22
22*22+1=485 donc m3=85
etc.
```

Voici le message qu'Alice a envoyé à Bob :

```
38 104 21 20 5 47 81 55 20 19 19 46 98 34 12 6 7
40 80 34 5 20 24 44 96 54 12 16
```

La réponse attendue est un mot de cinq lettres.