

Voici un chiffrement permettant de chiffrer des messages de multiples de n lettres.

On commence par établir un tableau de n cases. Dans chaque case, il y a un nombre entre 1 et n qu'on ne trouve qu'une fois dans le tableau, c'est notre clé. On va chiffrer notre message de n lettres en mettant chaque lettre dans la case du tableau correspondante. Une lettre de la case numéro 1 sera en tête du message chiffré, la lettre de la case numéro 2 sera en deuxième, etc...

Par exemple, voici le tableau d'une clé de 25 cases

| | | | | |
|----|----|----|----|----|
| 8 | 3 | 19 | 20 | 1 |
| 12 | 5 | 9 | 15 | 24 |
| 21 | 10 | 16 | 13 | 6 |
| 22 | 2 | 4 | 23 | 25 |
| 7 | 17 | 11 | 18 | 14 |

En prenant un message de 25 lettres « voici un chiffre compliqué eh » et en le mettant dans un tableau de 25 cases, on a :

| | | | | |
|---|---|---|---|---|
| V | O | I | C | I |
| U | N | C | H | I |
| F | F | R | E | C |
| O | M | P | L | I |
| Q | U | E | E | H |

Au final, si on lit les deux tableaux en même temps, on a que la lettre V sera en 8ème position du message chiffré, le O en 3ème position, etc.

On a le message chiffré : «IMOPCNQVCFEUEHHRUEICFOLII»

Dans le cas d'un message de 50 lettres, le résultat est la concaténation du chiffrement des 25 premières lettres et du chiffrement des 25 dernières. Ainsi de suite pour tout les multiples de 25

Avec la même clé que dans l'exemple, décryptez le message suivant :

néocrpPaveeissotruredrdymtulneletegemsugaelesnenfirdseerteuesiunscaivlumpoil<slmaxega>iefflr
 oraelrodoeinuct<lsisigtempn>tooenotutbmxlsnqoaircieruel<sr>rseca<TiPed>C<ateasne...
 sceoUaliecplass>>apd<apsrieumoscslaemepsntrxcsoop<e>ueseianadtldpdtionuvdoanrr5tiferu7sa2ee
 gprcaic