

## RÉSOLUTION D'UNE ÉNIGME COMPLEXE

Cette énigme est l'exercice n° 7 de l'épreuve finale du Concours Alkindi de 2019. Elle se présente comme suit :

4519560110316883496280  
3830579041125424031819  
6291822346635584477275  
5739236847633297043657  
8423125230523344095014  
5583905896406215202688  
2787490953255925630042  
800265405155387909963  
454133230174544843140  
170005037595951454684  
547092932622233310260  
9447618119065174509877  
965175098891097559751

Bon courage !

Aucune équipe n'a pu terminer cet exercice. Lors de l'épreuve finale du concours 2020, un exercice identique, l'exercice n° 8, a été proposé. Personne n'a pu le résoudre non plus.

Un an après, au printemps 2021, surprise ! La solution de l'énigme n°8 de la finale 2020 est donnée sur le site officiel du Concours AlKindi. Il suffit simplement de se rendre sur le site :

[https://concours-alkindi.fr/sujets\\_finale/resolution\\_enigme\\_dgse\\_2020.pdf](https://concours-alkindi.fr/sujets_finale/resolution_enigme_dgse_2020.pdf)

pour lire la solution de l'énigme. Elle avait été proposée par la DGSE, partenaire du concours AlKindi, et la solution est signée par « Julien, cryptanalyste à la DGSE ».

Sa lecture est très édifiante, car non seulement elle donne la solution, mais elle explique aussi avec clarté et avec humour quelles sont les questions à se poser devant une énigme et comment réfléchir. Avant de lire cette solution, il faut peut-être faire un bref détour mathématique par les nombres premiers, concept fondamental de l'énigme.

## Rappel mathématique : qu'est ce qu'un nombre premier ?

Un nombre premier est un nombre qui « n'est divisible que par 1 et par lui-même », comme disent les mathématiciens. Dit autrement, un nombre premier est un nombre qui n'est divisible par aucun autre nombre. La liste des nombres premiers est 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37 ....

Il existe une infinité de nombres premiers.

Si l'on décompose un nombre quelconque en facteurs, c'est à dire si l'on recherche les diviseurs de ce nombre, ces diviseurs sont des nombres premiers. Ils sont appelés facteurs premiers. Par exemple  $546 = 2 \times 3 \times 7 \times 13$ . Le nombre 546 est constitué de 4 facteurs : 2, 3, 7 et 13, qui sont des nombres premiers.

La lecture de la solution de l'exercice n° 8 de la finale 2020, telle que donnée sur le site Internet mentionné ci-dessus, est vivement conseillée pour le compréhension de la suite. En effet, cette énigme se déchiffre exactement de la même manière.

Rappelons donc le texte de l'énigme :

### Énigme :

4519560110316883496280  
3830579041125424031819  
6291822346635584477275  
5739236847633297043657  
8423125230523344095014  
5583905896406215202688  
2787490953255925630042  
800265405155387909963  
454133230174544843140  
170005037595951454684  
547092932622233310260  
9447618119065174509877  
965175098891097559751

Bon courage !

En suivant la méthodologie indiquée pour l'exercice n°8, sur le site déjà mentionné :

[https://concours-alkindi.fr/sujets\\_finale/resolution\\_enigme\\_dgse\\_2020.pdf](https://concours-alkindi.fr/sujets_finale/resolution_enigme_dgse_2020.pdf)

la solution s'établit comme suit :

1) Il faut considérer cet ensemble de chiffres comme un nombre, les lignes se suivent :

451956011031688349628038305790411254240318196291822346635584477275  
573923684763329704365784231252305233440950145583905896406215202688  
2787490953255925630042800265405155387909963454133230174544843140  
1700050375959514546845470929326222333102609447618119065174509877  
965175098891097559751

Ce nombre est donc constitué de 281 chiffres ! Appelons le X.

2) Il faut diviser ce nombre en facteurs premiers. Cette opération est réalisable sur le site *dcode.fr*, sur sa page <https://www.dcode.fr/decomposition-nombres-premiers>

Le résultat de la décomposition en facteurs premiers nous donne X =

$3 \times 719 \times 983 \times 1283 \times 1543 \times 1867 \times 2137 \times 2711 \times 3533 \times 4397 \times 4663 \times 5347 \times 6287 \times 7253 \times 8191 \times 9209 \times 10133 \times 11239 \times 11699 \times 12109 \times 12527 \times 13219 \times 14243 \times 15307 \times 15607 \times 16741 \times 17683 \times 18773 \times 19843 \times 20921 \times 21997 \times 23099 \times 24223 \times 24611 \times 25747 \times 26861 \times 28001 \times 29033 \times 30271 \times 30649 \times 31663 \times 32693 \times 33811 \times 34211 \times 35419 \times 36563 \times 37649 \times 38873 \times 40037 \times 41231 \times 42397 \times 42701 \times 43801 \times 44893 \times 45281 \times 46489 \times 46877 \times 47947 \times 49201 \times 50417 \times 51637 \times 52861 \times 54037 \times 55163 \times 55681 \times 56149 \times 56633$

Le nombre X est donc constitué de 67 facteurs premiers.

3) Il faut ensuite calculer la position de chacun de ces nombres dans la liste des nombres premiers.

Le site *dcode.fr* va nous y aider. La page <https://www.dcode.fr/fonction-compte-nombre-premier> nous indique le rang de chacun de ces nombres dans la suite des nombres premiers. Le chiffre 3 est au 2ème rang, 719 au 128ème, 983 est 166ème, 1283 au 208ème, etc. jusqu'à 56 633 qui est le 5743ème nombre premier. Ce qui nous donne la suite de nombres suivants :

2 128 166 208 243 285 322 395 494 599 631 707 818 928 1 028 1 142 etc..

*Encore une fois, cet exposé est très résumé, il faut suivre le raisonnement publié sur Internet.*

4) On calcule ensuite la différence entre chaque nombre et le précédent. On obtient la suite :

126 38 42 35 42 37 73 99 105 32 76 111 110 100 114 101 15 46 46 46 76 101 115 etc.

5) Enfin, l'examen de ces nombres, tous inférieurs à 128, permet de découvrir que nous sommes en présence d'un code ASCII. Une table de ce code prise sur Internet nous fournit la solution, ainsi que notre ami *dcode.fr* sur sa page <https://www.dcode.fr/code-ascii>

Et la solution est : ~&\*##\*% **Ici Londres...Les sanglots longs des violons de l'automne...**

On notera la présence de symboles et non de lettres en début de message pour induire le décrypteur en erreur et lui faire croire qu'il part sur une fausse piste. Astucieux...

### **Conclusion (très importante) :**

Cette énigme, petite merveille de complexité, présente également l'intérêt d'être une parfaite illustration du **Principe de Kerckhoffs** :

**« La sécurité d'un système de chiffrement ne doit reposer que sur le secret de la clef et non pas sur le secret de l'algorithme de chiffrement, qui peut être connu de l'ennemi. »**

En effet, l'algorithme de chiffrement de cette énigme est extrêmement compliqué. Pourtant, l'explication du décryptage de l'exercice n° 8 de la finale 2020 a permis de résoudre assez facilement cet exercice n° 7 de la finale 2019 en appliquant les mêmes opérations de déchiffrement.

Pourquoi ? **Parce qu'il n'y a pas de clef dans cette énigme.** Il n'y a qu'un algorithme, c'est à dire une suite d'opérations à effectuer. Si cette méthode, aussi complexe soit-elle, est appliquée à plusieurs messages et que l'ennemi la connaît, il pourra décrypter facilement tous les messages. L'énigme a bien entendu été construite dans cet esprit.

Il était évidemment impossible pour les candidats participants à la finale de résoudre cette dernière énigme dans le temps imparti pour l'épreuve et munis seulement d'un papier et d'un crayon. D'ailleurs il est même quasi-impossible de la résoudre chez soi avec son ordinateur si on ne connaît pas la méthode de calcul. L'analyste de la DGSE qui l'a conçue a sans doute voulu montrer un exemple de l'utilisation des concepts de la cryptographie moderne, comme par exemple dans le chiffrement RSA : nombre immensément grand de 281 chiffres, nombres premiers, code ASCII...

\*\*\*\*\*  
\*\*\*\*\*  
\*\*\*  
\*