

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://www.concours-alkindi.fr/docs/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 la 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://www.concours-alkindi.fr/docs/resolution_énigme_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 × 719 × 983 × 1283 × 1543 × 1867 × 2137 × 2711 × 3533 × 4397 × 4663 × 5347 × 6287 × 7253 × 8191 × 9209 × 10133 × 11239 × 11699 × 12109 × 12527 × 13219 × 14243 × 15307 × 15607 × 16741 × 17683 × 18773 × 19843 × 20921 × 21997 × 23099 × 24223 × 24611 × 25747 × 26861 × 28001 × 29033 × 30271 × 30649 × 31663 × 32693 × 33811 × 34211 × 35419 × 36563 × 37649 × 38873 × 40037 × 41231 × 42397 × 42701 × 43801 × 44893 × 45281 × 46489 × 46877 × 47947 × 49201 × 50417 × 51637 × 52861 × 54037 × 55163 × 55681 × 56149 × 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 46 46 46 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 cette énigme est extrêmement compliqué. Pourtant, l'explication 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 un 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'emploi de techniques de chiffrement complexes et modernes : nombre immensément grand de 281 chiffres, utilisation des nombres premiers, code ASCII...

*