RÉSOLUTION

d'une énigme complexe

DGSE
DIRECTION GÉNÉRALE DE LA SÉCURITÉ EXTÉRIEURE

Énigme

3 2 7 8 2 6 6
6 5 7 5 2 7 9
0 1 9 9 5 2 5
6 2 4 1 0 3 3
1 1 4 8 2 0 4
0 0 8 6 2 9 9
1 6 6 3 6 9 6
2 2 4 0 8 7 3
5 6 4 7 4 7 1
3 5 3 7 4 6 1
1 1 9 4 3 4 8
7 6 8 5 0 1 4
4 5 1 3 8 0 1
0 4 6 2 6 9 8
8 6 9 4 7 3 9
7 1 6 1 3 6 2
2 1 1 3 0 3 7
4 4 1 8 3 8 9
3 7 8 6 3 5 7
8 0 4 7 0 0 0
5 2 2 5 1 7 4
7 6 6 4 7 9 2
9 8 0 9 2 1 0
4 0 6 7 9 7 6
2 2 9 3 2 1 1
0 0 5 3 0 9 4
2 1 7 6 1 5 7
6 3 8 6 1 4 1
7 3 2 2 2 5 7
3 1 0 9 8 9 1
1 7 9 3 2 4 1
6 4 0 7 0 6 8
6 3 2

Résolution

Cette suite de chiffres est pour le moins énigmatique, elle est longue et *a priori* sans logique. Néanmoins, comme elle est proposée en tant qu'énigme, il doit bien y avoir une information d'intérêt qui s'y cache. La première étape quand on cherche à résoudre une énigme est d'y trouver **des points d'accroche, des choses qui attirent l'œil, qui interpellent** ou **qui rappellent un mécanisme déjà vu**. 😲

Vous l'aurez compris c'est donc grâce à **votre génie** et à **votre expérience** que vous pouvez retrouver ce qui se cache derrière !

La première chose qui interpelle ici c'est la mise en page : **pourquoi positionner ces chiffres en colonne et laisser tant d'espace blanc autour ?**

La deuxième chose qui interpelle, est la dernière ligne du tableau :

6	3	2

Pourquoi les chiffres ne sont pas espacés comme ceux situés au dessus ?
Ce sont les deux premiers points d'accroche.
On peut donc imaginer qu'ils ne sont pas dans le *bon ordre* et qu'il faut *réorganiser* tout ça.

Réorganiser ?
Pourquoi pas, mais comment ?
La mise en page verticale laisse penser que la notion de colonne a de l'importance : chaque colonne pourrait former un groupe logique. C'est une piste à creuser.

On peut également noter que l'énigme se compose de 7 colonnes. Comment réorganiser 7 colonnes… si on doit tout tester cela fait 7! possibilités (se lit 7 factoriel), soit 1 x 2 x 3 x 4 x 5 x 6 x 7 ou encore 5 040 possibilités. L'adage dit qu'un bon mathématicien est un mathématicien « fainéant ». On va donc tenter de trouver une façon astucieuse de tester les possibilités le plus rapidement possible.

Qu'est-ce qui a un rapport avec le chiffre 7 et qui pourrait nous aider dans ce contexte ?
7 est un nombre premier (les matheux aiment bien les nombres premiers) mais là ça n'aide pas plus que ça !

Les jours de la semaine ?
Il y en a bien 7, comme le nombre de colonnes dans cette énigme.

Voici ce qu'on obtient si on fait correspondre la première lettre de chaque jour de la semaine avec chaque colonne si on les réorganise ensuite par ordre alphabétique :

Extrait du tableau énigme

3	2	7	8	2	6	6
6	5	7	5	2	7	9

1	7	9	3	2	4	1
6	4	0	7	0	6	8
6				3	2	
L	**M**	**M**	**J**	**V**	**S**	**D**

Réorganisation des colonnes

6	8	3	2	7	6	2
9	5	6	5	7	7	2

1	3	1	7	9	4	2
8	7	6	4	0	6	0
		6			2	3
D	**J**	**L**	**M**	**M**	**S**	**V**

À noter qu'on aurait aussi pu partir du principe que les colonnes étaient rangées par ordre alphabétique et qu'il fallait les remettre dans l'ordre logique.

Mais, que viendrait faire les jours de la semaine dans notre énigme ?

Mmm... l'idée semble bonne mais peut-être faut-il trouver une autre clé pour réorganiser ces colonnes ?

Par exemple, le mot ALKINDI comporte 7 lettres et semble faire un bon candidat (en terme de rapport avec notre énigme c'est pas mal !)

Extrait du tableau énigme

3	2	7	8	2	6	6
6	5	7	5	2	7	9

1	7	9	3	2	4	1
6	4	0	7	0	6	8
6				3	2	
A	**L**	**K**	**I**	**N**	**D**	**I**

Réorganisation des colonnes

3	6	8	6	7	2	2
6	7	5	9	7	5	2

1	4	3	1	9	7	2
6	6	7	8	0	4	0
6	2					3
A	**D**	**I**	**I**	**K**	**L**	**N**

On remarque que, malgré la réorganisation des colonnes par ordre alphabétique, la dernière ligne présente toujours un aspect étrange :

Dernière ligne tableau

6					3	2

Réorganisation des colonnes

6	2					3

À ce stade, on n'a pas gagné grand-chose.

Et si c'était l'inverse : que les colonnes suivaient la logique alphabétique et qu'il fallait les remettre dans l'ordre logique du mot ALKINDI ?

Extrait du tableau énigme

3	2	7	8	2	6	6
6	5	7	5	2	7	9

1	7	9	3	2	4	1
6	4	0	7	0	6	8
6				3	2	
A	**D**	**I**	**I**	**K**	**L**	**N**

Réorganisation des colonnes

3	6	2	7	6	2	8
6	7	2	7	9	5	5

1	4	2	9	1	7	3
6	6	0	0	8	4	7
6	2	3				
A	**L**	**K**	**I**	**N**	**D**	**I**

Là, on arrive à une dernière ligne qui a une forme rassurante, proche de quelque chose que l'on connait, à quoi on est habitué. Comme si les chiffres avaient été mis les uns après les autres dans 7 colonnes et qu'à la fin il en restait 3 classés dans l'ordre.

On a donc un tableau qui a été rempli par colonne. Comme ces colonnes ont déjà servi pour mélanger les chiffres peut-être qu'elles ne servent plus dans la suite de l'énigme et qu'on doit maintenant regarder leur contenu comme une suite de chiffres telle que :

```
362762867279550259519630432110244180928906196666327843205744167364315714398147108465408115309668428379964763621123017134831948353877680040075712425797626491200894796607212912309054032517716641813675227323980119142917366008476623
```

Bon ! vous me direz : on est passé d'une suite de chiffres en colonne à une suite de chiffres en ligne. On n'a pas l'air d'avoir beaucoup avancé ! 😵 Néanmoins, maintenant on a l'impression d'avoir une suite de chiffres dans le bon ordre (car on a fait l'effort de remettre les colonnes dans un ordre qui semble logique).

En cryptanalyse, quand on voit autant de chiffres d'affilée, il y a un certain nombre de choses que l'on a envie de tenter : soit il peut s'agir d'une suite en hexadécimale, soit on peut découper 2 à 2 et tenter une représentation ASCII[1] de la phrase, soit c'est un (très) grand nombre. Je ne sais pas si je vous l'ai déjà dit, mais les matheux adorent les nombres premiers et en cryptanalyse on ne fait pas exception. 😉

Donc est-ce que ce très grand nombre (appelons le X) est un nombre premier ou pas ?

En essayant de le factoriser, on voit qu'il est divisible par 3. Il ne s'agit donc pas d'un nombre premier. Mais comme tout nombre entier, il peut se décomposer en unique produit de facteurs premiers.

$$
\begin{aligned}
X = \; & 362762867279550259519630432110244180928906196666327 \\
& 843205744167364315714398147108465408115309668 4 \\
& 283799647636211230171348319483538776800400757124257 \\
& 976264912008947966072129123090540325177166418136752 \\
& 27323980119142917366008476 23 \\
= \; & 3 \times 337 \times 1091 \times 1801 \times 2719 \times 3631 \times 3907 \times 4159 \times 4451 \times 5189 \times 6151 \\
& \times 7193 \times 8237 \times 8543 \times 9403 \times 10463 \times 11467 \times 12589 \times 12907 \times 13873 \\
& \times 14879 \times 15901 \times 16981 \times 17317 \times 18307 \times 19421 \times 19709 \times 20347 \\
& \times 21487 \times 22541 \times 23549 \times 24631 \times 25867 \times 26987 \times 28211 \times 28559 \\
& \times 29179 \times 30341 \times 31151 \times 32257 \times 33343 \times 34337 \times 35447 \times 3583 \\
& \times 36343 \times 36821 \times 37339 \times 37957 \times 38453 \times 38977 \times 39461 \times 40009 \\
& \times 40559 \times 40903 \times 41231
\end{aligned}
$$

En observant cette décomposition, un œil averti remarquera plusieurs choses étranges. Tout d'abord, il est plutôt inhabituel, pour un nombre de cette taille, de voir qu'aucun des facteurs premiers n'est présent plus d'une fois et de voir qu'il se factorise aussi bien (le plus grand facteur premier est assez petit par rapport au nombre X).

On peut désormais chercher des liens entre les facteurs premiers de X.

1. L'*American Standard Code for Information Interchange* est une norme informatique de codage des caractères mise au point dans les années 1960.

Commencent-ils tous par le même nombre ?

Est-ce que le poids de *Hamming*[2] de leur représentation binaire est toujours égal ?

Les différences entre deux facteurs premiers successifs suivent-elles une logique particulière ?
Mmm... rien de bien concluant pour l'instant. 🤔

Et si nous regardions la position de chaque facteur dans la grande suite des nombres premiers ?
Calculer l'ensemble des nombres premiers jusqu'à 50 000 par exemple vous permettra de construire cette liste :

Position dans la suite	1	2	3	4	...	5130	5131	5132
Nombre premier	2	3	5	7		49991	49993	49999

Et si maintenant on regarde la position de chaque facteur premier de X dans cette liste :

Position dans la suite	1	**2**	3	4	...	**67**	68	...	**539**	...	603	**604**	...	**690**	...	...
Nombre premier	2	**3**	5	7	...	**337**	347	...	**3907**	...	4447	**4451**	...	**5189**	...	...
Facteur premier de X ?	NON	**OUI**	NON	NON	...	**OUI**	NON	...	**OUI**	...	NON	**OUI**	...	**OUI**	...	...

2. Je pourrais vous donner une explication ici mais je suis sûr qu'en allant chercher sur internet vous découvrirez d'autres choses qui vous intéresseront.

On obtient la liste suivante :

Facteur premier de X	3	337	1091	1801	2719	3631	3907	4159	4451	...	...
Position dans la suite	1	67	181	278	396	507	539	572	604	...	...

On constate que les facteurs premiers qui composent X sont assez proches dans la liste des nombres premiers surtout si on les regarde 2 à 2.

En effet, si on regarde la différence de position entre le facteur *n* et le facteur *n-1* on constate que celle-ci est toujours inférieure à 128.

Facteur premier de X	3	337	1091	1801	2719	3631	3907	4159	4451	...
Position dans la suite	1	67	181	278	396	507	539	572	604	

66 114 97 118 111 32 33 32

Et donc, là on sent qu'on s'approche d'une solution réaliste. 🥳

En effet, en informatique chaque caractère ASCII est codé sur un peu moins de 1 octet (7 bits plus précisément) et peut prendre une valeur entre 0 et 127. En tentant donc de remplacer chaque différence par le caractère correspondant dans la table ASCII on voit un message apparaître :

Différences	66	114	97	118	111	32	33	32	86	111	...
Caractères ASCII	B	r	a	v	o	␣	!	␣	V	o	...

En répétant le processus on arrive au message suivant :

Bravo! Vous avez fini le Concours AlKindi 2019-2020!

Et franchement, si vous avez résolu l'énigme tout seul : vous avez le potentiel pour être un grand professionnel de la cryptanalyse.

Mais rassurez-vous, si vous n'y êtes pas parvenu... c'est normal ! Cette énigme a été spécialement conçue pour qu'il soit presque impossible de trouver la solution seul avec une feuille et un crayon. C'est d'ailleurs pour ça qu'elle avait été posée en 2020 comme ultime épreuve du concours Alkindi, afin de départager les meilleurs des meilleurs d'entre vous !

Dans tous les cas, j'espère que vous avez pris autant de plaisir à résoudre cette énigme ou à suivre cette solution que nous en prenons chaque jour dans nos métiers.

Julien (Cryptanalyste à la DGSE)

Notes