COMMENT RÉSOUDRE UNE ÉNIGME ?

Il est conseillé d'avoir un aperçu, même succinct, des principaux modes de chiffrement avant d'aborder cette fiche. Si vous êtes débutant, la lecture des fiches n° 3, 4, et 5 vous sera utile.

Voici donc quelques pistes pour aborder une énigme :

Tout d'abord, il convient de la lire soigneusement, deux ou trois fois. Est ce que ça me fait penser à quelque chose de connu, que j'ai déjà vu ? Puis il faut bien lire le titre et les indices donnés pour essayer de capter le thème de l'énigme et son environnement.

1. Au départ :

Souvent, l'énigme vous « parle » immédiatement, simplement en la regardant, ou avec le titre et les indices : on reconnaît du binaire, du Morse, de l'alphabet phonétique…

Dans sa résolution de l'énigme n° 8 de la finale 2020 du Concours Alkindi donnée sur Internet (https://concours-alkindi.fr/docs/resolution_enigme_dgse_2020.pdf), Julien, le cryptanalyste de la DGSE, écrit :

La première étape lorsque l'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.

Exemple : Vous lisez :

- une suite de nombres croissants de façon bizarre : vous pensez à la suite de Fibonacci.
- une suite de nombres inférieurs à 100 et il y a le mot « éléments » en sous-titre : vous pensez au tableau des éléments périodiques de Mendeleïev .

Au moins deux énigmes du site sont bâties sur ces 2 thèmes.

Ce sont des points de départ. Ensuite l'énigme peut présenter plus ou moins de difficultés, et il faut un peu chercher.

2. Pour continuer :

Il se peut que le texte ne vous dise rien au premier abord. Il y a alors plusieurs cas de figures :

- ***L'énigme est constituée de lettres***

Il peut y avoir y avoir une astuce dans la présentation : texte clair mais écrit à l'envers, ou sur deux colonnes de bas en haut, la première ou la dernière lettre de chaque mot, une charade, le rapport avec le cadran d'un vieux téléphone, etc...

Ces hypothèses une fois éliminées, il faut se poser la question basique : quel est ce type d'énigme : une substitution, une transposition, un code, un mélange d'un peu tout ça ?

a) ***Les lettres du message chiffré sont des lettres peu utilisées en français***

et le texte ressemble à des phrases. Dans ce cas, il y a de fortes chances que l'on soit en face de mots codées directement tels qu'ils sont. Il faut effectuer une analyse de fréquence et compter chaque lettre (voir fiche n° 3, analyse de fréquence).

- Si on est face à une belle distribution de lettres du type A= 15 %, B, C et D = 8 %, etc. un chiffrement en *substitution simple* est probable. Il peut s'agir tout simplement d'un code Jules César, mais aussi d'un codage lettres par lettres, donc il faut effectuer un travail d'analyse de chaque lettre et rechercher dans le crypto quelle est la lettre qui remplace le E, le S, les voyelles (voir fiche n° 3 paragraphe 3 , la substitution simple). Il faut de préférence que le texte soit assez long pour procéder à une analyse de fréquence, sinon c'est quasi mission impossible.

- Si l'analyse de fréquence révèle que chaque lettre est répartie à peu près uniformément dans le texte, il s'agit sans doute d'*une substitution avec clef*, du type tableau de Vigenère (fiche n° 3).
Il faut donc écrire le crypto sur une ligne, et ensuite tester des clefs.

C'est là où le contexte de l'énigme intervient : quel est son titre, qu'est-il écrit pour présenter cette énigme, y a-t-il un dessin (énigme 19) ? Ce sont des indices pour la clef. Les indices, le contexte de l'énigme, la personne qui l'a écrite, déterminent des clefs ou des mots probables.

Notons l'importance de *l'attaque* : il est souvent plus facile de travailler sur les premiers mots ou sur les derniers mots d'un message. Un message peut commencer par « bonjour, « salut », « le code », « cette énigme » ou se terminer par « la solution est », le code est » ou par une signature ... qui sont des indications précieuses de mots probables.

On n'insistera jamais assez sur l'importance de la recherche de mots probables et des mot courants dans un crypto. C'est une attaque de la sorte qui permit (entre autres) de déchiffrer les messages codés avec la machine Enigma et envoyés par les autorités allemandes à leurs sous-marins : dans les bulletins météo, ce sont souvent les mêmes mots que l'on retrouve.

Une astuce : nous avons vu dans la fiche n° 3, à propos du tableau de Vigenère, que pour chiffrer un texte nous avons la relation fondamentale :

Clair + Clef = Crypto

qui peut s'écrire : **Crypto – Clef = Clair**

On peut donc écrire le crypto, puis en utilisant un tableau de Vigenère, effectuer des hypothèses de clef qui feraient apparaître dans le clair un mot ayant du sens.

On a aussi la relation :

Crypto – Clair = Clef

cela signifie que l'on peut fonctionner à l'inverse et faire des hypothèses sur des mots probables du message permettant de trouver une clef qui soit un mot qui ait un sens en français. Le système fonctionne dans les deux sens.

b) ***Les lettres du message chiffré sont fréquentes en français***

(présence de E, de voyelles, de S, N, T, R, L ...) et surtout elles sont collées les unes aux autres : il y a de fortes chances que l'on se trouve face à un chiffrement par transposition, avec une grille rectangulaire de transposition (énigmes 14 , 15, 29).

Il faut alors trouver le bon ordre des lettres (voir fiche n° 5). D'abord, il convient de les compter. Le nombre de lettres est souvent le produit du nombre de lignes par le nombre de colonnes du carré ou du rectangle à partir duquel la transposition a été effectuée. Par exemple si l'on trouve 48 lettres, il est possible que le message ait été écrit sur 8 lignes et 6 colonnes (ou 6 lignes sur 8 colonnes). Bien sûr, des lettres nulles ont pu être ajoutées pour compléter le tableau. On écrit le texte en lignes et on essaye de faire apparaître des mots qui ont un sens en lisant en colonnes, ou inversement. Là encore on fonctionne par mots probables ou noms qui pourraient exister dans le message clair.

Si en plus les colonnes ont subi des permutations à partir d'une clef, les choses se compliquent fortement. (voir fiche n° 5).

Les chiffrements par transposition sont assez, voire très difficiles à décrypter (énigmes n° 29, 30 ,31). Elles demandent souvent de longues recherches, il faut faire de nombreuses hypothèses.

- ***L'énigme est constituée de chiffres***

Il faut tout d'abord examiner si l'on est face à un type de codage connu : ASCII, numération binaire, hexadécimale etc.

Si rien d'évident n'apparaît, plusieurs pistes :

- ces nombres sont compris entre 1 et 26, ou 1 et 36 : il faut bien sûr remplacer chaque nombre par une lettre. On raisonne plus facilement sur des lettres que sur des chiffres.

- ils sont plus grands : on peut essayer de les rectifier en modulo 26 ou autre modulo (énigme 32).

- est ce que ces nombres sont divisibles ou sont premiers ?

- est-ce que chaque nombre est constitué de 2 chiffres ? : il peut s'agir de la numérotation de lignes et de colonnes comme dans un carré de Polybe.

Il peut s'agir de nombres et de chiffres : sur l'une des énigmes de ce site, par exemple, les nombres correspondent aux nombres de jours terrestres nécessaires à une planète du système solaire pour effectuer sa révolution autour du soleil et les lettres ne sont pas chiffrées. Une fois la planète trouvée, on prend simplement la 1re lettre de son nom. Astucieux...

En résumé, il convient de faire correspondre ces chiffres à des lettres et avec un peu d'imagination, on trouve des solutions. Quand on a trouvé une série de lettres, on est alors ramené au problème précédent, comme on dit en mathématiques.

- ***L'énigme est constituée de symboles***

Il est vraisemblablement que nous sommes face à une substitution et que ces symboles représentent des lettres. Si ces symboles ne vous sont absolument pas connu (Templiers, Francs-maçons), un copié-collé du texte sur Google peut faciliter les choses. Vous ferez parfois des découvertes !

Comme pour les cas des nombres, *on peut remplacer les symboles par les lettres de l'alphabet* : on réfléchit plus facilement face à des lettres, dans un environnement connu et familier.

Enfin, mais non des moindres, si l'on ne trouve rien, il convient évidemment de consulter ***le forum*** relatif à l'énigme. On y trouve de précieux indices.

3. Le travail en équipe

Le travail en équipe est essentiel. Le concours Alkindi se fait par équipe et si l'on peut s'entraîner en groupe, c'est mieux. C'est une évidence.

Bien sûr, une équipe est fondée sur la complémentarité de ces membres. A ce sujet, vous avez vu à travers les fiches que pour résoudre une énigme, il faut parfois faire un peu de maths, mais qu'il faut également avoir des qualités en matière littéraire. C'est pourquoi il est important d'avoir dans une équipe **des matheux et des littéraire**s : ils sont complémentaires, chacun(e) fera progresser l'équipe grâce à ses compétences dans son domaine.

A Bletchley Park, près de Londres, pendant la Seconde Guerre mondiale, se trouvait le célèbre *Government Code and Cypher School* au sein duquel travaillaient des mathématiciens, des linguistes, un champion de jeu d'échec, des cruciverbistes etc. On y a recruté du personnel à partir de concours de mots croisés publiés dans le quotidien *Daily Telegraph*.

La résolution d'une énigme nécessite également des qualités d'analyse et de synthèse : analyse pour creuser à fond toutes les possibilités, synthèse pour de temps en temps prendre de la hauteur de vue, regarder de façon globale, revenir à l'essentiel. Ces qualités se trouvent plus ou moins développées en chacun(e) d'entre nous, et là encore la complémentarité des participant(e)s à l'équipe sera importante.

4. La question de la vitesse

La vitesse est également essentielle. Bien sûr, elle se travaille et s'acquiert par la pratique. Prenons par exemple ce message fréquent dans les livres traitant de codes secrets :

« Attaquez demain à 5 heures. Signé général Foch »

Si le message est décrypté par l'ennemi le jour de l'attaque vers quinze heures, cela n'a pas beaucoup d' importance. S'il est décrypté à 3 heures du matin, c'est plus ennuyeux…

Les épreuves de la finale du concours Alkindi se déroulent dans un temps très limité et sur ce site, pour s'entraîner, un bonus est donné au premier qui découvre l'énigme.

La vitesse de résolution d'une énigme est très importante. En équipe, on travaille beaucoup plus vite, on parle, on échange, les idées fusent, chacun apporte aux autres et on progresse beaucoup mieux.

5. Conclusion

Axel, l'administrateur principal de ce site, est allé deux fois en finale du Concours Alkindi avec son équipe. Il nous fait part de son expérience dans cette conclusion qu'il a tout spécialement écrite :

Pour résoudre une énigme, il faut se poser un millier de questions qui ont bien été détaillées dans cette fiche. Il faut chercher, se creuser la tête et ça passe souvent par l'utilisation d'un papier et un crayon.

Pour celles et ceux, futurs candidat(e)s du concours Alkindi qui liront cette fiche, il est important de beaucoup s'exercer. Une chose très importante a été dite dans la présentation des fiches : on pourrait comparer la crypto à des maths dans le sens où ça ne vient pas tout seul.

A moins d'être un(e) véritable génie, les mécanismes que vous devrez acquérir pour résoudre les énigmes si vous arrivez à accéder à la finale du concours Alkindi passent par l'entraînement et la répétition. Ça peut paraître difficile au premier abord mais une fois que vous avez franchi ce cap, ça devient génial ;-).

Une dernière chose à ne pas négliger est qu'il y a une grande différence entre décrypter seul et décrypter en équipe. Si vous participez au concours Alkindi en équipe, entraînez-vous évidemment seul pour progresser mais programmez-vous également des séances d'entraînement ensemble, cela est important pour pouvoir vous faire confiance, apprendre à vous dispatcher les tâches et ne pas paniquer le jour de la finale. Croyez-moi, c'est essentiel…

****
*****
***
*