Comment résoudre une énigme ?

Par Claude et Saint Erulo

Vous avez sous les yeux un message codé : une suite de lettres, de chiffres ou de symboles qui ne veulent rien dire. Que faire ? Pendant des siècles, la réponse a été simple : réfléchir, un crayon à la main. Aujourd'hui, on peut aussi s'aider de sites spécialisés, voire d'une intelligence artificielle. Ces outils font pleinement partie de la recherche : certaines énigmes, par exemple celles qui reposent sur de très grands nombres, ne peuvent tout simplement pas être résolues sans une aide extérieure. L'important est de savoir ce qu'on leur demande et de comprendre ce qu'ils répondent. Voici trois façons de chercher, du plus artisanal au plus moderne.

1. Le papier, le crayon et la gomme

C'est la méthode des débutants, et elle reste la meilleure école. Elle consiste à suivre une démarche, un peu comme un enquêteur.

Lire, observer, chercher des points d'accroche

On commence par lire l'énigme deux ou trois fois, sans se précipiter. On lit aussi le titre et les indices : ils donnent le thème de l'énigme, son environnement, et parfois même la clé. Puis on se pose une question simple : est-ce que cela me rappelle quelque chose que j'ai déjà vu ? Souvent, l'énigme « parle » tout de suite : on reconnaît du binaire, du Morse, l'alphabet phonétique… Les cryptanalystes parlent de **points d'accroche** : des détails qui attirent l'œil et rappellent un mécanisme connu. Une suite de nombres qui grandissent de façon bizarre fait penser à la suite de Fibonacci. Une série de nombres inférieurs à 100 avec le mot « éléments » en sous-titre évoque le tableau périodique de Mendeleïev.

Il faut aussi penser aux astuces de présentation : un texte clair écrit à l'envers, ou lu en colonnes de bas en haut, la première ou la dernière lettre de chaque mot, une charade, le cadran d'un vieux téléphone… Quand ces pistes sont éliminées, on se pose la question de fond : s'agit-il d'une substitution, d'une transposition, d'un code, d'un mélange de tout cela ?

Des lettres, des chiffres ou des symboles ?

Si l'énigme est faite de lettres, on les compte, une par une. C'est là que l'analyse de fréquence, inventée par Al-Kindi au IXe siècle, devient un outil précieux. Si certaines lettres reviennent très souvent et d'autres très rarement, on soupçonne une **substitution simple** : on suppose que la lettre la plus fréquente représente le E, puis on avance de proche en proche avec les couples de lettres (ES, LE, DE…) et les petits mots. Si, au contraire, toutes les lettres sont réparties à peu près uniformément, il s'agit sans doute d'une **substitution avec clé** de

type Vigenère, où une même lettre est chiffrée de plusieurs façons. Enfin, si les lettres ont les fréquences normales du français (beaucoup de E, de S, de A…) mais que le texte ne veut rien dire, c'est probablement une **transposition** : les lettres sont les bonnes, mais mélangées.

Attention : une analyse de fréquence n'a de sens que si le message est assez long. Sur quelques mots, elle ne sert à rien.

En cas de transposition, le nombre de lettres est un indice précieux. Il est souvent le produit du nombre de lignes par le nombre de colonnes d'un rectangle : 48 lettres, par exemple, peuvent avoir été écrites sur 6 lignes et 8 colonnes, ou l'inverse, avec parfois quelques lettres « nulles » ajoutées pour compléter. On écrit alors le texte en lignes et on essaie de lire en colonnes (ou l'inverse), en cherchant à faire apparaître des mots.

Si l'énigme est faite de chiffres, on regarde d'abord s'il s'agit d'un codage connu : binaire, ASCII, hexadécimal. Sinon, on essaie plusieurs pistes. Les nombres sont-ils compris entre 1 et 26 ? Il suffit alors de les remplacer par des lettres, car on raisonne bien plus facilement sur des lettres que sur des nombres. Sont-ils plus grands ? On peut les ramener à des nombres compris entre 1 et 26 en calculant leur reste dans une division par 26 (c'est ce qu'on appelle « modulo 26 »). Chaque nombre est-il fait de deux chiffres ? Il peut s'agir d'un numéro de ligne et d'un numéro de colonne, comme dans le carré de Polybe. Et il faut toujours se demander si ces nombres sont premiers ou divisibles par quelque chose : certaines énigmes jouent là-dessus. Dès qu'on a obtenu des lettres, on est ramené au cas précédent.

Si l'énigme est faite de symboles, on est très probablement face à une substitution où chaque symbole représente une lettre. On peut les remplacer par des lettres pour réfléchir dans un environnement plus familier. Et si les symboles évoquent quelque chose (le chiffre des Templiers, celui des francs-maçons…), un simple copier-coller dans un moteur de recherche permet parfois de faire de belles découvertes.

Le tableau ci-dessous résume ces premiers réflexes.

Ce que l'on observe	Hypothèse	Premier réflexe
Des lettres, certaines très fréquentes, d'autres rares ; les mots sont séparés	Substitution simple (César, alphabet inversé, alphabet mélangé…)	Compter les lettres, supposer que la plus fréquente est un E, tester les décalages de César
Des lettres réparties à peu près uniformément	Substitution avec clé (type Vigenère)	Chercher des mots probables, tester des clés suggérées par le titre et les indices
Des lettres aux fréquences normales (beaucoup de E, S, A, N, T, R…), mais un texte incompréhensible	Transposition	Compter les lettres, chercher les dimensions d'un rectangle, repérer des fragments de mots
Des nombres de 1 à 26 (ou de 1 à 36)	Une lettre par nombre (rang dans l'alphabet)	Remplacer chaque nombre par une lettre

Ce que l'on observe	Hypothèse	Premier réflexe
Des nombres de deux chiffres (ligne, colonne)	Carré de Polybe	Dessiner la grille 5 × 5
Des 0 et des 1, ou des nombres inférieurs à 128	Binaire, ASCII, hexadécimal	Utiliser une table de conversion
Des symboles	Substitution	Les remplacer par des lettres ; essayer un copier-coller sur un moteur de recherche

Les mots probables

Quand on a une hypothèse sur le mode de chiffrement, la recherche de **mots probables** est l'une des armes les plus efficaces. Il est souvent plus facile de s'attaquer au début ou à la fin du message : un texte commence volontiers par « bonjour » ou « cette énigme », et se termine par « la solution est » ou par une signature. Le contexte (le titre, les indices, la personne qui a écrit l'énigme) fournit aussi des mots et des clés possibles. C'est ainsi que les messages d'Enigma ont pu être attaqués : les bulletins météo envoyés aux sous-marins allemands contenaient souvent les mêmes mots.

Pour un chiffrement de type Vigenère, où la clé s'ajoute au message lettre à lettre, une petite relation est très utile : *clair* + *clé* = *chiffré*, donc *chiffré* − *clé* = *clair* et *chiffré* − *clair* = *clé*. Si l'on devine un mot du message, on peut en déduire un morceau de la clé ; et si l'on devine la clé, on retrouve le message. Cette relation ne vaut que pour ce type de chiffrement : dans une transposition avec clé, par exemple, la clé ne s'ajoute pas aux lettres, elle sert à remettre les colonnes dans l'ordre.

Ne pas rester seul

Enfin, on n'est pas obligé de chercher seul. Quand on est bloqué, le forum de l'énigme contient souvent de précieux indices. Au Concours Alkindi, on travaille en équipe, et c'est un atout : les matheux et les littéraires ne voient pas les mêmes choses, et les idées fusent plus vite quand on parle. La vitesse compte aussi, et elle s'acquiert par l'entraînement.

Une fois le principe identifié, on décrypte à la main, en tâtonnant, en faisant des hypothèses, en les effaçant et en recommençant. C'est long, parfois frustrant, mais c'est là qu'on comprend vraiment comment fonctionne un chiffrement.

2. Les sites spécialisés

Quand on est plus aguerri, et qu'on est las de décrypter à la main, on peut se tourner vers des sites comme **dcode.fr** ou **Cryptocrack**. Dcode, en particulier, est très efficace pour les francophones et vient à bout de beaucoup d'énigmes. Sa logique est classique : on passe d'abord par la page d'identification du chiffrement (https://www.dcode.fr/identification-chiffrement), qui propose les modes de chiffrement les plus probables, puis on se rend sur la page dédiée au chiffrement trouvé pour effectuer le décryptage.

Dcode n'est pas seulement un outil, c'est aussi une source de cours. Chaque page consacrée à un chiffrement explique son principe, son histoire, la façon de chiffrer et de déchiffrer, et

donne des exemples. C'est une bonne manière d'apprendre en pratiquant : on essaie l'outil, puis on lit l'explication pour comprendre ce qu'il vient de faire. Le site propose aussi des outils plus généraux, comme la décomposition d'un nombre en facteurs premiers, la conversion en ASCII ou l'analyse de fréquence.

Certaines énigmes sont même impossibles sans lui. L'exercice n° 7 de la finale du Concours Alkindi de 2019 se présentait comme un tableau de chiffres, qui forment ensemble un nombre de 281 chiffres. Pour le résoudre, il faut décomposer ce nombre en 67 facteurs premiers, calculer le rang de chacun dans la liste des nombres premiers, faire la différence entre chaque rang et le précédent, et reconnaître alors des codes ASCII qui donnent le message. Personne ne fait cela à la main ! Mais encore faut-il avoir l'idée de la méthode, et savoir quels outils demander à quel site.

L'avantage des sites spécialisés est la rapidité. Le piège est de cliquer sans comprendre : un site ne vous dit pas quel chiffrement il faut chercher, il vous propose des pistes. Si l'on ne sait pas pourquoi l'outil propose telle ou telle piste, on ne progresse pas, et on est perdu dès que l'énigme sort un peu des sentiers battus.

3. L'intelligence artificielle

Troisième étape : l'IA. On peut lui donner le texte de l'énigme et la laisser se débrouiller, ce qui convient très bien quand on ne sait pas programmer. On peut aussi procéder en deux temps, comme le font certains programmeurs : demander à l'IA d'identifier le mode de chiffrement, puis lui demander d'écrire un script Python qui effectue le décryptage.

Mais l'intérêt principal de l'IA est ailleurs : contrairement à un site qui donne un résultat brut, elle **explique son raisonnement**. On peut lui demander pourquoi elle pense à tel chiffrement, comment elle a trouvé la clé, ce qu'on aurait pu remarquer soi-même. C'est une occasion de réfléchir et d'approfondir ses connaissances en cryptographie. On peut aussi lui demander seulement des **pistes**, sans la solution : « Qu'est-ce que je devrais observer en premier ? », « Cette répartition de lettres te fait penser à quoi ? » L'IA devient alors un entraîneur plutôt qu'un solveur.

Pourquoi les programmes sont importants

Demander un programme à l'IA présente un double avantage. D'abord, on peut le relire, le comprendre, le modifier, le réutiliser pour une autre énigme : c'est une vraie méthode de travail, qui reste après la solution. Ensuite, c'est plus fiable. Un programme calcule de façon exacte, alors qu'une IA qui « réfléchit » sur des lettres peut se tromper en recopiant ou en comptant. Le programme sert donc de preuve : si le texte obtenu est du français lisible, la solution est bonne.

Certains programmes reposent sur des idées très astucieuses. Prenons une substitution simple, où chaque lettre est remplacée par une autre. Le nombre de clés possibles est de $26 \times 25 \times 24 \times \dots \times 1$, soit un nombre de 27 chiffres : impossible de toutes les essayer. Une méthode célèbre permet pourtant de retrouver la bonne clé en quelques secondes : le **recuit simulé**.

Son nom vient de la métallurgie : pour qu'un métal prenne une structure stable, on le chauffe, puis on le refroidit très lentement, ce qui laisse aux atomes le temps de s'organiser. Le programme fait de même avec la clé :

1. On part d'une clé prise au hasard, un alphabet de substitution quelconque.
2. On déchiffre le message avec cette clé et on donne une note au résultat : plus le texte ressemble à du français (groupes de lettres fréquents comme ES, LE, ENT, TION…), meilleure est la note.
3. On modifie un tout petit peu la clé, par exemple en échangeant deux lettres.
4. Si la note s'améliore, on garde la modification. Si elle baisse, on la garde quand même de temps en temps. Cette tolérance est grande au début (on dit que la « température » est élevée), puis diminue peu à peu.
5. On recommence des milliers de fois, en « refroidissant » progressivement. À la fin, la clé se stabilise : si le texte est assez long, c'est la bonne, et le message devient lisible.

Pourquoi accepter parfois de faire des erreurs ? Imaginez un randonneur qui cherche le sommet le plus haut dans le brouillard et qui monte toujours dans la direction la plus pentue. Il risque de s'arrêter au sommet d'une petite colline, sans jamais atteindre la vraie montagne. En acceptant de redescendre de temps en temps, le programme évite de rester coincé sur une « fausse bonne solution ». C'est aussi une belle idée à retenir pour les énigmes : quand on est bloqué, il faut parfois oser abandonner une piste qui semblait prometteuse.

On reconnaît dans cette méthode l'esprit d'Al-Kindi : on s'appuie sur les statistiques de la langue. La différence, c'est que l'ordinateur peut faire des milliers d'essais là où le cryptanalyste du IXe siècle comptait à la main. Et le même principe fonctionne pour d'autres chiffrements, comme la transposition avec clé. Il est tout à fait possible de demander à une IA : « Écris-moi un programme Python qui casse une substitution simple par recuit simulé, et explique-moi chaque étape. » C'est un excellent exercice pour comprendre à la fois la cryptographie et la programmation.

Un débutant doit-il passer par ces trois phases ?

Je réponds oui, et dans cet ordre, mais sans en faire un dogme. Un collégien ou un lycéen qui commence par l'IA risque d'obtenir la solution sans rien apprendre, et de se retrouver démuni le jour où l'outil n'est pas disponible. Les épreuves elles-mêmes peuvent d'ailleurs limiter les moyens autorisés : mieux vaut s'entraîner à la main pour être à l'aise le jour J. Celui qui a d'abord compté des lettres, testé des décalages et buté sur une impasse comprend, lui, ce que l'outil fait à sa place.

Il n'est pas nécessaire non plus de rester des heures sur la phase 1. Quelques énigmes à la main suffisent à acquérir les bons réflexes. Ensuite, les sites spécialisés et l'IA deviennent de vrais accélérateurs, et parfois la seule porte d'entrée, à condition de toujours chercher à comprendre la réponse.

Conclusion

Papier-crayon, sites spécialisés, intelligence artificielle : ces trois approches ne s'opposent pas, elles se complètent. La première forme l'esprit, la deuxième fait gagner du temps, la troisième aide à comprendre et à progresser. Pour vous qui vous préparez au Concours Alkindi, le meilleur conseil est sans doute celui-ci : **essayez d'abord seul, puis servez-vous des outils pour vérifier, comprendre et aller plus loin.** Le plaisir de résoudre les énigmes est à ce prix.

****

*****

***

*

2026 – clubalkindi.com – Tous droits réservés