Livret Escape Game de Noël

M.Breuillé-Jean

Décembre 2018

Table des matières

Chapitre 1

L'histoire

Enfer et damnation, le Père Noël a disparu !

C'est la stupeur à travers le monde. A quelques jours de Noël, le célèbre barbu au costume rouge n'est toujours pas revenu de ses vacances, entamées au lendemain de Noël dernier. Les derniers espoirs de l'humanité toute entière reposent sur les épaules de quelques lutins, au collège Henri IV de Poitiers, en France. Des indices ont été retrouvés qui pourraient mener au Père Noël, ce dernier les ayant visiblement semés intentionnellement pour être retrouvé... Les lutins sauront-ils relever le défi ?

Chapitre 2

Le Livret

Dans ce livret, vous pourrez trouver quelques informations utiles pour résoudre certaines énigmes. Mais attention, tout n'est pas forcément nécessaire non plus ! Une tablette est de plus à votre disposition, avec un accès internet. Fouillez, lisez, cherchez, les solutions sont peut-être sous vos yeux. Des indices peuvent aussi être demandés au maître du jeu, si vous vous retrouvez dans une impasse à un moment donné. Mais il faudra savoir le convaincre si vous souhaitez obtenir une aide de sa part !

Chapitre 3

Quelques codes

La cryptographie est une discipline s'attachant à protéger des messages en s'aidant de secrets ou de clés. Cette science s'est développée au fil des siècles dans des cadres souvent conflictuels (guerres, complots,...) : il était nécessaire de transmettre des informations entre différentes personnes de telle sorte que si le message était intercepté par l'ennemi, celui-ci ne puisse pas le déchiffrer. Il fallait donc coder le message et faire en sorte que seul le destinataire soit capable de le décoder. Ces techniques de codages et de décodages ont très vite fait intervenir des outils mathématiques. Aujourd'hui, l'essentiel des données numériques sont codées et utilisent des techniques de pointe des mathématiques (par exemple pour protéger les données bancaires). Il a même été dit que si la première guerre mondiale avait été celle des chimistes (premières utilisations d'armes chimiques), la deuxième guerre mondiale celle des physiciens (utilisation de la bombe atomique), la troisième guerre mondiale serait celle des mathématiciens, car les mathématiciens auraient le contrôle de ce qui est essentiel dans une guerre : l'information et la transmission d'informations.

Les premières méthodes employées pour transmettre des messages secrets faisaient appel à la stéganographie. La stéganographie consiste à cacher l'existence du message, par exemple en utilisant des encres invisibles. De nombreuses méthodes plus folles les unes que les autres ont été utilisées dans ce cadre. Il a par exemple été rapporté une histoire dans la Grèce Antique où le messager avait eu le message écrit sur son crâne rasé. L'expéditeur

du message avait alors attendu que les cheveux repoussent, et le messager avait pu voyager sans aucun problème. Arrivé au destinataire du message, il n'avait eu qu'à se raser à nouveau le crâne pour transmettre le message.
Le problème de la stéganographie, aussi intelligente que soit la méthode de dissimulation du message, est que si le message est intercepté, alors l'ennemi n'a aucune difficulté à l'interpréter, le message étant écrit normalement. C'est dans ce cadre qu'est apparue la cryptographie, science qui consiste à coder un message. Le message peut ensuite être dissimulé, bien sûr, mais le grand intérêt est que si par malheur l'ennemi l'intercepte, il aura du mal à le décoder s'il ne possède pas le système de décodage. Ces derniers siècles ont donc vu s'affronter deux catégories de personnes : celles créant les codes (les cryptographes), codes de plus en plus complexes, et celles cherchant à "casser" ces codes (les cryptanalystes), autrement dit celle cherchant des techniques rapides permettant de décoder des messages interceptés. Aujourd'hui, les techniques sont très évoluées et constituent une branche à part entière des mathématiques. Il est maintenant très difficile, voire impossible, de décoder un message si on ne possède pas la "clé" pour le faire, et la cryptographie est devenue un des nombreux terrains de jeux des mathématiciens. Mais ce ne fut pas toujours le cas, et quelques méthodes simples, qui furent utilisées par exemple par Jules César ou par Marie Stuart, dernière reine d'Ecosse, peuvent être suffisantes à notre niveau pour coder efficacement un message.

3.1 La Transposition

La transposition est une méthode de codage qui consiste juste à mélanger les lettres du message. Cette méthode par transposition est terriblement efficace pour coder un message, tellement efficace que si la transposition est faite de façon aléatoire sur un message plus long qu'un unique mot, il devient quasiment impossible à l'ennemi comme au destinataire de le déchiffrer. Cette méthode n'est donc pas satisfaisante : il faut que le destinataire

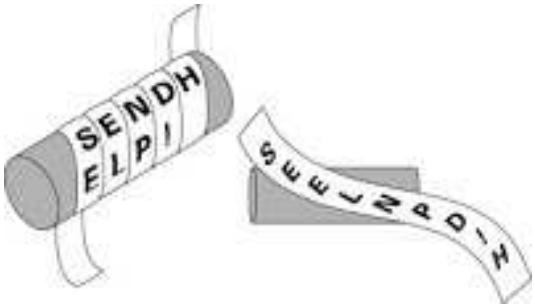
soit capable de comprendre le message ! Une méthode plus efficace serait donc de procéder par transposition, mais pas de façon aléatoire, comme l'explique Simon Singh dans son livre The Code Book :

"Pour que la transposition soit efficace, l'ordonnancement des lettres doit suivre un système rigoureux, sur lequel expéditeur et destinataire se sont préalablement entendus. Les écoliers s'amusent ainsi à s'envoyer des messages avec une transposition dite " en dents de scie ". Il s'agit d'écrire le message sur deux lignes, une lettre sur la ligne supérieure, une lettre sur la ligne inférieure. On enchaîne ensuite la suite des lettres de la ligne inférieure à celle de la ligne supérieure, pour réaliser le message crypté, comme ci-dessous :

TON SECRET EST TON PRISONNIER ; S'IL FUIT TU DEVIENDRAS SON PRISONNIER

TNERTSTNRSNIRIFITDVEDASNRSNIROSCEETOPIONESLUTUEIS

Il existe bien sûr beaucoup d'autres méthodes de transpositions, on peut par exemple utiliser un outil appelé scytale permettant de coder puis de décoder un message.



Ces méthodes de transpositions sont toutefois peu utilisées. On leur préfère souvent des méthodes de substitution.

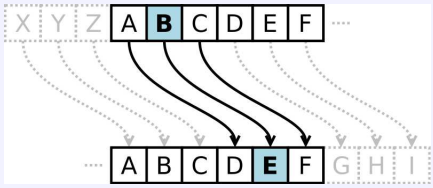
3.2 La substitution

La méthode par substitution consiste à coupler les lettres de l'alphabet et à remplacer chaque lettre du message par sa lettre partenaire. Par exemple, le A est remplacé par un T, le B par un F, le C par un U, etc, de telle sorte que chaque lettre est codée de façon unique (il ne sera pas possible que A soit codé en T et L soit codé aussi en T, sinon le message ne pourrait pas être décodé de façon certaine). Afin de pouvoir déchiffrer un message codé par substitution, il faut donc connaître la clé, c'est à dire savoir quelle lettre remplace quelle autre lettre. Notre alphabet possédant 26 lettres, il existe 400 000 000 000 000 000 000 000 000 façons de coupler les lettres. Autant dire que si on ne possède pas la clé, il semble impossible de tester toutes les combinaisons possibles afin de trouver le bon code et de déchiffrer le message ! Ce type de codage a donc été utilisé pendant de nombreux siècles, car il était facile à utiliser et semblait impossible à casser à moins de connaître la clé. Mais les codes les plus simples utilisent juste un décalage des lettres de l'alphabet.

3.2.1 Codes César

Principe :

Une des méthodes de substitution les plus célèbres fut utilisée par Jules César. Il l'utilisait avec un décalage de trois sur la droite pour ses correspondances secrètes.



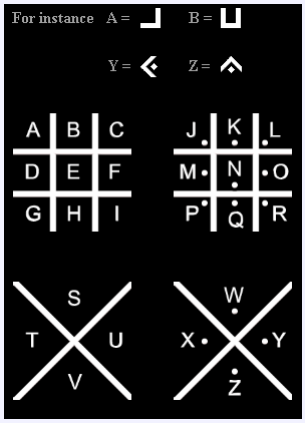
Avec ce principe,
la phrase : « L'attaque aura lieu demain à l'aube. »
devient : « O DWWDTXH DXUD OLHX GHPDLQ O DXEH. »

Pour décrypter ensuite le message, il s'agit de décaler les alphabets de trois sur la gauche. Une roue de César peut être utilisée à cet effet pour gagner du temps.

3.2.2 Code Pig Pen

Principe :

Le code Pig Pen est un code qui était utilisé par les Francs-Maçons, notamment, au 18ème siècle, afin de garder leurs documents secrets. Ce code ne remplace par une lettre par une autre, mais échange chaque lettre par un symbole. L'alphabet est écrit dans une grille, puis chaque lettre est codée en étant remplacée par le symbole correspondant à sa case dans la grille. Voici les grilles :



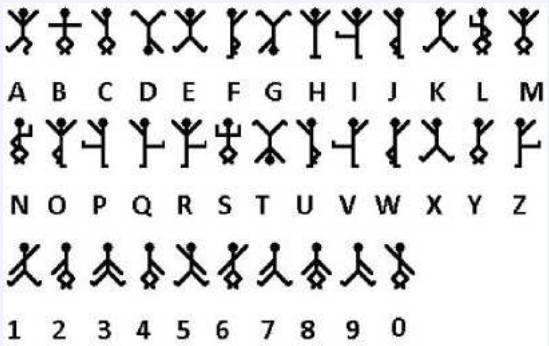
Et voici un exemple de message codé avec cette méthode :

3.2.3 Code des Hommes Dansants

Principe :

L ?intrigue de la nouvelle Les Hommes dansants repose sur une énigme cryptographique.

Ce codage est issu d'une nouvelle d'Arthur Conan Doyle. Dans cette nouvelle, Sherlock Holmes réussit à briser le code des messages chiffrés qui terrifient la femme de son client. Ces messages sont composés de suites de symboles différents, en forme de personnages (appelés stickmen) agitant les bras et les jambes, parfois munis de petits drapeaux : les "hommes dansants".



Sherlock Holmes parvient à comprendre la signification de ces séries de dessins en étudiant les fréquences d'apparition de chaque personnage, selon la méthode de l'analyse fréquentielle. Le chiffre de ce cryptogramme est en fait très simple. Il s'agit d'une substitution alphabétique : chaque petit personnage représente une lettre. L'intérêt de ce chiffre est sa discrétion : utilisé dans des messages gribouillés sur des murs ou des bouts de papier, il passe inaperçu car on peut le prendre pour un dessin d'enfant, ce que fait d'abord le docteur Watson, bien sûr ! Ces gribouillis sont en fait une forme de stéganographie, l'art de rendre anodins les messages les plus secrets.

Chapitre 4

Quelques distances

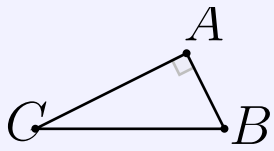
Voici quelques distances entre certaines villes à travers le globe.

Rio de Janeiro	*Londres*	*9320 km*
Bangkok	*Tokyo*	*4600 km*
Tokyo	*Moscou*	*7500 km*
New York	*Moscou*	*8500 km*
New York	*Lisbonne*	*5500 km*
Le Caire	*Bangkok*	*7300 km*
Le Caire	*Moscou*	*3600 km*
Lisbonne	*Londres*	*1600 km*
Londres	*Moscou*	*2500 km*
Tokyo	*New York*	*10900 km*
Londres	*Athènes*	*2400 km*
Le Caire	*Athènes*	*1100 km*
San Francisco	*Moscou*	*9500 km*
San Francisco	*Bangkok*	*12800 km*
Lisbonne	*Athènes*	*2800 km*
San Francisco	*New York*	*4200 km*
Rio de Janeiro	*Moscou*	*11600 km*
Rio de Janeiro	*Tokyo*	*18600 km*

Chapitre 5

Un peu de maths...

Théorème de Pythagore :

> *Un triangle est rectangle si et seulement si le carré de la longueur de l'hypoténuse est égal à la somme des carrés des longueurs des côtés de l'angle droit.*
>
> *On considère un triangle ABC de plus grand côté BC*
>
> 
>
>
> *ABC est un triangle rectangle en A si et seulement si on a : $AB^2 + AC^2 = BC^2$*

Théorème de Thalès :

- *Si on choisit ABC et AMN deux triangles tels que :*

$$\begin{cases} M \in (AB) \\ N \in (AC) \\ (BC)//(MN) \end{cases}$$

alors, d'après le théorème de Thalès, on a : $\dfrac{AM}{AB} = \dfrac{AN}{AC} = \dfrac{MN}{BC}$.

- *On choisit ABC et AMN deux triangles tels que : A, M, B et A, N, C sont alignés dans cet ordre et* $\dfrac{AM}{AB} = \dfrac{AN}{AC}$. *On sait alors que, d'après la réciproque de Thalès, (MN) et (BC) sont parallèles.*

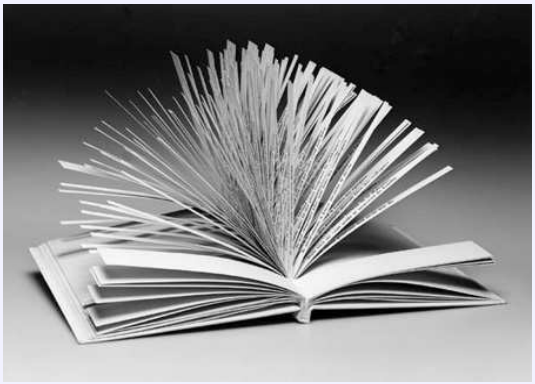
Nombres premiers :

- *On appelle nombre premier tout nombre entier naturel qui admet exactement deux diviseurs positifs distincts :* 1 *et lui-même.*

- $2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37,$ *... sont des nombres premiers : ils n'admettent pas de diviseurs en dehors de* 1 *et d'eux mêmes.*
- *Tout nombre entier supérieur ou égal à* 2 *peut s'écrire de façon unique comme un produit de nombres premiers.*

Chapitre 6

Et la littérature ?

> *Raymond Queneau (1903-1976) est un auteur français adepte des performances littéraires. Parmi ses oeuvres les plus célèbres figurent "Zazie dans le métro" ou encore "Figures de styles". Queneau était aussi féru de mathématiques combinatoires. Son ouvrage "Cent mille milliards de poèmes" est le fruit de la réunion des ses deux passions. "Cent mille milliards de poèmes" est un livre-objet qui offre au lecteur la possibilité de combiner lui-même des vers de façon à composer des poèmes de quatorze vers. Cent mille milliard est le nombre de combinaisons possibles calculé par Raymond Queneau. Mais est-ce bien vrai, autant de poèmes dans un si petit livre ? Les curieux pourront chercher...*
>
> 
>
> *Ce site internet permet de réaliser les combinaisons en ligne :*
> *http ://www.bevrowe.info/Poems/Copy%20of%20QueneauRandom.htm*