La cryptographie pour les enfants
(et les plus grands!)

Sans ordinateur
Sans imprimante

Par Pierre-Marie Lore
Avril 2020

Un peu de vocabulaire

En français, crypto- est un préfixe provenant de la racine grecque (kruptos) qui signifie « caché ». « Graphie » provient également du grec et signifie écrire. La cryptographie est en effet aussi vieille que l'écriture qui marque l'Antiquité. Elle est au cœur de grands moments de l'Histoire. Avec l'apparition de l'informatique, les techniques cryptographiques ont été automatisées mais les fondamentaux restent souvent les mêmes. Aujourd'hui ces procédés assurent notamment la confidentialité de nos données, de nos échanges, bref de tout ce que l'on souhaite garder secret!

Quelques mots souvent utilisés en cryptographie

Chiffrer – Transformer un message clair afin de le rendre illisible pour celui qui ne possède pas la clé. En cryptographie, on ne parle pas de « coder » ou de « crypter » un message.

Clé – Il s'agit de nombres ou de lettres permettant de chiffrer ou de déchiffrer l'ensemble d'un message. N'oublie donc pas de bien la protéger!

Cryptanalyser – Analyser un message chiffré afin d'accéder au texte en clair, sans en posséder la clé. On peut dire aussi « décrypter ».

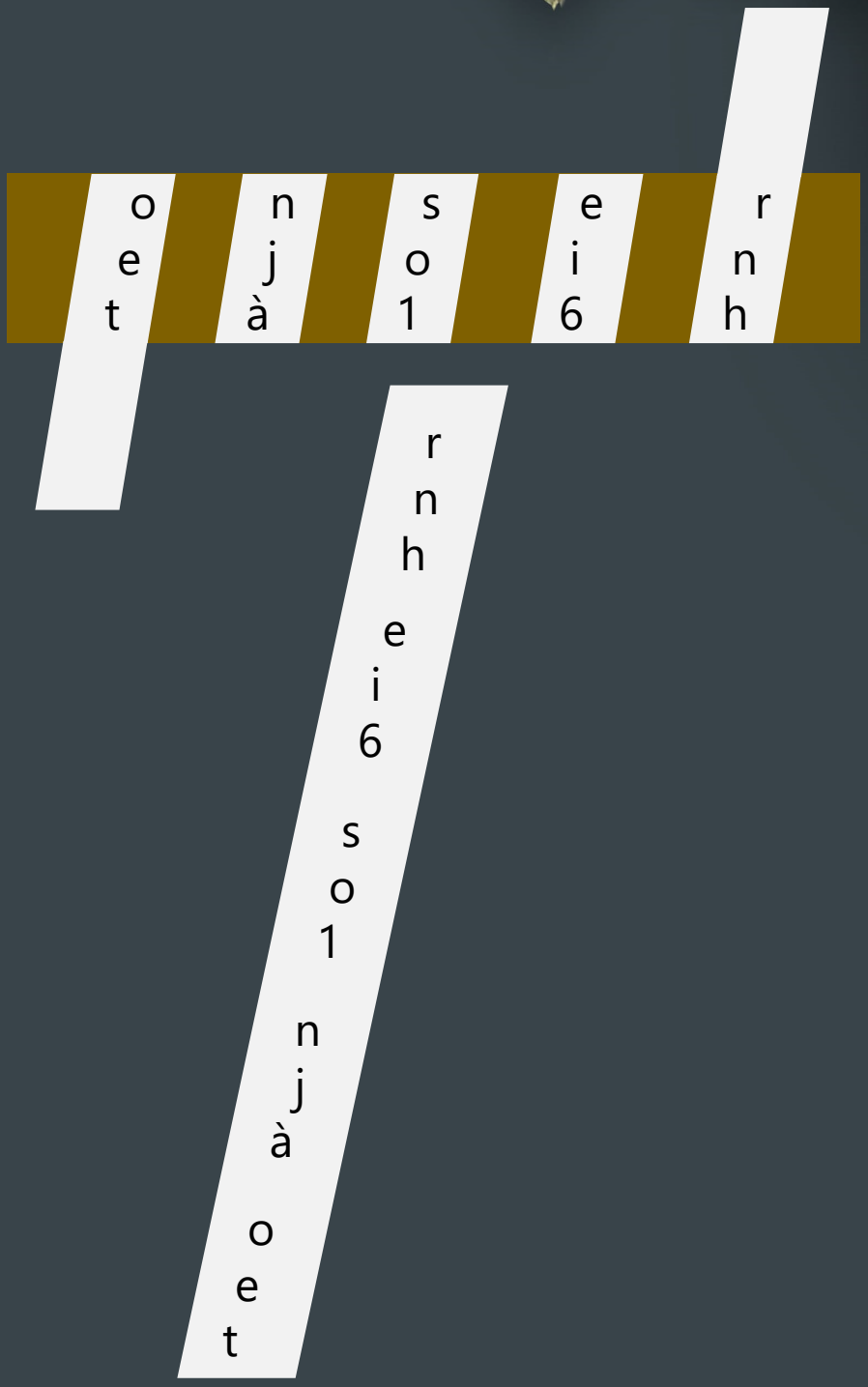
Cryptogramme – Message chiffré.

Déchiffrer – Effectuer l'opération inverse de chiffrer, à l'aide d'une clé que l'on possède légitimement.

La Scytale

Histoire

La Scytale désigne un bâton de bois utilisé par les Spartiates pour chiffrer des messages militaires. La ceinture de cuir des combattants était enroulée sur celui-ci puis un texte y était inscrit. Déroulée, la lanière de cuir faisait apparaître un message difficile à interpréter.... Sa création remonte à plusieurs siècles avant notre ère!



Principe

1. Enroule un ruban (ex: papier, tissu) sur un crayon ou un bâton quelconque.

2. Inscris le message de la gauche vers la droite en plaçant une lettre à chaque fois. Le message peut être écrit sur plusieurs lignes.

3. Déroule le ruban. Le message est méconnaissable!

4. Pour le déchiffrer, il faut l'enrouler à nouveau. Mais attention, le destinataire doit possèder un bâton de même diamètre!

Exemple

La phrase « On se rejoint à 16h » est méconnaissable une fois le ruban déroulé!

Le Parc à cochons

Histoire

Le Parc à cochons était utilisé par des sociétés secrètes autour du XVIe siècle. Il fût même repris au cours de la guerre d'indépendance des États-Unis de 1775 à 1783. Son nom vient du fait que l'on place les lettres de l'alphabet dans des cases qui rappellent les… parcs à cochons!

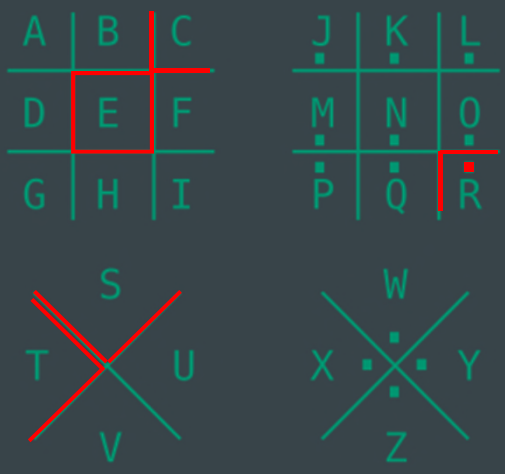
Principe

1. Placer l'alphabet dans l'ordre ou dans le désordre dans des « parcs » (dans ce cas, il faut s'assurer que la personne qui déchiffre possède cette grille).

2. On obtient cette grille (ci-contre).

3. Pour chiffrer un message, on conserve la partie de la grille dans laquelle est logée la lettre.

4. Pour chiffrer, faisons l'opération inverse.



Exemple

Pour chiffrer le mot « SECRET », les symboles correspondants sont 

Non, ce n'est pas un message extra-terrestre !

La grille simple

Principe

1. Dessine un tableau suffisamment grand pour contenir ce que tu souhaites chiffrer.

2. Place les lettres dans chaque case du tableau dans le sens de l'écriture (de la gauche vers la droite).

3. Pour écrire la phrase chiffrée, il suffit de sélectionner les lettres de haut en bas.

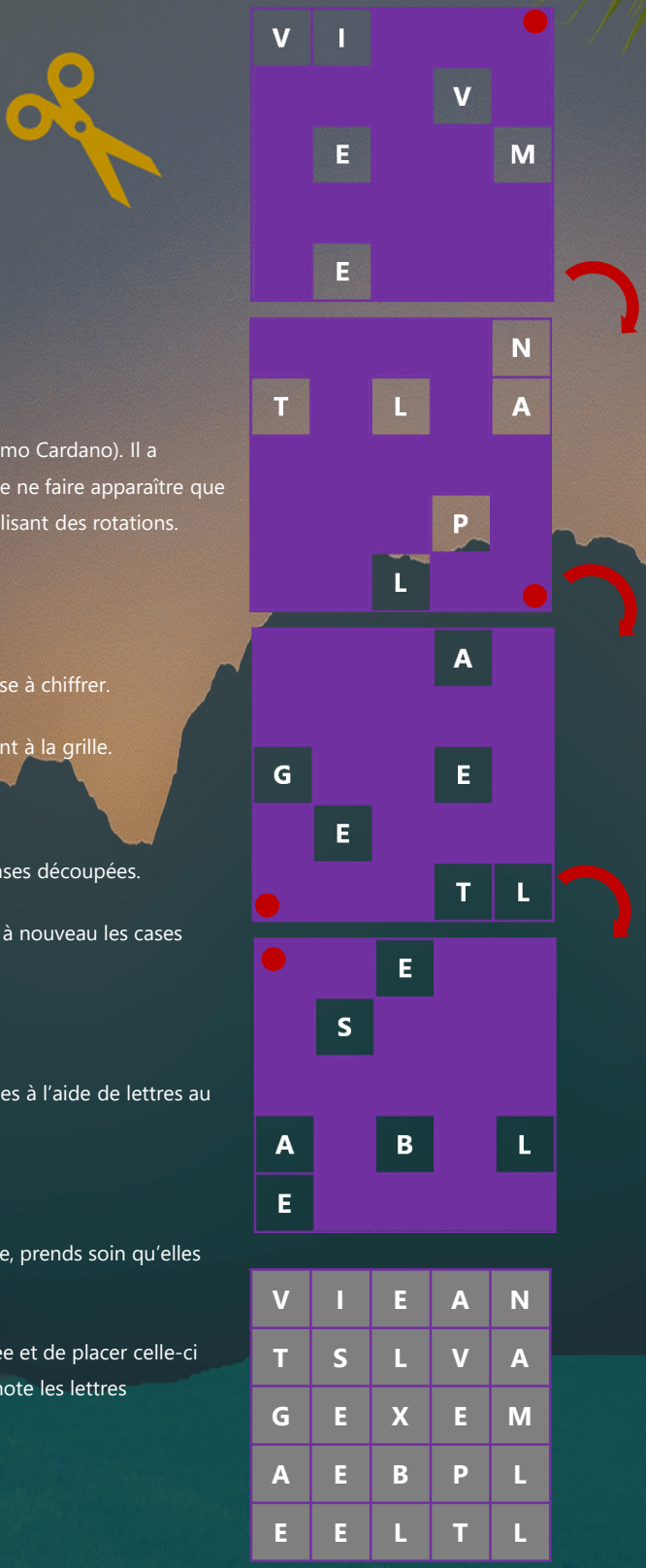
4. Pour déchiffrer, il suffit décrire les groupes de lettres dans chaque colonne.

J	**E**	**S**	**U**
I	**S**	**C**	**A**
C	**H**	**E**	**I**
C	**I**		

Exemple

Pour chiffrer la phrase « JE SUIS CACHE ICI », on écrit les lettres de gauche à droite puis on sélectionne les lettres de haut en bas dans les colonnes. Le cryptogramme est alors « JICC – ESHI – SCE – UAI ».

La grille de Cardan



Histoire

Jérôme Cardan était un scientifique italien du 16e siècle (Gerolamo Cardano). Il a d'abord inventé le principe d'une grille cartonnée permettant de ne faire apparaître que certains mots dans un texte. D'autres variantes ont été crées utilisant des rotations.

Principe

1. Trace une grille carrée pouvant contenir les lettres de la phrase à chiffrer.

2. Découpe des cases dans une feuilles cartonnée correspondant à la grille.

3. Place la feuille cartonnée sur la grille.

3. Écris les premières lettres de la phrase sur la grille dans les cases découpées.

4. Tourne la feuille cartonnée d'un quart de tour puis complète à nouveau les cases vides avec les lettres suivantes de la phrase.

5. Répète l'opération encore deux fois.

6. Retire la feuille cartonnée et remplie les éventuelles cases vides à l'aide de lettres au hasard.

Ton texte est totalement mélangé sur la grille!

Attention, lorsque tu découpes les cases dans la grille cartonnée, prends soin qu'elles ne se recouvrent pas lors des rotations.

Pour déchiffrer, il te suffit de posséder la même feuille cartonnée et de placer celle-ci sur la grille chiffrée en effectuant les rotations. Sur une feuille, note les lettres découvertes au fur et à mesure.

V	I	E	A	N
T	S	L	V	A
G	E	X	E	M
A	E	B	P	L
E	E	L	T	L

Exemple

Dans l'exemple ci-dessus, la phrase en clair est « VIVEMENT LA PLAGE ET LE SABLE ». La lettre X a été ajoutée dans la case vide au milieu.