

Queste de savoir

C'est toute une histoire : la cryptographie - Partie 2/3

12 août 2019

Table des matières

1.	Les Temps modernes	1
1.1.	Trithème	1
1.2.	Les bilitères de Bacon ou le chiffrement shakespearien	6
1.3.	Le Grand Chiffre de Rossignol père & fils	9
2.	Sources et liens	10
	Contenu masqué	10

Après le premier article paru il y a peu (que vous pouvez trouver [ici](#)  , voici le deuxième volet ! Ici seront abordées les méthodes utilisées pendant les Temps modernes (pour garder une suite temporelle logique) à savoir les tables trithémiennes, la stéganographie, les bilitères de Bacon, le Grand Chiffre et d'autres.

Bonne lecture à vous !

1. Les Temps modernes

Nous avons, dans le volet précédent, tracé (vite, certes) un tour d'horizon de l'avancée de la cryptographie au Moyen Âge, mais cette période est réputée pour ne pas être la plus fructueuse de l'Histoire. Rassurez-vous : vous aurez largement plus à vous mettre sous la dent avec la période qui suit. Les Temps modernes ont amené pas mal de nouveautés.

1.1. Trithème

Seulement 50 ans après Alberti (ce n'est pas grand-chose, mais c'est suffisant pour changer d'époque!), Trithème, qui était un abbé à Würzburg (prononcé *Vurtsbourgue*), ville de l'actuelle Allemagne située entre Francfort et Nuremberg, a fait beaucoup parler de lui à propos des chiffrements. Il a commencé par reprendre l'idée des carrés de Polybe pour les *améliorer*, et ensuite il a fait connaître la stéganographie. Si vous ne savez pas ce que c'est, ce n'est pas grave, c'est même probablement pour ça que vous êtes là !

1.1.1. Les tables rectangulaires de substitution

Commençons par parler des tables rectangulaires de substitution étant donné que c'est une inspiration des carrés de Polybe et du chiffre de César (lui-même, rappelons-le, inspiré du chiffrement hébreu **Albam**). Pour les tables rectangulaires, il vous faut un certain nombre de lignes et de colonnes (qui sont équivalentes¹ et qui correspondent à la longueur de l'alphabet). Dans ces lignes/colonnes, placez chaque lettre de l'alphabet de la sorte :

1. Les Temps modernes

	A	B	C	D	...	X	Y	
A								
B								
C								
D								
...								
Z								

Ensuite, sur chaque ligne, écrivez la version de l'alphabet commençant par la lettre de la ligne. Donc, commencez par l'alphabet commençant par A :

	A	B	C	D	...	X	Y	
A	A	B	C	D	...	X	Y	Z
B								
C								
D								
...								
Z								

Ensuite, sur la ligne suivante, écrivez la version de l'alphabet commençant par B. Vous devriez obtenir ceci :

	A	B	C	D	...	X	Y	
A	A	B	C	D	...	X	Y	Z
B	B	C	D	...	X	Y	Z	A
C								
D								
...								
Z								

1. Les Temps modernes

Recommencez pour l'alphabet commençant par C, puis D, etc. Voilà un tableau de rempli :

© Contenu masqué n°1



Bon on vous l'a fait, donc si quelqu'un ose se plaindre de ce magnifique tableau, il va avoir affaire au loup !

Ceci dit, vous savez faire le tableau, mais vous ne savez pas encore l'utiliser. Donc, voyons comment ça marche maintenant.

Pour utiliser ce tableau, il vous faut une lettre à chiffrer et une clé pour la chiffrer. Si vous désirez chiffrer la lettre 'F' avec la clé 'L', vous devez vous placer sur la ligne avec le **F** et vous devez aller jusqu'à la colonne correspondant à **L**. Ce tableau vous donnera **Q**. Alors, n'est-ce pas magnifique ? Posons-nous quelques questions :

- Premièrement, que se passe-t-il si vous échangez la clé et la lettre à chiffrer ?
- Que se passe-t-il si vous chiffrez une lettre avec la clé A ?
- Que se passe-t-il si vous chiffrez une lettre avec une clé, puis que vous rechiffrez ce résultat avec la même clé ?
- Et il nous reste tout plein de questions !

Vous pouvez donc remarquer que ce tableau est assez bien fait, car il a plusieurs caractéristiques plus qu'intéressantes. De plus, on a jusqu'à présent un moyen pour chiffrer chaque caractère avec une même clé... Que se passe-t-il si on utilise plusieurs clés ? Si nous chiffons "VIGENERE" avec une clé telle que 'A' ou 'F' ou 'R', on a un chiffrement de César. Et là, vous vous demandez pourquoi on a pris la peine de faire ce tableau interminable et de vous le montrer. Qu'à cela ne tienne, voyons ce que ce tableau nous apporte !

Nous voudrions chiffrer "ZESTEDESAVOIR" avec une clé moins évidente qu'un seul chiffre ou qu'une seule lettre. On aimerait donc utiliser un ensemble de clé. On se retrouve donc avec un message contenant plusieurs caractères et une clé contenant également plusieurs caractères. Nous allons chiffrer notre message habituel "ZESTEDESAVOIR" avec une clé de plusieurs caractères. Si nous choisissons "CLEM" comme clé, on se retrouve face à un problème : on sait chiffrer les quatre premières lettres du message, mais après on est coincés. Non, justement, tout est prévu, vous vous doutez bien. Vous devez recopier la clé un certain nombre de fois pour obtenir une longueur qui nous convient. Notre message fait 13 lettres, donc on doit mettre notre clé 4 fois de suite. La clé passe donc de simplement "CLEM" à "CLEMCLEMCLEMCLEM". On peut après réduire cette clé à la même longueur que le message, on ne garde donc que les 13 premiers caractères.

Notre message est toujours "ZESTEDESAVOIR" et notre clé est devenue "CLEMCLEMCLEMC". Maintenant, il suffit de chiffrer chaque lettre du message avec son homologue dans la clé. Donc le couple ('Z', 'C'), le couple ('E', 'L'), etc. Notre message chiffré est "BPWFGOIECGSUT". Nous avons maintenant trouvé un chiffrement qui est beaucoup plus sécurisé que tous les autres vus précédemment car nous n'utilisons plus une seule clé, mais un nombre indéfini (mais tout de même inférieur ou égal à la longueur du message clair) !

1. Les Temps modernes

Cependant, il y en a toujours un qui marmonne au fond... Encore un qui appelle ça le *chiffrement de Vigenère*, non ? C'est bien ça... Il faut faire attention, le monde scientifique est fourbe : on associe plein de noms à plein de choses, mais c'est rarement le bon. Dans l'article précédent, nous avons vu le chiffre de César qui n'est pas celui de César, et maintenant, il est question du chiffre de Vigenère qui n'est pas celui de Vigenère. Effectivement, vers 1560/1570, Blaise de Vigenère (un français), a écrit un livre reprenant des données venant d'Alberti, de Trithème et d'autres. Dans ce livre, il parle du chiffrement par substitution rectangulaire. C'est son nom qui a été retenu pour ça. Mais attention, n'oubliez jamais que ce n'est pas à Blaise de Vigenère que nous devons ce procédé !

1.1.2. La stéganographie

Trithème a également ramené l'utilisation de la *stéganographie* en cryptographie. Ce mot quelque peu agressif vient du grec *steganos* et *graphie* ce qui veut dire *écriture étanche*. Autrement dit, une écriture qui ne laisse pas passer le message qui est caché. La stéganographie n'est pas toujours considérée comme faisant partie de la cryptographie, mais nous en parlerons tout de même car Trithème a proposé un moyen assez ingénieux pour faire passer ses messages.

Ce que Trithème a fait, c'est qu'il a associé à chaque lettre une phrase, ou du moins une suite de mots. Mais ces mots ne sont pas choisis au hasard : Trithème était un abbé, il a donc choisi des groupes de mots en s'arrangeant pour que l'on obtienne une sorte de prière ou une litanie. C'est d'ailleurs pour cela que l'on parle également des *Ave Maria de Trithème*. Voici un exemple de table utilisée.

Lettre	Code
A	Dans les cieux
B	A tout jamais
C	Un monde sans fin
D	En une infinité
E	À perpétuité
F	Sempiternel
G	Durable
H	Sans cesse
I-J	Irrévocablement
K	Éternellement
L	Dans la gloire
M	Dans la lumière
N	En paradis
O	Toujours

1. Les Temps modernes

P	Dans la divinité
Q	Dans la déité
R	Dans la félicité
S	Dans son règne
T	Dans son royaume
U-V-W	Dans la béatitude
X	Dans la magnificence
Y	Au trône
Z	En toute éternité

TABLE 1. – Les *Ave Maria* de Trithème

À part la méthode pour déchiffrer, le principe reste le même : il faut remplacer chaque lettre par son homologue de la colonne de droite. Nous avons qualifié ce procédé d'ingénieux car pour le comprendre, il faut bien connaître la table. Et autant un message ressemblant à une chaîne de caractères incompréhensibles paraît chiffré à première vue, autant un ensemble de phrases parlant de béatitude, de félicité et de paradis le paraît beaucoup moins. Si à l'aide de l'alphabet que nous vous avons fourni ci-dessus, vous essayez de chiffrer le message "ZESTEDESAVOIR", vous devriez obtenir quelque chose de la sorte :

"En toute éternité à perpétuité,
Dans son règne dans son royaume,
À perpétuité en une infinité,
À perpétuité dans son règne,
Dans les cieux, dans la béatitude,
Toujours irrévocablement dans la félicité".

Après l'avoir chiffré, la phase de déchiffrage est assez simple : il vous suffit de chercher à quelle lettre correspond quelle partie de phrase. Ce procédé n'est donc pas si différent des précédents dans le principe (toujours de la substitution), mais il est différent au niveau de sa forme : au lieu de substituer une lettre par une lettre, on substitue une lettre par une suite de lettres qui ont un sens dans cet ordre.

1.1.3. Le procédé autoclave de Cardan

Cardan, un *savant* italien du XVI^e siècle a pensé à un procédé lui permettant de se débarrasser de la clé de chiffrement. Il s'est dit que s'il avait pour clé de chiffrement le message, il pourrait chiffrer un message à l'aide d'un tableau de substitution trithémien quelconque. Un chiffre est donc *autoclave* si et seulement s'il utilise le message clair (ou du moins partiellement) en tant que clé. Et il avait raison, ça marche. Mais le message n'est que très peu protégé. Car si on sait quelle table a été utilisée, on sait retrouver le message original sans difficulté. Alors

1. Les Temps modernes

Cardan a tenté d'améliorer son code. Il a choisi de tout de même utiliser une clé pour précéder le message.

Donc si vous tentez de chiffrer "ZESTEDESAVOIR" avec lui-même en tant que clé, avec un chiffrement de type trithémien, vous devriez obtenir "YIKMIGIKAQCQI". Mais là le message est facilement déchiffrable. Donc on rajoute une clé au début de notre ancienne clé. Donc si le message à chiffrer reste identique, mais qu'on utilise la clé "CLEM", on peut supposer que la clé va devenir "CLEMZESTEDESASA". Sauf que comme ça, on en revient à un chiffrement par substitutions trithémienne donc on a fait tout ça pour rien. Il faut savoir que ce procédé autoclave n'a pas été réellement utilisé dans ce type de chiffrement là mais qu'il a servi dans des chiffrements plus complexes où la clé était bien plus compliquée à deviner.

Cardan n'était pas ravi de finir sur un échec, il a donc tout de même décidé de déterminer une autre méthode qui devait porter son nom. Cette méthode se fait appeler *Grille de Cardan*. Cette grille n'est autre qu'un morceau de matériau rigide dans lequel sont coupées des formes pour écrire à travers comme sur la figure suivante.

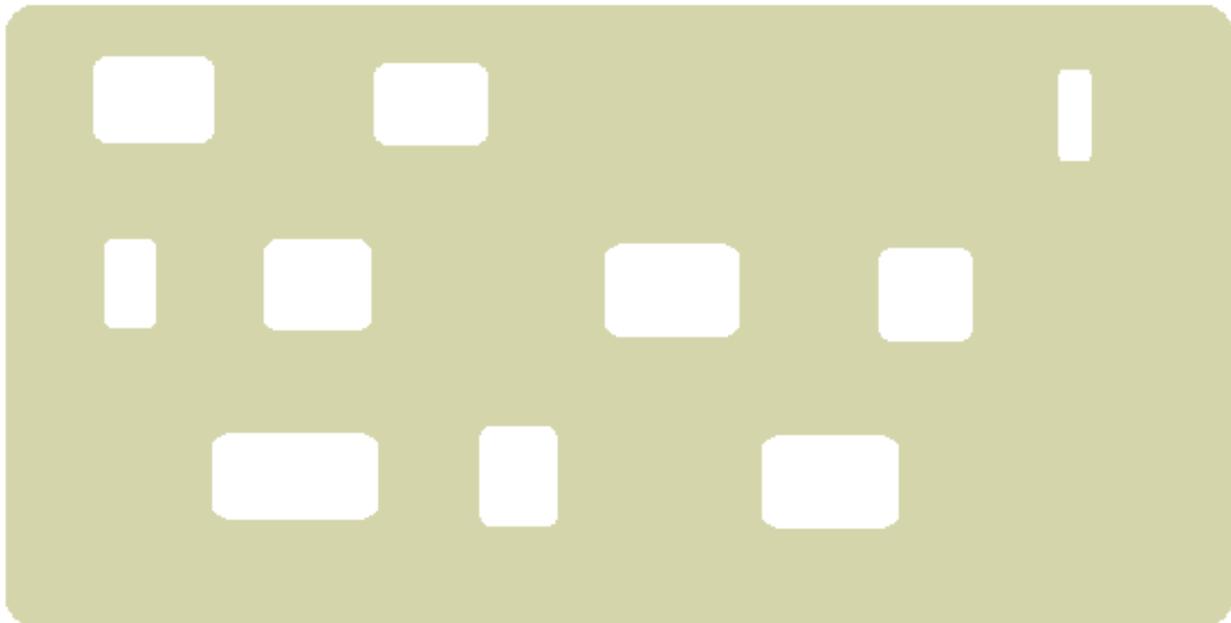


FIGURE 1. – Grille de Cardan (XVIe siècle).

Il faut poser cette grille sur une feuille, écrire sur la feuille, retirer la grille, puis combler les vides en écrivant des caractères aléatoires². Cette méthode n'est pas spécialement sûre non plus, car dès que des caractères se suivent, le mot peut être anticipé. Et en plus, la longueur du mot chiffré est horriblement plus longue que la longueur du message clair. Mais attention, même si cette méthode n'est pas la plus répandue car pas la plus sûre, elle a tout de même été utilisée par le cardinal Richelieu au XVIIe siècle.

1.2. Les bilitères de Bacon ou le chiffrement shakespearien

Vers 1600, Francis Bacon, un Britannique, s'est inspiré de la stéganographie de Cardan pour en faire son codage que l'on appelle des *bilitères*. Pourquoi parle-t-on de *bilitères*? Ce n'est pas très

1. Les Temps modernes

compliqué : *bi* veut dire *deux* et *litére* veut dire *lettre*. C'est donc un codage qui se base sur deux lettres et leurs permutations. Chaque lettre claire est donc chiffrée en une suite de 5 *A* ou *B*. Il en faut 5 car si on compte le nombre minimum de cases pouvant être remplies par deux symboles différents pour représenter 26 caractères différents, on a n le nombre de cases, m le nombre de symboles différents et p le nombre de permutations possibles au total tel que

$$\begin{aligned} p &= m^n \\ 26 &= 2^n \\ n &= \log_2(26) \\ n &\simeq 4.7 \end{aligned}$$

Bien évidemment, on ne peut pas avoir 4.7 cases, le nombre de cases doit être un nombre entier. Et comme on veut pouvoir écrire minimum 26 symboles différents, on arrondit vers le haut. SI on arrondissait vers le bas, on aurait que **16** possibilités. Et l'arrondi de 4.7 vers le haut (également appelé *fonction plafond de 4.7*) vaut 5, CQFD.

Cependant, Bacon n'a pas utilisé 26 lettres dans son code, mais uniquement 24 : il a fusionné les caractères I/J et U/V. Pour déterminer quelle lettre correspond à quel bilitère, il suffit de commencer en associant la lettre A au code "AAAAA", puis la lettre B au code "AAAAB", puis la lettre C au code "AAABA", etc. Ce qui donne un tableau de substitution semblable au suivant.

Lettre	Chiffré	Lettre	Chiffré
A	AAAAA	N	ABBAA
B	AAAAB	O	ABBAB
C	AAABA	P	ABBBA
D	AAABB	Q	ABBBB
E	AABAA	R	BAAAA
F	AABAB	S	BAAAB
G	AABBA	T	BAABA
H	AABBB	U/V	BAABB
I/J	ABAAA	W	BABAA
K	ABAAB	X	BABAB
L	ABABA	Y	BABBA
M	ABABB	Z	BABBB

Table : Table des bilitères

Pour ceux qui sont familiers au code binaire, changez les A en 0 et les B en 1, vous remarquerez qu'en réalité on compte de 0 à 23 en binaire mais avec deux symboles qui ne sont autres que les

1. Les Temps modernes

premières lettres de l'alphabet. Pour ceux qui ne le sont pas, faites-nous confiance, si on le dit, c'est que c'est vrai.

Essayons de chiffrer "ZESTEDESA VOIR" pour voir comment ça marche. On remplace chaque lettre par son code, mettons-les à la suite, séparés par un espace pour que l'on y voie plus clair : BABBB AABAA BAAAB BAABA AABAA AAABB AABAA BAAAB AAAAA BAABB ABBAB ABAAA BAAAA.

Et là, vous vous dites : on a reproché à la grille de Cardan d'augmenter considérablement la longueur du message... Et ici on fait pareil voire pire ! La longueur du message est multipliée par 5 (vu que chaque lettre devient une suite de 5 symboles). Oui, mais dans notre cas, vous allez voir que c'est beaucoup plus sécurisé.

Étant donné que les caractères chiffrés se suivent en binaire, il est plus qu'aisé de retrouver la lettre à partir du code. On commence par séparer le message chiffré par blocs de 5, puis on associe chaque bloc à la lettre correspondante. On peut se faire un tableau pour décoder plus facilement.

	AAA	AAB	ABA	ABB	BAA	BAB	BBA	
AA	A	B	C	D	E	F	G	H
AB	I/J	K	L	M	N	O	P	Q
BA	R	S	T	U/V	W	X	Y	Z

Table : Table inversée des bilitères

Les deux premières lettres du code définissent la ligne sur laquelle on se trouve et les trois suivantes définissent sur quelle colonne on va. Mais ce n'est malheureusement pas très sécurisé comme chiffrement... N'importe qui pourrait le décoder. C'est pour ça que Bacon y a ajouté quelque chose en plus : il retransforme sa suite de A et de B en une phrase qui représente le message chiffré. Il vous faut donc choisir une convention pour écrire une phrase (cette convention doit être la moins évidente possible bien entendu) afin que chaque lettre que vous allez écrire soit associée soit au symbole A soit au symbole B sans ambiguïté. Par exemple, les lettres majuscules donnent un A et les autres caractères (lettres minuscules ponctuation par exemple) donnent un B. Cette convention n'est pas du tout efficace car beaucoup trop prévisible. Mais il est bien plus aisé de comprendre avec un exemple simple. Voici la phrase chiffrée que nous vous avons concoctée : "les bilitères avec zestedesavoir, le site francophone qui en a dans le citron". Cette phrase fait 65 caractères sans les espaces (mais avec la virgule), ce qui est la même longueur que notre message initial une fois transformé en une suite de A et de B. Une fois tous les caractères devant représenter un A mis en majuscule, voilà la chaîne que nous obtenons : lEs biLiTErES AVec ZESTEDeSAVOIr, LE sITe FRAnCOPHOnE Qui En a DaNs LE CiTRON. C'est fait exprès que ce soit visible comme convention, c'est pour que vous compreniez bien.

Maintenant, dites-vous qu'il a déjà fallu 65 caractères à mettre en majuscules/minuscules uniquement pour chiffrer "ZESTEDESA VOIR". D'après vous, qui s'amuserait à chiffrer "LES SANGLOTS LONGS DES VIOLONS DE L'AUTOMNE BLESSENT MON CŒUR D'UNE LANGUEUR MONOTONE" ? C'est donc un chiffrement qui peut s'avérer très efficace pour quelqu'un ne connaissant pas la convention parce que ça peut très vite devenir très long à

1. Les Temps modernes

déchiffrer, mais c'est également un chiffrement moyennement utile car il faut chiffrer un nombre incroyable de symboles, ce qui peut devenir long, fastidieux et peut donc amener à des erreurs humaines.

Avant de finir cette partie, pour ceux qui se demanderaient pourquoi on parle aussi de chiffrement shakespearien comme mis dans le sous-titre, c'est parce que Bacon a souvent été soupçonné d'être l'auteur des pièces de Shakespeare, voire Shakespeare lui-même ! Actuellement, aucune de ces théories n'a été prouvée. Peut-être qu'un jour l'humanité découvrira que le grand Shakespeare ne faisait que signer des pièces codées en binitères dictées par les Illuminati désignant les dirigeants du monde pour des millénaires à venir. Ou pas...

1.3. Le Grand Chiffre de Rossignol père & fils

Il est temps pour nous d'achever la période des Temps modernes avec un des plus grands chiffrements jamais existé (qui porte d'ailleurs le nom de *Grand Chiffre*). Ce chiffrement a été inventé par la famille Rossignol pendant deux générations. Ce chiffre est très connu car il a amené beaucoup de nouveautés qui ont été fortement saluées et réutilisées pendant longtemps. Ce chiffre a vu le jour à la fin du XVII^e siècle et n'a été compris que 200 ans après par le général français Étienne Bazeris. Les Rossignol ont été au service de la couronne de France pendant des générations et des générations, c'est pour ça que ce chiffre a été utilisé par le roi de France Louis XIV, plus communément connu sous le nom de *Roi Soleil*.

Ce *Grand Chiffre* est composé de 587 nombres distincts représentant chacun une syllabe de la langue française. Mais attention, il n'existe pas 587 syllabes différentes ! Du moins il n'en existait pas autant à l'époque, mais la langue évolue. Attendez avec vos questions : c'est vrai que s'il y a un code par syllabe et 587 codes, on peut déduire qu'il y a 587 syllabes, mais nous venons de vous affirmer le contraire. Donc il y a un piège. Eh bien oui ! Le piège c'est que certains nombres ne veulent rien dire, d'autres ont une signification bien précise telle que :

- ignorer la syllabe précédente ;
- ignorer la syllabe suivante ;
- additionner le code précédent avec le suivant ;
- ...

On sait que vous vous attendez à un tableau comme pour les chiffres précédents... Mais franchement, 587 codes et leur homologue... Vous nous excuserez si on passe un tour !

Il a déjà fallu longtemps pour déterminer que les codes ne correspondaient plus à une lettre comme c'était le cas jusque là, mais bien une syllabe ou une partie de mot. Mais il a fallu encore plus longtemps pour comprendre que certains codes étaient là pour embrouiller les cryptanalystes³. Mais ce code a finalement été cassé, toutes les bonnes choses ont une fin. Il n'empêche que le Grand Chiffre reste très connu de nos jours, car il a été d'une robustesse exemplaire pendant plus de 200 ans.

Voici qui conclut la partie concernant les Temps modernes. Il nous reste une période à décrire, c'est l'Époque contemporaine, celle dans laquelle nous baignons actuellement. Elle n'est donc bien entendu pas achevée, mais il y a tout de même beaucoup à en dire !



Venez lire la dernière partie ↗ de notre série !

2. Sources et liens

Pour aller plus loin :

- pour le chiffre de Vigenère (enfin de Trithème), la [page Wikipédia ↗](#) est très complète et voici un [rab d'infos ↗](#) ;
- infos sur la stéganographie en général sur [Wikipédia ↗](#) et un [supplément sur les stéganographies en cryptographie ↗](#) ;
- concernant la [vie de Trithème ↗](#) ;
- sur le procédé autoclave, la [page Wikipédia ↗](#) (anglais) ;
- à propos des bilitères, le [fonctionnement ↗](#) ainsi que [quelques explications supplémentaires ↗](#) ;
- concernant le Grand Chiffre, voici une [explication très détaillée ↗](#) .

Contenu masqué

Contenu masqué n°1

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
A	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
B	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
C	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
D	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
E	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
F	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
G	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W

1. Effectivement, si le nombre de colonnes est égal au nombre de lignes, il s'agit d'un carré. Mais il n'est question ici que de ce qu'a trouvé Polybe, c'est plus tard qu'est venu le nom de *table rectangulaire* pour plus de souplesse.

2. Attention : si vous mettez des caractères aléatoires, le chiffrement va plus vite mais il est évident que c'est un message chiffré. Alors que si vous réussissez à intégrer les caractères de votre message clair dans un autre texte en français (ou anglais ou autre), personne ne se doutera qu'il s'agit d'un texte chiffré.

3. La cryptanalyse est la science en quelque sorte opposée à la cryptographie dans le sens que la cryptographie sert à chiffrer une information alors que la cryptanalyse sert à déterminer une information chiffrée sans en connaître la ou les clés.

H	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
I	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y
J	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
K	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
L	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
M	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
N	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
O	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
P	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
Q	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
R	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
S	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
T	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
U	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
V	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
W	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
X	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
Y	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
Z	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P

[Retourner au texte.](#)