Le chiffre de Vigenère

La phrase à déchiffrer était la suivante : *Le capitaine Kidd a caché son trésor sur l'île Sullivan.*

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

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

Imprimez ce document recto-verso, sur du papier A4, avec retournement sur le petit côté.

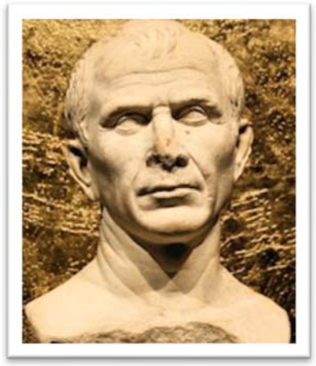
CRYPTOGRAPHIE

La ***cryptographie*** existe depuis l'antiquité. C'est un ensemble de techniques permettant de protéger les messages en les *chiffrant*.
Le ***chiffrement***, c'est la transformation, à l'aide d'une *clé*, d'un message clair en message incompréhensible.
L'opération inverse, le ***déchiffrement***, consiste à retrouver le message clair en utilisant la *clé*.
La cryptographie est utilisée chaque fois que le contenu des messages doit rester secret, pour des échanges militaires ou commerciaux par exemple.
L'apparition de ***l'informatique***, à la fin du 20ème siècle, a permis de développer des techniques de chiffrement de plus en plus complexes qui mettent à profit la rapidité de calcul des ordinateurs.

Ce petit livret présente quelques techniques de chiffrement et de déchiffrement au travers d'une petite histoire de la cryptographie.
Munissez-vous d'un crayon, d'une gomme, d'une feuille de papier et laissez-vous guider.

Les messages proposés dans ce livret sont tirés du « ***scarabée d'Or*** », une nouvelle d'***Edgar Poe*** dans laquelle le héros, William Legrand, découvre le fabuleux trésor du capitaine Kidd en déchiffrant un message laissé par ce dernier.

Le chiffre de César



Pour communiquer avec les nombreuses légions réparties sur son empire, Jules César utilisait un code très simple : le décalage alphabétique. Puis il l'envoyait porter par un messager. Si ce messager était capturé, l'ennemi trouvait un message illisible.

Pour comprendre le chiffre de César, tu dois :
- connaître l'alphabet
- savoir additionner et soustraire mentalement

Supposons que l'on ait choisi un décalage de 8 lettres vers l'avant (+8) :
Le A devient donc un H, le B un I, le C un J, etc.
On peut résumer le décalage (+8) dans un tableau comme celui-ci :

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

Pour décoder le message, le destinataire devra effectuer l'opération inverse : décaler de 8 lettres vers l'*arrière* (-8).
Voici 1 message à décoder. Il a été codé avec un décalage de (+4)
Attention, pour renforcer le cryptage et éviter que l'on reconnaisse les mots d'après leur nombre de lettres, celles-ci ont été regroupées par 5. Vous devrez donc remettre aux bonnes places les espaces séparant les mots, ainsi que la ponctuation, de façon à obtenir une phrase claire.

Message n° 1 : **AMPPM EQPIK VERHL EFMXI WYVPM PIHIW YPPMZ ER**

Texte en clair :

Cette méthode, bien qu'efficace à l'époque de Jules César, n'est pourtant pas très sûre. On peut assez facilement décrypter un message codé par décalage alphabétique, sans connaître le décalage utilisé, en se basant sur la **fréquence des lettres.**

Cela se fait en 3 étapes :

1. La lettre la plus utilisée en français est le E. Il faut donc rechercher la lettre la plus fréquente dans le message.
2. Cette lettre remplaçant le E, on peut calculer le *décalage*.
3. Il suffit ensuite d'appliquer le même décalage à toutes les lettres du message.

Le message suivant a été crypté avec le chiffre de César. A vous de le décoder.

OZQJX HJXFW KZYJR UJWJZ WIJXL FZQJX

Texte en clair :

Plaçons ensuite les lettres E S et A dans le tableau de déchiffrage :

S		■			■		E		S	E	S	■	A	■				A			S	E		
	E	■			E	S			■		E	■		E		A			E	■	■	■	■	
	A	S	■						E	■	E		■		A				E	■	■	■	■	

Certains mots se devinent facilement, ce qui permet d'obtenir d'autres lettres :

S		■			■		E		S	E	S	■	A	■				A			S	E		
	E	■			E	S			■		E	■		E		A			E	■	■	■	■	
P	A	S	■						E	■	E	T	■		A				E	■	■	■	■	

Une fois ces lettres replacées dans la grille, on devine les mots **LE TRESOR** et **PENSES**

S		■	T		■	P	E	N	S	E	S	■	A	■				A			S	E		
L	E	■	T	R	E	S	O	R	■		E	■		E		A			E	■	■	■	■	
P	A	S	■					T	E	■	E	T	■		A				E	■	■	■	■	

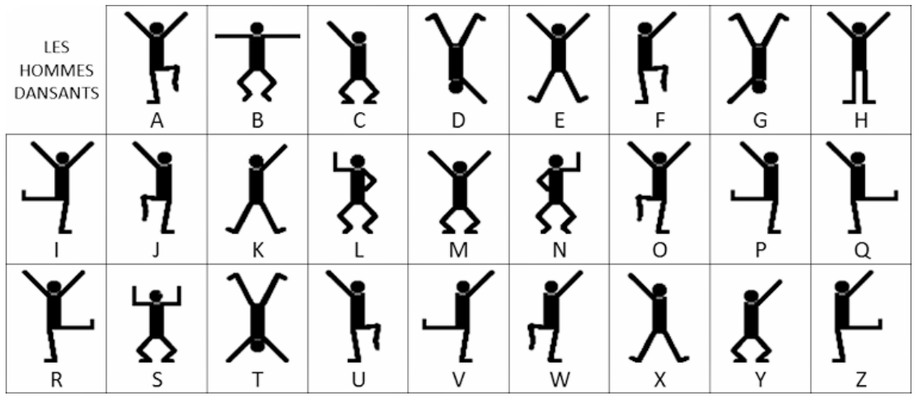
On remplace toutes les figurines représentant les nouvelles lettres (R, O, L et N) :

S		■	T		■	P	E	N	S	E	S	■	A	■	L	O		A	L		S	E	R
L	E	■	T	R	E	S	O	R	■	N	E	■		E	L	A	N		E	■	■	■	■	
P	A	S	■		R	O		T	E	■	E	T	■		A				E	■	■	■	■	

Il ne reste plus qu'à compléter :

S	I	■	T	U	■	P	E	N	S	E	S	■	A	■	L	O	C	A	L	I	S	E	R
L	E	■	T	R	E	S	O	R	■	N	E	■	M	E	L	A	N	G	E	■	■	■	■
P	A	S	■	D	R	O	I	T	E	■	E	T	■	G	A	U	C	H	E	■	■	■	■

Voici la table de correspondance ayant servi à coder ce message :



Le chiffre homophone

Voici le message en clair : *William Legrand et ses amis ont découvert un fabuleux trésor.*

Le chiffre du livre

Voici le message en clair : *Le drapeau des pirates est orné d'une tête de mort*

Le chiffre de Marie Stuart

Pour déchiffrer ce message, il suffit de remplacer chaque signe par la lettre ou le groupe de lettres correspondant. Les "nuls" ne seront pas remplacés et les "doublés" remplacés par la lettre qui suit.

ENHAUTDUPLATEAUSEDRESSAITUNMAGNIFIQUETULIPIERQUE
JUPITERDUTESCALADERAMAINSNUESAVECLESCARABEE

Ce qui, une fois les mots séparés, donne la phrase :
En haut du plateau se dressait un magnifique tulipier que Jupiter dut escalader à mains nues avec le scarabée.

Le Grand Chiffre de Louis XIV

Voici la traduction phonétique du message :

1216	1304	114	302	601	1706	1502	1002	602	1901	1101
sé	to	bou	de	la	bran	che	que	le	sca	ra

110	1814	1402	1101	1213	805	1303	603	1310
bé	trou	ve	ra	son	nu	ti	li	té

Ce qui donne la phrase suivante en clair :

C'est au bout de la branche que le scarabée trouvera son utilité.

Le chiffre des Templiers

Le message à déchiffrer disait ceci : *Le trésor est enfoui à cinquante pieds du tulipier.*

Les hommes dansants

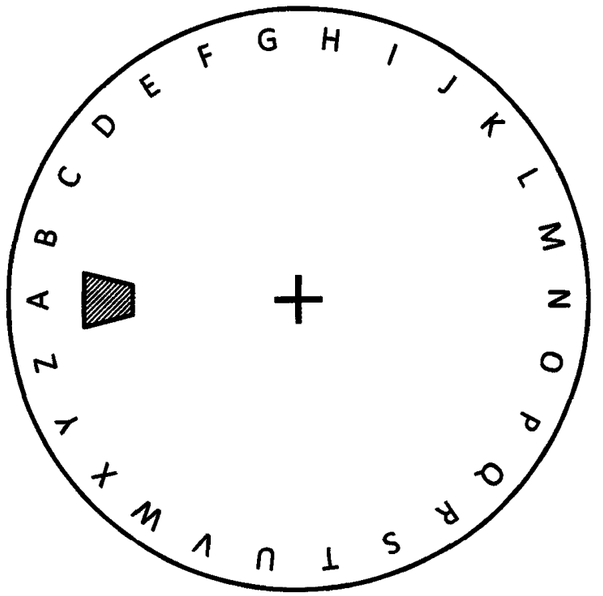
En observant et en comptant les figurines, on remarque les plus utilisées sont :

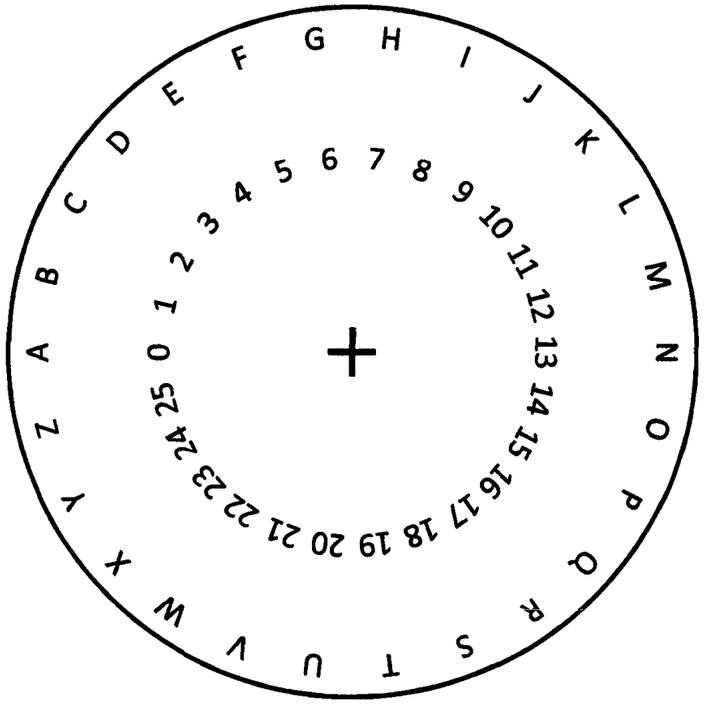
 10 fois, qui représente donc le **E**

 6 fois, qui représente donc le **S**

 5 fois, qui représente donc le **A**

Outil de chiffrement / déchiffrement
Pour les messages utilisant le chiffre de César





1. Découpez les deux disques
2. A l'aide d'un cutter, découpez la fenêtre trapézoïdale du premier disque.
3. Percez au compas les centres des deux disques (croix).
4. Assemblez les disques (le premier sur le deuxième) à l'aide d'une attache parisienne.

Le carré de Polybe

Polybe est un historien grec qui vécut entre -205 et -125. Il inventa une méthode très originale pour chiffrer les messages, basée sur un tableau de 5x5 cases, comme celui-ci :

	1	2	3	4	5
1	A	B	C	D	E
2	F	G	H	I J	K
3	L	M	N	O	P
4	Q	R	S	T	U
5	V	W	X	Y	Z

On remplace chaque lettre par ses coordonnées dans le tableau, en écrivant d'abord la ligne puis la colonne. Par exemple, le A devient 11, le B devient 12, le F devient 21, le P 35, etc. Comme il n'y a que 25 cases pour les 26 lettres de l'alphabet, le I et le J sont tous les deux codés par le nombre 24. Exemple : **POLYBE** devient **353431541215**

Le problème avec le carré de Polybe, c'est qu'il est connu de tous et donc ne garantit plus le secret des messages échangés de cette façon. Il faut le personnaliser. Voici comment on procède :

1. Les deux correspondants se mettent d'accord sur un mot-clé qu'ils sont les seuls à connaître. Par exemple SCARABEE.
2. Pour construire le carré de Polybe correspondant à ce mot-clé, on commence par en éliminer les lettres en double : SCAR~~A~~BE~~E~~ ce qui donne SCARBE
3. On inscrit les lettres obtenues dans les premières cases du carré, puis on complète avec l'alphabet, en partant de la lettre A, mais en sautant les lettres déjà présentes dans le carré (S-C-A-R-B-E). Le I et le J sont toujours associés dans la même case. Cela donne :

	1	2	3	4	5
1	S	C	A	R	B
2	E	D	F	G	H
3	I J	K	L	M	N
4	O	P	Q	T	U
5	V	W	X	Y	Z

Saurez-vous déchiffrer le message suivant, codé à l'aide du mot-clé SULLIVAN ?

4142222434 3145214114 4531144214 3322315541 4214243111
4214451112 4541422214 1331434212 4512223121 3232211445
3151453111 1441434245 5121225131

Écrivez le message en clair ci-dessous (mots bien séparés) :

SOLUTIONS

Le chiffre de César

Message n° 1 :

AMPPM EQPIK VERHL EFMXI WYVPM PIHIW YPPMZ ER
WILLI AMLEG RANDH ABITE SURLI LEDES ULLIV AN

William Legrand habite sur l'île de Sullivan.

Message n° 2 :

La lettre la plus utilisée dans ce message est le J:

OZQ**J**X H**J**XFW KZY**J**R U**J**W**J**Z WI**J**XL FZQ**J**X

Puisque le J remplace le E, le message a donc été codé avec un décalage de (+5).

E -> F -> G -> H -> I -> **J**

Pour déchiffrer, il suffit donc de lui appliquer un décalage de (-5), ce qui donne :

OZQJX HJXFW KZYJR UJWJZ WIJXL FZQJX
JULES CESAR FUTEM PEREU RDESG AULES

Jules César fut empereur des Gaules.

Le carré de Polybe

Voici le carré de Polybe construit avec le mot-clé SUL(L)IVAN :

	1	2	3	4	5
1	**S**	**U**	**L**	**I J**	**V**
2	**A**	**N**	B	C	D
3	E	F	G	H	K
4	M	O	P	Q	R
5	T	W	X	Y	Z

Et voici la traduction du message :

4142222434 3145214114 4531144214 3322315541 4214243111
M O N C H E R A M I R E J O I G N E Z M O I C E S

4214451112 4541422214 1331434212 4512223121 3232211445
O I R S U R M O N I L E P O U R U N E A F F A I R

3151453111 1441434245 5121225131
E T R E S I M P O R T A N T E

Mon cher ami, rejoignez-moi ce soir sur mon île pour une affaire très importante.

LE CHIFFRE DE VIGENERE

tableau de codage-décodage

LETTRE DE LA CLÉ

LETTRE A CODER

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

rf.sreitiop-ac@tneniv.naitsirhc

Le chiffre de Marie Stuart

Marie Stuart nait le 8 décembre 1542, en pleine guerre de religion qui oppose les catholiques écossais, dont elle hérite du trône, aux protestants anglais. Le roi d'Angleterre, **Henri VIII** rêve de réunifier **l'Angleterre** et **l'Écosse**, mais aussi de convertir l'Écosse catholique à la religion protestante. Il tente de marier son fils et Marie Stuart, ce qui aurait résolu le conflit de façon pacifique. Mais cette demande est rejetée par les nobles écossais.

Les Anglais s'apprêtent alors à attaquer l'Écosse, et la jeune reine Marie se réfugie en France, où elle épouse le roi François II.

Marie se retrouve alors à la fois reine de France *et* d'Écosse. Mais lors de son retour au pays, elle est très contestée, puis emprisonnée. On la force à abdiquer en faveur de son fils Jacques.

En mai 1568, Marie Stuart s'évade et lève une petite armée. Après une sévère défaite, elle se réfugie en Angleterre ou règne sa cousine **Élisabeth I**. Mais celle-ci la considère comme une rivale et la fait emprisonner au château de Chartley Hall. Marie a encore des partisans et communique avec eux grâce à des messages cachés dans les barriques de bières livrées au château. Au cas où un geôlier intercepterait ces messages, Marie a mis au point un *code*. Peu à peu, un complot s'organise : Ses partisans vont tenter de la faire évader après avoir assassiné Élisabeth.

Malheureusement pour Marie, l'un de ses partisans est un agent double qui transmet les messages chiffrés aux Anglais. Ceux-ci n'ont aucun mal à les déchiffrer car le code employé par Marie n'est qu'une simple substitution de lettres légèrement améliorée.

Marie sera jugée, déclarée coupable de complot contre la reine et exécutée le 8 février 1587.

Pour coder ses messages, Marie Stuart utilisait un dictionnaire comportant les lettres de l'alphabet ainsi que les mots les plus fréquents. Un signe peut donc remplacer soit une lettre, soit un mot en entier. Pour compliquer encore le déchiffrage, certains signes ne servent à rien (nuls) et d'autres à doubler la lettre qui suit (doublé). Marie Stuart était persuadée que son code était indéchiffrable, mais elle se trompait. Il est même assez simple à déchiffrer en se basant sur la fréquence des lettres et des mots les plus utilisés, comme pour le chiffre de César. Voici une adaptation française du chiffre de Marie Stuart :

Utilisez le tableau de la page suivante pour déchiffrer le message ci-dessous.
Écrivez le message en clair, en séparant les mots :

⋮ б ψ § ɜ ج Щ Ж ψ ⌂ r θ ƚ Ѡ o ɞ η ə § r ∩ Ø ӂ Ш Ѻ ə ɷ µ Ю

ə ج r ə Ѡ ƚ ɷ ٦ б ج ə Ж r ƚ ɜ Ж ɞ φ η Щ r √ ƚ η Ø ə Ђ ɞ Ђ

Б ᗰ ☼ Ю r ᗰ φ η ƚ η λ o Ѡ

A	η	K	ϙ	U	Б	AVEC	☼	MA	ø
B	λ	L	Ю	V	Ʊ	CELA	ʃ	TU	µ
C	φ	M	≁	W	ƨ	EN	⋮	NI	ш
D	θ	N	Ђ	X	‖	MAIS	Δ	ES	ɑ
E	ω	O	Ԓ	Y	э	UN	∩	EST	ʓ
F	O	P	ꜫ	Z	δ	DE	√	LA	щ
G	ѫ	Q	ɨ	Doublé	o	NE	‡	TE	Ж
H	б	R	Ł	Nuls	г	PAS	╤	AU	ψ
I	ə	S	в	ET	Л	SE	⌂	JE	ᴥ
J	٦	T	§	QUE	Ꙍ	DU	ɿ	IL	◊

Le chiffre de Vigenère

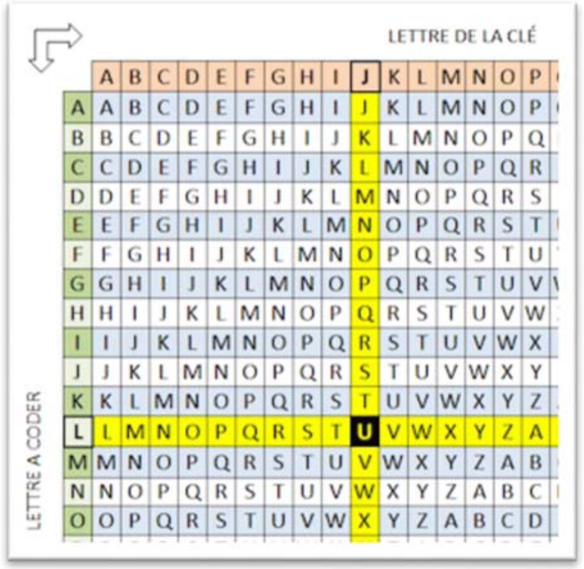
Pour finir notre série d'activités sur la cryptographie, l'art de coder et de décoder les messages, voici une technique simple et très efficace. En 1523, **Blaise Vigenère** mit au point un procédé de codage des messages qui résista à toutes les tentatives de décryptage pendant 3 siècles. Il eut l'idée d'utiliser un **chiffre de César**, mais donc le décalage changeait à chaque lettre en fonction d'un mot-clé connu des 2 correspondants. Il devenait alors impossible de se baser sur la fréquence des lettres pour localiser le E puis appliquer son décalage aux autres lettres.

Supposons que le mot clé soit JUPITER. On commence par l'écrire sous le message à coder, en le répétant si nécessaire :

L	E	T	R	E	S	O	R	E	S	T	D	A	N	S	U	N	C	O	F	F	R	E
J	U	P	I	T	E	R	J	U	P	I	T	E	R	J	U	P	I	T	E	R	J	U
U	Y	I	A	..	..	..																

Ensuite, à l'aide de la table de codage-décodage de la page suivante on procède lettre par lettre :

1. On repère la lettre à coder dans la colonne de gauche (verte)
2. On repère la lettre du mot-clé écrite en dessous dans la première ligne (rouge)
3. La lettre à écrire est à l'intersection de la ligne et de la colonne correspondantes.



LETTRE DE LA CLÉ

LETTRE A CODER

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

Pour décoder le message, on procède de façon inverse : on commence par écrire au-dessus du message reçu le mot-clé en le répétant autant de fois que nécessaire :

L	E	T	R	..	..	..	..	..														
J	U	P	I	T	E	R	J	U	P	I	T	E	R	J	U	P	I	T	E	R	J	U
U	Y	I	A	X	W	F	A	Y	H	B	W	E	E	B	O	C	K	H	J	W	A	Y

1. On repère la lettre du mot-clé dans la première ligne (rouge)
2. On cherche sur la colonne correspondante la lettre codée.
3. On remonte la ligne à gauche pour trouver la lettre d'origine (verte)

A vous maintenant de décoder le message suivant, qui a été chiffré avec la phrase-clé suivante : **CAROLINEDUSUD**

NETOA QGELH WELFD RQLKU IVIFN UGSFF DCEPL FWMXN LZJLV

Écrivez ci-dessous la phrase en clair, en séparant bien les mots :

=>

[1]PENDANT [2]UN [3]MOMENT, [4]JE [5]ME [6]SENTIS [7]TROP [8]ETOURDI [9]POUR [10]PENSER [11]CLAIREMENT. [12]JE [13]PRIS [14]ALORS [15]UNE [16]CHANDELLE, [17]ET, [18]M'ASSEYANT [19]A [20]L'AUTRE [21]BOUT [22]DE [23]LA [24]CHAMBRE, [25]JE [26]PROCEDAI [27]A [28]UNE [29]ANALYSE [30]PLUS [31]ATTENTIVE [32]DU [33]PARCHEMIN. [34]EN [35]LE [36]RETOURNANT, [37]JE [38]VIS [39]MA [40]PROPRE [41]ESQUISSE [42]SUR [43]LE [44]REVERS, [45]JUSTE [46]COMME [47]JE [48]L'AVAIS [49]FAITE. [50]MA [51]PREMIERE [52]IMPRESSION [53]FUT [54]SIMPLEMENT [55]DE [56]LA [57]SURPRISE : [58]DE [59]L'AUTRE [60]COTE [61]DU [62]PARCHEMIN [63]UNE [64]IMAGE [65]D'UN [66]CRANE, [67]QUE [68]JE [69]N'AVAIS [70]PAS [71]VU [72]AUPARAVANT, [73]SE [74]SUPERPOSAIT [75]EXACTEMENT [76]A [77]MON [78]DESSIN ! [79]CETTE [80]COÏNCIDENCE [81]ME [82]STUPEFIA. [83]MAIS [84]QUAND [85]JE [86]REVINS [87]DE [88]CETTE [89]STUPEUR, [90]JE [91]COMMENÇAI [92]A [93]ME [94]RAPPELER [95]QU'IL [96]N'Y [97]AVAIT [98]AUCUN [99]DESSIN [100]SUR [101]LE [102]PARCHEMIN [103]QUAND [104]J'Y [105]AVAIT [106]FAIT [107]MON [108]CROQUIS [109]DU [110]SCARABEE. [111]SI [112]LE [113]CRANE [114]AVAIT [115]ETE [116]VISIBLE, [117]JE [118]L'AURAIS [119]REMARQUE. [120]IL [121]Y [122]AVAIT [123]REELLEMENT [124]LA [125]UN [126]MYSTERE [127]QUE [128]JE [129]ME [130]SENTAIS [131]INCAPABLE [132]DE [133]DEBROUILLER. [134]JE [135]ME [136]LEVAI, [137]ET [138]SERRANT [139]SOIGNEUSEMENT [140]LE [141]PARCHEMIN, [142]JE [143]DECIDAI [144]DE [145]L'EXAMINER [146]PLUS [147]ATTENTIVEMENT [148]QUAND [149]JE [150]POURRAIS [151]ETRE [152]SEUL.

[153]QUAND [154]VOUS [155]FUTES [156]PARTI [157]ET [158]QUAND [159]JUPITER [160]FUT [161]BIEN [162]ENDORMI, [163]JE [164]ME [165]LIVRAI [166]A [167]UNE [168]INVESTIGATION [169]UN [170]PEU [171]PLUS [172]METHODIQUE [173]DE [174]LA [175]CHOSE. [176]ET [177]D'ABORD [178]JE [179]VOULUS [180]COMPRENDRE [181]DE [182]QUELLE [183]MANIERE [184]CE [185]PARCHEMIN [186]ETAIT [187]TOMBE [188]DANS [189]MES [190]MAINS. [191]L'ENDROIT [192]OU [193]NOUS [194]DECOUVRIMES [195]LE [196]SCARABEE [197]ETAIT [198]SUR [199]LA [200]COTE [201]DU [202]CONTINENT, [203]A [204]UN [205]MILLE [206]ENVIRON [207]A [208]L'EST [209]DE [210]L'ILE, [211]MAIS [212]A [213]UNE [214]PETITE [215]DISTANCE [216]AU-[217]DESSUS [218]DU [219]NIVEAU [220]DE [221]LA [222]MAREE [223]HAUTE. [224]QUAND [225]JE [226]M'EN [227]EMPARAI, [228]IL [229]ME [230]MORDIT [231]CRUELLEMENT, [232]ET [233]JE [234]LE [235]LACHAI. [236]JUPITER, [237]AVEC [238]SA [239]PRUDENCE [240]ACCOUTUMEE, [241]AVANT [242]DE [243]PRENDRE [244]L'INSECTE, [245]QUI [246]S'ETAIT [247]ENVOLE [248]DE [249]SON [250]COTE, [251]CHERCHA [252]AUTOUR [253]DE [254]LUI [255]UNE [256]FEUILLE [257]OU [258]QUELQUE [259]CHOSE [260]D'ANALOGUE, [261]AVEC [262]QUOI [263]IL [264]PUT [265]S'EN [266]EMPARER. [267]CE [268]FUT [269]A [270]CE [271]MOMENT [272]QUE [273]SES [274]YEUX [275]ET [276]LES [277]MIENS [278]TOMBERENT [279]SUR [280]LE [281]MORCEAU [282]DE [283]PARCHEMIN, [284]QUE [285]JE [286]PRIS [287]ALORS [288]POUR [289]DU [290]PAPIER. [291]IL [292]ETAIT [293]A [294]MOITIE [295]ENFONCE [296]DANS [297]LE [298]SABLE, [299]AVEC [300]UN [301]COIN [302]EN [303]L'AIR. [304]PRES [305]DE [306]L'ENDROIT [307]OU [308]NOUS [309]LE [310]TROUVAMES, [311]J'OBSERVAI [312]LES [313]RESTES [314]D'UNE [315]COQUE [316]DE [317]GRANDE [318]EMBARCATION. [319]CES [320]DEBRIS [321]DE [322]NAUFRAGE [323]ETAIENT [324]LA [325]PROBABLEMENT [326]DEPUIS [327]BIEN [328]LONGTEMPS, [329]CAR [330]ON [331]DEVINAIT [332]A [333]PEINE [334]LA [335]FORME [336]D'UNE [337]CHARPENTE [338]DE [339]BATEAU.

[340]JUPITER [341]RAMASSA [342]DONC [343]LE [344]PARCHEMIN, [345]ENVELOPPA [346]L'INSECTE [347]ET [348]ME [349]LE [350]DONNA. [351]PEU [352]DE [353]TEMPS [354]APRES, [355]NOUS [356]REPRIMES [357]LE [358]CHEMIN [359]DE [360]LA [361]HUTTE, [362]ET [363]NOUS [364]RENCONTRAMES [365]LE [366]LIEUTENANT. [367]JE [368]LUI [369]MONTRAI [370]L'INSECTE, [371]ET [372]IL [373]ME [374]PRIA [375]DE [376]LUI [377]PERMETTRE [378]DE [379]L'EMPORTER [380]AU [381]FORT. [382]IL [383]LE [384]FOURRA [385]DANS [386]LA [387]POCHE [388]DE [389]SON [390]GILET [391]SANS [392]LE [393]PARCHEMIN [394]QUI [395]LUI [396]SERVAIT [397]D'ENVELOPPE, [398]ET [399]QUE [400]JE [401]TENAIS [402]TOUJOURS [403]A [404]LA [405]MAIN [406]PENDANT [407]QU'IL [408]EXAMINAIT [409]LE [410]SCARABEE. [411]IL [412]EST [413]EVIDENT [414]QU'ALORS, [415]SANS [416]Y [417]PENSER, [418]J'AI [419]REMIS [420]LE [421]PARCHEMIN [422]DANS [423]MA [424]POCHE.

[425]VOUS [426]VOUS [427]RAPPELEZ [428]QUE, [429]LORSQUE [430]JE [431]M'ASSIS [432]A [433]LA [434]TABLE [435]POUR [436]FAIRE [437]UN [438]CROQUIS [439]DU [440]SCARABEE, [441]JE [442]NE [443]TROUVAI [444]PAS [445]DE [446]PAPIER

Le Grand Chiffre de Louis XIV

En **1626**, la petite ville protestante de Réalmont, dans le Tarn, est assiégée par l'armée de **Louis XIII**. Une lettre codée est interceptée sur un messager sortant de la ville. Elle est portée à **Antoine Rossignol**, un jeune mathématicien, qui déchiffre le jour même le message. Cette lettre révèle la situation désespérée des assiégés, incapables de se ravitailler. L'armée, qui ignorait que la condition des assiégés était si difficile, leur retourne le jour même le message en clair, accompagné d'une demande de reddition. Cette demande est acceptée aussitôt.

Depuis cet événement, la cour du roi de France a compris l'importance du chiffrement dans les activités diplomatiques et d'espionnage. Ainsi, Antoine Rossignol, puis son fils et son petit-fils, se mirent au service de Louis XIII, puis de **Louis XIV**.

Sous le règne de ce dernier, ils conçoivent le **Grand Chiffre**, un système de chiffrement utilisé par Louis XIV et ses ministres pour toutes les discussions diplomatiques ou les messages de la plus haute importance. Ce système est réputé infaillible : les messages sont constitués d'une suite de nombres du genre "132-25-89-345-..." et il faudra attendre 1890 pour qu'un autre mathématicien, Etienne Bazeries, se penche sur le Grand Chiffre et comprenne que chacun de ces nombres correspond en fait à une syllabe de la langue française. Il établit alors une table des syllabes qui permettra aux historiens de déchiffrer tout le courrier de Louis XIV.

Utilisez la table des syllabes de la page suivante pour décoder ce message :

1216-1304-114-302-601-1706-1502-1002-602-1901-1101-110-1814-1402-1101-1213-805-1303-603-1310

Écrivez ci-dessous le message en clair, en séparant bien les mots. Attention, le code traduit des sons et vous devrez reconstituer la phrase en bon français, sans faute d'orthographe !

		01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16
		a	e	i	o	u	an	au	ai	en	é	eu	in	on	ou	oi	è
1	b	ba	be	bi	bo	bu	ban	bau	bai	ben	bé	beu	bin	bon	bou	boi	bè
2	c	ca	ce	ci	co	cu	can	cau	cai	cen	cé	ceu	cin	con	cou	coi	cè
3	d	da	de	di	do	du	dan	dau	dai	den	dé	deu	din	don	dou	doi	dè
4	f	fa	fe	fi	fo	fu	fan	fau	fai	fen	fé	feu	fin	fon	fou	foi	fè
5	j	ja	je	ji	jo	ju	jan	jau	jai	jen	jé	jeu	jin	jon	jou	joi	jè
6	l	la	le	li	lo	lu	lan	lau	lai	len	lé	leu	lin	lon	lou	loi	lè
7	m	ma	me	mi	mo	mu	man	mau	mai	men	mé	meu	min	mon	mou	moi	mè
8	n	na	ne	ni	no	nu	nan	nau	nai	nen	né	neu	nin	non	nou	noi	nè
9	p	pa	pe	pi	po	pu	pan	pau	pai	pen	pé	peu	pin	pon	pou	poi	pè
10	qu	qua	que	qui	quo	quu	quan	quau	quai	quen	qué	queu	quin	quon	quou	quoi	què
11	r	ra	re	ri	ro	ru	ran	rau	rai	ren	ré	reu	rin	ron	rou	roi	rè
12	s	sa	se	si	so	su	san	sau	sai	sen	sé	seu	sin	son	sou	soi	sè
13	t	ta	te	ti	to	tu	tan	tau	tai	ten	té	teu	tin	ton	tou	toi	tè
14	v	va	ve	vi	vo	vu	van	vau	vai	ven	vé	veu	vin	von	vou	voi	vè
15	ch	cha	che	chi	cho	chu	chan	chau	chai	chen	ché	cheu	chin	chon	chou	choi	chè
16	g	ga	ge	gi	go	gu	gan	gau	gai	gen	gé	geu	gin	gon	gou	goi	gè
17	br	bra	bre	bri	bro	bru	bran	brau	brai	bren	bré	breu	brin	bron	brou	broi	brè
18	tr	tra	tre	tri	tro	tru	tran	trau	trai	tren	tré	treu	trin	tron	trou	troi	trè
19	sc	sca	sce	sci	sco	scu	scan	scau	scai	scen	scé	sceu	scin	scon	scou	scoi	scè

Le chiffre du livre

Les deux correspondants se seront mis d'accord sur le choix d'un **livre**, ou d'un extrait de livre, dont **les mots auront été numérotés** comme ceci :

[1]Pendant [2]un [3]moment, [4]je [5]me [6]sentis [7]trop [8]étourdi [9]pour [10]penser [11]clairement. [12]Je [13]pris [14]alors [15]une [16]chandelle, [17]et, [18]m'asseyant [19]à [20]l'autre [21]bout [22]de [23]la [24]chambre,

Chaque nombre sera utilisé pour représenter la première lettre du mot qui le suit. Ainsi, 1 représentera P, 3 représentera M, etc. Mais le P pourra aussi être codé avec 10 (**P**enser) ou 13 (**P**ris). Une même lettre pourra être codée de plusieurs façons différentes. Les messages seront alors très difficiles, voire impossibles à décoder.

Utilisez l'extrait page suivante, dont les mots ont été numérotés, et déchiffrez le message suivant. Pour retrouver le mot correspondant à un nombre, commencez par parcourir la première colonne pour trouver le nombre le plus proche, mais sans le dépasser. Avancez ensuite sur la ligne pour trouver le mot, puis sa première lettre.

118-275-188-36-216-435-41-166-437-22-247-389-156-64-419-252-443-115-6-295-410-278-307-86-460-412-78-125-308-413-7-75-187-41-422-302-190-330-119-310

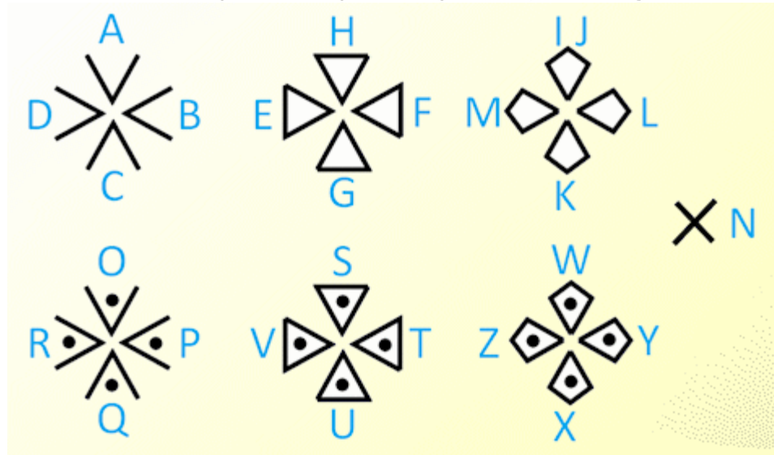
Écrivez ci-dessous le texte en clair du message, en séparant bien les mots.

=>

Lettre	Fréquence sur 100 lettres	Nombres de remplacement
A	8	20-27-33-42-52-61-78-90
B	1	53
C	3	21-34-54
D	4	28-43-62-66
E	17	44-55-63-65-67-79-91-99-01-08-13-16-17-18-19-00
F	1	22
G	1	56
H	1	29
I	7	35-57-64-68-80-92-02
J	1	23
K	1	45
L	5	36-58-69-81-93
M	3	30-70-82
N	7	46-71-83-94-03-09-07
O	5	24-37-47-72-84
P	3	38-73-85
Q	1	48
R	6	31-74-86-95-04-10
S	8	39-49-75-87-96-05-11-14
T	7	59-76-88-97-06-12-15
U	6	25-50-60-77-89-98
V	1	40
W	1	51
X	1	32
Y	1	41
Z	1	26

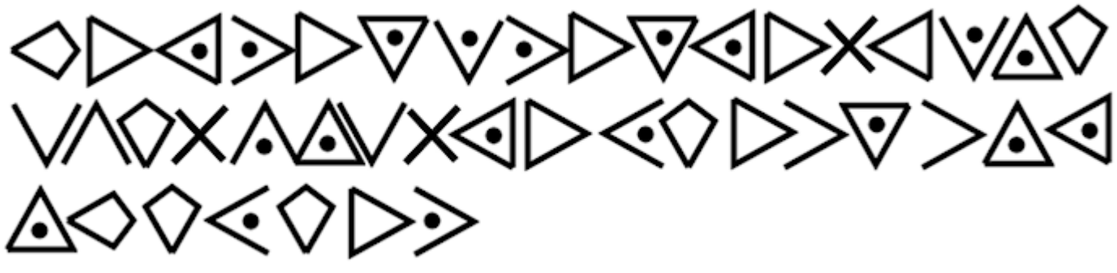
Le chiffre des Templiers

Plutôt que de remplacer chaque lettre par une autre, on peut utiliser des **symboles**. C'est ainsi que procédaient les **Templiers**, au moyen-âge.
Le Temple est à l'origine un ordre de moines fondé au XII^{ème} siècle pour assurer la sécurité des pèlerins qui se rendaient en Terre Sainte. Puis ils s'enrichirent considérablement et devinrent les trésoriers du roi et du Pape. Pour coder les lettres de crédit et les ordres de paiement qu'ils s'échangeaient, ils remplaçaient chaque lettre par un symbole, de la façon suivante :



Le code des Templiers n'est en fait pas très efficace, et très facile à déchiffrer. Chaque lettre étant toujours remplacée par le même signe, il suffit de se baser sur la **fréquence des lettres**, comme pour le **chiffre de César**, pour en venir à bout rapidement. Et comme il n'y avait pas de mot-clé, comme pour le **carré de Polybe**, il suffisait de connaître la correspondance lettres-signes pour déchiffrer ***tous*** les messages des Templiers...

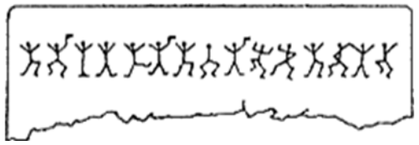
A vous de décoder le message suivant :



Écrivez ci-dessous le texte de ce message, en bon français :
=>

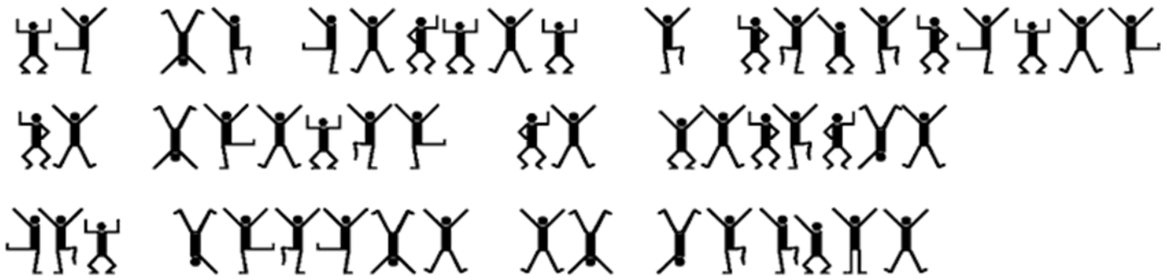
Les hommes dansants

Les hommes dansants est une nouvelle **d'Arthur Conan Doyle** (photo ci-contre), mettant en scène le célèbre détective **Sherlock Holmes**. Dans ce récit, un certain Mr Hilton Cubitt fait appel à lui pour déchiffrer de curieux messages qu'un inconnu trace à la craie sur les rebords de ses fenêtres.

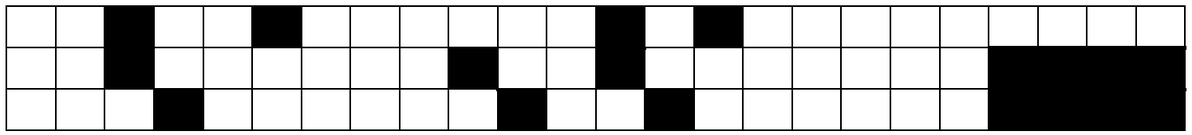


Sherlock Holmes émet l'hypothèse que chaque figurine correspond à une lettre de l'alphabet ce qui est, comme nous l'avons vu précédemment, un code assez facile à déchiffrer. Il suffit de se baser sur la fréquence des lettres, pourvu que le message soit assez long. Dans la langue française**, la lettre la plus utilisée est le E. Puis viennent dans l'ordre le S et le A.**

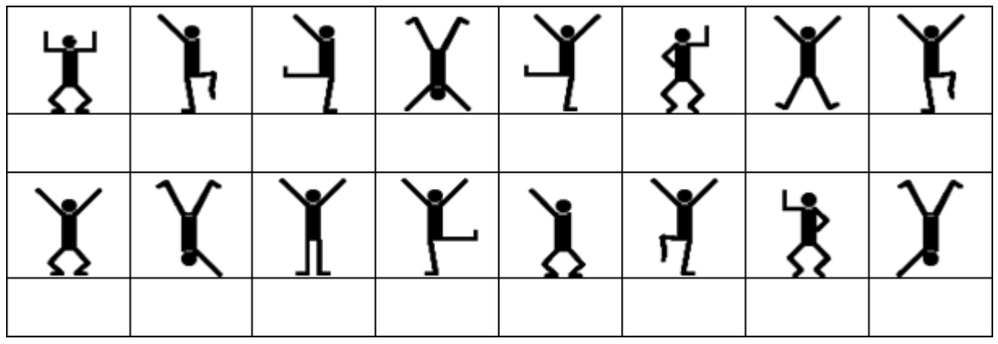
En utilisant cette information, ainsi que la séparation des mots, déchiffrez le message suivant :

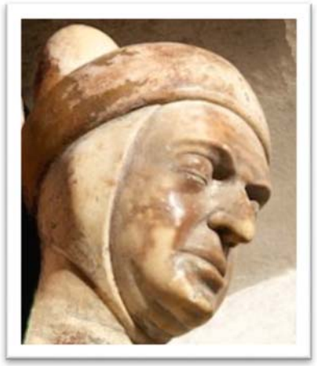


Utilisez le tableau ci-dessous pour saisir le texte en clair :



Il vous faudra bien sûr répertorier puis compter le nombre d'exemplaires de chaque figurine utilisée. Voici de quoi vous aider :





Le chiffre homophone

Nous avons vu précédemment que les systèmes de chiffrage qui se contentent de remplacer une lettre par un signe ou un symbole sont très faciles à décoder, en se basant sur la fréquence des lettres.
En 1411, **Michele Steno**, alors doge (président) de Venise, eut l'idée **d'associer plusieurs symboles à une même lettre**, de façon à empêcher le déchiffrage utilisant la fréquence des lettres.
Cette technique a été encore améliorée depuis : plus une lettre est fréquente, plus il y aura de symboles différents pour la remplacer, de façon à brouiller les pistes.

En utilisant la table de la page suivante, décodez le message suivant.

5135365857 2030694456 3127462855 5939654933 7068872483
8843915472 2540089597 7703226153 8981139832 0604000572 10

Écrivez ci-dessous la phrase en clair, en séparant bien les mots :

=>