LE CHIFFRE DE VIGENERE

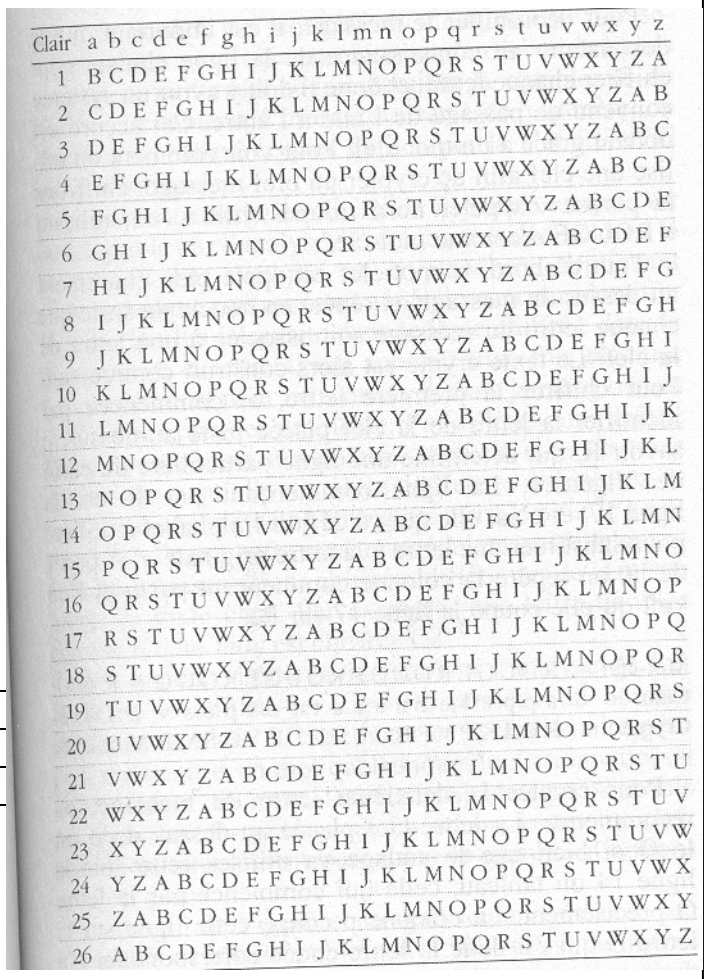
1. Description

La méthode d'analyse de fréquences a permis dès le IXe siècle de déchiffrer la plupart des chiffres connus jusqu'alors. Le diplomate français Blaise de Vigenère inventa au XVIe siècle un nouveau moyen de codage appelé chiffre de Vigenère que l'analyse des fréquences ne permettait pas de déchiffrer. La méthode consiste à utiliser non pas un alphabet pour coder, mais plusieurs .
Par exemple :

clair	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
codage 1	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
codage 2	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

Ce codage permet en utilisant alternativement les deux alphabets de coder BONJOUR en ESQNRYU : ainsi les O de BONJOUR deviennent deux lettres différentes S puis N ce qui complique le déchiffrage.

En fait, en pratique, on utilise un carré de Vigenère comme ci-dessous :



Clair	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
1	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
2	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
3	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
4	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
5	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
6	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
7	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
8	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
9	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
10	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
11	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
12	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
13	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
14	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
15	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
16	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
17	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
18	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
19	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
20	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
21	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
22	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
23	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
24	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
25	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
26	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

Pour chiffrer le message
APPELERNORDTROUPESVILLE,
on choisit un mot-clef, par exemple ROUGE,
et l'on procède comme suit,
la lettre du mot-clef correspondant
à la première lettre de la ligne
du carré de Vigenère à utiliser :

mot clair	APPELERNORDTROUPESVILLE
mot-clef	ROUGEROUGEROUGEROUGE
mot codé	RDJKPVFHUVUHLUYGSMBMCZY

2. Utilisation

Les deux messages suivants forment un télégramme envoyé par l’Allemagne au Mexique mais intercepté et décrypté par les Anglais et qui a pesé pour beaucoup dans l’entrée des Etats-Unis dans la première guerre mondiale.

a) Codage :

Coder le message suivant à l’aide du chiffre de Vigenère et du mot-clef CODAGE :
« Nous avons le projet de lancer une guerre sous-marine totale le premier février,e n nous efforçant malgré tout de préserver la neutralité américaine. Pour le cas où nous ne pourrions y parvenir, nous faisons au Mexique une proposition d’alliance sur la base suivante : faire la guerre ensemble, faire la paix ensemble, un soutien financier généreux, étant entendu de notre part que le Mexique doit reconquérir ses territoires perdus au Texas, au Nouveau-Mexique et en Arizona. A vous de prendre les dispositions appropriées. »

b) Décoder le message suivant à l'aide du chiffre de Vigenère et du mot-clef CODAGE :

XCXSO RHCUM KVGNO EVVGG LDKRV RHCKP CRDNY PGGHC XIVZH

_____ _____ _____ _____ _____ _____ _____ _____ _____

PRYUO ESUPW RHSWY GZHDK GNSQC NIOSQ TJINO JUKVT

_____ _____ _____ _____ _____ _____ _____ _____ _____

SDVKG NSVEZ EVGXN OWUSU AIITH DITIV OMOAX GFHZR

_____ _____ _____ _____ _____ _____ _____ _____

EUIJG KWVWR NWYKZ GEBVC OOOXW FSVAV VQDUE ORKHL AZMXS

_____ _____ _____ _____ _____ _____ _____ _____ _____

VORPK QLTKV NOGHK WKCQI SQGRL AZIFI MAVSP SWETQ GAHTK

_____ _____ _____ _____ _____ _____ _____ _____ _____

QRGHT XINSP EJMCH HUXIP HUERI LOSOT IVBRU YQGAH S

_____ _____ _____ _____ _____ _____ _____ _____ _