Un père de la cryptographie
Blaise de Vigenère
1523 - 1596

Par Daniel TANT

Ce diplomate français a inventé un système polyalphabétique permettant de remplacer une lettre par une autre avec un décalage variable.

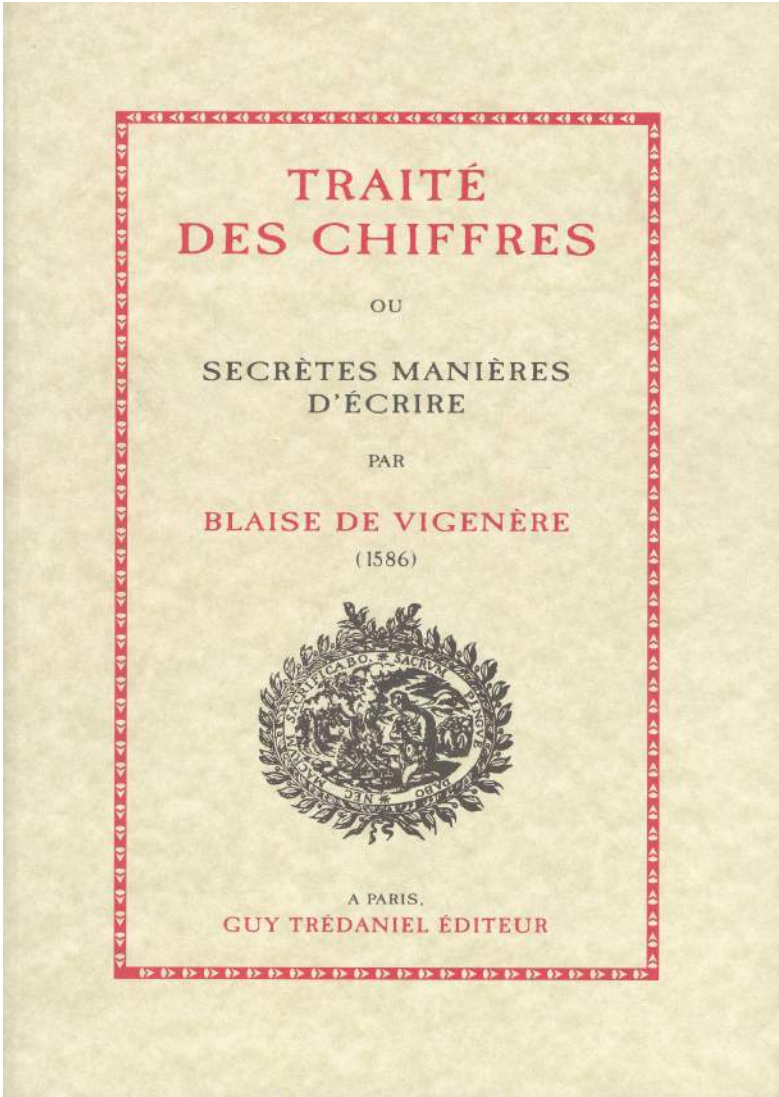
L'ensemble de sa méthode est publiée en 1587 dans « le traité des Chiffres »

Pour chiffrer selon la méthode de Vigenère, il faut d'abord disposer de 26 alphabets, l'un en dessous de l'autre, et décalés à chaque ligne.

Ensuite il faut convenir d'une clé littérale la plus longue possible et qu'il convient de répéter.

Prenons comme exemple de phrase à chiffrer : « Paul Durand viendra ce soir », et la clé : Marseille.

Pour chiffrer la première lettre (le P) il convient de se rendre sur la ligne horizontale correspondant à la première lettre de la clé (le M dans la colonne verte) et relever la lettre à l'angle


TRAITÉ
DES CHIFFRES
OU
SECRÈTES MANIÈRES
D'ÉCRIRE
PAR
BLAISE DE VIGENÈRE
(1586)
A PARIS,
GUY TRÉDANIEL ÉDITEUR

Les éditions Guy Trédaniel ont réédité en fac-simile l'ouvrage de Blaise de Vigenère par un travail très soigné.

de la ligne horizontale du M et de la ligne verticale commençant dans la zone bleue par le P. le chiffre obtenu est le B

Il suffit de continuer. Sur la ligne horizontale du A (vert), chercher la lettre à la verticale du A en clair (en bleu), et nous obtenons A.

Sur la ligne horizontale du R (vert), chercher la lettre à la verticale du U (bleu), et nous obtenons le L.

Et ainsi de suite. Voici le résultat : BALDHCCLRPVZWRLCLGQSJAV.

Clair :	P	A	U	L	D	U	R	A	N	D	V	I	E	N	D	R	A	C	E	S	O	I	R
Clé :	M	A	R	S	E	I	L	L	E	M	A	R	S	E	I	L	L	E	M	A	R	S	E
Chiffre	B	A	L	D	H	C	C	L	R	P	V	Z	W	R	L	C	L	G	Q	S	J	A	V

Association des Réservistes du Chiffre et de la Sécurité de l'Information

Lettres du message en clair

CLE DE CHIFFREMENT	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

ARCSI - Association des Réservistes du Chiffre et de la Sécurité de l'Information
Association régie par la loi de 1901 - N° SIRET : 511 069 569 00016
Tous droits de propriété intellectuelle réservés à l'ARCSI, association loi 1901, selon les règles du droit français