Les chiffrements polyalphabétiques

Ces systèmes de chiffrement sont plus solides que ceux rencontrés précédemment (chiffre de César ou chiffres hébreux). Dans les précédents systèmes, une lettre est toujours remplacée par une même lettre. Dans les systèmes polyalphabétiques, on remplace une lettre par une autre mais qui n'est pas toujours la même. On peut citer deux systèmes respectant ce principe : le chiffre de VIGENERE et le chiffre de PORTA

I- Le chiffre de VIGENERE

Blaise de VIGENERE était un diplomate français. Au début, son intérêt pour la cryptographie était purement pratique et lié à son activité diplomatique. Le chiffre de VIGENERE est une amélioration décisive du chiffre de César. Sa force réside dans l'utilisation non pas d'un mais de 26 alphabets différents pour chiffrer un message . Ce chiffre utilise une clé qui définit le décalage pour chaque lettre du message (A : décalage de 0 cran ; B : 1 cran , C : 2 crans ; ... ; Z : 25 crans). En voici le principe :

a) Principe

Ce chiffrement introduit la notion de clé qui est généralement un mot ou une phrase. Pour pouvoir chiffrer un message, on associe à chaque lettre du message une lettre du mot clé . Ainsi, si on veut chiffrer le mot MATHEMATIQUES avec le mot clé CRYPTO , on peut compléter le tableau suivant :

Clair	M	A	T	H	E	M	A	T	I	Q	U	E	S
Mot clé	C	R	Y	P	T	O	C	R	Y	P	T	O	C

Il faut alors avoir à disposition l'outil indispensable de ce système :

La Table de VIGENERE (voir en annexe)

On repère alors la colonne qui correspond à la lettre en clair puis la ligne qui correspond à la lettre du mot clé . Il ne reste plus qu'à lire la lettre située à l'intersection de cette ligne et de cette colonne.

Vérifier ainsi que MATHEMATIQUES est codée par : ORRWXACKGFNSU

b) Décryptage

Pour décoder un message avec VIGENERE connaissant le mot de passe , on procède comme précédemment c'est à dire que l'on fait correspondre chaque lettre du message codée avec une lettre du mot de passe. Par exemple, voici un message codée avec VIGENERE avec le mot de passe CRYPTO :

EVQIU OVVYJ

Codé	E	V	Q	I	U	O	V	V	Y	J
Mot clé	C	R	Y	P	T	O	C	R	Y	P

On repère alors la ligne qui correspond à la lettre du mot clé puis sur cette ligne, on repère la lettre codée. Il ne reste plus qu'à lire la lettre en clair correspondante.

Décrypter ce message :

II- Le chiffre de PORTA

Le physicien italien Giovani Battista Della Porta fut l'inventeur du premier système de chiffrement poly-alphabétique. Ce système extrêmement robuste pour l'époque fit que l'on considéra PORTA comme le père de la cryptographie moderne. Della Porta a inventé son système de chiffrement en 1563 et il a été utilisé avec succès pendant trois siècles. En voici le principe :

a) Principe

Porta utilise treize (onze à son époque) alphabets différents et un mot clé comme pour Vigenère. Si on reprend MATHEMATIQUES avec le mot clé CRYPTO , on procède alors comme Vigenère :

Clair	M	A	T	H	E	M	A	T	I	Q	U	E	S
Mot clé	C	R	Y	P	T	O	C	R	Y	P	T	O	C

On utilise alors les treize alphabets de PORTA (voir en annexe) :
On repère dans le tableau l'alphabet correspondant à la lettre du mot clé. Par exemple, pour C, on choisit l'alphabet CD. On remplace alors la lettre à coder M par Y (celle qui lui correspond dans cet alphabet). Ainsi, MATHEMATIQUES devient : YSFNVSZBWKDXG

b) Décryptage

Le chiffre de PORTA est un **chiffre réversible**, c'est à dire que pour le décrytpage, on procède de la même manière que pour le cryptage. Décoder ainsi le message suivant utilisant le même mot de passe que précédemment : QQSSV HHSWL V

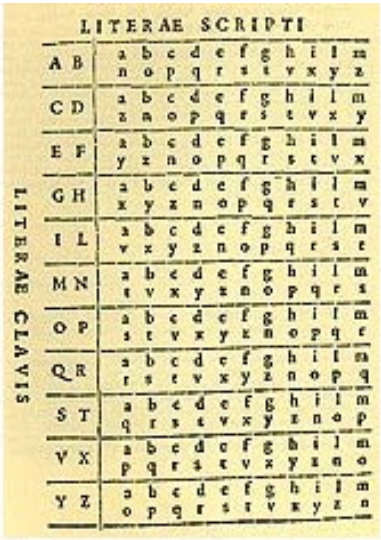
Réponse :

La Table de VIGENERE

CLE UTILISE	LETTRES EN 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**
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

Les Treize alphabets de PORTA

AB	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
CD	a b c d e f g h i j k l m z n o p q r s t u v w x y
EF	a b c d e f g h i j k l m y z n o p q r s t u v w x
GH	a b c d e f g h i j k l m x y z n o p q r s t u v w
IJ	a b c d e f g h i j k l m w x y z n o p q r s t u v
KL	a b c d e f g h i j k l m v w x y z n o p q r s t u
MN	a b c d e f g h i j k l m u v w x y z n o p q r s t
OP	a b c d e f g h i j k l m t u v w x y z n o p q r s
QR	a b c d e f g h i j k l m s t u v w x y z n o p q r
ST	a b c d e f g h i j k l m r s t u v wx y z n o p q
UV	a b c d e f g h i j k l m q r s t u v w x y z n o p
WX	a b c d e f g h i j k l m p q r s t u v w x y z n o
YZ	a b c d e f g h i j k l m o p q r s t u v w x y z n



III- Application

Décrypter les trois messages suivants sachant que deux des trois mots de passe utilisés sont LYCEEN et ETUDIANT

Message 1

BSCXV RECEL RVNGG RWREO WEXEP GPKIA TCWVW CCCPR IAEJG XVNTL NIWVY

EGRMR FPUEG UPRGR XDFYV VIOTJ NIXFP RNIWG PAJRM PTCPW YAMGN PIGLT

CRXYL PTMZR PBWGS AEPQP IHCJG WXRNF PMGVP LUZSA EQGRJ RCKGV EHIRQ

MPRER GWPRN MPXVB WCWVJ ELNRI EYLNQ VXRPR FIQNY BGPIO TJNIX

Message 2 :

WVCHN POJTT YQEFI RHBUB KYYST POQKF HDHPQ DFEMV WVSCE GKKWV EFURW

KXLLG KRYCW VBQGN LBPBL IJYUL DADQU RLZCX UBRRA AHEUL NFXVN ZTQEG

UDGVD CLEXV CVMFN AXAPM EIEOP PWVDZ UBKBF DUXNF MVNYK UYVYJ HJUBG

EYJCV KHGNL

Message 3:

ARLPZ PBSUP EEGZR RKLMX BSEXU RLEUR TGBIR BGRLE TZXBS TRBJR ECREP

LOSXG URSSR TURTS RMHBG MGRBT JEPAA RBSPU XETPU PAXES RRSAE RBBRB

SURNG UURSA XLEPU URETR BJREC REKPB TKPLS ERTSX GURSS RT