CHIFFREMENT DE VIGENÈRE

TI-Nspire™ CAS

Mots-clés : codage, décodage, clé, chiffrement, message, décalage, substitution, programme.

Fichiers associés : vigenere.tns

1. Objectifs

Prendre connaissance du chiffrement polyalphabétique de Vigenère.
Utiliser un tableur pour automatiser le codage et le décodage.
Pour aller plus loin, créer deux programmes permettant d'obtenir le codage et le décodage.

2. Présentation

Pour écrire des messages secrets, on a inventé des procédés de plus en plus sophistiqués. Ainsi, le chiffrement de César consistait simplement à opérer le même décalage, dans l'alphabet, sur toutes les lettres du message : si A est remplacé par D, B sera remplacé par E, … et ainsi de suite. Cette méthode de chiffrement est trop facile à « casser », par exemple en regardant quelle est la lettre la plus fréquente dans un texte qui pourra être E, d'où le décalage.
Blaise de Vigenère (1523 ; 1596), diplomate français, proposait de substituer des lettres par d'autres en utilisant une « clé ». Il ne décalait pas uniformément. Ainsi, si sa clé comporte trois lettres, par exemple ROC, lettres numérotées respectivement 17, 14 et 2 dans l'alphabet, on décale de 17 la première lettre du message, de 14 la 2^{e}, de 2 la 3^{e}, de nouveau de 17 la 4^{e}, de 14 la 5^{e}, etc., ce qui, *a priori*, rend plus difficile la découverte du procédé.
Nous nous proposons de coder des messages avec ce procédé.

N.B. Les lettres de l'alphabet seront numérotées de 0 à 25.

3. Conduite de l'activité

A. Chiffrement de Vigenère

2. Clé : SYMBOLE
Message : HEUREUX QUI COMME ULYSSE.
Message chiffré : ZCGSSFBISUDCXQWSXZGDI.

Justification :

	A	B	C	D	E	F	G
◆		=ord(a[])−65		=ord(c[])−65	=b[]+d[]	=mod(e[],26)	=char(f[]+65)
1	H	7	S	18	25	25	Z
2	E	4	Y	24	28	2	C
3	U	20	M	12	32	6	G
4	R	17	B	1	18	18	S
5	E	4	O	14	18	18	S
6	U	20	L	11	31	5	F
7	X	23	E	4	27	1	B
8	Q	16	S	18	34	8	I
9	U	20	Y	24	44	18	S
10	I	8	M	12	20	20	U
11	C	2	B	1	3	3	D
12	O	14	O	14	28	2	C
13	M	12	L	11	23	23	X

14	M	12	E	4	16	16 Q
15	E	4	S	18	22	22 W
16	U	20	Y	24	44	18 S
17	L	11	M	12	23	23 X
18	Y	24	B	1	25	25 Z
19	S	18	O	14	32	6 G
20	S	18	L	11	29	3 D
21	E	4	E	4	8	8 I

3. Message : A FAIT UN BEAU VOYAGE.
Message chiffré : SDMJHFRTCMVJZCSEQ. Voir Activité 1, page 2 du fichier tns.
4. Message : AAAAAAAA…AA (20 fois la lettre A).
Message chiffré : SYMBOLESYMBOLESYMBOL. Voir Activité 1, page 3 du fichier tns.
On retrouve facilement la clé. Le chiffrement de Vigenère est facile à casser.

B. Pour compliquer un peu
1. Avec ce procédé, si le message à coder est AAAAAAAAAAAAAAAAAAAA,
le message chiffré obtenu est : DJXMZWPDJXMZWPDJXMZW. Voir Activité 2, page 3 du fichier tns.
On s'aperçoit que la clé comporte 7 lettres… Casser le chiffre consiste alors à trouver quelle est exactement la clé. La répétition peut inciter à essayer d'avancer d'un cran chaque lettre, puis de deux crans, etc. jusqu'à trouver la clé qui rendra cohérente le message.
2.

	A	B	C	D	E	F	G
◆		=ord(a[])−65		=ord(c[])−65	=b[]+d[]+11	=mod(e[],26)	=char(f[]+65)
1	H	7	S	18	36	10	K
2	E	4	Y	24	39	13	N
3	U	20	M	12	43	17	R
4	R	17	B	1	29	3	D
5	E	4	O	14	29	3	D
6	U	20	L	11	42	16	Q
7	X	23	E	4	38	12	M
8	Q	16	S	18	45	19	T
9	U	20	Y	24	55	3	D
10	I	8	M	12	31	5	F
11	C	2	B	1	14	14	O
12	O	14	O	14	39	13	N
13	M	12	L	11	34	8	I
14	M	12	E	4	27	1	B
15	E	4	S	18	33	7	H
16	U	20	Y	24	55	3	D
17	L	11	M	12	34	8	I
18	Y	24	B	1	36	10	K
19	S	18	O	14	43	17	R
20	S	18	L	11	40	14	O
21	E	4	E	4	19	19	T

Message : HEUREUX QUI COMME ULYSSE.
Message chiffré : KNRDDQMTDFONIBHDIKROT.
Message : A FAIT UN BEAU VOYAGE.
Message chiffré : DOXUSQCENXGUKNDPB. Voir Activité 2, page 2 du fichier tns.

C. Décodage

	A	B	C	D	E	F	G
◆		=ord(a[])−65		=ord(c[])−65	=b[]−d[]−11	=mod(e[],26)	=char(f[]+65)
1	K	10	S	18	-19	7	H
2	N	13	Y	24	-22	4	E
3	R	17	M	12	-6	20	U
4	D	3	B	1	-9	17	R
5	D	3	O	14	-22	4	E
6	Q	16	L	11	-6	20	U
7	M	12	E	4	-3	23	X
8	T	19	S	18	-10	16	Q
9	D	3	Y	24	-32	20	U
10	F	5	M	12	-18	8	I
11	O	14	B	1	2	2	C
12	N	13	O	14	-12	14	O
13	I	8	L	11	-14	12	M

On vérifie bien, dans la colonne de droite, le texte initial.

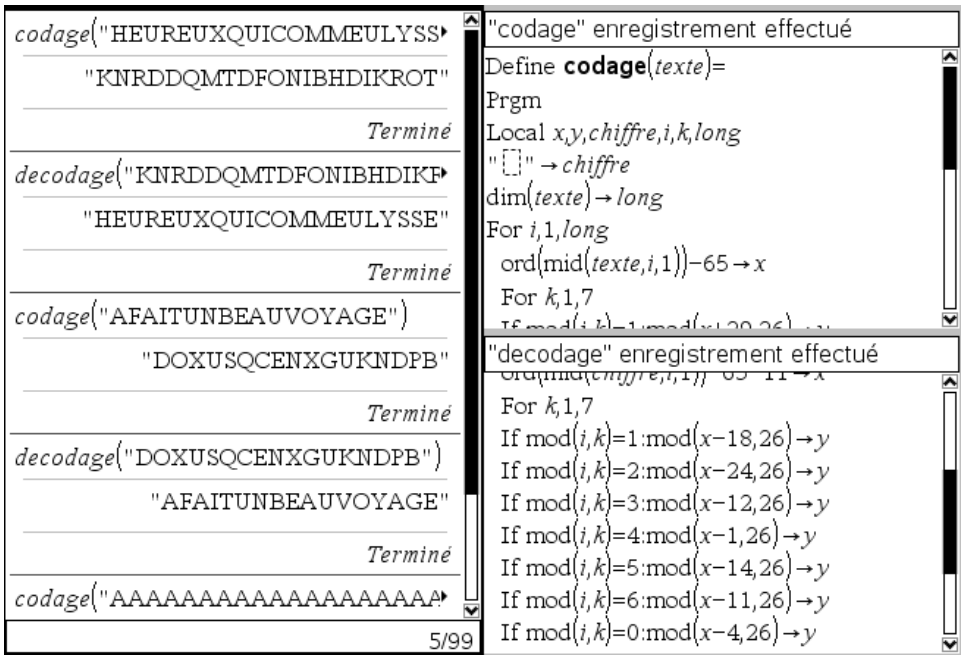
4. Pour aller plus loin : programmation

1. et **2.**

Programme codage	Programme decodage
Define codage(texte)=	Define decodage(chiffre)=
Prgm	Prgm
:Local x,y,chiffre,i,k,long	:Local x,y,texte,i,k,long
:""→chiffre	:""→texte
:dim(texte)→long	:dim(chiffre)→long
:For i,1,long	:For i,1,long
: ord(mid(texte,i,1))-65+11→x	: ord(mid(chiffre,i,1))-65-11→x
: For k,1,7	: For k,1,7
: If mod(i,k)=1:mod(x+18,26)→y	: If mod(i,k)=1:mod(x-18,26)→y
: If mod(i,k)=2:mod(x+24,26)→y	: If mod(i,k)=2:mod(x-24,26)→y
: If mod(i,k)=3:mod(x+12,26)→y	: If mod(i,k)=3:mod(x-12,26)→y
: If mod(i,k)=4:mod(x+1,26)→y	: If mod(i,k)=4:mod(x-1,26)→y
: If mod(i,k)=5:mod(x+14,26)→y	: If mod(i,k)=5:mod(x-14,26)→y
: If mod(i,k)=6:mod(x+11,26)→y	: If mod(i,k)=6:mod(x-11,26)→y
: If mod(i,k)=0:mod(x+4,26)→y	: If mod(i,k)=0:mod(x-4,26)→y
: EndFor	: EndFor
: chiffre&char(y+65)→chiffre	: texte&char(y+65)→texte
:EndFor	:EndFor
:Disp chiffre	:Disp texte
:EndPrgm	:EndPrgm

Les variables utilisées dans le programme, déclarées comme locales, ne sont pas affectées de valeurs hors du programme.
mid(texte,5,1) donne la 5e lettre du texte, mid(texte,5,3) donnerait les 5e, 6e et 7e lettres du texte.
Les lettres du mot SYMBOLE sont numérotées respectivement 18, 24, 12, 1, 14, 11 et 4.
On opère un décalage de 11.
chiffre&char(y+65) ajoute à la suite du mot chiffre déjà constitué la lettre correspondant à char(y+65) :
ainsi, "BEHC"&char(12+65) donne "BEHCM".

3.



5. Pour aller plus loin : compliquer la méthode de chiffrement

Clé de trois unités.

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

1. Message : HEUREUX QUI COMME ULYSSE.
Message chiffré : IOFKOFBSFOCLDPVXRBLAV.

Message chiffré : SOHLBMURLZAOGUTLKVLYRGRLFA.
Message initial : LESSANGLOTSLONGSDESVIOLONS

2. Connaissant la longueur de la clé, il suffit de proposer le message suivant pour reconstituer tout le tableau : AAABBBCCCDDDEEEFFF…ZZZ.

Quelques sources :

- Le chiffre de Vigenère, http://www.bibmath.net/crypto/poly/vigenere.php3

- Traicté des chiffres ou Secrètes manières d'escrire, par Blaise de Vigenère - A. L'Angelier (Paris) – 1586

http://gallica.bnf.fr/ark:/12148/bpt6k73371g.planchecontact.f1

- Wikipedia, http://fr.wikipedia.org/wiki/Chiffre_de_Vigen%C3%A8re