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 (0 pour A, 1 pour B, …, 25 pour Z).

3. Conduite de l'activité

A. Chiffrement de Vigenère

On choisit pour clé le mot SYMBOLE.

1. Le texte à coder est : HEUREUX QUI COMME ULYSSE
On ne tient pas compte des espaces, ni, quand il y en a, des lettres accentuées.
Créer un tableau comportant :
Ligne A : lettres du texte à coder ;
ligne B : numéro b de la lettre dans l'ordre alphabétique (de 0 à 25) ;
ligne C : lettres de la clé SYMBOLESYMBOLESYM… ;
ligne D : numéro d de la lettre ;
ligne E : somme de b et d ;
ligne F : reste de la division euclidienne de (b + d) par 26[1] ;
ligne G : lettre correspondant au reste de la ligne F.
Quel message obtient-on ?

2. Nous nous proposons d'utiliser le tableur de TI-Nspire pour coder les messages.
Attention ! Chaque lettre du message ou de la clé devra être saisie entre guillemets.
Pour remplacer une lettre par son numéro d'ordre dans l'alphabet, on utilise la fonction **ord**.
Ainsi, ord("M") – 65 donne 12.
Pour remplacer le numéro d'ordre par la lettre correspondante, on emploie la fonction **char**.
Ainsi, char(12 + 65) donne M.
Le reste de la division euclidienne d'un nombre par 26 s'obtient par la fonction **mod**.
Ainsi, mod(58,26) donne le reste de la division de 58 par 26.

[1] La somme b + d peut dépasser 25. Il faut donc utiliser le reste de la division de ce nombre par 26 pour tomber sur un nombre de 0 à 25. La lettre numérotée 26, 52, etc. est alors A (comme la lettre numérotée 0) et ainsi de suite.

En utilisant les fonctions ord, mod et char, reproduire, dans le tableur, les 7 lignes du tableau précédent (qu'on présentera en colonnes A à G).
Vérifier qu'on obtient bien le texte codé de la question **1**.
3. Coder le texte : A FAIT UN BEAU VOYAGE.
4. Coder le texte AAAAAAAA…AA (20 fois la lettre A).
Que remarque-t-on ? Le chiffrement de Vigenère est-il facile à casser ?

B. Pour compliquer un peu

On se propose de faire appel aux deux procédés (chiffres de Vigenère et chiffre de César).
Pour Vigenère, on choisit toujours pour clé le mot SYMBOLE.
Pour César, on décale chaque lettre de 11.

1. Dans une nouvelle activité, reproduire la page de tableur du **A**, en ajoutant 11 à chaque nombre de la colonne E. Qu'obtient-on avec le texte ne comportant que des A ? Que remarque-t-on ?

2. Coder avec ce nouveau procédé les deux textes du **A**.

C. Décodage

L'utilisateur qui connaît le code de Vigenère et le décalage de César n'a alors aucun mal à décoder le message.
Ouvrir une nouvelle page de tableur et, en partant de l'un des messages obtenus ci-dessus, créer les colonnes qui vont permettre le décodage de ce texte.
Vérifier que l'on obtient bien le message initial.

4. Pour aller plus loin : programmation

Nous nous proposons de créer un programme de codage et un programme de décodage en utilisant le chiffrement de la partie **4. C.**
Chaque programme devra comporter deux boucles itératives For, l'une pour examiner chaque lettre du message, l'autre pour se préoccuper du rang de cette lettre par rapport aux lettres de la clé SYMBOLE. En effet, si la lettre du message est en 1^{re} , 8^{e}, 15^{e}, etc. elle sera décalée d'un même nombre, mais ce nombre changera si la lettre est en 2^{e}, 9^{e}, 16^{e}, etc. et ainsi de suite.
Pour obtenir la $i^{ème}$ lettre du texte, on écrit : mid(texte, *i*, 1).

1. Ouvrir une page **Calculs** de TI-Nspire et écrire le programme **codage**.

2. Écrire le programme **decodage**.

3. Vérifier que ces deux programmes fonctionnent en utilisant les textes précédents.

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

La méthode de Vigenère consiste à opérer des substitutions de lettres. On peut donc imaginer d'opérer des substitutions qui figureraient dans un tableau porté à la connaissance de l'émetteur et du receveur tel que :

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
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

L'étude de la fréquence des lettres sur un long texte permettrait toutefois de casser, en partie, le codage.
On pourrait alors s'inspirer du chiffrement de Vigenère pour créer un codage qui dépend de la place de la lettre dans le message.

Ainsi, dans le tableau suivant, on utilise une clé de taille 3, c'est-à-dire que les 1^{re} , 4^{e}, 7^{e}, … lettres seront codées avec la lettre correspondante de la ligne 1, les 2^{e} , 5^{e}, 8^{e}, … lettres seront codées avec la lettre de la ligne 2 et les 3^{re} , 6^{e}, 9^{e}, … lettres seront codées avec la lettre de la ligne 3, avec un tableau du type du tableau suivant :

	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

Par exemple, TRIANGLE serait codé ZVRQUTSO.

1. Coder avec cette méthode HEUREUX QUI COMME ULYSSE.
Décoder : SOHLBMURLZAOGUTLKVLYRGRLFA.

2. Imaginer un texte qui permettrait de retrouver l'intégralité du tableau de codage.