CHIFFREMENT DE HILL

TI-Nspire™ CAS

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

Fichiers associés : hill.tns

1. Objectifs

Étudier la méthode de chiffrement polygraphique de Hill dans le cas bigraphique (chiffrement par paquets de 2).
Créer des programmes pour automatiser le codage et le décodage.

2. Présentation

En 1929, Lester S. Hill (1891 – 1961), mathématicien américain, a l'idée de proposer un codage en groupant les lettres du message par bloc de n lettres.
Nous nous proposons de coder des messages avec ce procédé.

Sur indication du professeur, on traitera soit la partie **3**, soit la partie **4**.

3. Conduite de l'activité

Les lettres de l'alphabet seront numérotées de 0 à 25. Les calculs peuvent conduire à des résultats n inférieurs à 0 ou supérieurs à 25. Il faut donc utiliser le reste de la division de n par 26 pour obtenir un nombre de 0 à 25. La lettre numérotée 26, 52, etc. est alors A (comme la lettre numérotée 0) et ainsi de suite.

A. Codage du message

Dans le message, on groupe les lettres par deux. Si le nombre de lettres est impair, on complète la dernière par une lettre arbitraire.

1. Message : BEAUCOUP DE BRUIT.

On groupe les lettres par deux : BE AU CO UP DE BR UI TA (on a complété par A).
Numéroter les lettres en utilisant l'ordre dans l'alphabet de 0 à 25.

Pour chaque groupe de deux lettres, si a et b sont les deux nombres correspondants, on obtient deux nouveaux nombres c et d par : $\begin{cases} c \equiv 11a + 5b \text{ (modulo 26)} \\ d \equiv 7a + 4b \text{ (modulo 26)} \end{cases}$

Quelle est la suite de nombres ainsi obtenue pour le message ci-dessus ?
Revenir aux lettres et donner le message chiffré.

2. On donne le message : TEL EST PRIS QUI CROYAIT PRENDRE.
Préciser le message chiffré obtenu.

B. Recherche du décodage

1. Résolution du système

$$\begin{cases} c \equiv 11a + 5b \text{ (modulo 26)} \\ d \equiv 7a + 4b \text{ (modulo 26)} \end{cases}$$

Éliminer b en utilisant la méthode de résolution par combinaisons.
La division n'est pas possible modulo 26. En revanche, comme le coefficient k de a est premier avec 26, il est inversible modulo 26, c'est-à-dire qu'il existe un nombre i tel que $k \times i \equiv 12$ (modulo 26) (théorème de Bézout).
Multiplier les deux membres de l'équation par i et en déduire a en fonction de c et d modulo 26.

Éliminer a par la même méthode et en déduire b en fonction de c et d modulo 26.

© Texas Instruments 2011 / Photocopie autorisée

2. Décodage

a. En utilisant le système obtenu et en suivant le procédé décrit en **A. 1.**, vérifier que l'on obtient bien les deux messages initiaux du **A**, à partir des deux messages chiffrés.

b. Déchiffrer le message suivant : LPIALPNWSXNWLP.

C. Une programmation

Nous nous proposons de créer un programme de codage et un programme de décodage.
Le programme de codage doit différencier le cas où le nombre de lettres du message est pair du cas où il est impair, puisque dans ce cas on ajoute la lettre A en fin de message.
Pour les fonctions à utiliser dans ces programmes, consulter la partie **5. Annexe : quelques consignes pour la programmation**.

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

2. Écrire le programme **decodage**, en utilisant le résultat de **B.1.**

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

4. Point de vue matriciel et programmation

A. Codage du message

Dans le message, on groupe les lettres par deux. Si le nombre de lettres est impair, on complète la dernière par une lettre arbitraire.

1. Message : BEAUCOUP DE BRUIT.

On groupe les lettres par deux : BE AU CO UP DE BR UI TA (on a complété par A).
Numéroter les lettres en utilisant l'ordre dans l'alphabet de 0 à 25.

Pour chaque groupe de deux lettres, si a et b sont les deux nombres correspondants, on obtient deux nouveaux nombres c et d par :

$\begin{pmatrix} 11 & 5 \\ 7 & 4 \end{pmatrix} * \begin{pmatrix} a \\ b \end{pmatrix} = \begin{pmatrix} x \\ y \end{pmatrix}$ et $c \equiv x$ (modulo 26), $d \equiv y$ (modulo 26).

Quelle est la suite de nombres ainsi obtenue pour le message ci-dessus ?
Revenir aux lettres et donner le message chiffré.

2. On donne le message : TEL EST PRIS QUI CROYAIT PRENDRE.
Préciser le message chiffré obtenu.

B. Recherche du décodage

1. Matrice de décodage

Comment obtenir la matrice de décodage ?
La difficulté réside dans le fait que tous les calculs se font modulo 26 et qu'en conséquence, il n'est pas possible d'obtenir directement la matrice inverse de la matrice M de codage.
• On a recours à la définition de la matrice inverse : la matrice inverse est obtenue en divisant, par le déterminant de M, la transposée de la comatrice de M.

La comatrice d'une matrice $M = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ est : $\begin{pmatrix} d & -c \\ -b & a \end{pmatrix}$.

La transposée d'une matrice $M = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ est : $\begin{pmatrix} a & c \\ b & d \end{pmatrix}$.

Quelle est la transposée M' de la comatrice de la matrice $\begin{pmatrix} 11 & 5 \\ 7 & 4 \end{pmatrix}$?

• La division n'est pas possible modulo 26. En revanche, comme le déterminant n de la matrice est premier avec 26, il est inversible modulo 26, c'est-à-dire qu'il existe un nombre i tel que $n \times i \equiv 1$ (modulo 26).
Déterminer l'inverse i du déterminant de la matrice donnée.

© Texas Instruments 2011 / Photocopie autorisée

• Multiplier la matrice *M'* par *i*.
• Pour les calculs, considérer les restes de la division par 26 des termes de la matrice obtenue.
Préciser quelle est la matrice de décodage.

2. Décodage

a. En utilisant le système obtenu et en suivant le procédé décrit en **A. 1.**, vérifier que l'on obtient bien les deux messages initiaux du **A**, à partir des deux messages chiffrés.

b. Déchiffrer le message suivant : LPIALPNWSXNWLP.

C. Une programmation

Nous nous proposons de créer un programme de codage, un programme de recherche de la matrice de décodage et un programme de décodage.
Le programme de codage doit différencier le cas où le nombre de lettres du message est pair du cas où il est impair, puisque dans ce cas on ajoute la lettre A en fin de message.
Pour les fonctions à utiliser dans ces programmes, consulter la partie **5. Annexe : quelques consignes pour la programmation**.

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

2. Écrire le programme **decodage**, en utilisant le résultat de **B.1.**

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

4. Écrire le programme **recherche**, permettant d'obtenir la matrice de décodage à partir des termes de la matrice de codage.

5. Annexe : quelques consignes pour la programmation

• Les textes de messages sont écrits entre guillemets : par exemple, "ALPHA".

• Pour ajouter une lettre en fin de texte donné, on utilise **&** : par exemple, "ALPHA"&"P" donne "ALPHAP".

• 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 6 de la division de 58 par 26.

• Pour obtenir la $i^{\text{ème}}$ lettre d'un texte, on écrit : mid(texte, *i*, 1).

© Texas Instruments 2011 / Photocopie autorisée