Chiffre de Hill

Résumé

Le chiffre de Hill est une méthode de cryptage symétrique qui utilise certaines propriétés du calcul matriciel. Au fil de ce TD, nous proposons de mettre en place cette technique de cryptage/décryptage de messages textuels.

1 Z_{26}

Durant la suite du TD, on se place dans Z_{26} : nous considérons uniquement des nombres de 0 à 25. Si lors des calculs certains résultats sont négatifs ou supérieurs à 25, les résultats seront ramenés à cet intervalle via l'opération de modulo 26.
Ainsi 13 * 13 = 169 mais 169 est supérieur à 25. On prend donc son résultat modulo 26 : 169 % 26 = 13.
On dit que i est inversible dans Z_{26} s'il existe j dans Z_{26} tel que $i * j(\%26) = 1$ dans Z_{26}.

x	1	3	5	7	9	11	15	17	19	21	23	25
x^{-1}	1	9	21	15	3	19	7	23	11	5	17	25

TABLE 1 – Inverses modulo 26

2 Rappels de calcul matriciel

Durant tout le TD, pour des raisons de simplicité de calcul, nous nous en tiendrons à gérer des **matrices carrées 2,2**. En effet, les formules simples qui suivent ne valent que pour des matrices 2,2.
Soit A une matrice 2,2 : $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$

Soit $com(A)$ la comatrice de A tel que : $com(A) = \begin{pmatrix} d & -c \\ -b & a \end{pmatrix}$

Soit ${}^t(A)$ la transposée de A tel que : ${}^t(A) = \begin{pmatrix} a & c \\ b & d \end{pmatrix}$

Le déterminant $Det(A)$ de la matrice A est calculé comme suit : $Det(A) = ad - cb$

On dit qu'une matrice A est inversible dans Z_{26} si $Det(A)$ possède un inverse dans Z_{26} (voir Tableau 1). L'inverse de $Det(A)$ est noté $Det(A)^{-1}$. La matrice inverse de A notée $(A)^{-1}$ est obtenue de la façon suivante : $(A)^{-1} = {}^t(com(A)) \cdot Det(A)^{-1}$

3 Le chiffre de Hill

3.1 L'encodage du message

Soit le message M codé numériquement suivant la correspondance suivante :

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
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

TABLE 2 – Table de correspondance lettre/nombre

Ainsi, par exemple $GEEK$ se code 6 4 4 10 en utilisant ce système.
Le message m est séparé en bloc de 2 lettres pour être encrypté. GEEK sera donc séparé en deux paires qui seront encryptés tout à tour. D'abord la paire $\begin{pmatrix}6\\4\end{pmatrix}$ puis la paire $\begin{pmatrix}4\\10\end{pmatrix}$.

3.2 Fonctionnement

Soit une matrice inversible $A = \begin{pmatrix}a & b\\c & d\end{pmatrix}$

Pour chiffrer chaque paire d'un message M notée M_i, il suffit d'appliquer une multiplication de matrice : $Chiffre(M_i) = A \cdot M_i$

Pour déchiffrer un message chiffré avec la matrice A, on utilise la matrice inverse A^{-1} : $M_i = A^{-1} \cdot Chiffre(M_i)$

3.3 Travail

Pour réaliser un programme capable d'encrypter/décrypter en utilisant le chiffre de Hill, nous proposons de réaliser plusieurs modules dont voici les rôles.
Conversion chaines de caractères - message numérique :
- Encoder un message reçu sous forme de chaine de caractères en un message numérique
- Encoder un message reçu sous forme numérique en une chaine de caractères

Calcul matriciel :
- Calculer un déterminant
- Vérifier l'inversibilité d'une matrice
- Multiplier deux matrices
- Obtenir la comatrice d'une matrice
- Obtenir la transposée d'une matrice
- Inverser une matrice

Chiffre de Hill :
- Chiffrer avec une matrice A un message M
- Déchiffrer avec une matrice A^{-1} un message M

Une interface utilisateur pour utiliser tous les modules ci-dessus.

4 Exemple

Soit la matrice $A = \begin{pmatrix} 13 & 24 \\ 10 & 13 \end{pmatrix}$ utilisé pour encrypter nos messages.

$Det(A) = 13 \cdot 13 - 10 \cdot 24 = 7$.
Puisque 7 a pour inverse 15 modulo 26 : $(7 \cdot 15)\%26 = 1$, la matrice A est inversible et peut donc nous servir à crypter nos messages.
On inverse donc A :
$(A)^{-1} = {}^t(com(A)) \cdot Det(A)^{-1} = \begin{pmatrix} 13 & 2 \\ 16 & 13 \end{pmatrix} \cdot 15$

$(A)^{-1} = \begin{pmatrix} 13 & 4 \\ 6 & 13 \end{pmatrix}$

Soit le message "BC" à crypter. Son encodage numérique sous forme matricielle est donné par : $\begin{pmatrix} 1 \\ 2 \end{pmatrix}$

Encryptage : $A \cdot \begin{pmatrix} 1 \\ 2 \end{pmatrix} = \begin{pmatrix} 9 \\ 10 \end{pmatrix}$ qui se traduit par le message "JK"

Décryptage : $A^{-1} \cdot \begin{pmatrix} 9 \\ 10 \end{pmatrix} = \begin{pmatrix} 1 \\ 2 \end{pmatrix}$