Cryptologie

Travaux Pratiques

L'objectif de ce TP est d'explorer le chiffrement de Hill.

L'idée de ce principe est qu'au lieu de chiffrer caractère par caractère, on va réunir les caractères par bloc. Ainsi tous les caractères du bloc "influeront" sur le chiffrement des autres.

Pour y arriver nous avons besoin d'un outil mathématique : les matrices.

Les matrices

Dans la suite on fixe un entier $n \geqslant 2$.

Définition

Une **matrice** 2×2 est la donnée d'un tableau à deux lignes et deux colonnes.

On note une matrice

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

On note $\mathcal{M}_2$ l'ensemble des matrices 2×2.

On peut bien sur généraliser cette définition à des matrices à n lignes et m colonnes pour définir $\mathcal{M}_{n,m}$. Cela ne sera pas nécessaire pour la suite.

Par exemple $\begin{pmatrix} 2 & 3 \\ -8 & 7 \end{pmatrix} \in \mathcal{M}_2$

L'ensemble des matrices porte une structure algébrique dit d'anneau. Cela signifie que l'on peut additionner et multiplier des matrices entre elles de manière cohérente.

Définition Opérations

Soient $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ et $B = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}$ des matrices de $\mathcal{M}_2$ et $\lambda \in \mathbb{Z}$

Addition. On pose :

$$A + B \equiv_n \begin{pmatrix} a & b \\ c & d \end{pmatrix} + \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \equiv_n \begin{pmatrix} a+\alpha & b+\beta \\ c+\gamma & d+\delta \end{pmatrix}$$

Multiplication matricielle. On pose

$$A.B \equiv_n \begin{pmatrix} a & b \\ c & d \end{pmatrix} . \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \equiv_n \begin{pmatrix} a\alpha + b\gamma & a\beta + b\delta \\ c\alpha + d\gamma & c\beta + d\delta \end{pmatrix}$$

Multiplication scalaire. On pose

$$\lambda.A \equiv_n \lambda. \begin{pmatrix} a & b \\ c & d \end{pmatrix} \equiv_n \begin{pmatrix} \lambda a & \lambda b \\ \lambda c & \lambda d \end{pmatrix}$$

Les "cohérences" de ces deux opérations sont résumés dans la proposition suivante

Proposition Structure algébrique

Soient A, B et C des matrices de M_2.

Commutativité $+$. $A+B \equiv_n B+A$

Associativité $+$. $(A+B)+C \equiv_n A+(B+C)$

Neutralité $+$. $A+0 \equiv_n 0+A \equiv_n A$ où $0 \equiv_n \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$

Symétrie $+$. $A+(-A) \equiv_n (-A)+A \equiv_n 0$ où $-A$ est la matrice où tous les coefficients ont changé de signe.

Associativité $\times$. $(A.B).C \equiv_n A.(B.C)$

Neutralité $\times$ $A.Id \equiv_n Id.A \equiv_n A$ où $Id \equiv_n \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$

Distributivité. $A(B+C) \equiv_n AB+AC$ et $(A+B)C \equiv_n AC+BC$

Il était nécessaire de donner la règle de la distributivité de la sorte (en précisant la distributivité à droite et a gauche) et cela pour la même raison qui fait que nous n'avons pas écrit la règle "Commutativité $\times$" : le produit des matrices n'est pas commutatif.

Pour le voir, il suffit de traiter un exemple. Considérons les matrices $A = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ et $B = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}$

Alors $AB \equiv_2 \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ et $BA \equiv_2 \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$

Il faut donc prendre garde ! En général, le produit des matrices n'est pas commutatif !

Une autre règle n'est pas vérifiée : celle que nous aurions pu appeler "Symétrie $\times$" qui consisterai à écrire $A.A^{-1} \equiv_n Id \equiv_n A^{-1}.A$. Le problème est que la multiplication étant "étrange" par définition, la division va aussi l'être.

Définition

Soit $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathcal{M}_2$.

On note $\det(A)$ le nombre $ad-bc$ que l'on appelle **déterminant** de A.

Par exemple si $A \equiv_{26} \begin{pmatrix} -5 & 2 \\ 8 & 7 \end{pmatrix} \in \mathcal{M}_2(\mathbb{Z}/26\mathbb{Z})$, alors $\det(A) \equiv_{26} (-5)\times(7)-(8)\times(2) \equiv_{26} -35-16 = -51 \equiv_{26} 1$.

Proposition 0.0.1

Soient A, B des matrices de $\mathcal{M}_2$.

$$\det(AB) \equiv_n \det(A)\det(B)$$

Démonstration. Écrivons $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ et $B = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}$. Alors $A.B \equiv_n \begin{pmatrix} a\alpha+b\gamma & a\beta+b\delta \\ c\alpha+d\gamma & c\beta+d\delta \end{pmatrix}$. Par définition $\det(A) = ad-bc$ et $\det(B) = \alpha\delta-\beta\gamma$. En multipliant ces résultats et en développant on arrive à

$$\det(A)\det(B) = ad\alpha\delta - ad\beta\gamma - bc\alpha\delta + bc\beta\gamma$$

D'autre par le déterminant de $A.B$ se calcul :

$$\begin{aligned}\det(A.B) &= (a\alpha + b\gamma)(c\beta + d\delta) - (c\alpha + d\gamma)(a\beta + b\delta)\\ &= (ac\alpha\beta + ad\alpha\delta + bc\beta\gamma + bd\gamma\delta)\\ &- (ac\alpha\beta + bc\alpha\delta + ad\beta\gamma + bd\gamma\delta)\\ &= ad\alpha\delta + bc\beta\gamma - bc\alpha\delta - ad\beta\gamma\end{aligned}$$

□

Théorème Inverse matricielle modulaire

Soit $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathcal{M}_2$.

La matrice A est inversible si et seulement si $\det(A) = ad - bc$ est inversible modulo n. Précisément, si on note A^{-1} cet inverse alors

$$A^{-1} \equiv_n \det(A)^{-1} \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}$$

où $\det(A)^{-1}$ désigne l'inverse de $\det(A)$ modulo n.

Démonstration. Si $\det(A)$ est inversible modulo n, on vérifie très facilement que $A.A^{-1} \equiv_n A^{-1}.A \equiv_n \mathrm{Id}$ pour le A^{-1} donné dans l'énoncé du théorème. Inversement si A est inversible alors il existe A^{-1} tel que $A.A^{-1} = A^{-1}.A = \mathrm{Id}$. En passant au déterminant et en utilisant la proposition précédente, on arrive à $\det(A)\det(A^{-1}) \equiv_n \det(A^{-1})\det(A) \equiv_n \det(\mathrm{Id}) \equiv_n 1$. □

Par exemple $A \equiv_{26} \begin{pmatrix} 5 & 3 \\ 4 & 2 \end{pmatrix} \in \mathcal{M}_2$. On a $\det(A) \equiv_{26} 10 - 12 \equiv_{26} -2$. Il faut voir si cet élément est inversible modulo 26. Il faut pour cela qu'il soit premier avec 26, ce qui n'est clairement pas le cas. Conclusion : la matrice A n'est pas inversible modulo 26.

Autre exemple avec $A \equiv_{26} \begin{pmatrix} 5 & 3 \\ -7 & -2 \end{pmatrix} \in \mathcal{M}_2$. On a $\det(A) \equiv_{26} (-10) - (-21) \equiv_{26} 11$.

En appliquant l'algorithme d'Euclide étendue, on détermine que $26(3) + (11)(-7) = 1$ soit encore $11(-7) \equiv_{26}$ et $11^{-1} \equiv_{26} -7$.

a	b	r	q	u	v
26	11	4	2	3	−7
11	4	3	2	−1	3
4	3	1	1	1	−1
3	1	0	3	0	1

En appliquant la formule on arrive à

$$\begin{pmatrix} 5 & 3 \\ -7 & -2 \end{pmatrix}^{-1} \equiv_{26} -7 \begin{pmatrix} -2 & -3 \\ 7 & 5 \end{pmatrix} \equiv_{26} \begin{pmatrix} 14 & 21 \\ -49 & -35 \end{pmatrix} \equiv_{26} \begin{pmatrix} 14 & 21 \\ 3 & 17 \end{pmatrix}$$

Principe du chiffrement

Les clefs de chiffrement de la méthode de Hill sont les matrices qui admettent un inverse modulaire.

Prenons comme exemple la matrice $A = \begin{pmatrix} 5 & 3 \\ -7 & -2 \end{pmatrix}$ qui est bien inversible puisque $\det(A) = 11$ est un nombre premier avec 26.

Chiffrons le message *CHIFFREMENTDEHILL*

Texte	C	H	I	F	F	R	E	M	E	N	T	D	E	H	I	L	L	
Codage	2	7	8	5	5	17	4	12	4	13	19	3	4	7	8	11	11	
Vecteur X	(2,7)		(8,5)		(5,17)		(4,12)		(4,13)		(19,3)		(4,7)		(8,11)		(11,0)	
A.X	(31,−28)		(55,−66)		(76,−69)		(56,−52)		(59,−54)		(104,−139)		(41,−42)		(73,−78)		(55,−77)	
$\equiv_{26}$	(5,24)		(3,12)		(24,9)		(4,0)		(7,24)		(0,17)		(15,10)		(21,0)		(3,1)	
Dépaquetage	5	24	3	12	24	9	4	0	7	24	0	17	15	10	21	0	3	1
Décodage	F	Y	D	M	Y	J	A	E	H	Y	A	R	P	K	V	A	D	B

Ainsi le message chiffré est *FYDMYJAEHYARPKVADB*.

Inversement : imaginons avoir reçu le *DTQUCTEQGDAA* obtenue par un chiffrement de Hill de matrice $A = \begin{pmatrix} 9 & 4 \\ 5 & 7 \end{pmatrix}$. La première étape consiste à déterminer l'inverse de A et avant cela il faut calculer son déterminant et l'inverse de celui-ci.

Calcul du déterminant. $\det(A) = 9 \times 7 - 5 \times 4 = 63 - 20 = 43 \equiv_{26} 17$

Calcul de l'inverse du déterminant.

a	b	r	q	u	v
26	17	9	1	2	−3
17	9	8	1	−1	2
9	8	1	1	1	−1
8	1	0	8	0	1

Ainsi $17^{-1} \equiv_{26} -3 (\equiv_{26} 23)$

Calcul de l'inverse de la matrice. On applique la formule :

$$A^{-1} \equiv_{26} -3 \begin{pmatrix} 7 & -4 \\ -5 & 9 \end{pmatrix} \equiv_{26} \begin{pmatrix} -21 & 12 \\ 15 & -27 \end{pmatrix} \equiv_{26} \begin{pmatrix} 5 & 12 \\ 15 & -1 \end{pmatrix}$$

Ceci étant on peut déchiffrer le message.

	D	T	Q	U	C	T	E	Q	G	D	A	
Codage	3	19	16	20	2	19	4	16	6	3	0	
Vecteur X	(3,19)		(16,20)		(2.19)		(4,16)		(6,3)		(0,0)	
$A^{-1}.X$	(243,26)		(320,220)		(238,11)		(212,44)		(66,87)		(0,0)	
$\equiv_{26}$	(9,0)		(8,12)		(4,11)		(4,18)		(14,9)		(0,0)	
Dépaquetage	9	0	8	12	4	11	4	18	14	9	0	0
Décodage	J	A	I	M	E	L	E	S	O	J	A	A

Cryptanalyse

L'attaque classique du chiffrement de Hill est l'**attaque à clair connu**.

Le principe de l'attaque à clair connu réside dans le fait que l'on ne possède pas seulement le message chiffré. On possède également un partie du texte claire [1].

Imaginons que vous interceptiez un flux d'information entre enseignants qui ont pris la peine de chiffrer leurs communications et ne se sont pas retenus de dire à leurs étudiants *"De toute manière nous utilisons un chiffrement de Hill pour toute nos communications."*. Vous interceptez un document `Exam_crypto.txt`. En l'ouvrant, bien sur tout est codé : *YXYIEZLD...*. Vous savez, que comme tout examen qui se respecte, il est fort probable que les premiers mots soient *EXAMENDECRYPTO*. Sachant qu'il s'agit d'un chiffrement de

1. C'est par ce type d'attaque qu'Alan Türing a réussi à casser *ENIGMA*

Hill, la clef est une matrice $A \equiv_{26} \begin{pmatrix} a & b \\ c & d \end{pmatrix}$. En comparant la chaine dans le document et la chaine supposé on en déduit que "A.EX=YX", "A.AM=YI", "A.EN=EZ" et "A.DE=LD". En replaçant par les valeurs numériques, on arrive à quatre équations :

1. $A \begin{pmatrix} E \\ X \end{pmatrix} = \begin{pmatrix} Y \\ X \end{pmatrix} \Leftrightarrow A \begin{pmatrix} 4 \\ 23 \end{pmatrix} \equiv_{26} \begin{pmatrix} 24 \\ 23 \end{pmatrix}$ **3.** $A \begin{pmatrix} E \\ N \end{pmatrix} = \begin{pmatrix} E \\ Z \end{pmatrix} \Leftrightarrow A \begin{pmatrix} 4 \\ 13 \end{pmatrix} \equiv_{26} \begin{pmatrix} 4 \\ 25 \end{pmatrix}$

2. $A \begin{pmatrix} A \\ M \end{pmatrix} = \begin{pmatrix} Y \\ I \end{pmatrix} \Leftrightarrow A \begin{pmatrix} 0 \\ 12 \end{pmatrix} \equiv_{26} \begin{pmatrix} 24 \\ 8 \end{pmatrix}$ **4.** $A \begin{pmatrix} D \\ E \end{pmatrix} = \begin{pmatrix} L \\ D \end{pmatrix} \Leftrightarrow A \begin{pmatrix} 3 \\ 4 \end{pmatrix} \equiv_{26} \begin{pmatrix} 11 \\ 3 \end{pmatrix}$

On peut, grâce aux définitions du calcul matricielle, "fusionner" deux équations. Par exemple l'équation 1 et l'équation 2 donnent l'équation 1.2 : $A \begin{pmatrix} 4 & 0 \\ 23 & 12 \end{pmatrix} = \begin{pmatrix} 24 & 24 \\ 23 & 8 \end{pmatrix}$ qui se résout simplement en inversant la matrice à droite de A. Précisément : $A = \begin{pmatrix} 24 & 24 \\ 23 & 8 \end{pmatrix} . \begin{pmatrix} 4 & 0 \\ 23 & 12 \end{pmatrix}^{-1}$. Pour pouvoir réaliser cette opération, il faut que la matrice soit inversible, c'est à dire que son déterminant, soit premier avec 26. Or $\texttt{det} \begin{pmatrix} 4 & 0 \\ 23 & 12 \end{pmatrix} = 48$ et $\text{PGCD}(26,48) = 2$. La matrice n'est donc pas inversible. Il faut être capable de trouver une matrice inversible en combinant les équations. Plus on dispose de *clair connu*, plus on dispose d'équation et donc plus il va être facile de trouver une matrice inversible. Dans cet exemple, avec les 4 équations dont nous disposons, nous pouvons former six matrices :

Équation 1.2 : $A \begin{pmatrix} 4 & 0 \\ 23 & 12 \end{pmatrix} \equiv_{26} \begin{pmatrix} 24 & 24 \\ 23 & 8 \end{pmatrix}$ et $\texttt{det} \begin{pmatrix} 4 & 0 \\ 23 & 12 \end{pmatrix} \equiv_{26} 48$ qui n'est pas premier avec 26.

Équation 1.3 : $A \begin{pmatrix} 4 & 4 \\ 23 & 13 \end{pmatrix} \equiv_{26} \begin{pmatrix} 24 & 4 \\ 23 & 25 \end{pmatrix}$ et $\texttt{det} \begin{pmatrix} 4 & 4 \\ 23 & 13 \end{pmatrix} \equiv_{26} -40$ qui n'est pas premier avec 26

Équation 1.4 : $A \begin{pmatrix} 4 & 3 \\ 23 & 4 \end{pmatrix} \equiv_{26} \begin{pmatrix} 24 & 11 \\ 23 & 3 \end{pmatrix}$ et $\texttt{det} \begin{pmatrix} 4 & 3 \\ 23 & 4 \end{pmatrix} \equiv_{26} -53 \equiv_{26} -1$ qui est premier avec 26.

Dans ce cas

$$A \equiv_{26} \begin{pmatrix} 24 & 11 \\ 23 & 3 \end{pmatrix} . \begin{pmatrix} 4 & 3 \\ 23 & 4 \end{pmatrix}^{-1} \equiv_{26} \begin{pmatrix} 24 & 11 \\ 23 & 3 \end{pmatrix} . \begin{pmatrix} -4 & 3 \\ 23 & -4 \end{pmatrix} \equiv_{26} \begin{pmatrix} 1 & 2 \\ 3 & 5 \end{pmatrix}$$

Équation 2.3 : $A \begin{pmatrix} 0 & 4 \\ 12 & 13 \end{pmatrix} \equiv_{26} \begin{pmatrix} 24 & 4 \\ 8 & 25 \end{pmatrix}$ et $\texttt{det} \begin{pmatrix} 0 & 4 \\ 12 & 13 \end{pmatrix} \equiv_{26} -48$ qui n'est pas premier avec 26

Équation 2.4 : $A \begin{pmatrix} 0 & 3 \\ 12 & 4 \end{pmatrix} \equiv_{26} \begin{pmatrix} 24 & 11 \\ 8 & 3 \end{pmatrix}$ et $\texttt{det} \begin{pmatrix} 0 & 3 \\ 12 & 4 \end{pmatrix} \equiv_{26} -36$ qui n'est pas premier avec 26

Équation 3.4 : $A \begin{pmatrix} 4 & 3 \\ 13 & 4 \end{pmatrix} \equiv_{26} \begin{pmatrix} 4 & 11 \\ 25 & 3 \end{pmatrix}$ et $\texttt{det} \begin{pmatrix} 4 & 3 \\ 13 & 4 \end{pmatrix} \equiv_{26} -23 \equiv_{26} 3$ qui est premier avec 26.

Dans ce cas

$$A \equiv_{26} \begin{pmatrix} 4 & 11 \\ 25 & 3 \end{pmatrix} . \begin{pmatrix} 4 & 3 \\ 13 & 4 \end{pmatrix}^{-1} \equiv_{26} \begin{pmatrix} 4 & 11 \\ 25 & 3 \end{pmatrix} . \begin{pmatrix} 10 & -1 \\ -13 & 10 \end{pmatrix} \equiv_{26} \begin{pmatrix} 1 & 2 \\ 3 & 5 \end{pmatrix}$$

A chaque fois qu'il est possible d'inverser la matrice on trouve $A \equiv_{26} \begin{pmatrix} 1 & 2 \\ 3 & 5 \end{pmatrix}$ qui est donc la clef de chiffrement.

Pour déchiffrer il faudra appliquer la matrice inverse $A^{-1} \equiv_{26} \begin{pmatrix} 1 & 2 \\ 3 & 5 \end{pmatrix}^{-1} \equiv_{26} \begin{pmatrix} -5 & 2 \\ 3 & -1 \end{pmatrix}$