Analyse mathématique de la cryptographie de Hill

Le but de ce problème est d'étudier, d'un point de vue mathématique, un algorithme de chiffrement dû à Lester Hill en 1929.

Description

Nous supposons que nous avons un message à coder écrit avec les lettres A jusque Z (en majuscules). L'idée de Lester Hill est de grouper les lettres du message par bloc de m lettres, puis de les coder simultanément. Dans toute la suite, nous prenons $m = 2$. D'abord, on remplace chaque lettre par un nombre compris entre 0 et 25 : A devient 0, B devient 1, ..., Z devient 25. On groupe les nombres ainsi obtenus 2 par 2 : x_1x_2,x_3x_4,...,$x_{2n-1}x_{2n}$. Chaque groupe de 2 nombres x_kx_{k+1} est codé en utilisant des combinaisons linéaires fixées au préalable :

$$\left\{ \begin{array}{rcl} y_k & = & ax_k + bx_{k+1} \\ y_{k+1} & = & cx_k + dx_{k+1} \end{array} \right.$$

a,b,c,d sont des entiers. On retransforme alors les nombres obtenus en lettres par la même opération que précédemment (0 devient A,...). Bien sûr, l'entier y_k n'est plus forcément compris entre 0 et 25, mais on le remplace alors par son reste modulo 26.

Mathématisation

Au choix de la combinaison linéaire, on associe une matrice de chiffrement

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

Puisque tous les calculs que nous effectuons sont modulo 26, on considère cette matrice d'entiers comme étant à coefficients dans $\mathbb{Z}|26\mathbb{Z}$. Le produit de deux matrices de $\mathbb{Z}|26\mathbb{Z}$ est défini comme usuellement. A tout vecteur $\begin{pmatrix} x_1 \\ x_2 \end{pmatrix}$ de $\mathbb{Z}|26\mathbb{Z}$, on associe $\begin{pmatrix} y_1 \\ y_2 \end{pmatrix} = A \begin{pmatrix} x_1 \\ x_2 \end{pmatrix}$.

$\begin{pmatrix} y_1 \\ y_2 \end{pmatrix}$ est le bloc codé correspondant à $\begin{pmatrix} x_1 \\ x_2 \end{pmatrix}$.

Exemple

On souhaite coder le mot ELECTION avec la clé (ou matrice) de chiffrement $\begin{pmatrix} 3 & 5 \\ 1 & 2 \end{pmatrix}$.

- On remplace par des nombres, et on sépare en blocs de 2 :

$$4 - 11|4 - 2|19 - 8|14 - 13.$$

- On calcule les vecteurs images :

$$\begin{pmatrix} 3 & 5 \\ 1 & 2 \end{pmatrix} \begin{pmatrix} 4 \\ 11 \end{pmatrix} = \begin{pmatrix} 15 \\ 0 \end{pmatrix}; \begin{pmatrix} 3 & 5 \\ 1 & 2 \end{pmatrix} \begin{pmatrix} 4 \\ 2 \end{pmatrix} = \begin{pmatrix} 22 \\ 8 \end{pmatrix}$$

$$\begin{pmatrix} 3 & 5 \\ 1 & 2 \end{pmatrix} \begin{pmatrix} 19 \\ 8 \end{pmatrix} = \begin{pmatrix} 19 \\ 9 \end{pmatrix}; \begin{pmatrix} 3 & 5 \\ 1 & 2 \end{pmatrix} \begin{pmatrix} 14 \\ 13 \end{pmatrix} = \begin{pmatrix} 3 \\ 14 \end{pmatrix}.$$

- On retranscrit en lettres : PAWITJDO

On peut remarquer un des intérêts du chiffre de Hill sur l'exemple précédent : la lettre E est une fois codée avec P, l'autre fois avec W. C'est ce que l'on appelle un chiffrement polyalphabétique.

Questions

1. Coder MATHEMATIQUE avec la clé $\begin{pmatrix} 9 & 4 \\ 5 & 7 \end{pmatrix}$.
2. Expliquer pourquoi les matrices de chiffrement $\begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$ et $\begin{pmatrix} 1 & 2 \\ 2 & 4 \end{pmatrix}$ ne peuvent convenir.

3. $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ étant une matrice de $\mathbb{Z}|26\mathbb{Z}$, on pose $B = \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}$. Calculer AB.
4. Montrer que A est inversible si, et seulement si, $\det A$ est inversible dans $\mathbb{Z}|26\mathbb{Z}$. Expliquer alors pourquoi le chiffrement de Hill est inversible.
5. Votre allié vous a envoyé le message suivant : UWGMWZRREIUB. Vous avez convenu avec lui d'utiliser le chiffrement de Hill, avec comme clé de chiffrement la matrice $\begin{pmatrix} 9 & 4 \\ 5 & 7 \end{pmatrix}$. Quel message voulait-il vous transmettre?
6. **Attaque du chiffre de Hill :** Vous avez intercepté le message suivant de vos ennemis : YKTZZUDCLWQOAGKIHXRVANYSPWBYDCLS. Votre espion vous a informé que pour communiquer, l'état-major adverse utilise le chiffrement de Hill. En outre, connaissant le côté protocolaire des messages militaires, vous êtes sûr que ce message commence par MONGENERAL. On note A la matrice de chiffrement.
   (a) Justifier que
   $$\begin{pmatrix} 24 & 19 \\ 10 & 25 \end{pmatrix} = A \begin{pmatrix} 12 & 13 \\ 14 & 6 \end{pmatrix}. \tag{1}$$
   (b) Que suffirait-il pour retrouver A. Pourquoi cela est impossible ici?
   (c) Retrouver A en exploitant une autre égalité comme (1).
   (d) (Subsidiaire) Décrypter le message complet!