Systèmes et sécurité : Introduction à la cryptographie

Fangan-Yssouf Dosso

dosso@univ-tln.fr

IMATH, Université de Toulon

April 12, 2021

Chiffre de Hill

On considère un alphabet de d caractères. Dans le cas de l'alphabet classique, $d = 26$.

Le principe

- Un schéma de chiffrement par **substitution polyalphabétique**.
- $\mathfrak{M} = \mathfrak{C} = \{$l'ensemble des textes possibles avec les d lettres de l'alphabet$\} = \{0, 1, 2, \ldots, (d-1)\}^*$
- $\mathfrak{K} = \{k \in \mathcal{M}_{n \times n}(\mathbb{Z}/d\mathbb{Z})$, tel que k est inversible$\}$, avec $n \in \mathbb{N}^*$.
- Le message est chiffré en substituant ses lettres par **bloc** (i.e. groupe de lettres).
- n est la **taille** des blocs.

substitution polyalphabétique : une même lettre peut être remplacée par des lettres différentes.

Chiffre de Hill : génération des paramètres

Dans l'ordre :

- On choisit un entier $n \geqslant 2$ qui sera la taille des blocs.
- On génère une matrice $A \in \mathcal{M}_{n\times n}(\mathbb{Z}/d\mathbb{Z})$ qui est inversible.
- On calcule l'inverse B de A dans $\mathcal{M}_{n\times n}(\mathbb{Z}/d\mathbb{Z})$.

Chiffre de Hill : génération des paramètres

Dans l'ordre :

- On choisit un entier $n \geqslant 2$ qui sera la taille des blocs.
- On génère une matrice $A \in \mathcal{M}_{n\times n}(\mathbb{Z}/d\mathbb{Z})$ qui est inversible.
- On calcule l'inverse B de A dans $\mathcal{M}_{n\times n}(\mathbb{Z}/d\mathbb{Z})$.

Remarque

- La matrice A est inversible dans $\mathcal{M}_{n\times n}(\mathbb{Z}/d\mathbb{Z})$ si et seulement si son déterminant $\det(A)$ est inversible dans $\mathbb{Z}/d\mathbb{Z}$.
  Donc, $\det(A)$ doit être premier avec d.
- Si d est un nombre premier, alors $\mathbb{Z}/d\mathbb{Z}$ est un corps.
  Dans ce cas, le calcul de l'inverse de A peut être fait en utilisant l'élimination de Gauss-Jordan (déjà vue au semestre 1).

Chiffre de Hill : exercice

On prend $n = 3$ et $d = 29$.
La matrice A ci-dessous est-elle inversible dans $\mathcal{M}_{3\times 3}(\mathbb{Z}/29\mathbb{Z})$?
Si oui, quel est son inverse ?

$$A = \begin{pmatrix} 14 & 17 & 4 \\ 28 & 20 & 10 \\ 19 & 20 & 27 \end{pmatrix}$$

Chiffre de Hill : chiffrement

Le principe

- Chaque caractère est d'abord codé par un nombre compris entre 0 et $d-1$.
- On découpe le message en blocs de taille n.
  Si le dernier bloc n'est pas de taille n, on le complétera de façon arbitraire, avec des éléments de $\mathbb{Z}/d\mathbb{Z}$, pour avoir la bonne taille.
- Chaque bloc est ensuite chiffré en le multipliant par la matrice A.

Chiffre de Hill : exemple de chiffrement

On prend $n = 3$ et $d = 26$. On identifie les lettres de l'alphabet aux nombres de 0 à 25, i.e. $a = 0$, $b = 1$, ..., $z = 25$.

- Texte en clair : Ceci est un cours sur le chiffre de Hill
- Clé :

$$A = \begin{pmatrix} 19 & 6 & 13 \\ 5 & 14 & 2 \\ 10 & 9 & 1 \end{pmatrix}$$

Le texte en clair découpé et complété donne les blocs suivants : $(2, 4, 2)$, $(8, 4, 18)$, $(19, 20, 13)$, $(2, 14, 20)$, $(17, 18, 18)$, $(20, 17, 11)$, $(4, 2, 7)$, $(8, 5, 5)$, $(17, 4, 3)$, $(4, 7, 8)$, $(11, 11, 0)$.

*les espaces sont ignorés.

Chiffre de Hill : exemple de chiffrement

On chiffre ensuite chacun des blocs avec la matrice A. Par exemple, le premier bloc $(2, 4, 2)$ est chiffré comme suit :

$$\begin{pmatrix} 10 \\ 18 \\ 6 \end{pmatrix} = \begin{pmatrix} 19 & 6 & 13 \\ 5 & 14 & 2 \\ 10 & 9 & 1 \end{pmatrix} \begin{pmatrix} 2 \\ 4 \\ 2 \end{pmatrix}$$

- En procédant de la même manière pour chacun des blocs, on obtient la séquence suivante : $(10, 18, 6)$, $(20, 2, 4)$, $(0, 11, 19)$, $(18, 12, 10)$, $(15, 9, 12)$, $(1, 22, 0)$, $(23, 10, 13)$, $(13, 16, 0)$, $(22, 17, 1)$, $(14, 4, 7)$, $(15, 1, 1)$.
- Le message chiffré est la concaténation des lettres associées aux chiffres de ces blocs :

  ksgucealtsmkpjmbwaxknnqawrboehpbb

Chiffre de Hill : déchiffrement

Le principe est le même que celui du chiffrement. L'unique différence est qu'on effectue ici les multiplications des blocs par l'inverse de la matrice A utilisée pour le chiffrement.

Exercice

Déchiffrer le message suivant :

rjhcbrqgkjzsiummntxknnqajjklgu

La clé de chiffrement est la matrice A de l'exemple précédent, avec $d = 26$.

Chiffre de Hill : cryptanalyse

Contexte

- L'objectif est de retrouver la valeur de la matrice de chiffrement A, pour ensuite déchiffrer tout le message.
- On suppose ici que les valeurs de n et d sont connues.
- Exemples d'attaques possibles : attaque par les digrammes, attaque à clairs (partiellement) connus, attaque à clairs choisis.

Chiffre de Hill : cryptanalyse

Contexte

- L'objectif est de retrouver la valeur de la matrice de chiffrement A, pour ensuite déchiffrer tout le message.
- On suppose ici que les valeurs de n et d sont connues.
- Exemples d'attaques possibles : attaque par les digrammes, attaque à clairs (partiellement) connus, attaque à clairs choisis.

Avec n n-grammes, on peut écrire une **égalité matricielle** qui permet de déterminer A, sous certaines conditions.

*n-gramme = bloc de taille n.

Chiffre de Hill : cryptanalyse

Exemple, avec $n = 2$.

Avec deux digrammes (x_1, x_2) et (x_3, x_4) qui sont chiffrés respectivement en (y_1, y_2) et (y_3, y_4), on peut écrire :

$$\begin{pmatrix} y_1 & y_3 \\ y_2 & y_4 \end{pmatrix} = A \begin{pmatrix} x_1 & x_3 \\ x_2 & x_4 \end{pmatrix}$$

Si la matrice $\begin{pmatrix} x_1 & x_3 \\ x_2 & x_4 \end{pmatrix}$ est **inversible** dans $\mathcal{M}_{2\times 2}(\mathbb{Z}/d\mathbb{Z})$, alors l'égalité ci-dessus peut être réécrite comme suit :

$$A = \begin{pmatrix} y_1 & y_3 \\ y_2 & y_4 \end{pmatrix} \begin{pmatrix} x_1 & x_3 \\ x_2 & x_4 \end{pmatrix}^{-1}$$

Chiffre de Hill : exercice de cryptanalyse

On suppose que $d = 26$ et $n = 3$.
Vous disposez des trigrammes $(1, 0, 0)$, $(0, 1, 0)$ et $(0, 0, 1)$ qui sont chiffrés respectivement en $(15, 15, 0)$, $(3, 7, 23)$ et $(12, 15, 17)$.
Déterminer la clé de chiffrement, puis le message clair associé au cryptogramme suivant :

tpwhcjsurlwdzyyedjiwgmjtuxjnwsrqnlpvybbdfrjlhsrjowgdzwhcjsurknb
ecldvgilwzpnhjoyuwedjzfvhcjsurknbsahdfalkjbhxjfgxtqyaannkowgpkz
uwrpbososoyyldtnwwkrdkkydqnbvypvenjbzimvxhsptkwkwrzdsrqflhni
sbjjiamndhkgphizujfurpuyiigjoynlgvvkpuyixfmgazzknlhrrliboowggorb
rrfqonqrfbbkyiiwgmjtuxjnwshxoewrjvaobhybbhxbpxwiia