Chiffrement de Lester Hill

Le chiffrement de Lester Hill est un crypto système conçu en 1929 pour résister aux analyses de fréquences.

Principe

Soit n et m deux entiers naturels supérieurs ou égaux à 2, et K une matrice carrée inversible de format (n, n) à coefficients dans $\mathbf{Z}_m$ (= $\mathbf{Z}/m\mathbf{Z}$**).**

L'application qui, à toute matrice colonne X de format (n,1) et à coefficients dans $\mathbf{Z}_m$, associe la matrice $Y = KX$, définit un **système de chiffrement symétrique** (i.e. la même clé est utilisée pour crypter et décrypter l'information) ou à *clef secrète*.

Pour le professeur

Propriété

Soit K une matrice appartenant à $M_n(\mathbf{Z}_m)$.
K est inversible dans $M_n(\mathbf{Z}_m)$ si, et seulement si, $\det(K)$ est inversible modulo m.

En effet :

- Si K est inversible dans $M_n(\mathbf{Z}_m)$, il existe $L \in M_n(\mathbf{Z}_m)$ telle que $KL = LK = I_n$ (modulo m).

Alors $\det(KL)=\det(LK) = 1 \pmod m$ d'où $\det(K) \times \det(L) = 1 \pmod m$, ce qui prouve que $\det(K)$ est inversible modulo m.

- Réciproquement : Supposons $\det(K)$ inversible modulo m.

Il existe donc ℓ, entier naturel inférieur ou égal à $m - 1$, tel que $\det(K)\times \ell = 1 \pmod m$.

Alors la matrice $L = \ell \times {}^t(\text{com } K)$ vérifie $KL = LK = I_n \pmod m$, ce qui prouve que K est inversible dans $M_n(\mathbf{Z}_m)$.

Propriété

Soit k un entier naturel. On note $\bar{k}$ sa classe de congruence modulo m.

$\bar{k}$ est inversible dans $\mathbf{Z}_m$ si, et seulement si, k et m sont premiers entre eux.

En effet : k et m sont premiers entre eux

si, et seulement si, il existe deux entiers u et v tels que $uk + vm = 1$,

si, et seulement si, il existe deux entiers u et v tels que $\overline{uk + vm} = \bar{1}$,

si, et seulement si, il existe un entier u tel que $\bar{u}\bar{k} = \bar{1}$.

Pour le professeur

On note $(\mathbf{Z}_m)^*$ l'ensemble des éléments inversibles de $\mathbf{Z}_m$ et $\varphi(m)$ son cardinal.

(φ est l'*indicatrice d'Euler*)

Si $m = \prod_{i=1}^{k} p_i^{\alpha_i}$ (décomposition de m en produit de facteurs premiers),

alors :

$$Card\ \mathbf{Z}_m^{\ *} = \varphi(m) = \prod_{i=1}^{k} p_i^{\alpha_i} - p_i^{\alpha_i - 1} = m \prod_{i=1}^{k} \left(1 - \frac{1}{p_i}\right)$$

Pour le professeur

Pour le démontrer, on utilise les deux propriétés suivantes :

Propriété 1
Si m et n sont premiers entre eux : $\varphi(mn) = \varphi(m)\varphi(n)$.

En effet, $\mathbf{Z}_{mn} \cong \mathbf{Z}_m \times \mathbf{Z}_n$, et donc $(\mathbf{Z}_{mn})^* \cong (\mathbf{Z}_m)^* \times (\mathbf{Z}_n)^*$.

Propriété 2
Soit p un nombre premier.
Pour tout entier naturel non nul α : $\varphi(p^\alpha) = p^\alpha - p^{\alpha-1}$.

Il y a en effet $p^{\alpha-1}$ entiers compris entre 0 et $p^\alpha - 1$, non premiers avec p^α.

Ce sont les nombres kp où $k \in \{0, 1, 2, \ldots, (p^{\alpha-1} - 1)\}$ (multiples de p strictement inférieurs à p^α).

Étude de quelques exemples

1. Chiffrement d'un texte à l'aide de 26 caractères

- Les 26 lettres de l'alphabet sont codées de 0 à 25 (0 pour A et 25 pour Z)
- On enlève les caractères non alphabétiques (espaces, ponctuation, chiffres…) ; on ne distingue pas les majuscules des minuscules.
- On découpe le texte par blocs de n lettres. La clé est une matrice K de $M_n(\mathbf{Z}_{26})$.

Exemple

Si $n = 2$ et $K = \begin{pmatrix} 1 & 2 \\ 3 & 7 \end{pmatrix}$, alors $\det(K) = 1$ et $K^{-1} = \begin{pmatrix} 7 & 24 \\ 23 & 1 \end{pmatrix}$.

Le texte clair OTTO, défini par les matrices colonnes $\begin{pmatrix} 14 \\ 19 \end{pmatrix}, \begin{pmatrix} 19 \\ 14 \end{pmatrix}$, est crypté en calculant $K\begin{pmatrix} 14 \\ 19 \end{pmatrix} \pmod{26}$ et $K\begin{pmatrix} 19 \\ 14 \end{pmatrix} \pmod{26}$ et donne les codes suivants : $\begin{pmatrix} 0 \\ 19 \end{pmatrix}, \begin{pmatrix} 21 \\ 25 \end{pmatrix}$.

Le texte crypté est donc : ATVZ.

Inversement le texte FX se décrypte en calculant $K^{-1}\begin{pmatrix} 5 \\ 23 \end{pmatrix} \pmod{26}$.

Le texte clair est donc PI.

Ressources sur *euler*

- **Chiffre de Hill**

  Outil : 4045

  (Codage d‘un texte à l’aide du chiffre de Hill)

  Apprentissage 4046/4046 (Coder/décoder un mot …)

- **Inverse d’une matrice modulo un entier**

  Outil : 4043

  Apprentissage, générateur, QCM : 4055, 4058, 4056, 4057

Pour le professeur

Le nombre de clés (nombre de matrices inversibles dans $M_n(\mathbf{Z}_{26})$) est : $\prod_{i=0}^{n-1} 2^n - 2^i \times \prod_{i=0}^{n-1} 13^n - 13^i$

Pour le démontrer, on utilise les deux propriétés suivantes :

Propriété 1

$\text{Card}\,(M_n(\mathbf{Z}_{26}))^* = \text{Card}\,(M_n(\mathbf{Z}_2))^* \times \text{Card}\,(M_n(\mathbf{Z}_{13}))^*$

Démonstration

Propriété 2

Si p est un nombre premier, alors : $\text{Card}\ M_n\ \mathbf{Z}_p\ ^* = \prod_{i=0}^{n-1} p^n - p^i$

Démonstration

Pour le professeur

Dans le cas d'un chiffrement de Hill avec $n = 2$ et 26 caractères,

Card $(M_2(\mathbf{Z}_{26}))^* = (2^2 - 1)(2^2 - 2)(13^2 - 1)(13^2 - 13)$,

soit **157 248 clés possibles**.

La probabilité qu'une matrice de $M_2(\mathbf{Z}_{26})$ choisie au hasard puisse être une matrice de chiffrement est égale à

Card $(M_2(\mathbf{Z}_{26}))^*$ / Card $M_2(\mathbf{Z}_{26})$ soit 0,34 (arrondi au centième).

Remarques

1. On peut dénombrer directement les matrices de $(M_2(Z_{26}))^*$.

Soit $K = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ où a, b, c, d sont 4 restes modulo 26

K est inversible ssi $ad - bc$ est premier avec 26, c'est-à-dire

ssi $ad - bc$ est impair et non divisible par 13.

2. Si l'on utilise **37 caractères** (les 26 lettres de l'alphabet, les 10 chiffres et l'espace) :

Card $(M_2(\mathbf{Z}_{37}))^* = (37^2 - 1)(37^2 - 37)$ soit **1 822 176 clés possibles** et la probabilité qu'une matrice de $M_2(\mathbf{Z}_{37})$ choisie au hasard puisse être une matrice de chiffrement est égale à

Card $(M_2(Z_{37}))^*$ / Card $M_2(Z_{37})$, soit **0,97** (arrondi au centième).

2. Chiffrement d'une image en niveaux de gris

D'un point de vue informatique, les « niveaux de gris » sont codés sous forme de nombres entiers compris entre 0 et 255 (avec huit bits, un maximum de $256 = 2^8$ valeurs distinctes de l'intensité lumineuse peut être atteint).

La valeur 0 représente alors la couleur noire, et la valeur 255 la couleur blanche.

Une première approche avec un tableur consiste à créer une image très simple (comme une spirale) et à visualiser directement cette image en associant la couleur d'arrière-plan de la cellule à la valeur de la cellule elle-même.

On peut ensuite crypter l'image en la découpant en blocs de n pixels (dans l'exemple de la spirale, $n = 2$) et en la chiffrant avec une clé K de $\mathrm{M}_n(\mathbf{Z}_{256})$

spirale

Démonstrations

Démontrons que Card $(M_n(\mathbf{Z}_{26}))^* = \text{Card}\,(M_n(\mathbf{Z}_2))^* \times \text{Card}\,(M_n(\mathbf{Z}_{13}))^*$.

Pour le professeur

Soit $K \in M_n(\mathbf{Z}_{26})$. K est inversible dans $M_n(\mathbf{Z}_{26})$ si, et seulement si K est inversible dans $M_n(\mathbf{Z}_2)$ et dans $M_n(\mathbf{Z}_{13})$ (en effet K est inversible dans $M_n(\mathbf{Z}_{26})$ si et seulement si $\det(K)$ n'est divisible ni par 2 ni par 13).

Considérons la relation : $\Phi : \quad M_n\ \mathbf{Z}_{26} \rightarrow M_n\ \mathbf{Z}_2 \times M_n\ \mathbf{Z}_{13}$

$$\overline{a_{i,j}}_{\ i,j}\ (\text{mod}26) \rightarrow \overline{a_{i,j}}_{\ i,j}\ (\text{mod}2),\ \overline{a_{i,j}}_{\ i,j}\ (\text{mod}13)$$

Φ définit une fonction car si $a_{ij} \equiv a'_{ij}\ (\text{mod } 26)$ alors $a_{ij} \equiv a'_{ij}\ (\text{mod } 2)$ et $a_{ij} \equiv a'_{ij}\ (\text{mod } 13)$.

On vérifie que Φ est un morphisme d'anneaux unitaires, injectif

(Ker $\Phi = \{(a_{ij})_{i,j}\ (\text{mod } 26)$ tel que $\forall(i,j), a_{ij} \equiv 0\ (\text{mod } 2)$ et $a_{ij} \equiv 0\ (\text{mod } 13)\}$; d'où $a_{ij} \equiv 0$ (mod 26) car 2 et 13 sont premiers entre eux).

Comme Card $M_n(\mathbf{Z}_{26})$ = Card $((M_n(\mathbf{Z}_2) \times M_n(\mathbf{Z}_{13}))$, **$\Phi$ est un isomorphisme d'anneaux** :

$M_n(\mathbf{Z}_{26}) \cong M_n(\mathbf{Z}_2) \times M_n(\mathbf{Z}_{13})$.

On en déduit que : $(M_n(\mathbf{Z}_{26}))^* \cong (M_n(\mathbf{Z}_2))^* \times (M_n(\mathbf{Z}_{13}))^*$.

Pour le professeur

Démontrons que $\text{Card}\ M_n\ \mathbf{Z}_p\ ^* = \prod_{i=0}^{n-1} p^n - p^i$

Si p est premier, $\mathbf{Z}_p$ est un corps. Dans ce cas, une matrice M de $M_n(\mathbf{Z}_p)$ est inversible si, et seulement si, ses vecteurs colonnes forment une base $B = \{e_1, e_2, \ldots, e_n\}$ d'un $\mathbf{Z}_p$ espace vectoriel de dimension n.

e_1 n'est pas nul : il y a donc $(p^n - 1)$ façons de le choisir ;

$e_2 \notin \text{Vect}(e_1)$: il y a donc $(p^n - p)$ façons de le choisir (on exclut 0, e_1, 2 e_1,…, $(p-1)e_1$) ;

$e_3 \notin \text{Vect}(e_1, e_2)$: il y a donc $(p^n - p^2)$ façons de le choisir (on exclut les combinaisons linéaires $ke_1 + \ell e_2$, où k et ℓ sont des entiers compris entre 0 et $p - 1$) ;

Etc…

Donc $\text{Card}\ M_n\ \mathbf{Z}_p\ ^* = \prod_{i=0}^{n-1} p^n - p^i$