Cryptographie de Hill

Stepec Murielle*

November 22, 2016

Abstract

Cet exercice fait appel aux notions de ***Matrices, congruences et théorème de Bézout, vues en Terminale S****.*
Merci à Renée de Graeve qui a crée l'activité et Bernard Parisse qui m'a dirigé pour la création de cette activité.

Nous allons étudier un exemple de codage utilisant le codage ASCII et le calcul matriciel.

Faisons tout d'abord des rappels sur le calcul matriciel.

Multiplication de matrices:

1) En préliminaire, rappelez-vous, les matrices ne peuvent être multipliées ensembles que si elles ont des dimensions compatibles, c'est à dire: le nombre de colonnes de la 1ière est le même que le nombre de lignes de la deuxième ($ex : (3 \times n) \times (n \times 7)$)

2)puis la méthode de multiplication:

$$\begin{pmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \\ 7 & 8 & 9 \end{pmatrix} \times \begin{pmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \\ 7 & 8 & 9 \end{pmatrix} = \begin{pmatrix} 1*1+2*4+3*7 & 36 & 42 \\ 66 & 81 & 96 \\ 102 & 126 & 150 \end{pmatrix}$$

Matrice inverse:

Soit la matrice carrée 2×2 :

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

*D'après Renée De Graeve, Bernard Parisse

1) On calcule le determinant $D = ad - bc$ si $D \neq 0$ alors la matrice inverse existe.
2) On calcule la matrice inverse, soit à l'aide de la méthode du pivot de gauss, soit à l'aide du determinant en utilisant la formule:

$$M^{-1} = \frac{1}{D} \times \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}$$

Le principe de la crytograghie de Hill

On code les nombres et les lettres en associant:
a) aux nombres 0,..9,10 les chiffres "0",.."9",":"
b) aux nombres 11,..36 les lettres "A",..,"Z".

chiffre ou lettre	0	1	2	3	4	5	6	7	8	9	:		
codage	0	1	2	3	4	5	6	7	8	9	10		
lettre	A	B	C	D	E	F	G	H	I	J	K	L	M
codage	11	12	13	14	15	16	17	18	19	20	21	22	23
lettre	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
codage	24	25	26	27	28	29	30	31	32	33	34	35	36

On obtient ainsi une liste de nombres avec des valeurs comprises entre 0 et 36 (un modulo de 37...)

On se fixe une matrice de codage 2×2 qui multipliera des paquets de 2 nombres. Afin que le destinataire puisse décoder le message, il faudra que cette matrice soit inversible et que son déterminant soit premier avec 37 donc $D \neq 0$ modulo 37.
Soit :

$$M = \begin{pmatrix} 7 & 11 \\ 8 & 11 \end{pmatrix}$$

Processus du codage

le message à coder formé de n caractères: lettres,chiffres et :

$\Downarrow$

On attribue le code ascii correspondant à ces caractères.

$\Downarrow$

On effectue le codage dans l'intervalle [0;36].

$\Downarrow$

On crée la matrice "message" de dimension $2 \times \frac{n}{2}$ colonnes.

$\Downarrow$

On définit une matrice de codage 2×2 , pour permettre le décodage elle devra être inversible.

$\Downarrow$

On multiple la matrice de codage par la matrice "message" modulo 37

$\Downarrow$

On transforme le résultat en une chaîne de caractères

$\Downarrow$

On attribut à ces caractères le chiffre ou la lettre correspondante

$\Downarrow$

On obtient notre message codé

Pour décoder on effectue le même processus avec la matrice inverse.

Quelques explications: Pourquoi les coefficients de matrice finale sont-ils modulo 37?
Réponse (partielle):

```
"le codage va de 0 a 36, donc un modulo de 37"
```

$$\text{lecodagevade0a36, doncunmodulode37}$$

Pourquoi utilise-t-on la fonction "iabcuv"?
Réponse (partielle):
On sait que $M \times M^{-1} = Id$ dans $\mathbb{Q}$, d'après la formule de la matrice inverse, on trouve dans $\mathbb{Z}$: $M \times N = D \times Id$, avec la matrice

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

Pour que les coefficients de la matrice inverse de M soient également entiers nous utilisons le théorème de Bézout

$$Du + 37v = 1$$

pour "inverser D modulo 37". Ainsi,

$$M \times uN = DuId = Id \pmod{37}$$

la matrice inverse de M modulo 37 sera donc : uN.
Pourquoi rajoute-t-on ":" lorsque le message a pour longueur un nombre impair?
Réponse:
Pour coder le message, on le multiple par une matrice 2×2 donc nous devons le rendre de longueur pair pour crée la matrice à multiplier de dimension $2 \times \frac{n}{2}$
.

Programme de cryptographie de Hill

On fixe une matrice de codage de dimension 2×2
par exemple on tape : `M:=[[7,11],[8,11]]`

$$\begin{pmatrix} 7 & 11 \\ 8 & 11 \end{pmatrix}$$

```
//lorsque c est un nombre de [0;36]
 //transforme 0.. 9 en "0".."9", 10 en ":" et 11..36 en
co(c):={
 "A".."Z"
 local n;
 si c<0 alors c:= c+37; fsi;
 si c<=10 alors c:=c+48; sinon c:=c+54; fsi;
 return char(c);
}:;
//lorsque l est un caractère de la liste ["0",..,"9",":","A",..,"Z"]
//cod(l) transforme  "0".."9" en 0..9, ":" en 10 et "A".."Z" en 11..36
cod(l):={    //code la chaine en ASCII, puis codée de 0 à 36
 local n;
 n:=op(asc(l));
 si 48<=n and n<=58 alors n:=n-48; sinon n:=n-54; fsi;
 return n;
}:;
//coda(s) renvoie la matrice B associée au message s
coda(s):={
 local j,n,B,p;
 n:=dim(s);
 si odd(n) alors s:=s+":"; n:=n+1; fsi;
 p:=n/2;B:=makemat(0,2,p);
 pour j de 0 jusque p-1 faire
   B[0,j]:=cod(s[2*j]);B[1,j]:=cod(s[2*j+1]);
 fpour;
 return B;
}:;
//codag(B) renvoie le message s associé à la matrice B
codag(B):={  //crée la chaine de caractère
 local s,n,j,k;
 n:=coldim(B);s:="";
```

```
 pour j de 0 jusque n-1 faire
   pour k de 0 jusque 1 faire
     s:=s+co(B[k,j]);
   fpour;
 fpour;
 return s;
}:;
//codag(B) renvoie le message s associé à la matrice B
codage(s,M):={
 local B,C;
 B:=coda(s);
 C:=irem(M*B,37);
 return codag(C);
}:;
//decodage(s,M) décode le message s codé au moyen de M
decodage(s,M):={
 local a,B,Q,P,N;
 B:=coda(s);
 a:=iabcuv(det(M),37,1)(1);
 Q:=[[M(2,2),-M(1,2)],[-M(2,1),M(1,1)]];
 P:=a*Q;
 N:=irem(P*B,37);
 return codag(N);
}:;
```

Pour coder un message on tape: codage(”le:message”,M)
Pour décoder le message on tape: decodage(”le:message”,M)
Par exemple:

```
cryptee:=codage("ABCD012",M)
```

NYMZAACE

```
decodage(cryptee,M)
```

ABCD012 :

Que dit ce message codé? : ”A8P0FPSGGZDS6FZTR1MXO1DZG9Y9B5N3”

Pour utiliser les commandes et les programmes, penser à appuyer sur les touches *OK*.
La touche *exec tout* *exécute toutes les commandes.*