Le chiffrement de Hill

Le mathématicien américain *Lester Hill* (1891-1961) a inventé, en 1929-1930, une méthode de chiffrement à clé symétrique (secrète) par substitution polygraphique (affine par bloc) utilisant des propriétés de l'arithmétique modulaire et du calcul matriciel.

A- Le principe du chiffrement de Hill

A-1 Codage

Nous supposons que nous avons un message à coder écrit avec les lettres A jusqu'à Z (en majuscules). L'idée de Hill est de grouper les lettres du message par blocs de m lettres, puis de les coder simultanément, ce code est noté Hill mxm. Chaque lettre est remplacée par un nombre compris entre 0 et 25 : A devient 0, B devient 1, ..., Z devient 25. On groupe les nombres ainsi obtenus par groupe de m : $x_1x_2x_3 \ldots x_m$, $x_{m+1}\, x_{m+2} \ldots x_{2m}$,.....

Si par exemple m=2, chaque groupe de 2 nombres $x_k\ x_{k+1}$ est codé en utilisant des combinaisons linéaires fixées au préalable, telles que :

$$(1)\ \begin{cases} y_k = ax_k + bx_{k+1} \\ y_{k+1} = cx_k + dx_{k+1} \end{cases}$$

où a,b,c,d sont des entiers fixes. Si l'entier y_k n'est pas compris entre 0 et 25, on le remplace alors par son reste modulo 26, puis on retransforme les nombres en lettres.

Le codage (1) peut se mettre sous la forme matricielle suivante Y=AX avec :

$A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$, $X = \begin{pmatrix} x_k \\ x_{k+1} \end{pmatrix}$ et $Y = \begin{pmatrix} y_k \\ y_{k+1} \end{pmatrix}$ où A est une matrice inversible.

Puisque tous les calculs que nous effectuons sont modulo 26, on considère cette matrice d'entiers comme étant à coefficients dans Z/26Z. Ici la clé de codage est la matrice A. La clé de déchiffrage est la matrice inverse de A. On rappelle que la matrice A est inversible dans Z/26Z ssi det(A) mod 26 est inversible dans Z/26Z.

Exemple :

1) si $A = \begin{pmatrix} 2 & 3 \\ 4 & 5 \end{pmatrix}$, cette matrice n'est pas inversible mod 26 car det(A)=24 mod 26 or 24 n'a pas d'inverse dans Z/26Z car pgcd(24,26)≠1. Montrer que la matrice B est inversible, $B = \begin{pmatrix} 2 & 3 \\ 7 & 5 \end{pmatrix}$.

2) Laquelle de ces deux matrices a un inverse dans Z/26Z : $C = \begin{pmatrix} 1 & 3 & 2 \\ 5 & 3 & 2 \\ 7 & 2 & 5 \end{pmatrix}$;

$D = \begin{pmatrix} 1 & 3 & 3 \\ 5 & 3 & 2 \\ 7 & 2 & 5 \end{pmatrix}$.

3) Coder l'information « HILL » par la matrice B.
4) Combien y a-t-il au **maximum** de clés possibles pour le code Hill 2x2 (resp. pour le code Hill 3x3).

A-2 Décodage

Une information codée par une clé A (inversible) est décodée tout simplement en écrivant : $X=A^{-1}Y \pmod{26}$.
Décoder le cryptogramme suivant « UWGMWZRREIUB » sachant que la clé de chiffrement est $A=\begin{pmatrix} 9 & 4 \\ 5 & 7 \end{pmatrix}$.

B- Cryptanalyse du code de Hill

Pour cette partie seul le cas m=2 est considéré.
Une attaque à force brute dans le cas m=2 est possible, car on a à traiter 157248 matrices ce qui est possible avec un ordinateur.
Il est possible de faire une attaque par les digrammes. On considère les digrammes qui apparaissent le plus souvent :

ES	DE	LE	EN	RE	NT	ON	ER	TE
3,3%	2,4%	2,3%	2,1%	1,9%	1,7%	1,6%	1,5%	1,5%

Mais on suppose ici que deux mots X sont connus ainsi que leurs codes Y.
1) À partir de ces données écrire le système algébrique permettant la construction de la matrice clé A (on suppose que $A=\begin{pmatrix} a & b \\ c & d \end{pmatrix}$) et déterminer A.

2) Les procédures :

a) Ecrire une procédure CrypteHill en Maple qui crypte un mot composé de deux lettres (ici n=2).
b) Ecrire une procédure DCrypteHill en Maple qui décrypte un code composé de deux lettres (ici n=2).
c) Ecrire une procédure AttackHill en Maple qui détermine la clé de cryptage M (ici n=2).

Extension de votre travail : lire l'article suivant : A secure image encryption algorithm based on Hill cipher system ; S.K. Muttoo, Deepika Aggarwal, Bhavya Ahuja, **Buletin Teknik Elektro dan Informatika,** Vol.1, No.1, March 2012, pp. 51~60

Ecrire le programme correspondant pour crypter des images.