Terminales S spé - DS3

MATHEMATIQUES

Lundi 10 février 2014

Partie A Cours

Citer le théorème de Bézout et le théorème de Gauss puis démontrer ce dernier.

Partie B Chiffrement de Hill (1929) : présentation.

Pour coder un message on pourrait remplacer chaque lettre du texte par une autre lettre.
Mais il est alors facile de le déchiffrer en utilisant les fréquences d'apparition de chaque lettre.
On évite ce problème découpant le message par paquets contenant le même nombre de lettres.
Puis on code paquet par paquet en remplaçant par exemple un couple de deux lettres consécutives par un autre couple de deux lettres.
Les lettres sont d'abord transformées en nombres dans l'ordre alphabétique (A=0, B=1, ..., Z=25).

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

On code chaque couple de nombres puis l'on revient aux lettres par (0=A, ... 25=Z)

Partie C Chiffrement de Hill : étude arithmétique.

$(x_1;x_2)$ est le couple numérique du départ, $(y_1;y_2)$ le couple numérique obtenu par codage.
La fonction de codage $f : (x_1;x_2) \longmapsto (y_1;y_2)$ est ici définie par :
y_1 est le reste de la division euclidienne de $9x_1+4x_2$ par 26.
y_2 est le reste de la division euclidienne de $5x_1+7x_2$ par 26.
Par exemple le couple (I ;M) deviendra (8 ;12) puis (16 ;20) et sera retranscrit (Q ;U).

1. Coder le couple (R ;A). Puis le mot RAPACE.

   Décodage.
   On cherche la fonction de décodage $g : (y_1;y_2) \longmapsto (x_1;x_2)$

2. Démontrer que : $\begin{cases} 43x_1 & \equiv & 7y_1-4y_2 & (mod 26) \\ 43x_2 & \equiv & -5y_1+9y_2 & (mod 26) \end{cases}$

   On est ainsi amené a chercher les entiers x_1 et x_2 dans $[0;25]$ tels que : $\begin{cases} 43x_1 \equiv 7y_1-4y_2 & (mod 26) \\ 43x_2 \equiv -5y_1+9y_2 & (mod 26) \end{cases}$

3. Prouver qu'il existe des entiers p et q tels que $43p+26q=1$

4. A l'aide de l'algorithme d'Euclide trouver un couple solution de cette équation.
   En déduire un entier p tel que $43p \equiv 1\ (mod 26)$

5. En déduire que : $\begin{cases} x_1 & \equiv & 5y_1+12y_2 & (mod 26) \\ x_2 & \equiv & 15y_1+25y_2 & (mod 26) \end{cases}$

6. Décoder le couple (F ;X) puis le mot FXVDIM.

Partie D Chiffrement de Hill : étude matricielle.

On dira que deux matrices M et N, à coefficients entiers sont congrues modulo 26 si leurs termes de même emplacement sont congrus modulo 26. On note alors $M \equiv N\ (mod 26)$
On garde les notations et les données des Parties B et C.
$x = (x_1\ x_2)$ est la matrice (numérique) du paquet de départ, $y = (y_1\ y_2)$ celle du paquet codé.
Soit la matrice $A = \begin{pmatrix} 9 & 5 \\ 4 & 7 \end{pmatrix}$.

1. Quel calcul matriciel permet d'obtenir la matrice y à partir des matrices x et A ?
   En déduire le codage du mot RIVAGE.

   Décodage.

2. On cherche une matrice B telle que les termes de la matrice x soient les restes de la division euclidienne par 26 des termes correspondants de la matrice $X = y.B$. On pense à l'inverse de A.
   Prouver que A est inversible et que $A^{-1} = \frac{1}{43}\begin{pmatrix} 7 & -5 \\ -4 & 9 \end{pmatrix}$.
   Pourquoi la matrice B cherchée ne peut-elle pas être égal à A^{-1} ?

3. On admet que la matrice B doit vérifier $BA \equiv I\ (mod 26)$.
   Prouver que la Matrice $B_1 = -3 \times 43 \times A^{-1}$ convient.
   En déduire que la matrice $B_2 = \begin{pmatrix} 5 & 15 \\ 12 & 25 \end{pmatrix}$ convient également.

4. Décoder le mot NFXHSG.

Partie A Cours

Théorème de Bézout :
2 entiers a et b sont premiers entre eux si et seulement si il existe 2 entiers u et v tels que $au+bv=1$.
Théorème de Gauss :
Soita,b,c trois entiers. Si a divise bc et si a est premier avec b alors a divise c.
Preuve : Si $a\wedge b=1$ alors d'après Bézout il existe $(u;v)$ tels que $au+bv=1$.
donc $auc+bvc=c$ or $a|bc$ et $a|auc$ donc $a|auc+bvc$ d'où $a|c$.

Partie C Chiffrement de Hill : étude arithmétique.

1. RA $\longmapsto$ XH ; RAPACE $\longmapsto$ XHFXIM

   Décodage.

2. On a : $\begin{cases} y_1 \equiv 9x_1+4x_2 \ (mod26) \\ y_2 \equiv 5x_1+7x_2 \ (mod26) \end{cases}$ d'où $\begin{cases} 7y_1-4y_2 \equiv 63x_1-20x_1 = 43x_1 \ (mod26) \\ -5y_1+9y_2 \equiv 63x_2-20x_2 = 43x_2 \ (mod26) \end{cases}$

3. $43\wedge 26=1$ donc il existe des entiers p et q tels que $43p+26q=1$ (d'après le th de Bézout)

4. $43=26+17; 26=17+9; 17=9+8; 9=8+1$ donc $5\times 26-3\times 43=1$
   d'où $-3\times 43\equiv 1\ (mod26)$ donc $23\times 43\equiv 1\ (mod26)$

5. Donc $-3\times 43x_1\equiv -21y_1+12y_2$ soit $x_1\equiv 5y_1+12y_2\ (mod26)$
   De même $-3\times 43x_2\equiv 15y_1-27y_2$ soit $x_2\equiv 15y_1+25y_2\ (mod26)$

6. FX $\longmapsto$ PA ; FXVDIM $\longmapsto$ PALACE

Partie D Chiffrement de Hill : étude matricielle.

1. Soit $Y=(Y_1\ Y_2)=x.A$; alors y est la matrice des restes des divisions euclidiennes des termes de Y par 26 car : $\begin{cases} Y_1 = 9x_1+4x_2 \\ Y_2 = 5x_1+7x_2 \end{cases}$. D'où RIVAGE $\longmapsto$ DLHBSG.

   Décodage.

2. A est inversible car $ad-bc=9\times 7-4\times 5=43\neq 0$
   Avec $A=\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ et alors $A^{-1}=\dfrac{1}{ad-bc}\begin{pmatrix} d & -c \\ -b & a \end{pmatrix}=\dfrac{1}{43}\begin{pmatrix} 7 & -4 \\ -5 & 9 \end{pmatrix}$.
   Les termes de la matrice B doivent être entiers donc B ne peut pas être égal à A^{-1}.

3. $B_1=-3\times 43\times A^{-1}=\begin{pmatrix} -21 & 12 \\ 15 & -27 \end{pmatrix}$. D'où $B_1.A=\begin{pmatrix} -129 & 0 \\ 0 & -129 \end{pmatrix}\equiv\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}\ (mod26)$
   $B_2\equiv B_1\ (mod26)$ donc $B_2.A\equiv B_1.A\equiv I\ (mod26)$ d'où la matrice $B_2=\begin{pmatrix} 5 & 15 \\ 12 & 25 \end{pmatrix}$ convient aussi.

4. NFXHSG $\longmapsto$ VIRAGE