Index

Problème 2 page 94 chiffrement et déchiffrement....1
Problème 4 page 96 Chiffrement de Hill (1891- 1961)....2

Problème 2 page 94 chiffrement et déchiffrement

Voir le problème 5 de la page 17 dans le chapitre 1

1) Clé (5 ; 22)

La lettre M est associée à l'entier 12

$y = 5\times12 + 22 = 82$ et $82 = 26\times3 + 4$
le reste $c(x) = 4$. La lettre associée à 4 est E
M est codé par E.

2) Clé (7 ; 23)
Le mot codé est XYYMZKSMZ
a) Par définition du chiffrement affine de clé (7 ; 23), on a : $y \equiv 7x + 23$ (26)
Comme $23 \equiv -3$ (26), on a : $y + 3 \equiv 7x$ (26)

b) 7 et 26 étant premiers entre eux, il existe deux entiers u et v' tels que $7u + 26v' = 1$
En posant $v' = -v$, $7u - 26v = 1$

c) Recherche d'un couple (u_0, v_0) solution de l'équation du 2/b).
On peut utiliser l'algorithme d'Euclide :
$26 = 7\times3 + 5$ (Soit : $5 = 26 - 7\times3$)
$7 = 5\times1 + 2$ (soit : $2 = 7 - 5\times1 = 7 - 26 + 7\times3 = 7\times4 - 26$)
$5 = 2\times2 + 1$, donc : $1 = 5 - 2\times2 = 26 - 7\times3 - (7\times4 - 26) \times 2 = 26\times3 - 11\times7$
On peut prendre $u_0 = -11$ et $v_0 = -3$
(On peut trouver une infinité de couples :
autres couples possibles $(-11 + 26k ; -3 + 7k)$ (Application du théorème de Gauss))

d) Puisque $7u_0 - 26v_0 = 1$, on a : $7u_0 \equiv 1$ (26)
L'équation du 2a) est : $7x \equiv y + 3$ (26)
on multiplie les deux membres de la congruence par u_0,
d'où : $7u_0x \equiv u_0(y + 3)$ (26) et comme $7u_0 \equiv 1$ (26), il vient : $x \equiv u_0\, y + 3u_0$ (26)
$u_0 = -11$ et $-33 \equiv 19$ (26)
par conséquent : $x \equiv -11y + 19$ (26)
D'autre part, par définition du chiffrement affine, $y \equiv c(x)$ (26)

e) Le déchiffrement du texte s'obtient avec la clé (–11, 19) (Remarque : (15 ; 19) convient aussi ...)
Le mot décodé : APPRENDRE

3) Dès que a est premier avec 26, **il existe un couple (u_0, v_0) solution de l'équation $au - 26v = 1$**
En multipliant les deux membres de la congruence : $y \equiv ax + b$ (26) par u_0, on obtient :
$u_0\, y \equiv x + bu_0$ (26), soit : $x \equiv u_0\, y - bu_0$ (26)
Le déchiffrement est donc obtenu avec la clé $(u_0, -bu_0)$
Retenir :

Résoudre une équation de la forme $ax \equiv c \ (d)$
Lorsque a et d sont premiers entre eux, il existe un couple (u, v) d'entiers tels que $u\,a + v\,d = 1$,
d'où, $u\,a \equiv 1 \ (d)$
En multipliant chaque membre de l'équation $ax \equiv c \ (d)$ par u, il vient : $x \equiv cu \ (d)$ (la multiplication est associative et commutative).

Problème 4 page 96 Chiffrement de Hill (1891- 1961)

Les lettres de l'alphabet sont codées de 0 à 25, mais, le codage est fait par blocs.

Ici, on code par blocs de deux lettres .

Un couple d'entiers $(x ; y)$ est codé par un couple $(x' ; y')$ où $\begin{cases} x' \equiv ax+b \pmod{26} \\ y' \equiv cx+d \pmod{26} \end{cases}$

a, b, c, d sont des entiers (clé du chiffrement).

A- Exemples de chiffrement :
Chiffrement de ETUDIER
On partage le mot en bloc de deux lettres :

si le nombre de lettres est impair, on complète au hasard le dernier bloc.

ET-UD-IE-R*A*

1) $a = -5$, $b = 8$, $c = -2$, $d = 3$.

a) b) c)

Le chiffrement du mot ET-UD-IE-R est CX-CV-SW-T

Le premier E est chiffré par C et le deuxième par W.

L'analyse fréquentielle est donc rendue beaucoup plus difficile …

	A	B	C	D	E	F	G	H	I
1	Clé	a =	6	b =	7	c =	-8	d =	5
2									
3	Texte en clair	E	T	U	D	I	E	R	A
4	u, v	4	19	20	3	8	4	17	0
5	x, y	157	63	141	-145	76	-44	102	-136
6	Nombres entre 0 et 25	1	11	11	11	24	8	24	20
7	Texte chiffré	B	L	L	L	Y	I	Y	U

Le couple de lettres (U ; D)est codé par (L ; L).

B- À la recherche de deux peintres

1) Clé de codage : $a = 3$, $b = 5$, $c = 4$ et $d = 7$.

Nom codé : KTCEMAHS

a) $\begin{cases} x' = 3x + 5y \\ y' = 4x + 7y \end{cases}$ équivaut à $\begin{pmatrix} x' \\ y' \end{pmatrix} = \begin{pmatrix} 3 & 5 \\ 4 & 7 \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix}$

b) Soit A = $\begin{pmatrix} 3 & 5 \\ 4 & 7 \end{pmatrix}$. Le déterminant de A vaut : $3\times7 - 4\times5 = 1$.

comme dét(A) ≠ 0, la matrice A est inversible et $A^{-1} = \frac{1}{dét(A)} \begin{pmatrix} 7 & -5 \\ -4 & 3 \end{pmatrix} = \begin{pmatrix} 7 & -5 \\ -4 & 3 \end{pmatrix}$

On a donc : $\begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} 7 & -5 \\ -4 & 3 \end{pmatrix} \begin{pmatrix} x' \\ y' \end{pmatrix}$

c) Décodage de KTCEMAHS

Clé de décodage		$a = 7$	$b = -5$		$c = -4$		$d = 3$	
Texte codé	K	T	C	E	M	A	H	S
x' ; y'	10	19	2	4	12	0	7	18
x ; y	1	17	20	4	6	4	11	0
Texte décodé	B	R	U	E	G	E	L	A
Nom du peintre	BRUEGEL (tableau : *La Tour de Babel* (1563))							

Pieter Brueghel ou Bruegel dit l'Ancien est un peintre brabançon né à Bruegel (près de Bréda) vers 1525 et mort le 9 septembre 1569 à Bruxelles.

$\begin{pmatrix} 7 & -5 \\ -4 & 3 \end{pmatrix} \begin{pmatrix} 10 \\ 19 \end{pmatrix} = \begin{pmatrix} -25 \\ 17 \end{pmatrix}$ et $-25 \equiv 1\ (26)$ $\quad$ $\begin{pmatrix} 7 & -5 \\ -4 & 3 \end{pmatrix} \begin{pmatrix} 2 \\ 4 \end{pmatrix} = \begin{pmatrix} -6 \\ 4 \end{pmatrix}$ et $-6 \equiv 20\ (26)$

$\begin{pmatrix} 7 & -5 \\ -4 & 3 \end{pmatrix} \begin{pmatrix} 12 \\ 0 \end{pmatrix} = \begin{pmatrix} 84 \\ -48 \end{pmatrix}$ et $84 = 3\times26 + 6$, $-48 = 2\times52 + 4$;

$\begin{pmatrix} 7 & -5 \\ -4 & 3 \end{pmatrix} \begin{pmatrix} 7 \\ 18 \end{pmatrix} = \begin{pmatrix} -41 \\ 26 \end{pmatrix}$ et $-41 \equiv 11\ (26)$; $26 \equiv 0\ (26)$

La dernière lettre S du chiffrement correspond à la lettre A, rajoutée au nom pour avoir un nombre pair de lettres. Le chiffrement de Hill porte sur des couples de lettres. Si on supprime le S, ou si on remplace cette lettre par une autre, on ne retrouve pas la terminaison L du nom.

2. Nom codé : JPXH clé de codage : 3 ; 2 ; 5 ; 7.

a.La matrice de codage est A = $\begin{pmatrix} 3 & 2 \\ 5 & 7 \end{pmatrix}$. Elle est inversible puisque det(A) = 11 ≠ 0.

La matrice inverse est $A^{-1} = \frac{1}{11} \begin{pmatrix} 7 & -2 \\ -5 & 3 \end{pmatrix}$

En posant $\begin{pmatrix} x \\ y \end{pmatrix} = A^{-1} \begin{pmatrix} x' \\ y' \end{pmatrix}$, alors, si x' et y' sont des entiers alors x et y ne sont pas entiers.

On ne peut pas décoder avec cette matrice.

b) Recherche d'un couple (u, v) solution de : $11u - 26v = 1$

$26 = 11\times2 + 4$

$11 = 4\times2 + 3$

$4 = 3 + 1$,

d'où, $1 = 4 – 3 = 4 – (11 – 4\times2) = 3\times4 – 11 = 3\times(26 – 2\times11) – 11 = – 7\times11 –(–3)\times26$

$u = –7$ et $v = –3$

c) $11u – 26v = 1$ mène à $11u \equiv 1$ (26)

–7 est l'inverse de 11 modulo 26.

d) Soit $B = 11\times A^{-1} = \begin{pmatrix} 7 & -2 \\ -5 & 3 \end{pmatrix}$, d'où, uB.A $= u \begin{pmatrix} 7 & -2 \\ -5 & 3 \end{pmatrix} \begin{pmatrix} 3 & 2 \\ 5 & 7 \end{pmatrix} = u \begin{pmatrix} 11 & 0 \\ 0 & 11 \end{pmatrix} = \begin{pmatrix} 11u & 0 \\ 0 & 11u \end{pmatrix}$

Comme $11u \equiv 1$ (26), on a : uB.A $\equiv \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ (modulo 26)

$uBA \equiv 1\times I_2$ (26)

e) On a : $\begin{pmatrix} x' \\ y' \end{pmatrix} = A \begin{pmatrix} x \\ y \end{pmatrix}$

On multiplie les deux membres de l'égalité à gauche par uB, d'où, uB $\begin{pmatrix} x' \\ y' \end{pmatrix} = uBA \begin{pmatrix} x \\ y \end{pmatrix}$

soit, par congruence modulo 26, uB $\begin{pmatrix} x' \\ y' \end{pmatrix} \equiv \begin{pmatrix} x \\ y \end{pmatrix}$ (modulo 26).

Comme $u = –7$ et $B = \begin{pmatrix} 7 & -2 \\ -5 & 3 \end{pmatrix}$, on a : uB $= \begin{pmatrix} -49 & 14 \\ 35 & -21 \end{pmatrix}$ et,

par congruence modulo 26, uB $\equiv \begin{pmatrix} 3 & 14 \\ 9 & 5 \end{pmatrix}$ (26)

On en déduit : $\begin{cases} x = 3x' + 14y' \\ y = 9x' + 5y' \end{cases}$

f) Décodage :

JP est codé par : 9 ; 15, $\begin{pmatrix} 3 & 14 \\ 9 & 5 \end{pmatrix} \begin{pmatrix} 9 \\ 15 \end{pmatrix} = \begin{pmatrix} 237 \\ 156 \end{pmatrix} \equiv \begin{pmatrix} 3 \\ 0 \end{pmatrix}$ (26). JP est décodé par DA

XH est codé par : 23 ; 7 , $\begin{pmatrix} 3 & 14 \\ 9 & 5 \end{pmatrix} \begin{pmatrix} 23 \\ 7 \end{pmatrix} = \begin{pmatrix} 167 \\ 242 \end{pmatrix} \equiv \begin{pmatrix} 11 \\ 8 \end{pmatrix}$ (26). XH est décodé par LI

Le nom du peintre est : DALI.

Salvador Dalí Domènech (Figueras 1904 – 1989),(Tableau : Plage d'El llane à Cadaquès (1921))

3) Soit le déterminant d de la matrice A.

$du – 26v = 1$ si et seulement si d et u sont premiers entre eux.

À la question A.2, la matrice $A = \begin{pmatrix} 6 & 7 \\ -8 & 5 \end{pmatrix}$ a pour déterminant $d = 86$

86 et 26 ne sont pas premiers entre eux.

Le codage du couple (U, D) a donné (L, L) : soit (11, 11).

Ce qui est affirmé sans preuve peut être nié sans preuve. *Euclide d'Alexandrie*

Si on veut décoder, on cherche x et y solutions de : $\begin{cases} 6x+7y=11 \\ -8x+5y=11 \end{cases}$, soit : $\begin{cases} 30x+35y=55 \\ -56x+35y=77 \end{cases}$,

$86x = -22$. $8x \equiv 4\ (26)$ qui n'a pas de solutions.

Table de multiplication des congruences modulo 26 :

	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	AA
1		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	26
2	1	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	0
3	2	2	4	6	8	10	12	14	16	18	20	22	24	0	2	4	6	8	10	12	14	16	18	20	22	24	0
4	3	3	6	9	12	15	18	21	24	1	4	7	10	13	16	19	22	25	2	5	8	11	14	17	20	23	0
5	4	4	8	12	16	20	24	2	6	10	14	18	22	0	4	8	12	16	20	24	2	6	10	14	18	22	0
6	5	5	10	15	20	25	4	9	14	19	24	3	8	13	18	23	2	7	12	17	22	1	6	11	16	21	0
7	6	6	12	18	24	4	10	16	22	2	8	14	20	0	6	12	18	24	4	10	16	22	2	8	14	20	0
8	7	7	14	21	2	9	16	23	4	11	18	25	6	13	20	1	8	15	22	3	10	17	24	5	12	19	0
9	8	8	16	24	6	14	22	4	12	20	2	10	18	0	8	16	24	6	14	22	4	12	20	2	10	18	0
10	9	9	18	1	10	19	2	11	20	3	12	21	4	13	22	5	14	23	6	15	24	7	16	25	8	17	0
11	10	10	20	4	14	24	8	18	2	12	22	6	16	0	10	20	4	14	24	8	18	2	12	22	6	16	0
12	11	11	22	7	18	3	14	25	10	21	6	17	2	13	24	9	20	5	16	1	12	23	8	19	4	15	0
13	12	12	24	10	22	8	20	6	18	4	16	2	14	0	12	24	10	22	8	20	6	18	4	16	2	14	0
14	13	13	0	13	0	13	0	13	0	13	0	13	0	13	0	13	0	13	0	13	0	13	0	13	0	13	0
15	14	14	2	16	4	18	6	20	8	22	10	24	12	0	14	2	16	4	18	6	20	8	22	10	24	12	0
16	15	15	4	19	8	23	12	1	16	5	20	9	24	13	2	17	6	21	10	25	14	3	18	7	22	11	0
17	16	16	6	22	12	2	18	8	24	14	4	20	10	0	16	6	22	12	2	18	8	24	14	4	20	10	0
18	17	17	8	25	16	7	24	15	6	23	14	5	22	13	4	21	12	3	20	11	2	19	10	1	18	9	0
19	18	18	10	2	20	12	4	22	14	6	24	16	8	0	18	10	2	20	12	4	22	14	6	24	16	8	0
20	19	19	12	5	24	17	10	3	22	15	8	1	20	13	6	25	18	11	4	23	16	9	2	21	14	7	0
21	20	20	14	8	2	22	16	10	4	24	18	12	6	0	20	14	8	2	22	16	10	4	24	18	12	6	0
22	21	21	16	11	6	1	22	17	12	7	2	23	18	13	8	3	24	19	14	9	4	25	20	15	10	5	0
23	22	22	18	14	10	6	2	24	20	16	12	8	4	0	22	18	14	10	6	2	24	20	16	12	8	4	0
24	23	23	20	17	14	11	8	5	2	25	22	19	16	13	10	7	4	1	24	21	18	15	12	9	6	3	0
25	24	24	22	20	18	16	14	12	10	8	6	4	2	0	24	22	20	18	16	14	12	10	8	6	4	2	0
26	25	25	24	23	22	21	20	19	18	17	16	15	14	13	12	11	10	9	8	7	6	5	4	3	2	1	0
27	26	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0

Les éléments ayant un inverse modulo 26, apparaissent lorsque le produit est égal à 1