ASSIGNMENT 1 ON CRYPTOGRAPHY		
Student's Code	AIMS African Institute for Mathematical Sciences CAMEROON	Deadline
iMTR815ja		**05.03.23, 11:59 pm**
March 5, 2023		Ac. Year: 2022 - 2023
		Lecturer(s): Prof. Giulio Codogni

1 Solution of Exercise 2.14

a)-Let's prove that $\det A \equiv \pm 1 (\mod 26)$ if A is a matrix over $\mathbb{Z}/26$ such that $A = A^{-1}$.

Let's suppose that A is a matrix over $\mathbb{Z}/26$ such that $A = A^{-1}$

As $A = A^{-1}$ so $A.A = A^{-1}.A = Id$. So we have $A^2 = Id$.

As we have $\det A^2 = (\det A)^2 = \det Id = 1$ so $\det A = \pm 1$ then we have $\det A \equiv \pm 1 (\mod 26)$.

b)-Let's use the formula given in Corollary 2.4 to determine the number of involutory keys in the Hill Cipher (over $\mathbb{Z}/26$) in the case $m = 2$.

According to Corollary 2.4, Suppose

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

is a matrix having entries in $\mathbb{Z}_n$, and $\det K = ad - cb$ is invertible in $\mathbb{Z}_n$. Then

$$A^{-1} = (\det A)^{-1} \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}$$

To find the number of involutary keys in the Hill Cipher, we are looking for all the matrices A such that $A = A^{-1}$ and it means that all the matrices A whose $\det A = \pm 1$.

According to the corollary,

$$A^{-1} = A = (\det A)^{-1} \begin{pmatrix} d & -b \\ -c & a \end{pmatrix} \qquad \text{where } \det A = \pm 1$$

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

Case $\det A = 1$

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

So we have $a = d$, $b = -b$, $c = -c$.

$$b = -b \implies 2b = 0 \mod 26 \implies b = 13 \text{ or } b = 0 \tag{1}$$

$$c = -c \implies 2c = 0 \mod 26 \implies c = 13 \text{ or } c = 0 \tag{2}$$

Let's solve

$$\det A = ad - cb = a^2 - cb = 1 \tag{3}$$

If $c = b = 0$ so we have $a^2 = 1 \implies a = \pm 1$ 2 possibilities, which are

$$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \qquad \begin{pmatrix} 25 & 0 \\ 0 & 25 \end{pmatrix}$$

If $c = 13$, $b = 0$ so we have $a^2 = 1 \implies a = \pm 1$ with have 2 possibilities

$$\begin{pmatrix} 1 & 0 \\ 13 & 1 \end{pmatrix} \qquad \begin{pmatrix} 25 & 0 \\ 13 & 25 \end{pmatrix}$$

and same for $c = 0$ and $b = 13$

$$\begin{pmatrix} 1 & 13 \\ 0 & 1 \end{pmatrix} \qquad \begin{pmatrix} 25 & 13 \\ 0 & 25 \end{pmatrix}$$

If $c = 13$, $b = 13$ implies

$$a^2 - 13^2 = 1 \tag{4}$$
$$a^2 = 1 + 13 \tag{5}$$
$$a^2 = 14 \implies a = 14 \text{ or } a = 12 \text{ which is 2 possibilities} \tag{6}$$

$$\begin{pmatrix} 14 & 13 \\ 13 & 14 \end{pmatrix} \qquad \begin{pmatrix} 12 & 13 \\ 13 & 12 \end{pmatrix}$$

So we have 8 matices over $\mathbb{Z}_{26}$ such that $\det A = 1$ for each matrix A.

Case $\det A = -1$

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

So we have $a = -d$ Let's solve

$$\det A = ad - cb = a^2 - cb = -1 \tag{7}$$

As 26 is a product of 2 and 13 which are two prime numbers so

$$\mathbb{Z}_{26} \to \mathbb{Z}_2 \times \mathbb{Z}_{13}$$

In $\mathbb{Z}_2$, $a = -d \implies a = d = 0$ or $a = d = 1$.

If $a = 0$ then $ad - cb = -1 = 1 \implies c = d = 1$, which is $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$

If $a = 1$ then $cb = 0 \implies c = 0$ or $b = 0$ or $c = b = 0$. So we have 4 possibilities in $\mathbb{Z}_2$, which are

$$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \qquad \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \qquad \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$$

In $\mathbb{Z}_{13}$, $ad - cb = -1$ with $a = -d$ implies $a^2 + bc = 1$.

If $a^2 = 1$ so we have $bc = 0$ First case, if $a = 1$ and $b = 0$ so we have 12 choices of c such that $c \neq 0$. And same if $a = 1$ and $c = 0$, we have 12 choices of b such that $b \neq 0$. The last case is $a = 0$, $b = 0$ and also $c = 0$. So we have 25 possibilities for $a = 1$.

If $a = -1$, we have the same possibility as in $a = 1$. So for $a = \pm 1$, we have 2×25 possibilities.

If $a \neq \pm 1$ so there is 11 possibilities of a. And as $\mathbb{Z}_{13}$ is a field so $cb \in \mathbb{Z}_{13}$ and has 12 possibilities in $\mathbb{Z}_{13}^*$. So for $a \neq \pm 1$ we have 11×12 possibility of matrices.

So, there are $25 \times 2 + 11 \times 12 = 182$ matrices of determinants equal to -1 in $\mathbb{Z}_{13}$ so in $\mathbb{Z}_2 \times \mathbb{Z}_{13}$ there are 4×182 matrices of determinant equal to -1 which is the same number in $\mathbb{Z}_{26}$.

To conclude, the number of involutory key in the Hill Cipher is the sum of the number of matrix of determinant equal to 1 and the number of matrix of determinant equal to -1 which is equal to $8 + 728 = 736$. So there are 736 involutory keys.

2 Solution of Exercise 2.23

Suppose we are told that the plaintext

`breathtaking`

yields the ciphertext

`RUPOTENTOIFV`

where the Hill Cipher is used (but m is not specified). Let's determine the encryption matrix.

a	b	c	d	e	f	g	h	i	j	k	l	m
0	1	2	3	4	5	6	7	8	9	10	11	12

n	o	p	q	r	s	t	u	v	w	x	y	z
13	14	15	16	17	18	19	20	21	22	23	24	25

The plaintext

b	r	e	a	t	h	t	a	k	i	n	g
1	17	4	0	19	7	19	0	10	8	5	21

The ciphertext

R	U	P	O	T	E	N	T	O	I	F	V
17	20	15	14	19	4	13	19	14	8	5	21

As the length of our message is 12 so the possible value of m is a divisor of 12 so m may be equal to 1,2,3,4 or 6.

If m=1

So, $e_K(1) = 17 \implies 17 = 1.K \implies K = 17$
We also have that $e_K(17) = 20$ so $17K = 20 \implies 17^2 = 20 \mod 26$ which is false so $m \neq 1$

If m=2

So,

$$e_K(1\ 17) = (17\ 20) \tag{8}$$
$$e_K(4\ 0) = (15\ 14) \tag{9}$$

From the first two plaintext-ciphertext pair, we get the matrix equation

$$\begin{pmatrix} 1 & 17 \\ 4 & 0 \end{pmatrix} = \begin{pmatrix} 17 & 20 \\ 15 & 14 \end{pmatrix}.K$$

So $K = \begin{pmatrix} 17 & 20 \\ 15 & 14 \end{pmatrix}^{-1} . \begin{pmatrix} 1 & 17 \\ 4 & 0 \end{pmatrix}$ or det $\begin{vmatrix} 17 & 20 \\ 15 & 14 \end{vmatrix} = 17 \times 14 - 15 \times 20 = 10$ which is not coprime to 26 so the matrix is not invertible. So $m \neq 2$.

If m=3

So,

$$e_K(1\ 17\ 4) = (17\ 20\ 15) \tag{10}$$
$$e_K(0\ 19\ 7) = (14\ 19\ 4) \tag{11}$$
$$e_K(19\ 0\ 10) = (13\ 19\ 14) \tag{12}$$

From the first three plaintext-ciphertext, we get the matrix equation

$$\begin{pmatrix} 17 & 20 & 15 \\ 14 & 19 & 4 \\ 13 & 19 & 14 \end{pmatrix} = \begin{pmatrix} 1 & 17 & 4 \\ 0 & 19 & 7 \\ 19 & 0 & 10 \end{pmatrix}.K$$

So $K = \begin{pmatrix} 1 & 17 & 4 \\ 0 & 19 & 7 \\ 19 & 0 & 10 \end{pmatrix}^{-1} . \begin{pmatrix} 17 & 20 & 15 \\ 14 & 19 & 4 \\ 13 & 19 & 14 \end{pmatrix}$ where $\begin{pmatrix} 1 & 17 & 4 \\ 0 & 19 & 7 \\ 19 & 0 & 10 \end{pmatrix}^{-1} = \begin{pmatrix} 10 & 2 & 5 \\ 7 & 2 & 1 \\ 7 & 17 & 1 \end{pmatrix}$

So

$$K = \begin{pmatrix} 10 & 2 & 5 \\ 7 & 2 & 1 \\ 7 & 17 & 1 \end{pmatrix} . \begin{pmatrix} 17 & 20 & 15 \\ 14 & 19 & 4 \\ 13 & 19 & 14 \end{pmatrix} \tag{13}$$
$$K = \begin{pmatrix} 3 & 21 & 20 \\ 4 & 15 & 23 \\ 6 & 14 & 5 \end{pmatrix} \tag{14}$$