Computer security

Section 3

Eng: Ahmed safar

Row Transposition Cipher

- ❑ In general write message in a number of columns and then use some rule to read off from these columns.
- ❑ Key could be a series of number being the order to: read off the cipher; or write in the plaintext

Example 1

Plaint text : **Security game**

Key :41532

Answer

1	2	3	4	5
s	e	c	u	r
i	t	y	g	a
m	e	x	x	x

4	1	5	3	2
u	s	r	c	e
g	i	a	y	t
x	m	x	x	e

Cipher text :usrcegiaytxmxxe

Example 2

Plaint text : **computer science**

Key :ahmed

Answer

A	d	e	H	m
C	O	M	P	U
T	E	R	S	C
I	E	N	C	e

a	h	M	E	d
C	P	U	M	O
T	S	C	R	E
I	C	e	N	E

Cipher text :cpumotscreicene

Hill cipher Cipher

- Deduce corresponding cipher text using a 2*2 *hill cipher.*

- C = KP mod 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
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

Example 1

Plaint text : **attack**

Key : $\begin{pmatrix} 2 & 3 \\ 3 & 6 \end{pmatrix}$

Answer

- ☑ **C = KP mod 26**

$$\begin{pmatrix} 2 & 3 \\ 3 & 6 \end{pmatrix} \begin{pmatrix} 0 & 19 \\ 19 & 0 \end{pmatrix} = \begin{pmatrix} 57 & 38 \\ 114 & 57 \end{pmatrix} \text{ mod } 26 = \begin{pmatrix} 5 & 12 \\ 10 & 5 \end{pmatrix} = \begin{pmatrix} f & m \\ k & f \end{pmatrix}$$

$$\begin{pmatrix} 2 & 3 \\ 3 & 6 \end{pmatrix} \begin{pmatrix} 2 \\ 10 \end{pmatrix} = \begin{pmatrix} 34 \\ 66 \end{pmatrix} \text{ mod } 26 = \begin{pmatrix} 8 \\ 14 \end{pmatrix} = \begin{pmatrix} i \\ o \end{pmatrix}$$

Cipher text :fkmfio

Example 2

Plaint text : **Hi my friend**

Key : $\begin{pmatrix} 15 & 15 \\ 20 & 25 \end{pmatrix}$

Answer

Hi my

$$\begin{pmatrix} C1 & C3 \\ C2 & C4 \end{pmatrix} = \begin{pmatrix} 15 & 15 \\ 20 & 25 \end{pmatrix} \begin{bmatrix} 7 & 12 \\ 8 & 24 \end{bmatrix} \text{mod } 26 = \begin{pmatrix} 225 & 540 \\ 340 & 840 \end{pmatrix} = \begin{bmatrix} 17 & 20 \\ 2 & 8 \end{bmatrix} \text{mod26} = \begin{matrix} r & u \\ c & i \end{matrix}$$

Frie

$$\begin{pmatrix} C5 & C7 \\ C6 & C8 \end{pmatrix} = \begin{pmatrix} 15 & 15 \\ 20 & 25 \end{pmatrix} \begin{bmatrix} 5 & 8 \\ 17 & 4 \end{bmatrix} \text{mod } 26 = \begin{bmatrix} 330 & 180 \\ 525 & 260 \end{bmatrix} \text{mod26} = \begin{bmatrix} 18 & 24 \\ 5 & 0 \end{bmatrix} = \begin{matrix} s & y \\ f & a \end{matrix}$$

nd

$$\begin{pmatrix} C9 \\ C10 \end{pmatrix} = \begin{pmatrix} 15 & 15 \\ 20 & 25 \end{pmatrix} \begin{bmatrix} 13 \\ 3 \end{bmatrix} \text{mod } 26 = \begin{bmatrix} 240 \\ 335 \end{bmatrix} \text{mod26} = \begin{bmatrix} 6 \\ 23 \end{bmatrix} = \begin{matrix} g \\ x \end{matrix}$$

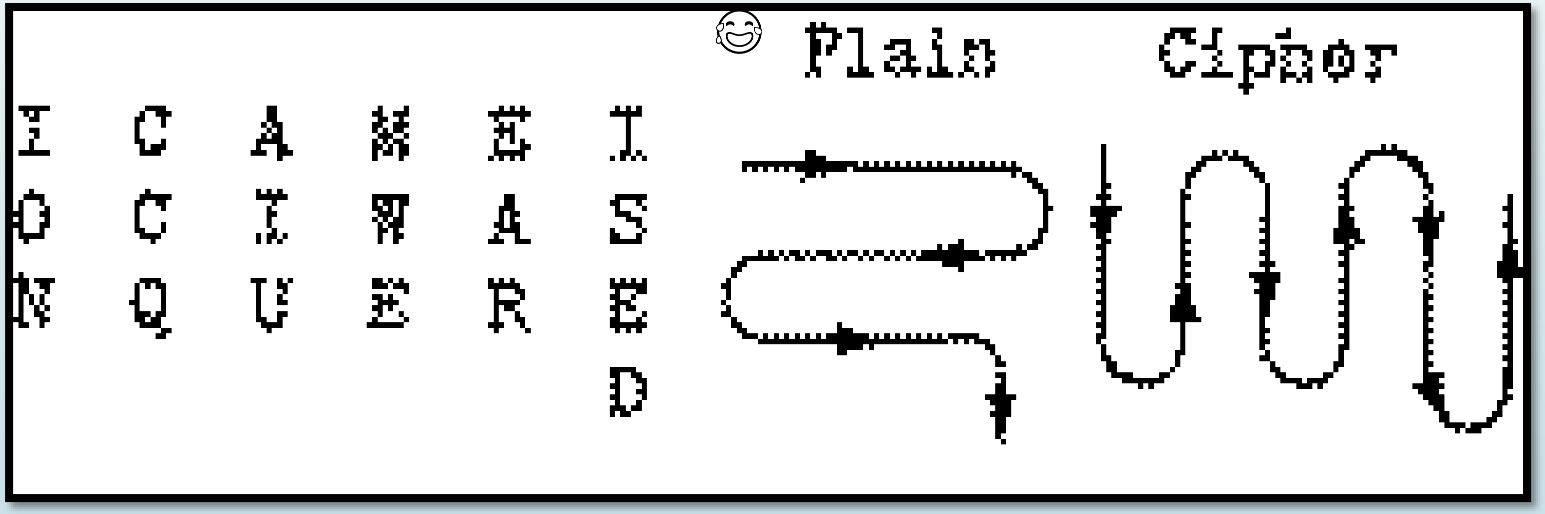
Cipher text : rcuisfyagx

Geometric

Write message following one pattern and read out with another

Plain: I CAME I SAW I CONQUERED

Key : 6



I	C	A	M	E	I
O	C	I	W	A	S
N	Q	U	E	R	E
					D

Cipher text :IONQCCAIUEWMEARDESI

Geometric

Write message following one pattern and read out with another

Plain: I CAME I SAW I CONQUERED

Key : 4

😂

I	c	a	m
A	s	l	e
W	l	c	o
E	u	q	n
R	e	d	

Cipher text :iawereuiscaicqdnoem