Tanvi Kurhade 1910IB0048

Page No.:
Date: 20-8-21

CNS - OPEN BOOK TEST

1. Vigenere Cipher

P : Practice Problem

K : CNS

C : ?

Encryption :

a) P = P r a c t i c e P r o b l e m

15 17 0 2 19 8 2 4 15 17 14 1 11 4 12

b) K = C N S

2 13 18

c) Divide the PT into no. of char of Key

	P	r	a	c	t	i	c	e	p	r	o	b	l	e	m
P =	15	17	0	2	19	8	2	4	15	17	14	1	11	4	12
K =	2	13	18	2	13	18	2	13	18	2	13	18	2	13	18

Now,

$C = (P + K) \bmod 26$

$C_1 = (15+2) \bmod 26 = 17$

$C_2 = (17+13) \bmod 26 = 4$

$C_3 = (0 + 18) \bmod 26 = 18$

$C_4 = (2+2) \bmod 26 = 4$

$C_5 = (19+13) \bmod 26 = 6$

$C_6 = (8+18) \bmod 26 = 0$

$C_7 = (2+2) \bmod 26 = 4$

$C_8 = (4+13) \bmod 26 = 17$

$C_9 = (15+18) \bmod 26 = 7$

$C_{10} = (17+2) \bmod 26 = 19$

$C_{11} = (14+13) \bmod 26 = 1$

$C_{12} = (1+18) \bmod 26 = 19$

$C_{13} = (11+2) \bmod 26 = 13$

$C_{14} = (4 + 13) \bmod 26 = 17$

$C_{15} = (12 + 18) \bmod 26 = 4$

C :	17	4	18	4	6	0	4	17	7	19	1	19	13	17	4
	r	e	s	e	g	a	e	r	h	t	b	t	n	r	e

C : resegaerhtbtnre

2. Hill cipher

P : ACT

K : YashShah

C : ?

$$K = \begin{bmatrix} y & a & s \\ h & s & h \\ a & h & x \end{bmatrix}$$

Encryption : $C = P \times K \bmod 26$ [matrix]

1) PT matrix = 2 x 1

P : ACT = $\begin{bmatrix} A \\ C \\ T \end{bmatrix}$ 3x1

~~T~~

~~x~~ ~~2x1~~

2) Key matrix = 3 x 3

$$C_1 = P_1 \times K \bmod 26 = \begin{bmatrix} A \\ C \\ T \end{bmatrix} \times \begin{bmatrix} 24 & 0 & 18 \\ 7 & 18 & 7 \\ 0 & 7 & 23 \end{bmatrix} \bmod 26$$

$$= \begin{bmatrix} 0 \\ 2 \\ 19 \end{bmatrix} \times \begin{bmatrix} 23 & 0 & 18 \\ 7 & 18 & 7 \\ 0 & 7 & 23 \end{bmatrix} \bmod 26$$

$$= \begin{bmatrix} 342 \\ 169 \\ 451 \end{bmatrix} \bmod 26 = \begin{bmatrix} 4 \\ 13 \\ 9 \end{bmatrix} = \begin{bmatrix} e \\ n \\ j \end{bmatrix}$$

~~$C_2 = P_2 \times K \bmod 26 = \begin{bmatrix} T \\ x \end{bmatrix} \times$ mod 26~~

C : enj

~~mod 26~~

$= \begin{bmatrix} 19 \\ 23 \end{bmatrix}$ ~~mod~~ X

$\neq$

3. Keyless Transposition (Row) Cipher

P : Practice Problem

K : CNS

C = ?

4 x 4 matrix

p	t	p	l
r	i	r	e
a	c	o	m
c	e	b	x

→

ptpl rire acom cebx

C : ptpl rire acom cebx

4. Keyed (column) Cipher

P : Practice Problem

K : FIRE = ~~3124~~ 2341 ~~3124~~

C : ?

4 x 4 matrix

~~2~~	3	4	~~1~~
p	r	a	c
t	i	c	e
p	r	o	b
l	e	m	x

C = cebx ptpl rire acom

~~C : rire acom ptpl cebx~~

5. Affine

P : Good Morning

K : (7, 9) , $K_1 = 7$, $K_2 = 9$

Encryption :

P :	G	o	o	d	m	o	r	n	i	n	g
	6	14	14	3	12	14	17	13	8	13	6

$C_1 = (6 \times 7 + 9) \bmod 26 = 51 \rightarrow 25 = z$

$C_2 = (14 \times 7 + 9) \bmod 26 = 107 \rightarrow 3 = d$

$C_3 = (14 \times 7 + 9) \bmod 26 = 107 \rightarrow 3 = d$

$C_4 = (3 \times 7 + 9) \bmod 26 = 30 \rightarrow 4 = e$

$C_5 = (12 \times 7 + 9) \bmod 26 = 93 \rightarrow 15 = p$

$C_6 = (14 \times 7 + 9) \bmod 26 = 107 \rightarrow 3 = d$

$C_7 = (17 \times 7 + 9) \bmod 26 = 128 \rightarrow 24 = y$

$C_8 = (13 \times 7 + 9) \bmod 26 = 100 \rightarrow 22 = w$

$C_9 = (8 \times 7 + 9) \bmod 26 = 65 \rightarrow 13 = n$

$C_{10} = (13 \times 7 + 9) \bmod 26 = 100 \rightarrow 22 = w$

$C_{11} = (6 \times 7 + 9) \bmod 26 = 51 \rightarrow 25 = z$

e : sqqwkqmayas

C = zddepdywnwz

6. Decrypt Affine Cipher

P: aevjvjztsdwcn = 0 4 21 9 21 9 25 19 18 3 22 2 13

K = (17, 15)

$K_1 = 17 \quad \therefore K_1^{-1} = 23$

$K_2 = 15 \quad \therefore K_2^{-1} = -15$

~~$P_1 = [(0 - 15 \times 0) \times (-15)] \bmod 26$~~

0 $P_1 = [0 - (-15) \times 23] \bmod 26 = 19 = t$

4 $P_2 = [4 - (-15) \times 23] \bmod 26 = h$

21 $P_3 = [(21 - 15) \times 23] \bmod 26 = i$

9 $P_4 = [(9 - 15) \times 23] \bmod 26 = s$

21 $P_5 = [(21 - 15) \times 23] \bmod 26 = i$

9 $P_6 = [(9 - 15) \times 23] \bmod 26 = s$

25 $P_7 = [(25 - 15) \times 23] \bmod 26 = w$

19 $P_8 = [(19 - 15) \times 23] \bmod 26 = o$

18 $P_9 = [(18 - 15) \times 23] \bmod 26 = r$

3 $P_{10} = [(3 - 15) \times 23] \bmod 26 = k$

22 $P_{11} = [(22 - 15) \times 23] \bmod 26 = i$

2 $P_{12} = [(2 - 15) \times 23] \bmod 26 = n$

13 $P_{13} = [(13 - 15) \times 23] \bmod 26 = g$

1. Playfair

P : Good Morning

K : stayhappy

s	t	a	y	h
p	b	c	d	e
f	g	i/j	k	l
m	n	o	q	r
u	v	w	x	z

5x5

good morning

go od mo rn in gx

go = in

od = qc

mo = nq

rn = mo

in = go

gx = kv

C = inqcnqmogokv

8. Playfair

C : qomqyekcxl
K : hello

h	e	l	o	a
b	c	d	f	g
i/j	k	m	n	p
q	r	s	t	u
v	w	x	y	z

5x5

qo mq ye kc xl

qo = th
mq = is
ye = wo
kc = rk
xl = ld

14. C = eeyxlovxhorelenx
K : HACK = 3124

3	1	2	4
e	l	h	l
e	v	o	e
y	o	r	n
x	x	e	x

hore eeyx lvox lenx

h	e	l	l
o	e	v	e
r	y	o	n
e	x	x	x

P = Hello everyone

9. ~~Affine Cipher~~
P: ~~Hello everyone~~
K = ~~(7, 5)~~

13. Keyless (column)
C: horeeeyxlovxlenx

4x4 matrix

h	o	r	e
e	e	y	x
l	o	v	x
l	e	n	x

hell oeoe ryvn exxx

Decryt"

h	e	l	l
o	e	~~l~~	e
r	y	o	n
e	x	x	x

hello e~~l~~ery one x x x