ASSIGNMENT-1

YASH

1. Playfair cipher

Plaintext : Introduction to cryptography

Key : Practice

P	R	A	C	T
I/J	E	B	D	F
G	H	K	L	M
N	O	Q	S	U
V	W	X	Y	Z

after split → In th od uc ti on to

encrypted → in = gv, th = pa, od = se, uc = st,
ti = pf, on = qo ; to = ru

after split → cr yp to gr ap hy

encrypted → cr = ta yp = vc to = ru

Encrypted Text ⇒ gvpa se st pf qo ru to vc ru"

YASH

2. Hill Cipher with m=2

Plain text → Introduction to cryptography

Key => abcd

$C = Kp \bmod 26 \Rightarrow \begin{bmatrix} C_1 \\ C_2 \end{bmatrix} = \begin{bmatrix} K_{11} & K_{12} \\ K_{21} & K_{22} \end{bmatrix} \begin{bmatrix} P_1 \\ P_2 \end{bmatrix} \bmod 26$

in: $= \begin{bmatrix} a & b \\ c & d \end{bmatrix} \begin{bmatrix} 0 \\ 13 \end{bmatrix} \bmod 26 = \begin{bmatrix} 0 & 1 \\ 2 & 3 \end{bmatrix} \begin{bmatrix} 8 \\ 13 \end{bmatrix} \bmod 26$

$= \begin{bmatrix} 0+13 \\ 16+39 \end{bmatrix} \bmod 26 = \begin{bmatrix} 13 \\ 55 \end{bmatrix} \bmod 26 = \frac{13}{3} \approx \begin{bmatrix} n \\ d \end{bmatrix}$

in = nd

tr: $\begin{bmatrix} 0 & 1 \\ 2 & 3 \end{bmatrix} \begin{bmatrix} t \\ r \end{bmatrix} = \begin{bmatrix} 0 & 1 \\ 2 & 3 \end{bmatrix} \begin{bmatrix} 19 \\ 17 \end{bmatrix} = \begin{bmatrix} 17 \\ 89 \end{bmatrix} \bmod 26 = \frac{17}{11} \approx \begin{bmatrix} r \\ l \end{bmatrix}$

tr = rl

od: $\begin{bmatrix} 0 & 1 \\ 2 & 3 \end{bmatrix} \begin{bmatrix} 14 \\ 3 \end{bmatrix} = \begin{bmatrix} 3 \\ 37 \end{bmatrix} \bmod 26 = \frac{3}{37} \Rightarrow \begin{bmatrix} d \\ l \end{bmatrix}$.

od = dl

uc: $\begin{bmatrix} 0 & 1 \\ 2 & 3 \end{bmatrix} \begin{bmatrix} 20 \\ 2 \end{bmatrix} \bmod 26 = \begin{bmatrix} 2 \\ 46 \end{bmatrix} \bmod 26 = \frac{2}{20} \approx \begin{bmatrix} b \\ u \end{bmatrix}$

uc = bu

ti: $\begin{bmatrix} 0 & 1 \\ 2 & 3 \end{bmatrix} \begin{bmatrix} 19 \\ 8 \end{bmatrix} = \begin{bmatrix} 8 \\ 62 \end{bmatrix} \bmod 26 = \begin{bmatrix} 8 \\ 10 \end{bmatrix} \approx \begin{bmatrix} i \\ k \end{bmatrix}$

ti = ik

on: $\begin{bmatrix} 0 & 1 \\ 2 & 3 \end{bmatrix} \begin{bmatrix} 14 \\ 13 \end{bmatrix} = \begin{bmatrix} 13 \\ 67 \end{bmatrix} \bmod 26 = \begin{bmatrix} 13 \\ 15 \end{bmatrix} = \begin{bmatrix} n \\ p \end{bmatrix}$

on = np

to: $\begin{bmatrix} 0 & 1 \\ 2 & 3 \end{bmatrix}\begin{bmatrix} 19 \\ 14 \end{bmatrix} = \begin{bmatrix} 14 \\ 80 \end{bmatrix} \bmod 26 = \begin{bmatrix} 14 \\ 2 \end{bmatrix} = \begin{bmatrix} O \\ C \end{bmatrix}$ YASH

to = OC

or: $\begin{bmatrix} 0 & 1 \\ 2 & 3 \end{bmatrix}\begin{bmatrix} 2 \\ 17 \end{bmatrix} = \begin{bmatrix} 17 \\ 55 \end{bmatrix} \bmod 26 = \begin{bmatrix} 17 \\ 3 \end{bmatrix} \approx \begin{bmatrix} R \\ D \end{bmatrix}$

or = RD

yp: $\begin{bmatrix} 0 & 1 \\ 2 & 3 \end{bmatrix}\begin{bmatrix} 24 \\ 15 \end{bmatrix} = \begin{bmatrix} 15 \\ 15 \end{bmatrix} \approx \begin{bmatrix} P \\ P \end{bmatrix}$

yp = PP

to = OC

gr: $\begin{bmatrix} 0 & 1 \\ 2 & 3 \end{bmatrix}\begin{bmatrix} 6 \\ 17 \end{bmatrix} = \begin{bmatrix} 17 \\ 11 \end{bmatrix} = \begin{bmatrix} R \\ L \end{bmatrix}$

gr = RL

ap: $\begin{bmatrix} 0 & 1 \\ 2 & 3 \end{bmatrix}\begin{bmatrix} 0 \\ 15 \end{bmatrix} = \begin{bmatrix} 15 \\ 45 \end{bmatrix} \bmod 26 = \begin{bmatrix} 15 \\ 19 \end{bmatrix} \approx \begin{bmatrix} P \\ T \end{bmatrix}$

ap = PT

hy: $\begin{bmatrix} 0 & 1 \\ 2 & 3 \end{bmatrix}\begin{bmatrix} 7 \\ 24 \end{bmatrix} \bmod 26 = \begin{bmatrix} 24 \\ 8 \end{bmatrix} = \begin{bmatrix} Y \\ I \end{bmatrix}$

hy = YI

encrypted key = ndRL dL buIKn pOcRd PPRLPT YI

YASH

Ans. 3 ① 5 2 3 1 4

c r y p t
o g r a p
h y a n d
n e t w o
r k s e c
u r i t y
p r i n c
i p l e s

⇒ panwetne rg yek
rrpyra ts ii l tp
d ocy.cs cohn
rupi

⇒ 5 2 3 1 4

② 5 2 3 1 4

p a n w e
t n e rg
y e k r r r
p y r a t
s i i l t
p d o c y
c s c o u
n r u p i

⇒ wrr al c op an eyid
s r ne k r i o c u e g
r t t yu i p ty p s p c n

YASH

(3)

5	2	3	1	4
w	r	r	a	l
c	o	p	a	n
e	y	i	d	s
r	n	e	k	r
i	o	c	u	e
g	r	t	t	y
w	i	p	t	y
p	s	p	c	n

⇒ aadkuttcroyno ris rpie ctpp lnsre yyn wce rigwp

4. Plaintext - cryptography and network security principles
key : william
OTP

2(c)	17(r)	24(y)	15(p)	19(t)
+ 22(w)	8(i)	11(l)	11(l)	8(i)
24	25	35	26	27

mod 26 -

⇒ 24(y) 25(z) 9(j) 0(a) 1(b)

14(o)	16(g)	17(r)	0(a)	15(p)
+ 0(a)	12(m)	22(w)	8(i)	11(l)
14	28	39	8	26

mod 26 -

⇒ 14(o) 2(c) 13(n) 8(i) 0(a)

YASH

	7(n)	24(y)	0(a)	13(n)	3(d)
+	11(l)	8(i)	0(a)	12(m)	22(w)
	18	32	0	25	24

mod 26 -

18(s)	6(g)	0(a)	25(z)	24(y)

13(n)	4(e)	19(t)	22(w)	14(o)
+ 8(i)	11(l)	11(l)	8(i)	0(a)
21	15	30	30	14(o)

17(q)	10(k)	18(s)	4(e)	2(c)
+ 12(m)	22(w)	8(i)	11(l)	11(e)
29	32	26	15	13

mod 26 -

3(d)	6(g)	0(a)	15(p)	13(n)

20(u)	17(q)	8(i)	19(t)	24(y)
+ 8(i)	0(a)	12(m)	22(w)	8(i)

mod 26

2(c)	17(q)	20(u)	15(p)	6(g)

8(i)	15(p)	11(l)	4(e)	18(s)
+ 22(w)	8(i)	11(l)	11(l)	8(i)
4(e)	23(x)	22(w)	15(p)	0(a)

YZJABDCNIASGAZYVPEEODGAPNCRVPGACQ
NOEXWPA