	Tanvi kushade 191018
	Page No.:
	CNS - OPEN BOOK TEST
	C ICH DOOR ILST
	· Vigenere Cipher
-	P: Practice Problem
	K: CNS
	c : ?
	Encouption:
	Encryption: a) P=PracticeProblem
	a) F=F r a c t 1 C t 17 14 1 11 4 12
_	15 17 0 2 19 8 2 4 15 17 14 1 11 4 12
	b) K = C N 5
	2 13 18
	c) Divide the PT into no. of char of Key
	Practice problem
The state of the s	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) mod 26
<u> </u>	
	$C_1 = (15+2) \mod 26 = 17$
_	$C_2 = (17+13) \mod 26 = 4$
-	$C_3 = (0 + 18) \mod 26 = 18$
	$C_4 = (2+2) \mod 26 = 4$
	$C_5 = (19 + 13) \mod 26 = 6$
	$C_6 = (8+18) \mod 26 = 0$
	$(7 = (2+2) \mod 26 = 4$
	$C_8 = (4+13) \mod 26 = 17$
	$C_9 = (15 + 18) \mod 26 = 7$
	$C_{10} = (17+2) \mod 26 = 19$
1	$C_{11} = (14+13) \mod 26 = 1$
_	$C_{12} = (1+18) \mod 26 = 19$
 	
-	$C_{13} = (11+2) \mod 26 = 13$
4	

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

PT matrix =
$$2 \times 1$$

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

T

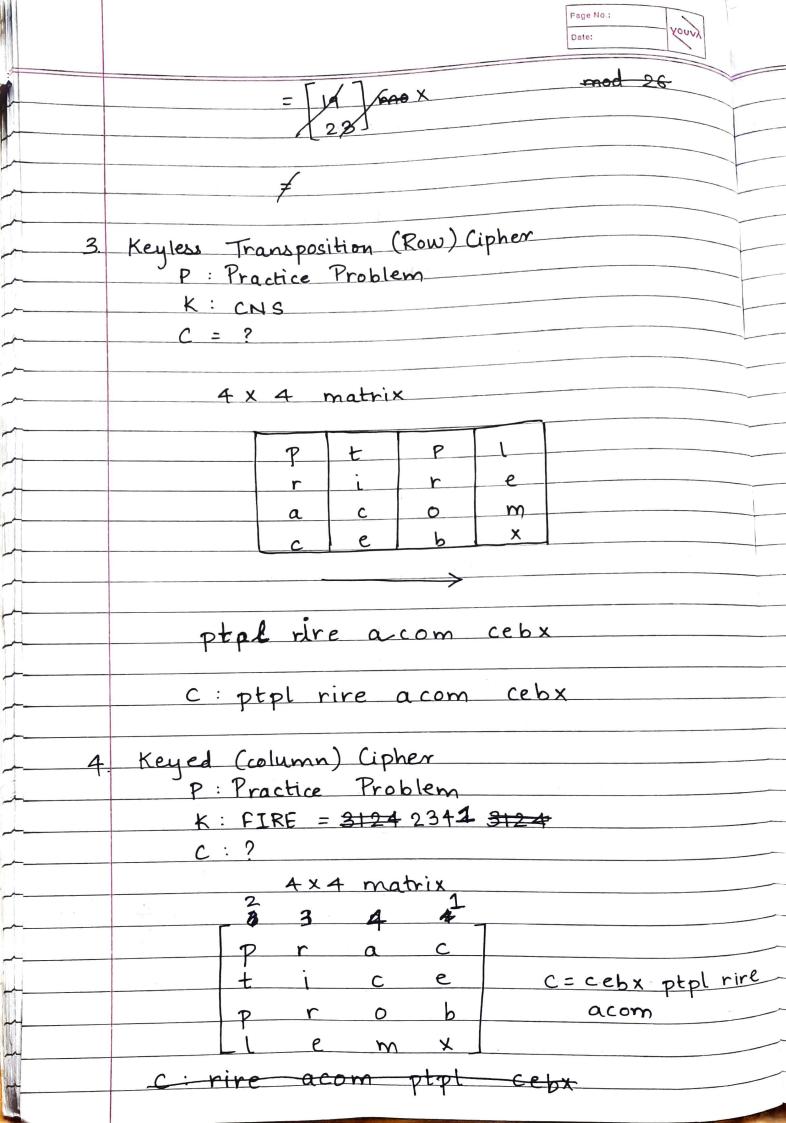
T

$$C_{1} = P_{1} \times K \mod 26 = \begin{bmatrix} A \\ A \end{bmatrix} \times \begin{bmatrix} 24 & 0 & 18 \\ 7 & 18 & 7 \\ 0 & 7 & 23 \end{bmatrix} \mod 26$$

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

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

$$\frac{e_{2}}{451} \times K \mod 26 = \begin{bmatrix} 7 \\ 451 \end{bmatrix} \times \mod 26$$



Affine

P: Good Morning $K: (\tilde{7}, \tilde{9}), K_1 = 1, K_2 = 9$

Encryption:

P: Grood morning 6 14 14 3 12 14 17 13 8 13 6

C1 = (6 x 73 mod 26 = 18 - 8 = 25 -> z C2 = (14 x 73 mod 26 = C3 = (14 × 47 + 9) mod 26 = 16 -> 9 = 3 -> d C4 = (3 x 7+9) mod 26 = 22/3 K = 4 > e C5 = (12x7+9) mod 26 = 10 -> K = 15 -> p C6 = (14x7+9) mod 26 = 16/ -> 1 = 3 -> d C7 = (17 x 7+9) mod 26 = 12 ->/ m = 24 -> y $C_8 = (13 \times 7 + 9) \mod 26 = 0 / \rightarrow / a = 22 \rightarrow w$

Cq = (8 x 7+9) mod 26 = 24 7 y = 13 →n (10 = (13 x 7 + 9) mod 26 = 0/

C11 = (6x7+9) mod 26 = 18 S = 25 →z

e: sqqwkqmayas

C = zddepdywnwz

6 Decrypt Affine Cipher P: aevjvjztsdwcn = 0 4 21 9 21 9 25 19 18 3 22 K = (17, 15)

$$K_1 = 17$$
 ... $K_1 = 423$
 $K_2 = 15$... $K_2^{-1} = 4 - 15$

Pr = [(2-15 x 0) x(-15)] mod 26

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

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

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

21
$$P_5 = [(21-15) \times 23] \mod 26 = 1$$

9
$$P_6 = [(9-15) \times 23] \mod 26 = 5$$

25
$$P_7 = [(25-15) \times 23] \mod 26 = W$$

18
$$P_q = [(18-15) \times 23] \mod 26 = r$$

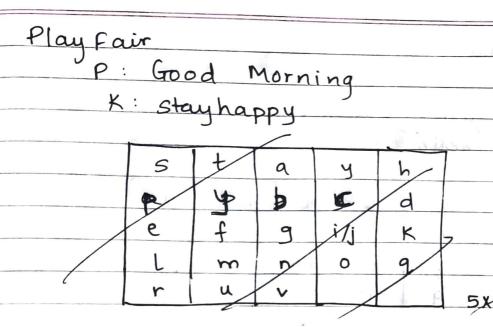
$$\begin{array}{lll} 19 & P_8 = \left[(19 - 15) \times 23 \right] \mod 26 & = 0 \\ 18 & P_9 = \left[(18 - 15) \times 23 \right] \mod 26 & = r \\ 3 & P_{10} = \left[(3 - 15) \times 23 \right] \mod 26 & = K \end{array}$$

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

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

13 P₁₃ =
$$[(13-15) \times 23]$$
 mod = 26 = 9

Youv



Ş	t	a	4	h	
P	Ь	C	ام	e	
£	9	i/i	K	L	
m	n	0	9	r	
u	V	\ w	X	2	5×5
					,

good morning

go od morn in gx

90 = in

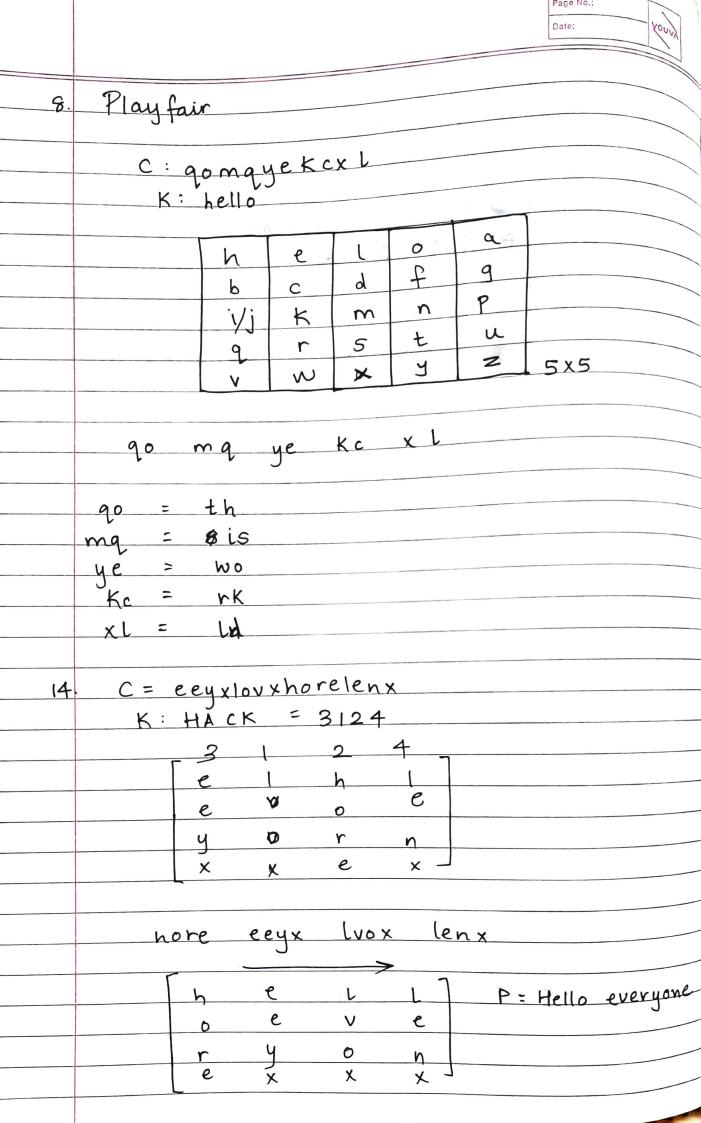
mo = nq

rn = mo

in = 90

qx = kv

C = inqcnamogokv

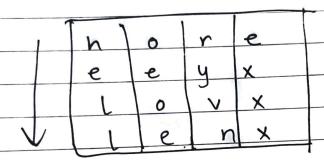


a. A	Hine	Ciph	er	
·	P	•		exyone
	К	= (7	, 5)	3

13. Keyless (column)

c: horeeeyxlovxlenx

4x4 matrix



hell oeol ryvn exxx

Decryt"

h	e		L
0	e	ø	e
~	ч	0	M
2	V	X	*
1	-	1	

hello exeryone x x x