-	Date:	
	Tutorial 5	
		35.4
01	Use a hill cipher to encipher the message "are line in an insecure	
,	message "are line in an insecure	world"
	Use the following key	· AMAG
	$K = \begin{bmatrix} 03 & 02 \end{bmatrix}$	
	05 07	
	messages = 1 we 122,4	1
	li 11, 8	
	$\frac{ve}{in} = \frac{21}{8}, \frac{4}{13}$	1. 2.
	0,13	Tall
	in 8,13	15
	se 18, 4	1
	2,20	3
	re)7, 4	
	wo 22, 14	NO.
	nl 17, 11	
	$\frac{d^2}{d^2}$ 4, 25	
	111 - 1/ V mages - 24 - 25 - 42	- 1
	cipher = K x message, nector	
	19 111	7
	71, 133	
	50, 131	
	26,91 mod 26	
	50,131	
	62,118	
3	46, 150	
	51, 113	<u></u>
	63 1 162	
No. No. of the last of the las	62,1950	2.3.5

Page:

1	Date:
	= [22, 8 [wi
	123, 7' Xh
	19,3 td
	24,1
77 (1)	0,13 = an
,	24, 1 H b
	10,14 kg
	20,20
\$17 Va	7,9
) Özlər	16,0 ga
6	11,6
	10, 13] kn]
l'an	
	≥ = cipher = wixh b dyban ybko uu hjalah
3)9	The plaintext "letus meet now" and the

The plaintext "letus meet now" and the corresponding righertext "HBCD FNOP IK IB" are given. You know that the algorithm is a Hill cipher; but you don't know the size of the key. Find the key matrix.

P = [11, 4, 19, 20, 18, 12, 18, 22, 14, 22, 23]C = [7, 1, 2, 3, 5, 13, 15, 10, 8, 11, 1]

Key matrix, K = [a b]

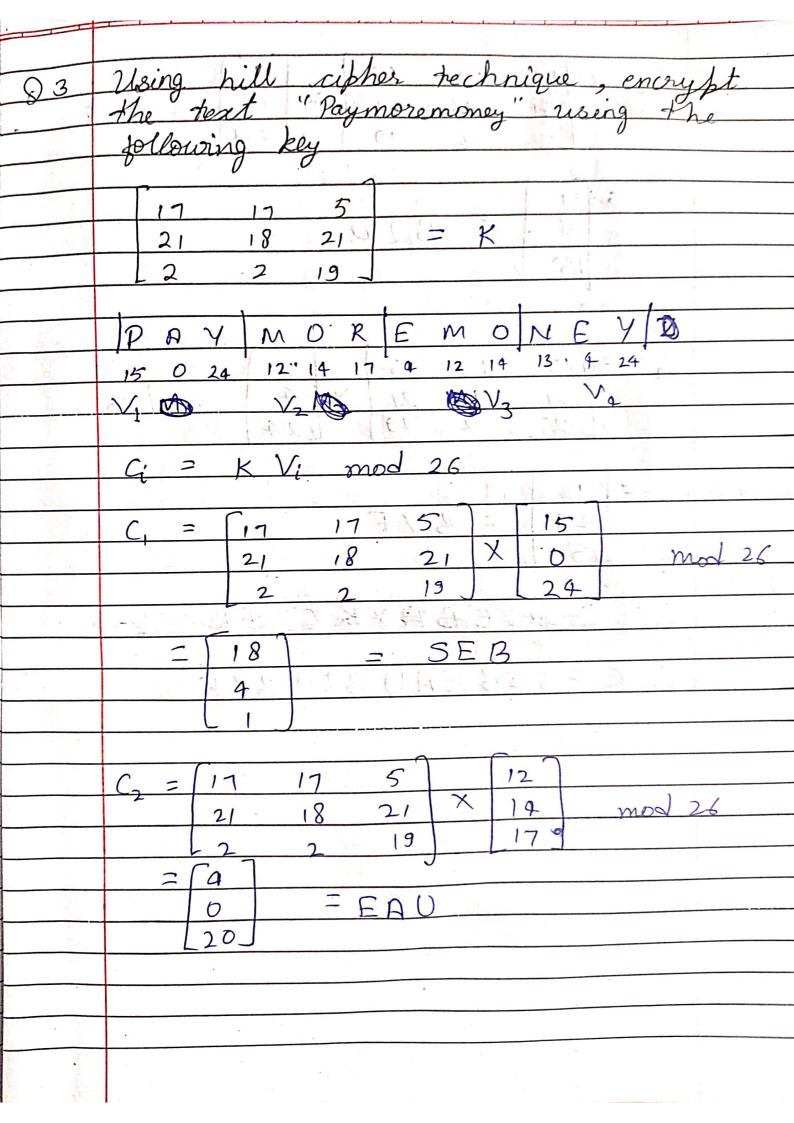
: C = K x P mod 26

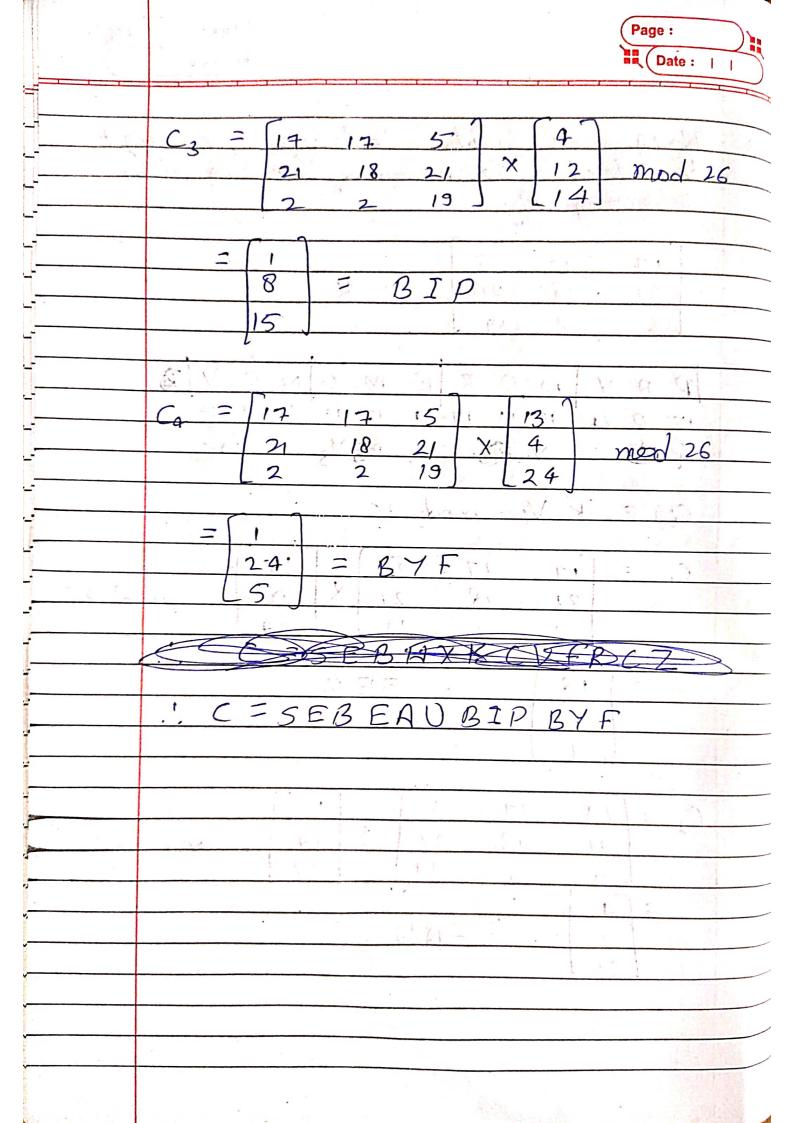
Page: Date:

	1 50			12. 1	1 10 7	
	NVE	Ta	5	X	4	
2	4 mas	C	1	11	.119	71.
3	1 1/			\	20	
5	- A	-		pt - 1	18	mod 26
13	1			()	12	Tie
15	N 4			, å (18	
10				· (-	22	
8	, .!			V =	14	
11	9.3		ii.	10	22	
L1	Jev	,	Ţ.,		23	

11a + 4b = 7 mod 26 $199 + 20b = 1 \mod 26$ $18a + 12b = 2 \mod 26$ 18c+22d = 3 mod 26 14a+22b = 5 mod 26 23 c = 1 mod 26 11C+22d = 13 mod 26 4 C + 19 d = 15 mod 26 20 C + 18 d = 10 mod 26 18 c + 1.4d = 8 mod 26 12c + 22d = 11 mod 26

a = 3b = a K= 4 C = 1d = 3



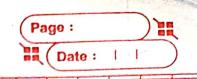


Date:	Page :			111
	Date :	1	1	

84	Encrupt the following using blandair
0	eigher using the keyword MONARCHY
	Encrypt the following using playfair appear using the keyword MONARCHY "SWARAJ IS MY BIRTH RIGHT", Use X as blank space.
7	as blank shace.
	The second secon
	MONBR
	C H MY B D
	E F G I/J K
	LPQST
	LUVWXZJ
4	Living as with
•	ESW AR AT IS MY BI RT HR TO
4	JJ RD TK RO OT CT PE GT
	Land House Court Miles In the
	S H)T
	SW -> & Xminum Menu tonical
	AR - RMany with with different
	AJ - 35
	75 -9 5 X
	MY -> NC
	BT - D5
	$RT \rightarrow DZ$
1	HR -> DO
	IGSKI
	HTOP
	5 0 10 120 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
	=> Cipher = 'QXRMBSSXMCDSDZDOKIDP"

M

85	Discuss the properties that are satisfied by Groups, Rings & Fields
47	satisfied by Growns Rings & Fields
10 × 2	LANGE WITERS AND DE TO CHENNERS
, , , , , , , , , , , , , , , , , , , ,	Group
	- Closure
	- Associativity
	- Existence of identity element
`	Existence of identity element Existence of innerse
	Ring X X X
	- Abelian group
n T i	Abelian group Closure under multiplication
	Associativity of multiplication
Str. je	Associativity of multiplication Distributive laws
	Fields
	integral Longin
	integral domain annerse
	2 5 6 6 6
	Y E & E
	7 d + TA
	TO (1) TO (1)
	THE STATE OF THE S
	MAN TANK C



	Compare substitution & bransportation. Transportation
86	Compare substitution & transportation.
er fri	
	Substitution
1	
()	Plaintext characters Plaintext characters are are replaced with nearranged
1	are replaced with rearranged
	Plaintext characters Plaintext characters are are replaced with rearranged other characters.
	0
ii	Mono alphabetic Keyless & Keyed
	Mono alphabetic Keyless & Keyed & Polyalphabetic transposition ciphers
	V.
iii	Character's identity Position is changed is changed while but identity remains its position remains unchanged.
	is changed while but dentity remains
	its position gemains unchanged.
	unchanged
iv)	The letter with high The keys which are frequency can detect nearer to correct key blaintext. can disclose plaintext.
	frequency can letect neaver to correct key
	plaintent. can disclose plaintent.
~)	Caesar cipher, hill Columnar, rail-fence cipher, playfair cipher cipher.
	cipher, playfair cipher cipher.