+ HILL CIPHERING TECHNIQUE: >

Ex Can encrypt digraph, trigraph or polygraph at once.

let's take sample matrix of 3rd order:

Key marix =
$$\begin{bmatrix} 17 & 17 & 8 \\ 21 & 18 & 21 \\ 2 & 2 & 19 \end{bmatrix}$$
 Key = qubqrbeus
$$\begin{cases} \text{Key} = \text{qubqrbeus} \\ \text{Yey} = \text{pubqrbeus} \end{cases}$$

sur have taken a 3rd order matrix, so we can go for trigraph solution.

let's convert /cipher.

"National university of computer and

emerging sciences.

Cipher Table:

	7	a	t	,	0	n	a	Ł.	u	n	i	V	e	8	S	9.0	t	4	A STATE OF
and the state of t	14	1	20	19	15	14	l	12	21	14	9	त्रश	\$	18	19	9	20	125	State of water or

0	f	C	0	m	P	a	te	3	Ÿ	a	~	d	e	m	е	7	9	Section Sections
15	6	3	is	13	16	21	20	8	18	١	14	4	5	13	5	18	7	Side and property of

action in						
- water-	And the second s	5 C	C	e	n G	e 5 5
	9 14 7	19 3	9	\$	14 3	5 19 19

	-, - ,
Now , let's try to implement Hill cipher	on first trigraph,
i.e 'Nat'.	
so, $AC = E(K,P) = PK \mod 26$	
P = D(kie) = CK mod 26	
= PKK' mod?	16
SO, (C1 C2 C3) = (P1 P2 P3) / K11 K12 K13	
K21 K22 K23	
Here: K31 K32 K3	3
(P.P2P3) = (nat); (GC2C3) =?	
Cr plain text Cr cipher to	ext
is torm:	
C = Primod26 ;	K = Key moutrix
$(e_1C_2C_3)_{\text{nat}} = (i4 \ i \ 20)/i7 \ i7$	57
21 18	al mod 26
2 2	19
1 200 200 (121) made	1 26
= (299 296 471) mod	m : ()
= (13 10 3) => (1	
So, plain text	
$(nat) \longrightarrow (mjc)$	The second secon
similary, we convert all of trigr	aphs.
	And the state of t

To find determinant:

so, after calculating determinant:

Det(Key) = -3 mod 26

To find adjoint of key matrix:

Adj c7
$$\text{Rey} = \begin{pmatrix} 17 & 17 & 5 & 17 & 19 \\ 21 & 18 & 21 & 21 & 18 \\ 2 & 2 & 19 & 2 & 2 \end{pmatrix}$$

800

$$= \begin{cases} 18 \times 19 - 2 \times 21 & 2 \times 5 - 12 \times 19 & 12 \times 21 - 18 \times 5 \\ 21 \times 2 - 19 \times 21 & 19 \times 12 - 5 \times 2 & 5 \times 21 - 21 \times 12 \end{cases}$$

$$= \begin{cases} 21 \times 2 - 19 \times 21 & 19 \times 12 - 18 \times 5 \\ 21 \times 2 - 2 \times 19 & 2 \times 13 - 18 \times 2 \end{cases}$$

$$= \begin{cases} 18 \times 19 - 2 \times 21 & 19 \times 12 - 18 \times 5 \\ 21 \times 2 - 2 \times 19 & 2 \times 13 - 18 \times 2 \end{cases}$$

$$= \begin{cases} 18 \times 19 - 2 \times 19 & 19 \times 12 - 18 \times 5 \\ 21 \times 2 - 2 \times 19 & 2 \times 13 - 18 \times 2 \end{cases}$$

= / 300 - 313 267
-357 313 -252 mod 26
6 0 -51
= / 14 -1 7
-19 1 -18 mod 26
6 0 -21
Adj of key = (14 25 7) (add med to)
3 3 8
601/
K" = 1 x Holy of A
(A)
- 1 / 14 25 7
23 7 mod 26
. 6 0 1/
ev 23"/14 25 7
7 1 8 mod 26
6 0 1
find 23' ??
we , use ; Evoliden Algorithm;
$ax = 1 \mod 26$, $a = 23$,
So, 26 = (1)(23)+(3)
23 = (7)(3)+(2)
3 = (1)(2)+(1).

800 1.3-1(1.23-7.3) 1= 1.3 - 1.23 + 2.3 1= 8(1.26-1.23)-1.23 1 = 8.26 -9.23 (= (8)(26)+ (-9)(13) 80, X=-9+26=17 23 = 17 80, 80, 25 K, = 17 mod 26 6 0 . 238 425 1191 119 17 136 mod 26 102 17 K-1 = 9 15 15 17 6 24 by proceeding verify x" KK-1 = I (KK-1) mod 26 =] Formula for decryption: P = Ct 1 mod 26

	$0 = (13 \ 10 \ 3) \left(\frac{4}{15} \ \frac{9}{17} \ 6 \right) \mod 26$
,	12 1 mad 26
D	(13 10 3) (15 17 6) 11100226
and the second of the second o	24 0 17
· ·	
The second secon	· ·
and the second s	= (274 287 306) mod 26
the second section of the second section of the second section is the second section of the second section of the second section is the second section of the section of the section of the second section of the section of t	god francis Parisine and Parisi
	= (14 1 20)
and the sale producting the sale of the sa	= (nat)
	= (Mat)
The second secon	Cothis was our original plain
The state of the s	text & we decepted.
and the same of th	text & we accepted
Market and the second of the s	
	uf au trigraphs can be encuppted and va some technique.
	why all thoraphs can be encuppted with
Simile	w zee region
1001 Unred	va same technique.
accorpices.	
and the same of th	
. •	
The second received delivered with one one plant the second received the second receiv	
Minimiter dig an exact implicing motivating of executions against Manageric problems and any form the exact implications of the execution of t	
And the second commence of the second commenc	
	the second secon
The state of the s	
Manufactures and the second of the second second second section and a second se	the second secon
Anger a special has been a special has been a special and the	the state of the s
The state of the s	the state of the same and a same which we wished the same and the same
Andrew speciments are an interest and the speciments are the speciments and	
	the state of the s
The second section of the second section of the second section of the second section of	The state of the s
	and the second s
the state of the s	
	and the state of t