MANIPAL INSTITUTE OF TECHNOLOGY
MANIPAL – 576 104, S. INDIA

Chapter 2

Introduction

Original msg → Plaintext

msg through channel → ciphertext

Encryption $C = E_K(P)$

Decryption $P = D_K(C)$

$D_K(E_K(x)) = E_K(D_K(x)) = x$

Proof

$C = E_K(P) \rightarrow (1)$

$P_1 = D_K(C)$

$= D_K(E_K(P)) = P$ [From 1]

Kerchoff Principle

Bob sender

Eve reciever.

1) Eve knows both encryption/decryption
2) Make adversary diffcult to find the key.

Cryptanalysis → science/art of breaking codes.

4 types of attacks

1) ciphertext only → intruder intercepts the

ciphertext and tries to get the plain text by analyzing it.

① Brute force

Exhaustive search tries all possible keys to decode the ciphertext to get plain text

② statistical attack

inherent characteristics of plain text language is exploited

Ex) Most used letter in English is 'e'/'a'
Apply this to the most used ciphertext character & try to decode.

③ Pattern attack

Analyze the pattern to decode.

④ Known Plain text attack

Both plain text and cipher text are analyzed to break next msg from alice to bob. provided the key is not changed.

⑤ chosen cipher text

decrypts a cipher text and tries to recover a key

⑥ chosen plain text

Attacker encrypts the plain text and analyze with the key.

oblems

Unit 2 – symmetric Mathematics

GCD – Euclidean

$gcd(a, b) = gcd(b, r)$; $r \rightarrow$ rem

$gcd(a, 0) = a$

$gcd(25, 60)$

r1	r2	r	
25	60	25	(25 mod 60)
60	25	10	(60 mod 25)
25	10	5	(25 mod 10)
10	5	0	(10 mod 5)
5	0		(a mod 0 = a)
5			

To calculate mod →

60 mod 25 → $\frac{60}{25} = 2.4$

→ Take only decimal ⇒ 2.4 − 2 = 0.4

→ Multiply by divisor

= 10

Extended Euclid

$gcd(161, 28) = s \times a + t \times b$

q	r_1	r_2	r	s_1	s_2	s	t_1	t_2	t
				01	0	1	1	0	1
5	161	28	21	0	1	-1	1	-5	6
1	28	21	7	1	-1	1	-5	6	-23
3	21	7	0	-1	1		6	-23	
	7	0							

Assume $s_1 = 01$ $t_1 = 0$

$s_2 = 0$ $t_2 = 1$

$s \mid t \mid r = r_1 \mid s_1 \mid t_1 - q \times r_2 \mid t_2 \mid s_2$

Always shift $s_2 \rightarrow s_1$, $s \rightarrow s_2$ } at the next iteration

Here $r = 7 = gcd$

$s = -1$

$t = 6$

$s \times a + t \times b$

$-1 \times 161 + 6 \times 28 = 7$

Multiplicative Inverse

$k = 20$ Domain $= 73$

$k^{-1} = 20$

If $gcd(K, D) = gcd(20, 73) = 1$ then K^{-1} is possible

q	r_1	r_2	r
3	73	20	13
1	20	13	7
1	13	7	6
1	7	6	1
6	6	1	0
	1	0	

t_1	t_2	t
0	1	−3
1	−3	4
−3	4	−7
4	−7	11
−7	11	−73
11	−73	

Multiplicative Inverse Exists!!

$t/r = t_1/r_1 - q \times t_2/r_2$

∴ Multiplicative Inverse of Key $= 20$ $= 11$

Additive inverse

① digit 2 domain 26

Ans $26 - 2 = 24 = 2^{-1}$

② -11^{-1} domain 26

$-11 + 26 = 15$

Auto key cipher

$C_i = K_i + P_i \bmod 26$

$P_i = C_i - K_i \bmod 26$

P_t = Hello (7 4 11 11 14)

$K = 13$

Key stream → 13 7 4 11 11 → P_T values

size of P_T

C_T = 20 11 15 22 25

V L P W Z → Different cipher text for repeating text

$P_T = (20 - 13) \bmod 26 = 7$

$(11 - 7) \bmod 26 = 4$

$(15 - 4) \bmod 26 = 11$

$(22 - 11) \bmod 26 = 11$

$(25 - 11) \bmod 26 = 14$

itive cipher

Encryption

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

Decryption

$D = (C - K) \bmod n$

Key 3.

Hello → Plain text

H E L L O
↓ ↓ ↓ ↓ ↓
7 4 11 11 14

Cipher text

Encryption

$(7+3) \bmod 26 = 10 \rightarrow K$
$(4+3) \bmod 26 = 7 \rightarrow h$
$(11+3) \bmod 26 = 14 \rightarrow O$
$(11+3) \bmod 26 = 14 - O$
$(14+3) \bmod 26 = 17 \rightarrow r.$

decryption

$(10-3) \bmod 26 = 7 \quad h$
$(7-3) \bmod 26 = 4 \quad e$
$(14-3) \bmod 26 = 11 \quad l$
$(14-3) \bmod 26 = 11 \quad l$
$(17-3) \bmod 26 = 14 \quad o$

MANIPAL

Playfair

5 x 5

Multiplication cipher

$E(c \times k) \bmod 26$

$D = (c \times k^{-1}) \bmod 26$

He llo → Pt key = 7

↓ ↓ ↓ ↓ ↓

7 4 11 11 14

Encryption

$(7 \times 7) \bmod 26 = 23$ X

$(4 \times 7) \bmod 26 = 2$ C

$(11 \times 07) \bmod 26 = 25$ Z

$(11 \times 07) \bmod 26 = 25$ Z

$(14 \times 7) \bmod 26 = 20$ U

Multiplicative inverse of 7, gcd(7, 26)

q	r_1	r_2	r	t_1	t_2	t
3	26	7	5	0	1	−3
1	7	5	2	1	−3	4
2	5	2	1	−3	4	−11
2	2	1	0	4	−11	26
	1	0		−11	26	

→ doing additive inverse as no. is −ve

$-11 + 26 = 15$

Decryption

$(23 \times 15) \bmod 26 = 7$ H

$(2 \times 15) \bmod 26 = 4$ E

$(25 \times 15) \bmod 26 = 11$ LL

$(20 \times 15) \bmod 26 = 14$ O

MANIPAL INSTITUTE OF TECHNOLOGY

MANIPAL – 576 104, S. INDIA

Playfair cipher

5 x 5 matrix → key matrix

→ Write all letters which are not in key

→ In place of i write i/j (26 letters 25 cells)

→ while encrypting "balloon"

→ Balloon → bal x l ~~o~~ o n

Key → m o n a r

c h y b d

e f g i/j k

l p q s t

u v w x z.

Key → I, both alphabets are same in the key write only once ex brain brown write b r n only once.

Rules for encryption/decryption

→ 2 letters on the same row as secret key replace each by letter on the right in same row. Replace by letter on the left for decryption

→ 2 letters on same column as secret key replace each by letter beneath in same column. Not in same row/colum. Replace by letter above for decryption

→ Not in same row/colum. Replace by letter above encrypted letter is the letter in same row but same column as other letter

"we are discovered"

For decryption letter in the same row but column of other letter

We ar ed is co ve re dx (no pair put x)
↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓
ug rm kc sx hm uf mk bz
(R3) (R1) (R3) (R2) (R1) (R3) (R3) (R3)

Decryption

we ar ed is co ve re dx
(3) (1) (3) (2) (1) (3) (3) (3)

Vigenere Cipher

$C_i = (P_i + K_i) \bmod 26$

$P_i = (C_i - K_i) \bmod 26$

Pascal
15 0 18 2 0 11

s h e is listening
18 7 4 8 18 11 8 18 13 6
15 0 18 2 0 11 15 0 18 04 13 08 13
2 0 11 15 00

C → (15 + 18) mod 26
(70) mod 26
(4 + 18) mod 26
(8 + 2) mod 26
(18 + 0) mod 26
(11 + 11) mod 26
(8 + 15) mod 26
and so on...

E → 7 7 22 10 18 22
h h w k s w
23 18 11 6 13 19
x s l g n t
2 6
c g

Decryption → 7 − 15 mod 26
−8 mod 26
(−8 + 26) mod 26
18 mod 26
18

MANIPAL INSTITUTE OF TECHNOLOGY
MANIPAL – 576 104, S. INDIA

Hill cipher

$$\text{Key} = \begin{bmatrix} 3 & 3 \\ 2 & 5 \end{bmatrix}$$

No. of columns in text = rows of key

HATS
↓ ↓ ↓ ↓
7 0 19 18

Encryption → HA

$$\begin{bmatrix} 3 & 3 \\ 3 & 5 \end{bmatrix}_{2\times 2} \begin{bmatrix} 7 \\ 0 \end{bmatrix}_{2\times 1} = \begin{bmatrix} 3\times 7+3\times 0 \\ 2\times 7+5\times 0 \end{bmatrix}_{2\times 1}$$

$$= \begin{bmatrix} 21 \\ 14 \end{bmatrix} \bmod 26 = \begin{bmatrix} 21 \\ 14 \end{bmatrix}$$

TS

$$\begin{bmatrix} 3 & 3 \\ 2 & 5 \end{bmatrix} \begin{bmatrix} 19 \\ 18 \end{bmatrix} = \begin{bmatrix} 3\times 19+3\times 18 \\ 2\times 19+5\times 18 \end{bmatrix} \bmod 26$$

$$\begin{bmatrix} 111 \\ 128 \end{bmatrix} \bmod 26 = \begin{bmatrix} 7 \\ 24 \end{bmatrix}$$

Cipher → 21 14 7 24

Decryption of Key → Find Inverse of matrix mod 26

$$\begin{bmatrix} d & -b \\ -c & a \end{bmatrix} = \begin{bmatrix} 5 & -3 \\ -2 & 3 \end{bmatrix}$$

$d = ad - bc = 3\times 5 - 3\times 2 = 9$

$9 \times \frac{1}{9} = 1$

$9x \equiv 1 \bmod 26$ Inverse of $9 = 3$

$$3\begin{bmatrix} 5 & -3 \\ -2 & 3 \end{bmatrix} \rightarrow \text{Or} \begin{bmatrix} 15 & -9 \\ -6 & 9 \end{bmatrix}$$

Applying additive inverse

$26-3=23$

$26-2=24$

$$3\begin{bmatrix} 5 & 23 \\ 24 & 3 \end{bmatrix}$$

$$\begin{bmatrix} 15 & 69 \\ 72 & 9 \end{bmatrix} \bmod 26$$

Now apply additive inverse

$$\begin{bmatrix} 15 & 17 \\ 20 & 9 \end{bmatrix} \bmod 26 = \begin{bmatrix} 15 & 17 \\ 20 & 9 \end{bmatrix}$$

$$\begin{bmatrix} 15 & 17 \\ 20 & 9 \end{bmatrix} \rightarrow \text{Decryption key}$$

Decryption of text

$$\underset{2\times 2}{\begin{bmatrix} 15 & 17 \\ 20 & 9 \end{bmatrix}} \underset{2\times 1}{\begin{bmatrix} 21 \\ 14 \end{bmatrix}} = \begin{bmatrix} 21\times 15 + 14\times 17 \\ 20\times 21 + 9\times 14 \end{bmatrix}$$

$$\downarrow$$

$$[VO] = \begin{bmatrix} 553 \\ \vdots \\ 546 \end{bmatrix} \bmod 26$$

$$= \begin{bmatrix} 7 \\ 0 \end{bmatrix} \begin{matrix} H \\ A \end{matrix}$$

HY

$$\begin{bmatrix} 15 & 17 \\ 20 & 9 \end{bmatrix}\begin{bmatrix} 7 \\ 24 \end{bmatrix} = \begin{bmatrix} 7\times 15 + 24\times 17 \\ 20\times 7 + 9\times 24 \end{bmatrix} = \begin{bmatrix} 513 \\ 356 \end{bmatrix} \bmod$$

$$= \begin{bmatrix} 19 \\ 18 \end{bmatrix} \begin{matrix} T \\ S \end{matrix}$$

MANIPAL INSTITUTE OF TECHNOLOGY

MANIPAL – 576 104, S. INDIA

Playfair cipher

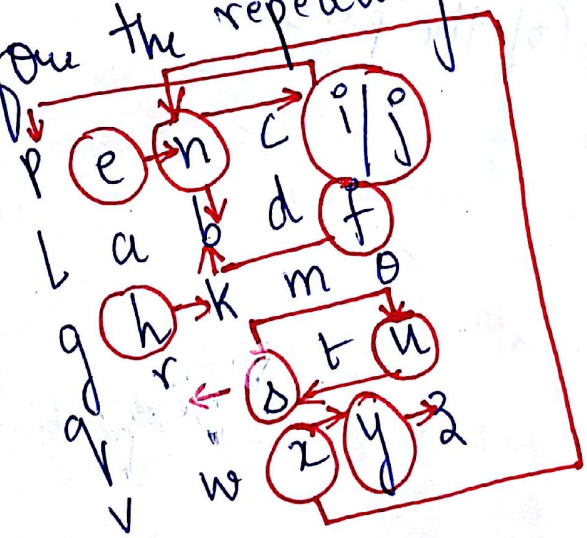
With Repeating letters in key & text

Keyword → Pencil

→ I/J are put into 1 frame
→ Write keyword left to write
→ Donot repeat a character
→ Fill up the rest with the other letters in the alphabet
→ Put i/j in same block. (26 letters 25 words)
→ 6x6 playfair cipher has 0-9 after alphabet.

Plain text → she is funny
Rule Put x before the repeating character

Block → 5x5



Pt → sh ei sf un xn yz → add x as the last letter so that all letters are paired up
↓ ↓ ↓ ↓ ↓ ↓
rk. np ub si nb zy

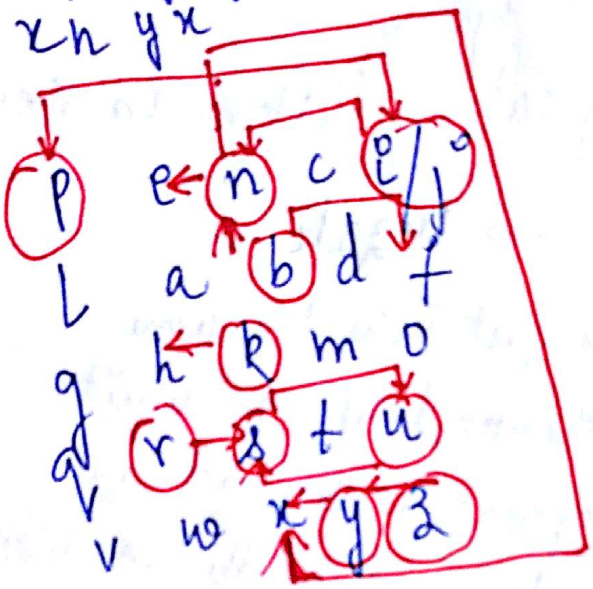
Decryption

rk hp ub si nb ay

↓ ↓ ↓ ↓ ↓ ↓

sh ei of un xh yx

She is funny



Decryption

① Same row → Place the letter on the right

② same column → Place the letter above in column

③ Different row/column

→ letter in same row but column of other letter (of the pair)

MANIPAL INSTITUTE OF TECHNOLOGY
MANIPAL – 576 104, S. INDIA

Transposition Cipher

Keyless → Rail fence

H L O O A E O
E L H W R Y U

Cipher HLLOAEOELHWRYU.

Keyed

Hello how are you

Key 4 5 3 1 2

4	5	3	1	2	
h	e	l	l	o	
h	o	w	a	r	
e	y	o	u	(x)	→ Padding

Now arrange columns according to asunding order of key.

1	2	3	4	5
l	o	l	h	e
a	r	w	h	o
u	x	o	e	y

→ lauorxlwo hheeoy

Scanned by CamScanner

Keyed with alphabet

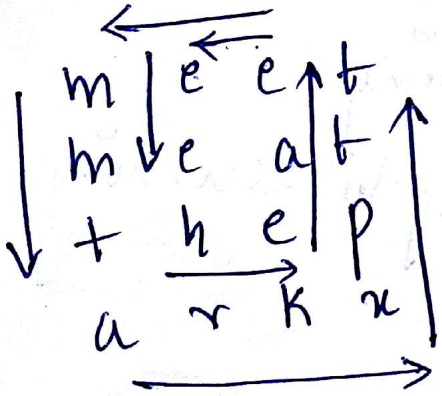
Key — german — no. of columns

text defend the east wall of the castle

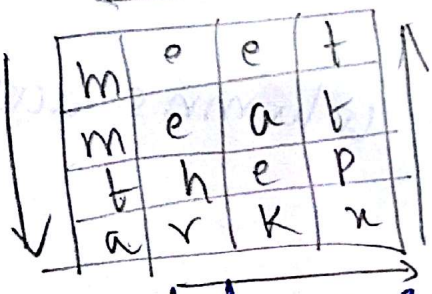
3 2 6 4 1 5
g e r m a n
d e f e n d
t h e e a s
t w a l l o
f t h e c a
s t l e x x

→ nalcxehwtt
dttfseelee
dsoaxfeahl

Route cipher → No. of columns & rows are agreed b/w sender & reciever

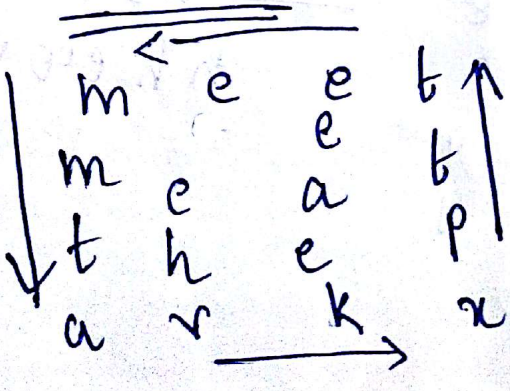


Also the route



arkxpttceemmtheae

Decryption



...ems

...verse

Matrix = $\begin{bmatrix} 2 & -1 & 0 \\ 0 & 1 & 2 \\ 1 & 1 & 0 \end{bmatrix}$

Dt. $= 2(1\times0 - 2\times1) - -1(0\times0 - 2\times1) + 0$
$(0\times1 - 1\times1)$
$= 2(1-2) + 1(0-2) + 0(-1)$
$= -4 - 2 = -6$

Matrix of minors

For 2 → $1\times0 - 2\times1 \Rightarrow -2$
For −1 → $0\times0 - 2\times1 \rightarrow -2$
For 0 → $0\times1 - 1\times1 \rightarrow -1$
For 0 → $-1\times0 - 0\times1 \rightarrow 0$
For 1 → $2\times0 - 0\times1 \rightarrow 0$
For 2 → $2\times1 - -1\times1 \rightarrow 3$
For 1 → $-2 - 0\times1 \rightarrow -2$
For 1 → $2\times2 - 0\times0 \rightarrow 4$
for 0 → $2\times1 - -1\times0 \rightarrow 2$

$\begin{bmatrix} -2 & -2 & -1 \\ 0 & 0 & 3 \\ -2 & 4 & 2 \end{bmatrix} \begin{bmatrix} + & - & + \\ - & + & - \\ + & - & + \end{bmatrix} = \begin{bmatrix} -2 & 2 & -1 \\ 0 & 0 & -3 \\ -2 & -4 & 2 \end{bmatrix}^T$

$\downarrow$

$\begin{bmatrix} -2 & 0 & -2 \\ 2 & 0 & -4 \\ -1 & -3 & 2 \end{bmatrix}$

Inverse of a matrix

$$= \frac{1}{D} \text{ cofactor}$$

$$= \frac{1}{-6} \begin{bmatrix} -2 & 0 & -2 \\ 2 & 0 & -4 \\ -1 & -3 & 2 \end{bmatrix}$$

$$= \begin{bmatrix} 1/3 & 0 & 1/3 \\ -1/3 & 0 & 2/3 \\ 1/6 & 1/2 & -1/3 \end{bmatrix}$$

MANIPAL INSTITUTE OF TECHNOLOGY

MANIPAL – 576 104, S. INDIA

$$K = \begin{bmatrix} 3 & 10 & 20 \\ 20 & 9 & 17 \\ 9 & 4 & 17 \end{bmatrix}$$

Dt $= 3(9\times17 - 17\times4) - 10(20\times17 - 9\times17) + 20(20\times4 - 9\times9)$

$= -1635$ [Range is 26]

$-1635 \bmod 26 = -23 \bmod 26$ [additive inverse]

$= 3$

Inverse

$3 \to 9\times17 - 17\times4$

$10 \to 20\times17 - 9\times17$

$20 \to 20\times4 - 9\times9$

$20 \to 10\times17 - 20\times4$

$9 \to 3\times17 - 20\times9$

$17 \to 3\times4 - 10\times9$

$9 \to 10\times17 - 20\times9$

$4 \to 3\times17 - 20\times20$

$17 \to 3\times9 - 20\times10$

Matrix of Minors

$$\begin{bmatrix} 85 & 187 & -1 \\ 90 & -129 & -78 \\ -10 & -349 & -173 \end{bmatrix} \begin{bmatrix} + & - & + \\ - & + & - \\ + & - & + \end{bmatrix}$$

$$\begin{bmatrix} 85 & -187 & -1 \\ -90 & -129 & +78 \\ -10 & +349 & -173 \end{bmatrix}^T$$

Matrix of cofactors

$$\begin{bmatrix} 85 & -90 & -10 \\ -187 & -129 & 349 \\ -1 & +78 & -173 \end{bmatrix}$$

Adj (key)

$DT^{-1} \times Adj^{\circ}(key) = K^{-1}$

$3^{-1} =$

9	r_1	r_2	r	t_1	t_2	t
	26	3	2	0	1	−8
8				1	−8	9
1	3	2	1	−8	9	−26
	2	2	1	9	−26	
		1	0			

$$9 \times \begin{bmatrix} 85 & -90 & -10 \\ -187 & -129 & 349 \\ -1 & 78 & -173 \end{bmatrix} \bmod 26.$$

$$\begin{bmatrix} 765 & -810 & -90 \\ -1683 & -1161 & 3141 \\ -9 & 702 & -1557 \end{bmatrix} \bmod 26$$

$$\begin{bmatrix} 11 & -4 & -12 \\ -19 & -17 & 21 \\ -9 & 0 & 23 \end{bmatrix} = \begin{bmatrix} 11 & 22 & 14 \\ 7 & 9 & 21 \\ 17 & 0 & 23 \end{bmatrix}$$

Additive Inverse

MANIPAL INSTITUTE OF TECHNOLOGY

MANIPAL – 576 104, S. INDIA

Attix → Attack is tonight

$$\text{Key} = \begin{bmatrix} 3 & 10 & 20 \\ 20 & 9 & 17 \\ 9 & 4 & 17 \end{bmatrix}_{3\times 3}$$

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

Matrices

$$\begin{bmatrix} A & T & T \\ A & C & K \\ I & S & T \\ O & N & I \\ G & H & T \end{bmatrix} = \begin{bmatrix} 0 & 19 & 19 \\ 0 & 2 & 10 \\ 8 & 18 & 19 \\ 14 & 13 & 8 \\ 6 & 7 & 19 \end{bmatrix}$$

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

$$\begin{bmatrix} 0 & 19 & 19 \\ 0 & 2 & 10 \\ 8 & 18 & 19 \\ 14 & 13 & 8 \\ 6 & 7 & 19 \end{bmatrix}_{5\times 3} \times \begin{bmatrix} 3 & 10 & 20 \\ 20 & 9 & 17 \\ 9 & 4 & 17 \end{bmatrix}_{3\times 3} = \begin{bmatrix} 551 & 274 & 646 \\ 230 & 58 & 204 \\ 555 & 318 & 789 \\ 374 & 289 & 637 \\ 329 & 199 & 562 \end{bmatrix} \bmod 26$$

$0\times 3 + 19\times 20 + 19\times 9$

$0\times 10 + 19\times 9 + 19\times 4$

$0\times 20 + 19\times 19 + 19\times 17$

$0\times 3 + 2\times 20 + 10\times 9$

$0\times 10 + 2\times 9 \times 10\times 4$

$0\times 20 + 2\times 17 + 10\times 17$

$8\times 3 + 18\times 20 + 19\times 9$

$8\times 10 + 18\times 9 + 19\times 4$

$8\times 20 + 18\times 17 + 19\times 17$

$14\times 3 + 13\times 20 + 8\times 9$

$14\times 10 + 13\times 9 + 8\times 4$

$14\times 20 + 13\times 17 + 8\times 17$

$6\times 3 + 7\times 20 + 19\times 9$

$6\times 10 + 7\times 9 + 19\times 4$

$6\times 20 + 7\times 17 + 19\times 17$

$$\begin{bmatrix} 5 & 13 & 22 \\ 22 & 6 & 22 \\ 9 & 6 & 9 \\ 10 & 3 & 13 \\ 17 & 17 & 16 \end{bmatrix} \rightarrow \text{Encrypted text}$$

Decryption

$$(C \times K^{-1}) \bmod 26$$

$$\begin{bmatrix} 5 & 13 & 22 \\ 22 & 6 & 22 \\ 9 & 6 & 9 \\ 10 & 3 & 13 \\ 17 & 17 & 16 \end{bmatrix} \times \begin{bmatrix} 11 & 22 & 14 \\ 7 & 9 & 21 \\ 17 & 0 & 23 \end{bmatrix}$$

$$\begin{bmatrix} 0 & 19 & 19 \\ 0 & 2 & 10 \\ 8 & 18 & 19 \\ 14 & 13 & 8 \\ 6 & 7 & 19 \end{bmatrix}$$

MANIPAL INSTITUTE OF TECHNOLOGY

MANIPAL – 576 104, S. INDIA

Route cipher decryption

aes can out rul nnn nee Rlc
fte lnv leg ls with rows of length = 8
No of columns = 10×3 + 2 = 32/4 = 8

Route downwards

	1	2	3	4
1	A	T	E	L
2	E	V	E	V
3	S	V	R	L
4	E	I	L	E
5	A	N	C	R
6	O	N	F	L
7	O	N	T	S
8	I	N	E	

Keyed decryption

nac smt naa aot kep aot bc → key plan

No. of rows = 20/4 = 5

	2	1	3
	l	a	n
1	a t	h	o
2	o h	a	t
3	t a	c	k
4	b a	s	e
5	c a	m	p

Transposition cipher
Rail fence decryption tbpteetokaeheoqr

Key = 3 = row
column = no. of characters in the text

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17
1	t				b				p				t			e
2		e		t		o		k		a		e		h		e
3			x				o				q				r	

Encryption

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17
1	t				b				p				t			e
2		e		t		o		k		a		e		h		e
3			x				o				q				r	

tbpteetokaeheoqr