



Sardar Patel Institute of Technology

Bhavan's Campus, Munshi Nagar, Andheri (West), Mumbai-400058-India
(Autonomous College Affiliated to University of Mumbai)

Mid Semester Examination

Sept 2018

Max. Marks: 20

Class: B.E.

Course Code: CPC702

Name of the Course: Cryptography and System Security

Duration: 1 hr

Semester: VII

Branch: Computer

Instructions:

- (1) All Questions are Compulsory
- (2) Draw neat diagrams
- (3) Assume suitable data if necessary

Q. No.	
Q 1	<p>Marks Distribution: Each Term explained properly ----- 01 mk for each term</p> <p>Confidentiality: Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information. A loss of confidentiality is the unauthorized disclosure of information.</p> <p>Availability: Ensuring timely and reliable access to and use of information. A loss of availability is the disruption of access to or use of information or an information system.</p> <p>Integrity: Guarding against improper information modification or destruction, including ensuring information non-repudiation and authenticity. A loss of integrity is the unauthorized modification or destruction of information.</p>



Sardar Patel Institute of Technology

Bhavan's Campus, Munshi Nagar, Andheri (West), Mumbai-400058-India
(Autonomous College Affiliated to University of Mumbai)

Q2

Marks Distribution: Solved Properly with all steps shown----- 04mks

Key = HILL
PT = CIPHER
CT = ?

→ $\begin{bmatrix} H & I \\ L & L \end{bmatrix}$ 2x2 matrix for Key $\begin{bmatrix} 7 & 8 \\ 11 & 11 \end{bmatrix}$

⇒ In the same manner 2x2 matrix for PT

AGFI IX
CIPH ER

$\begin{bmatrix} H & I \\ L & L \end{bmatrix} \begin{bmatrix} C \\ I \end{bmatrix}$

$\begin{bmatrix} 7 & 8 \\ 11 & 11 \end{bmatrix} \begin{bmatrix} 2 \\ 8 \end{bmatrix} = \begin{pmatrix} 14+64 \\ 22+88 \end{pmatrix} = \begin{bmatrix} 78 \\ 110 \end{bmatrix} \pmod{26}$

$= \begin{bmatrix} 0 \\ 6 \end{bmatrix} \begin{bmatrix} A \\ G \end{bmatrix}$

$110/26 = 4.23076$

$4.23076 - 4 = 0.23076$

$0.23076 \times 26 = 6$

$\begin{bmatrix} H & I \\ L & L \end{bmatrix} \begin{bmatrix} P \\ H \end{bmatrix} \Rightarrow \begin{bmatrix} 7 & 8 \\ 11 & 11 \end{bmatrix} \begin{bmatrix} 15 \\ 7 \end{bmatrix}$

$= \begin{bmatrix} 161 \\ 102 \end{bmatrix} \pmod{26}$

$= \begin{bmatrix} 5 \\ 8 \end{bmatrix} = \begin{bmatrix} F \\ J \end{bmatrix}$

$\begin{bmatrix} H & I \\ L & L \end{bmatrix} \begin{bmatrix} E \\ R \end{bmatrix} = \begin{bmatrix} 7 & 8 \\ 11 & 11 \end{bmatrix} \begin{bmatrix} 4 \\ 17 \end{bmatrix} = \begin{bmatrix} 164 \\ 231 \end{bmatrix} \pmod{26}$

A=0
B=1
C=2
D=3
E=4
F=5
G=6
H=7
I=8
J=9
K=10
L=11
M=12
N=13
O=14
P=15
Q=16
R=17
S=18
T=19
U=20
V=21
W=22
X=23
Y=24
Z=25



Sardar Patel Institute of Technology

Bhavan's Campus, Munshi Nagar, Andheri (West), Mumbai-400058-India
(Autonomous College Affiliated to University of Mumbai)

$$= \begin{bmatrix} 8 \\ 23 \end{bmatrix} = \begin{bmatrix} I \\ X \end{bmatrix}$$

2. Ciphertext = A Q F T I X

OR

Marks Distribution:

Explain Row Transposition cipher----- 02 mks

Problem Solving----- 02mks

Row Transposition Cipher:

A more complex scheme to write the message in a rectangle, row by row, and read the message off, column by column, but it permute the order of the columns. The order of the columns then becomes the key to the algorithm. For example,

Key: 4 3 1 2 5 6 7

Plaintext: a t t a c k p

o s t p o n e

d u n t i l t

w o a m x y z

Ciphertext: TTNAAPTMTSUOAODWCOIXKNLYPETZ

As shown in above example, the key is 4312567. To encrypt, start with the column tha labeled 1, in this case column 3. Write down all the letters in that column. Proceed to column 4, which is labeled 2, then column 2, then column 1, then columns 5, 6, and 7.



Sardar Patel Institute of Technology

Bhavan's Campus, Munshi Nagar, Andheri (West), Mumbai-400058-India
(Autonomous College Affiliated to University of Mumbai)

Problem Solving :

2 P.T. → 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

P.T. → LAUORXLWO HHEEOY

Q3

Marks Distribution:

Expalined RSA Key Generation Algorithm-----02mks
Expalined RSA Encryption Algorithm-----01mks
Expalined RSADecryption Algorithm-----01mks
Solved one example correctly-----02mks

OR

Marks Distribution:

Explained Cipher Block Chaining Mode with diagram-----02mks
Explained Output Feedback Mode with diagram-----02mks
Explained Counter Mode with diagram-----02mks
Explained Cipher Block Chaining Mode without diagram-----01mk
Explained Output Feedback Mode without diagram-----01mk
Explained Counter Mode without diagram-----01mk

Q4

Marks Distribution:

Explained properly DES with Feistel Structure with correct Block Diagram----- 07mks
Explained properly DES with Feistel Structure with incorrect/without Block Diagram---03mks