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 | **Duration: 1 hr**
Class: B.E. | **Semester: VII**
Course Code: CPC702 | **Branch: Computer**
Name of the Course: Cryptography and System Security

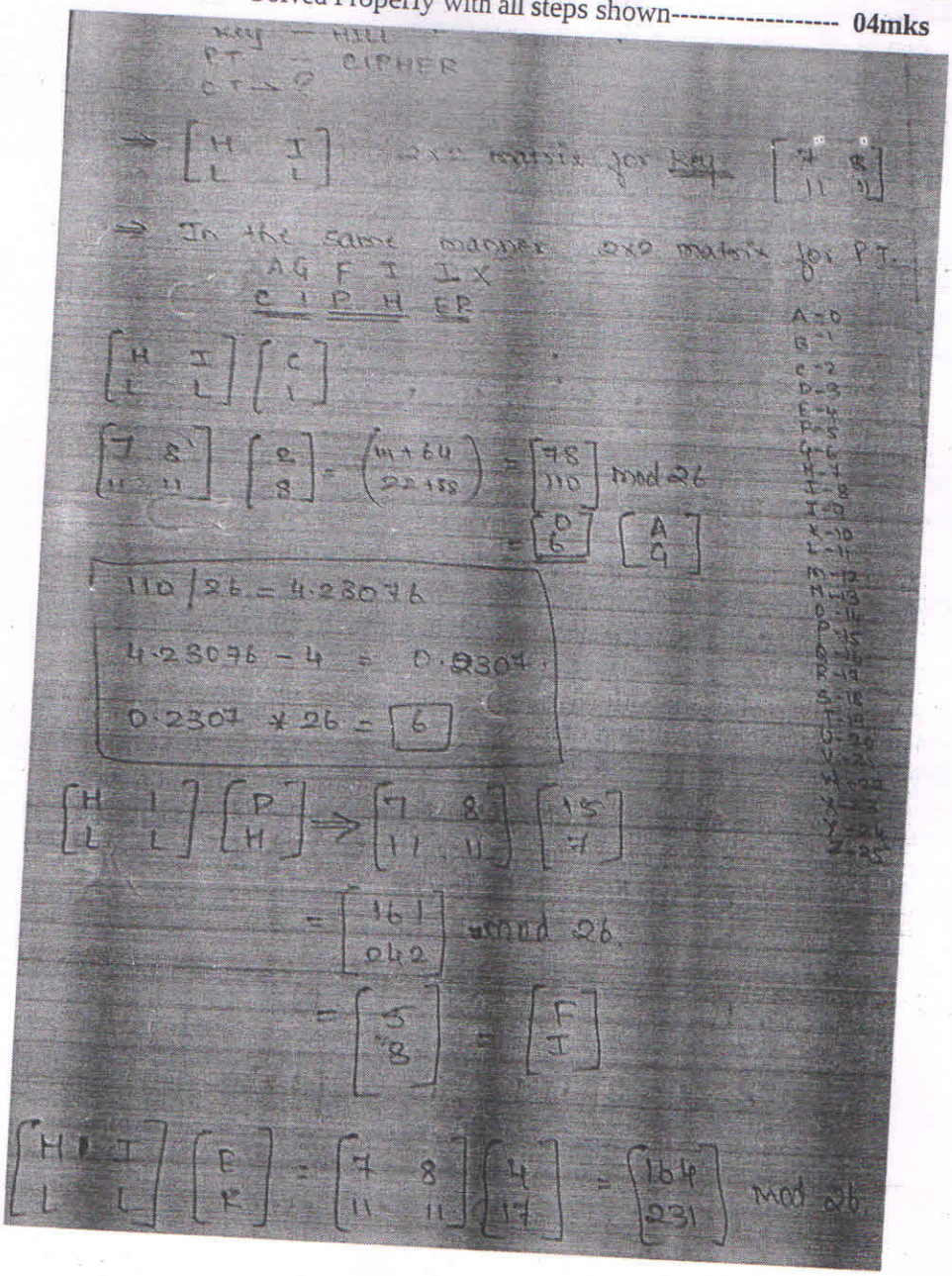
Instructions:

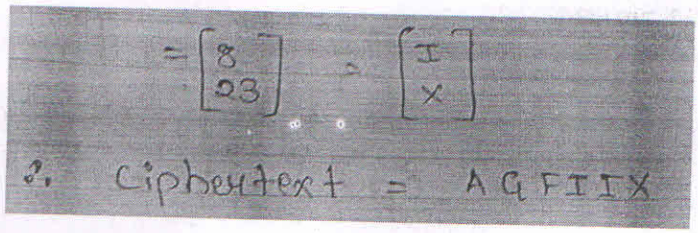
(1) All Questions are Compulsory
(2) Draw neat diagrams
(3) Assume suitable data if necessary

Q. No.	
Q 1	**Marks Distribution:** Each Term explained properly ---------- **01 mk** for each term **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. **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. **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.

Q2

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





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

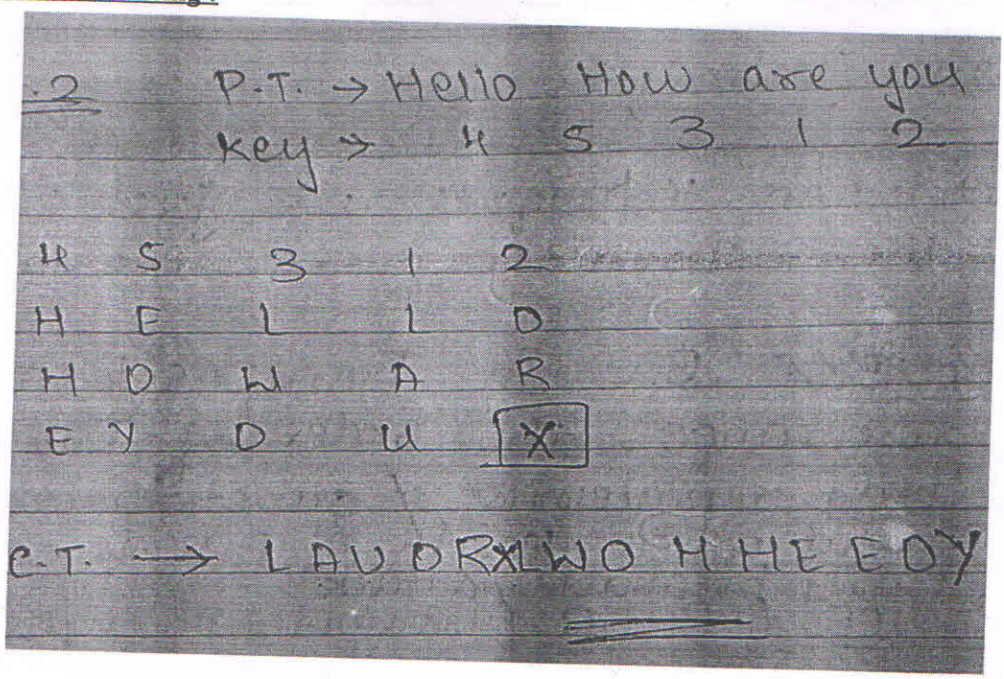
o s t p o n e

d u n t i l t

w o a m x yz

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.

	Problem Solving : 
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**