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

March 2020

Max. Marks: 20
Class: T.E.
Course Code: CE62
Name of the Course: Cryptography and System Security

Duration: 1 hr
Semester: VI
Branch: Computer

Instructions:

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

Q No.		Max. Marks	CO-BL-PI
Q1	What are the three key objectives / goals of computer security. Explain them with diagram.	04	1-1-2.1.3
Q2	State the rules to convert Plain-text to Cipher-text in Play fair Cipher Technique. Encrypt "HELLO" using Play-Fair Cipher technique with keyword "NETWORK". (Assume the Alphabet value starts from 0)	02 03	1-1-2.4.1
Q3	Explain Single Round function of DES algorithm in detail with the help of diagram.	06	2-1-2.1.3
Q4	Find Cipher text for Plaintext =88 using RSA Algorithm, Find public key and secret key. n= 187. Select the lowest number as public key ? OR Find shared secret key using diffie hellman key exchange algorithm for user A and B, P=23 , Q=5, private number of A, i.e Xa=4 and private number of B, i.e Xb=3. Find random numbers and shared key among user A and B ?	05	2-3-2.4.1