



Sardar Patel Institute of Technology

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

End Semester Examination (Make-up)

July ~~May~~ 2019

Max. Marks: 60

Class: T.E.

Course Code: CE62

Name of the Course: Cryptography and System Security

Duration: 3 hr

Semester: ~~IV~~ VI

Branch: Computer

Instructions:

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

Q. No.		Max. Mks	CO
Q1.a.	What are the three key objectives / goals of computer security. Explain them with diagram.	06	CO1
Q1.b.	Explain Symmetric Cipher Model.	06	CO1
Q2.	Explain Diffie Hellman Key Exchange algorithm. Solve one example of it. OR Describe International Data Encryption Algorithm with diagram.	10	CO2
Q3.	Explain how message digest is generated using SHA-512	12	CO3
Q4.	Explain PGP Cryptographic Functions for confidentiality only and both confidentiality and authentication. OR Explain X.509 Certificate Format	06	CO3
Q5.	How do client and sever establish an SSL connection? Explain with diagram.	10	CO4
Q6.	Explain different types of Firewall with diagram. OR Write short notes on: (any two) 1. SSL Protocol Stack 2. PGP 3. SQL Injection	10	CO4