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
Nov 2018

Max. Marks: 60 | **Duration: 3 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.		Max. Mks	CO
Q 1.a)	Describe the difference between Diffusion and Confusion?	05	CO1
Q 1.b)	What are the three key objectives / goals of computer security. Explain them with diagram.	05	CO1
Q 2)	Explain DES Encryption algorithm and Single Round of DES algorithm with the help of diagram. **OR** Describe International Data Encryption Algorithm with diagram.	10	CO2
Q3	Explain HMAC algorithm with structure.	10	CO3
Q4. a)	Explain PGP Cryptographic Functions for authentication only, confidentiality only and both confidentiality and authentication.	05	CO4
Q4. b)	Explain different types of malicious software.	05	CO5
Q5. a)	Explain the different Protocols in SSL. How do client and sever establish an SSL connection	10	CO4
Q5. b)	Explain different DMZ and VPN Firewall configuration and its location. **OR** Write short notes on: (any two) i. Intrusion Detection ii. Multilevel Databases iii. Password Management	10	CO5