Sardar Patel Institute of Technology

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

Re-Examination
July 2019

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
Q1.a	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".	06	CO1
Q1.b	What are the three key objectives / goals of computer security. Explain them with diagram.	06	CO1
Q2.a	Explain RSA Key generation, Encryption and Decryption Algorithm. **OR** With the help of diagram explain the Cipher Feedback Mode block ciphers encryption and decryption.	06	CO2
Q2.b	Explain DES Encryption algorithm and Single Round of DES algorithm with the help of diagram.	12	CO2
Q3	Explain HMAC algorithm with structure.	10	CO3
Q4	Explain ESP Packet Format with diagram. **OR** Explain PGP Cryptographic Functions for authentication only, confidentiality only and both confidentiality and authentication.	10	CO4

Q5	Explain different types of Firewall with diagram.
	OR
	Write short notes on: (any two)
	  i. Intrusion Detection ii. Multilevel Databases
	  iii. Password Management
		10	CO5