# 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~~ Jan-2019

## Make-up Exam

Max. Marks: 60
Class: B.E.
Course Code: CPC702
Name of the Course: Cryptography and System Security

Duration: 3 hr
Semester: IV - VII
Branch: Computer.

**Instructions:**

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

| Q. No. | | Max. Mks | CO |
|---|---|---|---|
| Q 1 (a) | What are block ciphers? Explain the CBC and ECB modes of block ciphers with the help of diagrams | 05 | CO1 |
| Q 1 (b) | What are the Security Attacks? Explain them. | 05 | CO1 |
| Q2 | Illustrate Blowfish algorithm with diagram<br>**OR**<br>Explain Diffie Hellman Key Exchange algorithm. Solve one example of it. | 10 | CO2 |
| Q3 | What are the Digital Signatures? Explain ElGamal Digital Signatures Scheme. | 10 | CO3 |
| Q4 (a) | Describe PKIX Architectural Model and Management Functions and Protocols<br>**OR**<br>Explain ESP Packet Format with diagram | 10 | CO4 |
| Q4 (b) | State and explain the principles differences between version-4 and version-5 of Kerberos with the Message Exchanges | 10 | CO4 |
| Q5 | Explain different types of Firewall with diagram. | 10 | CO5 |