

Code: CS7T3

**IV B.Tech - I Semester – Regular / Supplementary Examinations
JANUARY - 2022**

**INFORMATION SECURITY
(COMPUTER SCIENCE AND ENGINEERING)**

Duration: 3 hours

Max. Marks: 70

PART – A

Answer *all* the questions. All questions carry equal marks

11 x 2 = 22 M

1.

- a) How is Internet security different from Information security?
- b) Define Interception and fabrication.
- c) What is cryptography and cryptology?
- d) Define Ciphertext only and Chosen plaintext attacks.
- e) What is Electronic Code Book (ECB)?
- f) Define key distribution and digital signatures.
- g) What is Kerberos and mention its requirements.
- h) What is IPsec and what are its applications?
- i) Define the requirements of SET protocol.
- j) Mention the need of trusted system.
- k) What is the difference between Keylogger and Logic bomb?

PART – B

Answer any **THREE** questions. All questions carry equal marks.

3 x 16 = 48 M

2. a) Explain in detail about security services and security mechanisms. 8 M
- b) Describe in detail the formation of the Internet draft and explain various Internet standards with a diagram. 8 M
3. a) Explain in detail the Simplified DES scheme. 8 M
- b) What are the steps involved in the MD5 message-digest algorithm? 8 M
4. a) Write about the working of the RSA algorithm with an example. 8 M
- b) Outline the operations of Pretty Good Privacy (PGP). 8 M
5. a) Illustrate IPsec architecture and its services. 8 M
- b) Describe ISAKMP header and payload types in detail. 8 M
6. a) Write about different classes of Intruders and Intrusion detection techniques. 8 M
- b) Discuss in detail the Design goals of the Firewall, and Types of firewalls. 8 M