

Code: CS7T3

**IV B.Tech - I Semester – Regular/Supplementary Examinations  
October - 2018**

**INFORMATION SECURITY  
(COMPUTER SCIENCE & 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) Explain Non-repudiation.
- b) Explain Caesar Cipher encryption.
- c) Define Hash Function.
- d) What is a Digital Certificate?
- e) Define Asymmetric key cryptography.
- f) What is SET?
- g) State the purpose of KDC.
- h) What is PGP?
- i) Define a Trusted System.
- j) What is a Trojan horse?
- k) List the types of intruders.

## PART – B

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

3 x 16 = 48 M

2. a) Explain various security services and mechanisms. 8 M
- b) Illustrate the model for Network Security. 8 M
3. a) Explain Single round of DES algorithm in detail. 8 M
- b) Explain CBC, CFB and OFB Block cipher modes of operation. 8 M
4. a) Let  $p=17$  and  $q=11$ , assume  $e$  as 7. Calculate the public and private keys. Use these keys for encrypting plain text  $M=88$  in RSA. 8 M
- b) State and explain the overview of Kerberos with a neat diagram. 8 M
5. a) Explain IP security architecture in detail. 8 M
- b) Write about TLS. 8 M
6. a) State Firewall Design characteristics and capabilities. 8 M
- b) What is a virus? Explain different types of viruses. 8 M