**PVP 14**

Code: CS7T3

**IV B.Tech - I Semester – Regular Examinations – October - 2017**

# 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

1.

a) Define confidentiality, authentication, availability and non-repudiation.
b) Comment on the strength of DES.
c) What is network security model? Draw a neat diagram of it.
d) Define the terms encryption and decryption.
e) What is HMAC?
f) Define public key and private key cryptography.
g) Briefly explain the importance of Kerberos.
h) What is hand shaking protocol?
i) Define Secure Electronic Transactions.
j) Write about firewall.
k) Define intrusion detection system.

PART – B

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

3 x 16 = 48 M

2. a) Explain various security attacks and Security Mechanisms in detail. 8 M

   b) Explain about internet standards and RFC's. 8 M

3. a) Briefly explain different conventional algorithms. 8 M

   b) Explain about ECB and CFB block cipher modes of operations. 8 M

4. a) What is digital signature? Explain how the public key algorithms' are used for obtaining digital signature. 7 M

   b) Write Deffi-Hellman key Exchange Algorithm with suitable example. 9 M

5. a) Explain web security requirements. 5 M

   b) Explain SSL header. 6 M

   c) Explain differences between SSL and TLS. 5 M

6. a) Write notes on SNMP and list its categories. 8 M

b) What is a virus? Explain different viruses. 8 M