PVP 12

Code: IT6T4

III B.Tech - II Semester – Regular Examinations - May 2015

CRYPTOGRAPHY AND NETWORK SECURITY
(INFORMATION TECHNOLOGY)

Duration: 3 hours Marks: 5x14=70

Answer any FIVE questions. All questions carry equal marks

1 a) What is security attack? Explain the concept of model for network security in detail. 9 M

b) Discuss about categories of Security services. 5 M

2 a) Discuss about ingredients of a symmetric encryption scheme. 6 M

b) How rotor machines functionality is connected to classical encryption techniques? 8 M

3 a) What are the facts that strengthen DES? 5 M

b) Illustrate the essentiality of differential and linear cryptanalysis. 9 M

4 a) Explain Encryption and Authentication concepts with neat diagrams in public key cryptography. 8 M

b) Discuss in detail about first practicable public-key cryptosystem widely used for secure data transmission. 6 M

5 a) How Diffie–Hellman key exchange method is used for exchanging cryptographic keys over a public channel? 7 M

b) Discuss about fast implementation of elliptic curve arithmetic. 7 M

6 What are the Extensions that inform specific usage of a certificate in X.509? Give any two examples for certificate chains and cross-certification. 14 M

7 a) What is pretty good privacy? Discuss about Encryption and Decryption concepts in PGP with neat diagrams. 8 M

b) Discuss about Authentication header and Encapsulated security payload concepts in IP security. 6 M

8 a) Define the term virus and discuss about different types of viruses and related threats. 7 M

b) How the terms system availability and data confidentiality are violated by intruders who attempts to gain unauthorized access to a system? 7 M