PVP 12

Code: IT6T4

III B.Tech - II Semester – Regular Examinations – April 2016

CRYPTOGRAPHY AND NETWORK SECURITY

(INFORMATION TECHNOLOGY)

Duration: 3 hours Max. Marks: 70

Answer any FIVE questions. All questions carry equal marks

1.

a) List the different types of attacks. Explain. 7 M

b) Give a model for network security and explain. 7 M

2.

a) Explain different substitution techniques. 8 M

b) Give a model for symmetric crypto system and explain. 6 M

3.

a) Explain in detail about single round of DES algorithm. 8 M

b) Briefly explain the design principles of block cipher. 6 M

4.

a) Write the characteristics of public key cryptography and explain RSA algorithm. 8 M

b) Explain about public key encryption and decryption with neat diagrams. 6 M

5.

a) Explain about Elliptic curve crypto system. 7 M

b) Users A and B uses diffie-hellman key exchange protocol with a common prime q=71 and a primitive root $\propto$=7. If user A has private key Xa=5, and B has a private key Xb=6 then find the common shared key for A and B. 7 M

6.

a) Explain user authentication with symmetric key crypto system. 6 M

b) Give an over view of kerberos authentication service with a neat diagram. 8 M

7.

a) Explain Pretty Good Privacy (PGP) cryptographic functions with suitable diagrams. How confidentiality and authentication have been achieved simultaneously in PGP? 8 M

b) Explain about IPv4 header format using ESP authentication and encryption. 6 M

8. Explain briefly the following: 14 M

a) Trusted systems.

b) Intrusion detection systems.