[07 – 4221]

IV/IV B.Tech. DEGREE EXAMINATION.

Second Semester

Computer Science and Engineering

CRYPTOGRAPHY AND NETWORK SECURITY

(Common with Information Technology)

(Effective from the admitted batch of 2006–2007)

Time : Three hours Maximum : 70 marks

Question No. 1 is compulsory.

Answer any FOUR from the remaining.

All questions carry equal marks.

Answer All part of any questions at one place.

1. (a) What is a transposition cipher?

(b) How do you differentiate diffusion and confusion?

(c) What is the purpose of state array?

(d) What do you mean by traffic padding?

(e) What is trusted system?

(f) What is the purpose of the X.509 standard?

(g) What is a replay attack?

2. (a) Explain the importance of the Fiestel cipher.

   (b) Explain the differences between block cipher and stream cipher.

3. (a) In AES, how the encryption key is expanded to produce keys for 10 rounds.

   (b) Write pseudo code for implementing BLOWFISH algorithm.

4. (a) Explain digital signature algorithm.

   (b) Explain how birthday attack is done.

5. (a) Discuss about XML security concepts.

   (b) Explain about private key management.

6. (a) Discuss about SET-3D secure protocol.

   (b) Describe wireless application protocol security.

7. (a) What is password based encryption? What are the problems associated with it?

   (b) Explain how the security is provided by UNIX operating system.

8. (a) Write the characteristics of a good firewall implementation.

   (b) Discuss about secure inter-branch payment transactions.