[07 – 4221]

IV/IV B.Tech. DEGREE EXAMINATION.

Second Semester

Computer Science and Engineering

CRYPTOGRAPHY AND NETWORK SECURITY

(Effective from the Admitted Batch of 2006–2007)

Time : Three hours Maximum : 70 marks

Answer to question No.1 is compulsory

Answer any FOUR from the remaining.

All questions carry equal marks.

Answer all parts of any question at one place.

1. (a) What is Caesar cipher?

   (b) What do you mean by diffusion?

   (c) What is triple encryption?

   (d) What is one-way function?

   (e) What is message authentication code?

   (f) What is electronic money?

   (g) What is an application-level gateway?

2. (a) What do you mean by security? Write about principles of security.

   (b) Explain the generation of subkey and S-Box from the given 32 bits key by Blowfish.

3. (a) Explain in detail a traffic analysis attack.

   (b) Explain the blowfish algorithm.

4. Describe RSA algorithm with an example.

5. (a) Discuss how signing and verification is done using DSS.

   (b) Explain knapsack algorithm.

6. (a) Write about private key management.

   (b) Explain XML security concepts.

7. (a) Write about wireless application protocol security.

   (b) Discuss about biometric authentication.

8. (a) Explain in detail about Java cryptography architecture.

   (b) What are the characteristics of good firewall implementation?
