AR – 651

Fifth Semester B. C. A. (Part – III) Examination

NETWORK SECURITY

Paper – 5 ST 2

P. Pages : 3

Time : Three Hours] [Max. Marks : 60

Note : (1) All questions are compulsory.
(2) All questions carry equal marks.

1. (a) What is active and passive attacks ? Explain with its security threats. 6

   (b) Explain transposition techniques in detail. 6

OR

2. (a) Explain substitution cipher and transposition cipher and write difference between them. 12

3. (a) Explain Advanced Encryption Standard AES cipher. 6

   (b) Discuss the operation of Data Encryption Standard. (DES) 6

OR

4. (a) Explain strength of Data Encryption Standard (DES). 6

   (b) Explain the Cipher Block Chaining Mode. 6

5. (a) Explain the Fermat's theorem. 6

   (b) Describe the divisibility and the division algorithm. 6

OR

6. (a) Discuss Moduler Arithmetic Operation. 6

   (b) Explain testing for primarility. 6

7. (a) Explain one way hash function. 6

   (b) What is Digital signature ? Explain. 6

OR

8. (a) Differentiate between conventional and public key encryption. 6

   (b) What is role of Kerberos during secure communication ? Explain. 6

9. (a) Explain following :—

   (1) Intruders

   (2) Viruses

   (3) Firewalls. 6

   (b) Explain pretty good privacy in E–mail security. 6

OR

10. (a) Explain various services provided by IP security. 6

    (b) Compare between PGP and S/MIME. 6