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

NETWORK SECURITY

Paper–5 ST 2

Time : Three Hours] [Maximum Marks : 60

N.B. :– (1) **ALL** questions are compulsory.

(2) All questions carry equal marks.

1. (a) Explain the model for Network Security. 6
   (b) What is Monoalphabetic Cipher ? Explain with example. 6

OR

2. (a) Explain Security Mechanism. 6
   (b) Explain Symmetric Cipher Model. 6
3. (a) Explain the DES encryption algorithm. 6
   (b) What are the stream cipher and block cipher ? 6

OR

4. Explain Advanced Encryption Standard in detail. 12
5. (a) State and prove the Euler's theorem. 6
   (b) Describe the divisibility and division algorithm. 6

OR

6. (a) Explain modular arithmetic operations with example. 6
   (b) Explain Fermat's theorem. 6
7. (a) Explain one-way Hash function with example. 6
   (b) Distinguish between conventional and public key encryption. 6

OR

8. Explain the RSA public key encryption algorithm with example. 12
9. (a) Discuss Transport Layer Security. 6
   (b) What is PGP ? State and explain any three principle services provided by PGP. 6

OR

10. (a) Describe the services of firewall. 6
    (b) What is Intruder ? Explain. 6