B.C.A. Part—III (Semester—V) Examination
NETWORK SECURITY
Paper—5ST2

Time : Three Hours]   [Maximum Marks : 60

Note :— (1) **ALL** questions are compulsory.

(2) All questions carry equal marks.

1. (a) What are the essential ingredients of Symmetric Cipher ? Explain with diagram. 6

   (b) Explain Model for Network Security in brief. 6

OR

2. (a) Explain the module for Network Security. 6

   (b) Explain the Symmetric Cipher Model. 6

3. (a) Explain Cipher Block Chaining. 6

   (b) Describe the concept of Block Cipher and Stream Cipher. 6

OR

4. (a) Explain the parameters and design choices that determine the actual algorithm of Feistal Cipher. 6

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

5. (a) Discuss Modular Arithmetic Operation. 6

   (b) State and prove Euler's Theorem. 6

OR

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

   (b) Explain the following terms :—

   (1) Group

   (2) Ring

   (3) Field. 6

7. (a) Explain RSA Public Key Encryption Algorithm. 6

   (b) What are the principal elements of Public-key Crypto System ? 6

OR

8. (a) Explain Public Key Cryptography with suitable diagram. 6

   (b) Write importance of Digital Signature. 6

9. (a) Give examples of application of IP Security. 3

   (b) What are Firewalls ? Explain. 3

   (c) What are MIME and S/MIME ? Explain. 6

OR

10. (a) Explain Transport Layer Security. 6

    (b) Explain pretty good Privacy in e-mail security. 6