

AU-207

**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) List and explain the categories of security services. 6
- (b) Explain model for Network Security in brief. 6

**OR**

2. (a) What is stenography ? Explain. 6
- (b) Explain symmetric cipher model of encryption. 6
3. (a) Explain DES encryption algorithm. 6
- (b) What is product cipher ? Explain. 3
- (c) What is avalanche effect ? Explain. 3

**OR**

4. (a) Explain structure of classical Feistel Network. 6
- (b) Explain Advanced Encryption Standard (AES) cipher. 6
5. (a) Explain Euclidean Algorithm. 6
- (b) Describe divisibility and division algorithm. 6

**OR**

6. (a) Explain the following terms :
  - (i) Group
  - (ii) Ring
  - (iii) Field. 6
- (b) State and prove Fermal's Theorem. 6

7. (a) Explain RSA public key encryption algorithm. 6  
(b) Explain properties of Hash function. 6

OR

8. (a) Explain public key cryptography with suitable diagram. 6  
(b) Explain need of Digital Signature and Kerberos. 6
9. (a) What is PGP ? State and explain services provided by PGP. 6  
(b) What are MIME and S/MIME ? Explain in brief. 6

OR

10. (a) Give examples of application of IP security. 3  
(b) State the services that are provided by IP security. 3  
(c) What parameters identify security association ? 3  
(d) What are Firewalls ? Explain. 3