AT–446

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) Explain security mechanism. 6

(b) Explain active and passive attacks with its security threats. 6

OR

2. (a) Explain OSI security architecture. 6

(b) Explain transposition technique of Encryption. 6

3. (a) Explain cipher block chaining. 6

(b) Explain the operation of DES. 6

OR

4. (a) Describe the concept of block cipher and stream cipher. 6

(b) Explain the concept of diffusion and confusion. 6

5. (a) What is testing of primality ? 3

(b) What is Euclidean algorithm ? 3

(c) Define and explain with an example of modular arithmetic. 6

OR

6. (a) Write any three differences between index and discrete algorithm. 3

(b) What is prime number ? Explain. 3

(c) State and prove Euler's theorem. 6

7. (a) What characteristics are needed in secure hash function ? 6

(b) Differentiate between conventional and public key encryption. 6

OR

8. (a) What is need of message authentication ? Explain message authentication code in brief. 6

(b) Write importance and properties of digital signature. 6

9. (a) Explain transport layer security. 6

(b) Explain various services provided by IP security. 6

OR

10. (a) Explain the following terms :

(1) Firewall

(2) Viruses

(3) Threats. 6

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