

AL - 539

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 question carry equal marks.

1. (a) What do you understand by Active and passive attacks ? Explain with its security threats.

6

- (b) List and explain the categories of security services.

6

OR

2. (a) Explain transposition technique of encryption.

6

- (b) What is steganography ? Explain.

6

3. (a) Explain the difference between differential and linear cryptanalysis.

6

AL - 539

P.T.O.

- (b) Describe the concept of block cipher and stream cipher. 6

OR

4. (a) Explain the concept of diffusion and confusion. 6
- (b) What is reversible and irreversible mapping in feistel cipher structure? 6

5. (a) What is testing for primality? 3
- (b) What is Euler's totient function? 3
- (c) Define and explain with an example the modular arithmetic. 6

OR

6. (a) What is the difference between an index and a discrete logarithm? 3
- (b) What is a prime number? 3
- (c) State and prove Euler's theorem. 6

7. State the principles of Public key cryptosystem. Explain its important characteristics with suitable diagram. 12

OR

8. (a) What characteristics are needed in a secure hash function? 6
- (b) Differentiate between conventional and public key encryption. 6
9. What is IP security? State its principle features and explain an IP security scenario with some of the benefits of IP sec. 12

OR

10. (a) Give examples of applications of IP sec. 3
- (b) State the services that are provided by IP sec. 3
- (c) What parameters identify a security Association (SA)? 3
- (d) What are firewalls? 3

