CRYPTOGRAPHY AND NETWORK SECURITY

(Code : CST-603)

Full Marks : 70

Time : 3 hours

Answer any five questions

Figures in the right-hand margin indicate marks

1. (a) Differentiate between plain text and cipher text. 2

   (b) Explain the working principle of RSA algorithm through an example. 5

   (c) Explain the different types of attacks that may occur in the field of computer networking. 7

2. (a) What is a digital envelope ? 2

   (b) Explain the various types of data encryption standards. 5

(c) Explain the various symmetric key algorithm types used in the field of cryptography and network security. 7

3. (a) Explain the following terms used in cryptography and network security : 2

   (i) Authentication

   (ii) Integrity

   (iii) Confidentiality

   (iv) Non-repudiation.

   (b) Differentiate between symmetric key cryptography and asymmetric key cryptography. 5

   (c) Explain the various types of transposition technique in cryptography. 7

4. (a) What is data Encryption ? 2

   (b) Explain certificate based authentication and Biometrics based authentication used for user authentication. 5

   (c) What is TCP/IP ? Explain the function of each layer in TCP/IP suite. 7

(3)

5. (a) What is the role of SHTTP in cryptography ? 2

(b) What is VPN ? Explain its working principle in the field of network security. 5

(c) Explain the PKIX model in detail. 7

6. (a) What is firewall ? 2

(b) What is digital certificate and write different steps used in obtaining a digital certificate ? 5

(c) Explain the various types of substitution techniques used in cryptography. 7

7. Write short notes on the following (any *four*) : $3\frac{1}{2} \times 4$

(i) IP security

(ii) Authentication Basics

(iii) SSL

(iv) Principles of security

(v) Digital signature

(vi) Authentication Tokens.

———