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*) Distinguish between Plain text and Cipher text with example. 2

(*b*) Write the compression between Symmetric and Asymmetric key cryptography. 5

(*c*) What do you mean by Secure Electronic Transaction ? Explain the Set process. 7

2. (*a*) Name various types of attack on computer system. 2

(*b*) Explain Digital Certificate. What are certificate creations procedures ? 5

(*c*) Explain the RSA algorithm. Describe the example of RSA. 7

3. (*a*) Define Smart Card. 2

(*b*) Describe Biometric Authentication. 5

(*c*) Define Authentication Tokens. How does this works ? Explain its type. 7

4. (*a*) Define IP security. 2

(*b*) Write the compression between Symmetric and Asymmetric key cryptography. 5

(*c*) Describe Substitution Technique and transposition technique. 7

5. (*a*) Define time stamping protocol. 2

(*b*) Explain private key management. 5

(*c*) What do you mean by DES ? Explain how DES works ? 7

6. (*a*) Distinguish between Encryption and Decryption. 2

(*b*) What are different principles of Security explain with example. 5

(*c*) Explain Virtual Private Network. Describe VPN Architecture. 7

7. (*a*) Define Password. What do you mean by Plain Text password ? 2

(*b*) Describe the position of SSL in TCP/IP protocol suite with Diagram. 5

(*c*) Write short notes on any *two* : $3\frac{1}{2} \times 2$

(*i*) TCP/IP

(*ii*) Certificate-based Authentication

(*iii*) Firewall

(*iv*) Digital Signature.
