



C14-CM-606/C14-IT-606

4734

BOARD DIPLOMA EXAMINATION, (C-14)
MARCH/APRIL—2017
DCME—SIXTH SEMESTER EXAMINATION
CRYPTOGRAPHY AND NETWORK SECURITY

Time : 3 hours]

[*Total Marks* : 80

PART—A

3×10=30

Instructions : (1) Answer **all** questions.
(2) Each question carries **three** marks.
(3) Answers should be brief and straight to the point and shall not exceed *five* simple sentences.

1. What is security attack?
2. Write about the main goals of cryptography.
3. Define encryption and decryption.
4. What is meant by ciphertext-only attack?
5. Write the differences between monoalphabetic and polyalphabetic cipher.
6. What is the role of public and private key?
7. List the digital signature requirements.
8. Define virus and worm.
9. List the types of Malicious software.
10. List the types of firewall.

*

PART—B

10×5=50

- Instructions :** (1) Answer *any five* questions.
(2) Each question carries **ten** marks.
(3) Answers should be comprehensive and the criterion for valuation is the content but not the length of the answer.

- 11.** Explain the following : 10
(a) Data confidentiality
(b) Integrity
(c) Masquerade
(d) Denial of service
- 12.** (a) Draw the model for network security. Explain. 5
(b) Decrypt the following text by using caesar cipher. Assume the key value $k=4$:
“STATE BOARD OF TECHNICAL EDUCATION” 5
- 13.** Explain the concept of hill cipher with an example. 10
- 14.** Explain the transposition cipher with an example. 10
- 15.** Write about the concept of digital signature and also write its properties. 10
- 16.** Describe the procedure of message authentication and its requirements. 10
- 17.** Explain about various anti-virus approaches and anti-virus techniques. 10
- 18.** (a) Define firewall. Discuss about firewall characteristics. 5
(b) Explain digital rights management. 5
