C14–CM–606/C14–IT–**606**

4734

BOARD DIPLOMA EXAMINATION, (C–14)
OCT/NOV—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. Define security and network security.

2. List the categories of security services.

3. Define decryption.

4. List the ingredients of a symmetric cipher.

5. Define transposition cipher.

6. List the message authentication functions.

7. List the applications of cryptographic Hash function.

8. Define virus and worms.

9. List any three Malicious softwares.

10. Define firewall.

<div align="center">

PART—B 10×5=50

</div>

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 categories of passive and active attacks.

12. *(a)* Explain about authentication and confidentiality. 5

(b) Differences between mono and polyalphabetic ciphers. 5

13. *(a)* Explain functions used in encryption algorithm. 5

(b) Explain steganography. 5

14. Explain hill cipher with example.

15. Explain about message authentication.

16. Define digital signature and explain the properties of digital signature. 2+8=10

17. Explain about propagation of worm.

18. Explain about computer crime and cyber crime. 10

<div align="center">

★ ★ ★

</div>