Roll No. ....   Total Pages : 3

INFORMATION SECURITY

Paper : MCA-14-45(I)

Time : Three Hours]   [Maximum Marks : 80

Note : Attempt *five* questions in all. Question No. 1 is compulsory. Attempt *four* more questions, selecting *one* question from each unit.

Compulsory Question

1. Answer the following in short :

    (a) What do you mean by Programming bug?

    (b) List the different types of attacks.

    (c) What do you mean by Cryptography?

    (d) Write a brief note on Digital signature.

    (e) Differentiate between Tunnel mode and Transport mode of IPSec.

    (f) Discuss Packet sniffing.

    (g) What are Trusted systems?

    (h) What do you mean by Firewalls?   (2×8=16)

UNIT–I

2. (a) What are the goals of security? Discuss security threats and vulnerabilities.

(b) How you will identify that a password is weak/strong? Explain Password cracking. (8×2=16)

3. Explain Wireless network security model and the important parameters associated with it. Highlight the security issues in Wireless. 16

UNIT–II

4. What are the characteristics of a good Encryption system? Discuss Encryption techniques in detail. 16

5. (a) Define Hashing function? What are the properties of hashing function in cryptography?

   (b) Explain International data encryption algorithm. (8×2=16)

UNIT–III

6. Write the authentication dialogue exchanged between a user and authentication server in Kerberos V4. 16

7. (a) What protocols comprise SSL? Explain about SSL Handshake protocol.

   (b) Elaborate Internet security. How threat to this security is prevented? (8×2=16)

UNIT–IV

8. (a) Explain about the trust mechanism and certificates used by PGP and S/MIME.

   (b) Discuss Electronic payment protocols in detail.

   (8×2=16)

9. Distinguish between Virus and Threats. What are the different types of viruses? Discuss the counter measures for virus infection.   16

———————