Reg. No. : | | | | | | | | | | | | |

Question Paper Code : 45907

5 Year M.Sc. DEGREE EXAMINATION, NOVEMBER/DECEMBER 2014.

Nineth Semester

Software Engineering

XCS 593/10677 SW 903 — NETWORK SECURITY

(Common to 5 Year M.Sc. Computer Technology and M.Sc. Information Technology)

(Regulation 2003/2010)

Time : Three hours Maximum : 100 marks

Answer ALL questions.

PART A — (10 × 2 = 20 marks)

1. Differentiate between worms and viruses.
2. What is the use of a hash function in network security?
3. What is the use of modulo-2 arithmetic?
4. What is a zero knowledge proof system?
5. Define the role of trusted systems.
6. State any four rules for setting a secure password.
7. What is KDC?
8. What is the use of authentication header?
9. Define the term non repudiation.
10. What is cookie?

PART B — (5 × 16 = 80 marks)

11. (a) (i) Discuss the multi level model for security. (12)

(ii) How do you ensure authentication and confidentiality using public key cryptography? (4)

Or

(b) (i) Explain the working mechanism of IDEA. (8)

(ii) Explain the working mechanism of DES. (8)

12. (a) State and explain the steps involved in RSA encryption with an example. (16)

Or

(b) Explain the DSS algorithm along with the working and verification procedure. (16)

13. (a) Discuss the following :

(i) Password based authentication (8)

(ii) Password as cryptographic keys. (8)

Or

(b) Discuss the following :

(i) Initial password distribution (8)

(ii) Authentication tokens. (8)

14. (a) Explain the steps involved in kerberos authentication system. (16)

Or

(b) (i) Differentiate IPv4 and IPv6.

(ii) Explain about Encapsulated Security Payload.

15. (a) (i) Discuss about E-mail security. (10)

(ii) Discuss about distribution list. (6)

Or

(b) (i) Explain about packet filtering firewall. (8)

(ii) Explain about DBOS attach. (8)
