LDB
31/12/15 FN

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

Question Paper Code : 95614

5 Year M.Sc. DEGREE EXAMINATION, NOVEMBER/DECEMBER 2015.

Nineth Semester

Software Engineering

ESE 093 — NETWORK SECURITY

(Regulations 2010)

Time : Three hours Maximum : 100 marks

Answer ALL questions.

PART A — (10 × 2 = 20 marks)

1. Give the use of Secret Key Cryptography.

2. What do you mean by computation resistance in terms of MAC?

3. What is Zero Knowledge proof system?

4. Define PKCS.

5. Define authentication and list any two authentication protocol.

6. Define Eavesdropping.

7. Give the uses of ESP.

8. Draw the format of the IPv4 header.

9. What is store and forward in security?

10. List down any four cookies rules.

PART B — (5 × 16 = 80 marks)

11. (a) Describe the Data Encryption Standard (DES) algorithm with a neat block diagram. (16)

Or

(b) How IDEA is used for encryption/decryption? Discuss with an example. (16)

12. (a) Explain the RSA algorithm in detail. Also perform encryption and decryption using RSA algorithm for the given values : p = 3, q = 11, e = 7, m = 5. (16)

Or

(b) Describe the steps in Digital Signature Standard (DSS) Algorithm and write the working principle and verification procedure in DSS. (16)

13. (a) Explain the various cryptographic authentication protocols in details. (16)

Or

(b) (i) Discuss in detail about session key establishment. (8)

(ii) Write notes on Authentication Tokens. (8)

14. (a) Discuss in detail about Kerberos System. (16)

Or

(b) (i) Explain Tickets and Ticket Granting Tickets. (8)

(ii) Discuss IPV6 Authentication Header in detail. (8)

15. (a) (i) Explain the security services for Electronic Mail. (8)

(ii) Write notes on Non Repudiation. (8)

Or

(b) Discuss the different types of firewall with an example for each. (16)