LIB
19/12/15 FN

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

Question Paper Code : 95417

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

Ninth Semester

Software Engineering

XCS 593/10677 SW 903 – NETWORK SECURITY

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

(Regulations 2003/2010)

Time : Three hours Maximum : 100 marks

Answer ALL questions.

PART A — (10 × 2 = 20 marks)

1. List some of the network vehicles through which a network worm replicates.
2. What are the advantages of CTR mode in block cipher?
3. State Fermat's theorem.
4. Why is RSA secure?
5. List some password selection strategies.
6. What are authentication tokens?
7. What is Euler's function?
8. What is the difference between MAC and message digest?
9. What is the role of cookies in web security?
10. Define Denial of Service (DOS) attack.

PART B — (5 × 16 = 80 marks)

11. (a) Explain the steps involved in IDEA to encrypt a 64-bit block of plain text.

Or

(b) Explain the various modes of operations used to encrypt a message larger than 64 bits.

12. (a) (i) Develop the Euclidean Algorithm to find the GCD of two positive integers and find GCD (1970, 1066), using the developed algorithm. (8)

(ii) Discuss the simple countermeasures that can be provided to timing attack. (8)

Or

(b) (i) Explain the arbitrated digital signature and how is it beneficial when compared to direct digital signature. (8)

(ii) Describe the roles of discrete logarithms in cryptography. (8)

13. (a) (i) Discuss the authentication tokens with examples. (10)

(ii) List the advantages of Certification Authority (CA) over KDC. (6)

Or

(b) (i) Discuss multiple trusted intermediaries. (10)

(ii) List the problems in using passwords for authentication. (6)

14. (a) Discuss the Kerberos authentication services.

Or

(b) Explain the IP Security architecture.

15. (a) (i) Explain the threats in network. Also discuss network vulnerabilities. (8)

(ii) Discuss the security services for Email. (8)

Or

(b) Discuss the various approaches to intrusion detection. (16)

———————