LIB
16/12/13 FN

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

Question Paper Code : 75565

5 Year M.Sc. DEGREE EXAMINATION, NOVEMBER/DECEMBER 2013.

Nineth Semester

Computer Technology

XCS 593 — NETWORK SECURITY

(Common to 5 Year M.Sc. Software Engineering/ M.Sc. Information Technology)

(Regulation 2003)

Time : Three hours Maximum : 100 marks

Answer ALL questions.

PART A — (10 × 2 = 20 marks)

1. What is a worm? What is the difference between a worm and a virus?
2. What is Avalanche Effect?
3. Differentiate between weak and strong collision resistance.
4. Why ECC is considered to be better than RSA?
5. How does a server know user's password?
6. What are the common techniques used to protect a password file?
7. What is IP address spoofing?
8. Why does an ESP include a padding field?
9. What is a DoS attack?
10. What are honey pots?

PART B — (5 × 16 = 80 marks)

11. (a) Briefly explain the DES algorithm. (16)

Or

(b) (i) Discuss the differences between conventional and Public-key encryption. (8)

(ii) Discuss with diagram the OFB and CFB Block cipher modes of operation. (8)

12. (a) (i) List the requirements that public key cryptosystems should fulfill to be a secure algorithm? (6)

(ii) Explain the Digital Signature algorithm with the functions of signing and verifying. (10)

Or

(b) (i) Perform the encryption and decryption using RSA algorithm for the following: (8)

(1). $p = 17; q = 11; e = 7; M = 88$

(2) $p = 17: q = 31; e = 7; M = 2$

(ii) Describe the possible approaches to attack the RSA algorithm. (8)

13. (a) Briefly explain the Address-Based Authentication. (16)

Or

(b) (i) Discuss the need for authentication protocols to establish a session key during authentication. (8)

(ii) How does key distribution work with multiple KDC domains? (8)

14. (a) Explain how the Kerberos provide a mechanism for supporting Interrealm authentication. (16)

Or

(b) Explain the Transport and Tunnel Mode operations in IPSec with IP diagram. (16)

15. (a) (i) What type of firewall is used when system administrator trusts internal users? (6)

(ii) Discuss the difference between a packet filter and an application level gateway. (6)

(iii) Explain HTTP Digest Authentication. (4)

Or

(b) (i) List the different security services needed for an Electronic Mail. (8)

(ii) How will you track users based on Cookies? (8)

———————