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

Question Paper Code : Z 9361

5 Year M.Sc. DEGREE EXAMINATION, NOVEMBER/DECEMBER 2009.

Ninth Semester

Computer Technology

XCS 593 — NETWORK SECURITY

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

(Regulation 2003)

Time : Three hours Maximum : 100 marks

Answer ALL questions.

PART A — (10 × 2 = 20 marks)

1. What are the key principles of security?

2. What are replay attacks? Give an example.

3. What would be the transformation of a message "Wish you a happy birthday" using Rail Fence technique?

4. Define nounce and its use in entity authentication

5. What is a worm? What is the difference between a worm and a virus?

6. What are honeypots?

7. What is Euler's function?

8. What is the difference between MAC and message digest?

9. What is NAT?

10. How is secret key different from a private key?

PART B — (5 × 16 = 80 marks)

11. (a) (i) Discuss the various Block cipher modes of operation. (8)

(ii) Explain the single round of DES Algorithm with diagram. (8)

Or

(b) (i) Briefly describe the Hill Cipher method with an example. (6)

(ii) Describe the IDEA in detail. (10)

12. (a) (i) Explain the RSA algorithm. (10)

(ii) Perform the encryption and decryption using the RSA algorithm for the following : (6)

(1) p=11; q=13 e=11; M=7

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

Or

(b) (i) Briefly explain the categories of security services. (8)

(ii) Explain the RSA digital signature scheme and compare it with RSA cryptosystem. (8)

13. (a) (i) Describe a dictionary attack and suggest measure to prevent it. (8)

(ii) Explain the general idea behind challenge-response entity authentication. (8)

Or

(b) (i) List the problems with using passwords for authentication. (8)

(ii) Explain cryptographic authentication protocols. (8)

14. (a) Explain the different types of Firewalls. (16)

Or

(b) (i) Describe the IP security architecture. (8)

(ii) Explain the Kerberos architecture. (8)

15. (a) (i) Explain the Threats in network and what makes a network vulnerable ? (8)

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

Or

(b) Discuss the various approaches to Intrusion Detection. (16)

———————