G 6170

M.E. DEGREE EXAMINATION, MAY/JUNE 2007.

Second Semester

Network Engineering

CS 1629 — NETWORK SECURITY

(Common to ME – Computer Science and Engineering)

(Regulation 2005)

Time : Three hours Maximum : 100 marks

Answer ALL questions.

PART A — (10 × 2 = 20 marks)

1. Differentiate passive and active attacks.

2. What is a meet-in-the-middle attack?

3. State Euler's Theorem.

4. In which situation RSA algorithm is well suited?

5. How message digest is differ from Hash function?

6. What are the possibility of attacks in a communication network?

7. List the requirements of Kerberos.

8. Draw the general format of PGP message.

9. List the general approaches to intrusion detection.

10. What is a Digital Immune System?

PART B — (5 × 16 = 80 marks)

11. (a) Explain the types of substitution and transposition techniques with example.

Or

(b) Explain the various block cipher modes of operation.

12. (a) (i) What is the meaning on the expression a divides b ? Explain. (8)

(ii) Explain Fermat's theorem with example. (8)

Or

(b) Explain Elliptic Curve Cryptography with algorithm.

13. (a) (i) Discuss the categories of digital signatures. (8)

(ii) Explain HMAC algorithm. (8)

Or

(b) Explain the types of authentication functions with neat diagram.

14. (a) Explain the four phases handled in SSL Handshake Protocol.

Or

(b) Discuss X.509 certificate parameters and its authentication procedure.

15. (a) (i) Explain the virus counter measures. (8)

(ii) How the password is protected? Discuss the UNIX password scheme. (8)

Or

(b) (i) What are the design goals of firewall and its limitations? (8)

(ii) Explain Trusted System with example. (8)
