D.C, 4

Reg. No. : □□□□□□□□□□□

K 6132

M.E. DEGREE EXAMINATION, NOVEMBER/DECEMBER 2007.

Second Semester

Network Engineering

CS 1629 — NETWORK SECURITY

(Common to M.E. Computer Science and Engineering)

(Regulation 2005)

Time : Three hours Maximum : 100 marks

Answer ALL questions.

PART A — (10 × 2 = 20 marks)

1. Distinguish information security from data security.

2. Give the simplified model of conventional encryption.

3. Using Fermat's Theorem find 3^{201} mod 11.

4. Prove the following using examples.

   [(a mod n) + (b mod n)] mod n = (a + b) mod n.

   [(a mod n) * (b mod n)] mod n = (a * b) mod n.

5. What is the role of a compression function in hashing?

6. Distinguish between direct and arbitrated digital signature.

7. Draw the general format of X.509 certificate.

8. State the functions of IPSec in the routing architecture required for Internet working.

9. What are the four stages, a typical virus goes through during its lifetime?

10. What is a Honey pot?

PART B — (5 × 16 = 80 marks)

11. (a) (i) What are the design goals of a firewall. Write down the general techniques that fire walls use to control access and enforce site's security policy. (8)

(ii) Discuss the features of 3 common firewall configurations. (8)

Or

(b) (i) Explain the Distributed Intrusion Detection scheme. (8)

(ii) What are the features of a trusted system? Explain in depth. (8)

12. (a) (i) Bring out the essential features of the various types of ciphers used in substitution technique. (10)

(ii) Show that in DES the first 24 bits of each subkey come from the same subset of 28 bits of the initial key and that the second 24 bits of each subkey come from a disjoint subset of 28 bits of initial key. (6)

Or

(b) (i) Explain any two Block Cipher Modes of Operation. (8)

(ii) Briefly explain the Line Encryption and End-to-End Encryption with a neat diagram. (8)

13. (a) (i) Explain RSA Public-Key Encryption Algorithm. Given prime numbers p = 17 and q = 11, perform Encryption and Decryption using RSA Algorithm. (8)

(ii) Explain in detail the Diffie-Hellman Key Exchange Algorithm. (8)

Or

(b) (i) State and prove Euler's Theorem. (8)

(ii) Consider the Elliptic Curve $E_{11}(1,6)$. The curve is defined by $y^2 = x^3 + x + 6$ with a modulus of p = 11. Determine all the points in E_{11} (1,6). (Hint : Start by calculating the right-hand side of the equation for all values of x). (8)

14. (a) (i) Describe the Digital Signature Algorithm with an example. (8)

(ii) Discuss in detail the Public-Key Encryption approach of Mutual Authentication Protocol. (8)

Or

(b) (i) Explain the ways in which a hash code can be used to provide Message Authentication. (8)

(ii) Compare Hash function and Digest function. (8)

15. (a) (i) Explain in detail the operation of PGP with a neat diagram. (10)

(ii) Give the overview of Kerberos. (6)

Or

(b) (i) With a suitable diagram describe IPSec Document overview. Enumerate IPSec services. (6)

(ii) Enumerate SSL Handshake protocol message types. Illustrate Handshake protocol action. Describe briefly the four phases involved in the initial exchange needed to establish a logical connection between client and server. (10)

———————