Name : .....

Roll No. : .....

Invigilator's Signature : .....

CS/B.TECH(CSE)/SEPARATE SUPPLE /SEM-8/CS-802D/2011

2011

NETWORK SECURITY

Time Allotted : 3 Hours *Full Marks* : 70

The figures in the margin indicate full marks.

Candidates are required to give their answers in their own words as far as practicable.

GROUP – A

(Multiple Choice Type Questions)

1. Choose the correct alternatives for the following : $10 \times 1 = 10$

   i) The principle of ..... ensures that sender of a message cannot later claim that the message was never sent.

   a) Access control b) Authentication

   c) Availability d) Non-repudiation.

   ii) In ..... attacks, there is no modification to message contents.

   a) passive b) active

   c) both (a) and (b) d) none of these.

   iii) A worm ..... modify a program.

   a) does not b) does

   c) may or may not d) none of these.

iv) The process writing the text as diagonals and reading it as sequence of rows is called

a) Rail Fence Technique

b) Caesar Cipher

c) Mono-Alphabetic Cipher

d) Homophonic Substitution Cipher.

v) DES encrypts blocks of

a) 32 bits b) 56 bits

c) 64 bits d) 128 bits.

vi) In IDEA, the key size is

a) 64 bits b) 128 bits

c) 256 bits d) 56 bits.

vii) SSL works between ..... and ..... .

a) web browser, web server

b) web browser, application server

c) web server, application server

d) application server, database server.

viii) The ..... protocol is similar to SSL.

a) HTTP b) HTTPS

c) TLS d) SHTTP.

ix) Firewall is a specialized form of a

a) bridge b) disk

c) printer d) router.

x) Information about possible intruders can be obtained by examining the

a) router log b) host log

c) IPsec entries d) audit log.

GROUP – B
(Short Answer Type Questions)

Answer any *three* of the following $3 \times 5 = 15$

2. Explain with examples the different Active and Passive attacks that can be performed by an intruder.
3. What is Symmetric and Asymmetric Cipher ? What are the drawbacks of Symmetric Cipher and how is it overcome in Asymmetric Cipher ?
4. What is Digital Signature ? Give a scheme for implementing digital signature using public key cryptography.
5. Explain why substitution or transposition cipher alone cannot provide the desired level of security. Define product Cipher.
6. Explain Packet filtering Firewall and Application Gateway Firewall in brief.

GROUP – C
(Long Answer Type Questions)

Answer any *three* of the following. $3 \times 15 = 45$

7. a) Describe the various issues of Network security and how these can be taken care of by Cryptography.
   b) Why and in what respect mono alphabetic Cipher is superior to poly alphabetic Cipher ?
   c) Explain how one can break a vigenere cipher ? 6 + 4 + 5
8. a) What is Public Key Cryptography ?
   b) Explain the RSA key generation and encryption algorithm in details.
   c) What are the drawbacks of RSA algorithm and the measures to alleviate those drawbacks ? 2 + 7 + 6
9. a) What is Key Distribution Problem ?
   b) Explain the Diffie Helman Key Exchange protocol in detail.
   c) State and compare the different models of a block cipher. 2 + 5 + 8

10. a) State and explain the diffusion and confusion property of a block cipher.

    b) Explain the DES algorithm with a suitable diagram.

    c) Write a note on the strength and weakness of DES algorithm. 4 + 8 + 3

11. Write short notes on any *three* of the following : 3 × 5 = 15

    a) IP tunneling

    b) IP spoofing and Denial of Service attack

    c) PGP

    d) Kerberos

    e) Virus and worm.

==========