Name : .....

Roll No. : .....

Invigilator's Signature : .....

CS/B.Tech (CSE)/SEM-8/CS-802D/2010

2010
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 × 1 = 10

   i) Message digest length n SHA-1 is ..... bits.

   a) 128 b) 160

   c) 64 d) 54.

   ii) Intercepti n is an attack on

   a) Availa ility b) Confidentiality

   c Integrity d) Authenticity.

   iii) .... prevents either sender or receiver from denying a transmitted message.

   a) Access control b) Non-repudiation

   c) Masquerade d) Integrity.

   iv) DES encrypts blocks of ..... bits.

   a) 32 b) 56

   c) 64 d) 128.

v) TDEA uses ..... keys and ..... executions of the DES algorithm.

a) 3, 3 b) 3, 4

c) 4, 3 d) 4, 5.

vi) In RSA, 19^5 mod 119 is

a) 96 b) 17

c) 66 d) 77.

vii) Compression function of secure hash algorithm consists of ..... rounds of processing of .... steps each.

a) 4, 20 b) 5, 20

c) 20, 80 d) 4 80.

viii) The IPSec specification consists of numerous documents. Four most important of these, issued in November of 1998 are RFCs 2401, 2402, 2406 and

a) 2403 b) 2404

c) 2407 d) 2408.

ix) A macro virus is

a) Platform dependent b) Platform independent

c) Idle d) Hidden.

x) "A computer program with an apparently or actually useful function that contains additional functions that surreptitiously exploit the legitimate authorizations of the invoking process to the detriment of security." This is the definition of

a) Trojan Horse b) Virus

c) Worm d) None.

GROUP – B

(Short Answer Type Questions)

Answer any *three* of the following. 3 × 5 = 15

2. What are passive threats and active threats ? Differentiate them.

3. Show that DES decryption is the inverse of DES encryption.

4. What is MAC ? Describe the functioning of MAC.

5. Draw the IP security authentication header.

6. List and briefly explain types of Firewalls.

GROUP – C

(Long Answer Type Questions)

Answer any *three* of the following. 3 × 15 = 45

7. a) Draw a model for network security. 3

   b) Explain Feistel cipher structure. 7

   c) Differentiate between block cipher and stream cipher. Define crypt analysis. 3 + 2

8. a) Explain link encryption and end to end encryption in the location of encryption devices. 5

   b) Explain RSA public key encryption algorithm with example. 7

   c) What do you mean by message digest. 3

9. a) Compare MD5 and SHA-1 algorithms. 5

   b) Explain IPSec services. 5

   c) List and explain applications of IPSec. 5

10. a) Explain with the figure how secure socket layer (SSL) is accommodated in TCP/IP protocol suite. 5

b) Explain Handshake Protocol. 10

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

a) Intruders

b) Malicious programs

c) Digital signatures

d) Key management

e) Firewall.