Name : ....

Roll No. : ....

Invigilator's Signature : ....

CS/B.TECH(CSE)/SEP.SUPPLE/SEM-8/CS-802D/2012

2012

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 in MD-5 is .... bits.

a) 128 b) 160

c) 64 d) 54.

ii) AES encrypts blocks of .... bits.

a) 160 b) 128

c) 256 d) 80.

iii) Digital Signature is used to ensure

a) authentication

b) confidentiality

c) authentication and integrity

d) authentication and confidentiality.

iv) Hill Cipher is vulnerable to the

a) cipher text only attack

b) known plain text attack

c) chosen plain text attack

d) chosen cipher text attack.

v) A worm .... modify a program.

a) does not b) does

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

vi) .... is possible in absence of proper authentication mechanism.

a) Non-repudiation b) Interruption

c) Access control d) Fabrication.

vii) Firewall is a specialized form of a

a) bridge b) disk

c) switch d) router.

viii) 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.

ix) SSL works between .... and ....

a) Web Browser, Application Server

b) Web Browser, Web Server

c) Application Server, Database Server

d) Web Server, Application Server.

x) In IDEA, the key size is

a) 64 bits b) 128 bits

c) 256 bits d) 56 bits.

GROUP – B

(Short Answer Type Questions)

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

2. a) Discuss about the four basic principles related to the security of a message.

   b) What is access control. 4 + 1

3. Explain how the Diffie-Hellman key exchange algorithm might become vulnerable.

4. Explain briefly the Kerbæros version 4.

5. Draw the IP security authentication header.

6. What is initialization vector. Define passive threat and active threat with example. 1 + (2 + 2)

GROUP – C

(Long Answer Type Questions)

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

7. a) Define linear cryptanalysis and differential cryptanalysis.

   b) What is packet spoofing ?

   c) Define Brute-force attack and Man-in-the Middle attack.

   d) Explain how data security is achieved through digital certificate. (2 + 2) + 2 + (2 + 2) + 5

8. a) Compare the characteristics of SHA-1 and MD5 algorithms.

   b) Compare Asymmetric Key Cryptography and Symmetric Key Cryptography.

   c) Compare Substitution Cipher & Transposition Cipher. Compare IDEA and AES. 5 + 5 + (2 + 3)

9. a) Explain different types of attack on RSA.

b) Describe the decryption technique of Triple DES. (Explain in brief).

c) Provide a scheme for implementing digital signature using public key cryptography. 6 + 6 + 3

10. a) What is H-MAC ? Describe the functioning of MAC.

b) Describe the utility of secure DNS. Describe the fields of SSL record protocol header.

c) Explain in brief Secure Electronic Transaction (SET).

(2 + 3) + (2 + 3) + 5

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

a) OFB mode

b) Malicious program

c) IPSec

d) S/MIME

e) Digital Signature

f) Blow Fish

g) H-Mac.

=============