Name : ....

Roll No. : ....

Invigilator's Signature : ....

CS/B.TECH (CSE)/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 from the following : 10 × 1 = 10

i) Number of keys used in asymmetric key cryptography is

a) 04 b) 02

c) 08 d) 16 .

ii) Vigenere cipher is an example of

a) polyalphabetic cipher b) monoalphabetic cipher

c) ceasar cipher d) product cipher.

iii) Firewall may be described as a specialized form of

a) router b) operating system

c) bridge d) architecture.

iv) Tool for implementing security policy may be called as

a) security process

b) security authentication

c) security gaps

d) security mechanism.

v) In MD-5 the length of the message digest is

a) 160 b) 128

c) 64 d) 54 .

vi) RC4 is an example of

a) hash algorithm b) stream cipher

c) block cipher d) none of these.

vii) For confidentiality, data to be sent is

a) encrypted b) decrypted

c) corrected d) both (a) and (b).

viii) A polymorphic virus undergoes

a) crossover b) mutation

c) genetic processing d) none of these.

ix) A macro virus is

a) platform dependent b) platform independent

c) hidden d) idle.

x) We require .... to verify digital signature.

a) receiver's public key b) sender's private key

c) sender's public key d) receiver's private key.

GROUP – B

(Short Answer Type Questions)

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

2. What are :

a) Brute force attack

b) Man-in-the Middle attack ? $2 \times 2\frac{1}{2}$

3. a) What do you understand by threat ?

b) What is PGP ? 2 + 3

4. a) What is intrusion ? Who is an intruder ?

b) How may intrusion be detected ? 2 + 3

5. What type of key is generated or exchanged by using Diffie-Hellmann key exchange algorithm ? Justify your answer. 5

6. a) What is the difference between virus and worm ?

b) What is WEP ? $2 \times 2\frac{1}{2}$

GROUP – C

(Long Answer Type Questions)

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

7. a) What is the difference between stream cipher and block cipher ?

b) What types of attacks may occur on block ciphers ?

c) What type of cipher is DES ?

d) What active attacks may be encountered while providing network security ?

e) What does packet filtering router do ?

2 + 4 + 1 + 5 + 3

8. a) Discuss about any two password selection strategies with their advantages and disadvantages.

b) How does Secure Electronic Transaction take place ?

c) Where do you find AH protocol ? 6 + 8 + 1

9. a) Briefly describe the RSA algorithm and show how it provides security to message / data.

b) How digital signatures can be generated ? What does it provide to a message ? 9 + 6

10. a) What is message digest ?

b) What is HMAC ?

c) Compare and contrast MD5 and SHA-1 algorithms.

d) How is SHTTP different from SSL ?

e) What is private key crypolsystem ? 2 + 2 + 5 + 4 + 2

11. a) What are the services provided by IPSec ?

b) Briefly describe IPSec Architecture

c) What are the different protocols associated with SSL ?

d) What are the main functions of Kerberos ?

3 + 5 + 4 + 3