Name : .....

Roll No. : .....

Invigilator's Signature : .....

CS/B.Tech/CSE/SEM-8/CS-802D/2013

2013

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) Which one of the following is active attack ?

a) Masquerade b) Traffic analysis

c) Eaves ropping d) Shoulder surfing.

ii) Which one of the following is passive attack ?

a) Masquerade b) Traffic analysis

c) Replay attack d) Denial of service.

iii) Key used in the symmetric key cryptography is called

a) Public key b) Session key

c) Permanent key d) Secret key.

iv) Key used in the asymmetric key cryptography is called

a) Public key b) Session key

c) Permanent key d) Private key.

v) Number of keys used in Public key cryptography is

a) 2 b) 4

c) 6 d) 8.

vi) Chosen Cipher text attack is based on

a) Cryptoanalysis b) Cryptography

c) Encryption d) Decryption.

vii) Authentication service that can be used on Windows platform is

a) DES b) RSA

c) KERBEROS d) MD5.

viii) A firewall that u es two TCP connections is

a) Bastion

b) Application Gateway

c) Circui level Gateway

d Packet Filter.

ix) A virus that cannot be detected by Antivirus Software is

a) Parasitic b) Polymorphic

c) Stealth d) Worm.

x) An attack on Authenticity is

a) Interruption b) Interception

c) Fabrication d) Violation.

GROUP – B
(Short Answer Type Questions)

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

2. What is a digital envelope ? Explain, how it works. 2 + 3

3. Explain suitable Cipher Feedback mode with a suitable diagram.

4. Differentiate between transport and tunnel modes of operation of IPsec.

5. Explain briefly the working principle of HMAC.

6. What are the differences between symmetric key and asymmetric key cryptography ? What is ma querade ? 3 + 2

GROUP – C
(Long Answer Type Questions)

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

7. a) What are the four main stages in AES operation ? 4

   b) Let the state matrix in any intermediate stage of AES is

ac	21	34	ec
02	76	ea	02
13	50	46	a4
92	76	ab	Ba

   What would be the state matrix after the Shift Row Oper tion ? 3

   c) In an AES cryptosystem the Round Key for Round 6 is

   EA BC 73 23 45 67 32 87 E2 3D 9B 02 33 4E A2 F0

   Find the first 4 bytes of the Round key for round 7.

   The values of RC[j] in Hexa-decimal is given as follows :

J	1	2	3	4	5	6	7	8	9	10
RC[j]	01	02	04	08	10	20	40	80	1B	36

8

8. a) What would be the transformation of a message 'We the people of India' using Rail Fence technique ? 4

   b) Explain the Diffie-Hellman key exchange mechanism. With an example explain the man-in-the middle attack in the Diffie-Hellman key exchange algorithm. 6 + 5

9. a) What are different algorithm modes ? Explain those which are applied on block ciphers. 4

   b) State and explain how IDEA works. 7

   c) For a Vernam Cipher do the following : 4

      i) Using pad "ARE" encode "TZP"

      ii) Using pad "ARX" decode "YFR".

10. a) Write down RSA algorithm. 6

    b) In an RSA system the public key of a user is 17 and $N = 187$. What will be the private key of this user ? 6

    c) What is the difference between MAC and Message Digest ? 3

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

    a) D gital signature

    b) RC5

    c) DES

    d) SHA

    e) SSL and TLS.