Name : .....

Roll No. : .....

Invigilator's Signature : .....

CS/M.TECH(CSE)/SEM-1/MCSE-105A/2012-13

2012

CRYPTOGRAPHY AND 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

(Objective Type Questions)

1. Answer any *seven* of the following : $7 \times 2 = 14$

   i) Distinguish between Symmetric key and Asymmetric key cryptography.

   ii) What is digital envelope ?

   iii) What is MAC ? Why it is important ?

   iv) What is firewall ?

   v) What is message digest ?

   vi) Distinguish between Stream and Block ciphers.

   vii) How can the same key be reused in triple DES ?

   viii) What is worm ? What is the significant difference between worm and virus ?

ix) What is the difference between Substitution cipher and Transposition cipher ?

x) What would be the transformation of a message "computer science and engineering" using Rail Fence Technique ?

GROUP – B

(Long Answer Type Questions)

Answer any *four* of the following. $4 \times 14 = 56$

2. a) Starting with two large prime numbers first find the keys and with those keys encode and decode the word 'safe' (convention should be explicitly mentioned)

   b) Briefly discuss sub-key generation in IDEA.

   c) What are the key principles of security ? 6 + 4 + 4

3. a) Briefly describe MD5 logic and SHA-1 logic.

   b) Make a comparison between these two hash algorithms.

   c) Why do MD5 and SHA-1 require padding of messages that are already multiple of 512 bits ? 8 + 3 + 3

4. a) Describe Diffie-Hellman key exchange algorithm and examine its vulnerability.

   b) In Diffie-Hellman protocol, what happens if users *A* and *B* choose by accident same numbers as their private keys (say X_A and X_B) ? Will the value of their public keys (say Y_A and Y_B) be same ? Will the value of the shared session key calculated by *A* and *B* the same ? Use example to prove your claim.

   c) What is Secure Electronic Transaction ? 6 + 6 + 2

5. a) With a suitable example show the Knapsack algorithm can be used as a symmetric key cryptographic technique.
   b) With emphasis on the term 'virtual' discuss the architecture of VPN in brief.
   c) What is Zero Knowledge Protocol ? Explain briefly.
   d) How SSL helps in web page security ? 5 + 3 + 3 + 3

6. a) Briefly explain AES.
   b) What do you mean by 'Man in Middle' attack ?
   c) Why add and multiply in IDEA is based on modulo 2^{16} and $(2^{16}+1)$?
   d) Briefly explain the concept of digital certificate.

   6 + 3 + 2 + 3

7. Write short notes on any *four* of the following : 4 × 3½
   a) Key Distribution Centre (KDC)
   b) KERBEROS
   c) RFID
   d) ECC
   e) P.G.P.
   f) P.E.M.

==========