MCN0533/MIT0512 USN | | | | | | | | | | |

First Semester M.Tech (CNE/IT) Examination - January 2015
(Autonomous Scheme)
Information and Network Security

Time: 3 Hrs Max. Marks: 100

Note: Answer all the questions.

1. a) Distinguish between the following pairs of terms: 8
   i) Mono and ploy alphabetic ciphers.
   ii) Cryptanalysis and Brute force attack.
   iii) Block and stream ciphers.
   iv) Steganography and cryptography.

   b) Explain the concept of play fair cipher. Using a key "MIRACLE" encode the message "This is an example". 7

2. a) Explain the principle of public-private key cryptography. What is the function of one way function in them? How can it be used for (i) message security and (ii) message authentication? 8

   b) State and explain the RSA algorithm. 7

OR

2. c) State the Diffie-Hellman key exchange algorithm. Prove its correctness. 8

   d) What is an abelian group? 5

   e) What is an elliptic curve? What is its importance in cryptography? 2

3. a) Narrate a typical key distribution scenario involving an initiator A, Responder B and a Key Distribution Centre KDC. Provide both key distribution and authentication steps. 10

   b) What is a session key? What factors affect it's life time? 5

4. a) What are the four general principles used to authenticate a user's identify? 5

   b) What is the authentication protocol suggested by Denning for Remote user authentication using symmetric keys? How can it lead to suppress-replay attack? 10

OR

4. c) What are the security threats in a wireless network? 10

   d) Briefly explain the 802.11 protocol stack. 5

5. With necessary diagram, provide a typical handshake protocol sequence diagram of SSL. 15

6. In the contex of IPsec, provide an overview of the following briefly. 15
   (i) Its benefits (ii) Documents (iii) Services.

7. a) What is avalanche effect? 2

   b) What is meant by revocation of certificates by X.509? Under what circumstances is it resorted to? 3

   c) Name the 5 phases of 802.11i. 3

   d) How do Transport mode ESP and tunnel mode ESP compare in terms of security. 2

****