Name : ....

Roll No. : ....

Invigilator's Signature : ....

CS/M. Tech (ECE (N))/SEM-3/MCE-302/2011-12

2011

INTERNET 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

(Short Answer Type Questions)

Answer any *five* of the following questions. 5 × 2 = 10

1. a) Write the differences between authentication and non-repudiation.

   b) What are honeypots ?

   c) What do you mean by Steganography ?

   d) What is the difference between Symmetric Key Cryptography and Public Key Cryptography ?

   e) What is key wrapping ? How is it useful ?

   f) Why is the SSL Layer positioned between the application layer and the transport layer ?

   g) What is the strength of IDEA ?

GROUP – B

(Long Answer Type Questions)

Answer any *five* of the following questions.

5 × 12 = 60

2. a) Decrypt the cipher text "KWUM PMZM" to find out the plain text using Modified Caesar cipher method.

   b) Encrypt the message "MY NAME IS ATUL" using Playfair Cipher method to find the cipher text.

   c) Mention the types of attacks possible on plaintext and cipher text. 4 + 6 + 2

3. a) Encrypt the plain text message "DOG" using Hill Cipher method to find the cipher text. Then, decrypt the cipher text to find the original plain text.

   b) What would be the cipher text message of a plain text message "Happy birth day to you" using Rail Fence technique.

   c) State and explain at least two attacks that can break the security of a packet filter. (3 + 3) + 3 + 3

4. a) Alice and Bob want to establish a secret key using the Diffie-Hellman Key Exchange protocol. Assuming the values as $n = 11$, $g = 5$, $x = 2$ and $y = 3$, find out the values of A, B and the secret key ($K1$ or $K2$)

b) Explain with an example how Diffie-Hellman Key Exchange protocol can fall pray to the man-in-the-middle attack.

c) What is a proxy server ? How does it work ?

d) What are the types of intruders found that try to intrude into the privacy of a network ? 3 + 4 + (1 + 2) + 2

5. a) Consider a plain text 10. Using the RSA algorithm, find out what this plain tex encrypts to and verify upon decryption, it transforms back to plain text. Give two prime numbers $P = 7$, $Q = 17$ and the encryption key (E) as 5.

b) Write a short note on Kerberos. 7 + 5

6. a) Is it possible to combine symmetric key and asymmetric key cryptography so that better of the two can be combined ?

b) Why is SHA more secured than MDS ?

c) What are significances of an MCA? 5 + 4 + 3

7. a) How can the same key be reused in triple DES ?

b) Explain the principles of the IDEA algorithm.

c) Discuss about the sub-key creation process in RC5.

4 + 4 + 4

8. a) Briefly describe the SSL architecture.

b) Explain the concept of key rings in PGP. 6 + 6