Name : .....

Roll No. : .....

Invigilator's Signature : .....

CS/M.TECH (ECE-NEW)/SEM-2/MCE-204A/2011

2011
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.

Question no. 1 is compulsory and answer any *four* questions from the rest.

1. Attempt all questions : 7 × 2

   a) Differentiate active and passive security attacks.

   b) What do you mean by authentication ?

   c) What is traffic padding and when is it required ?

   d) Differentiate virus and worm.

   e) What is Brute force attack ?

   f) What are the number of rounds in AES cipher for key size 128 bits and 256 bits ?

   g) What do you mean by one-way property of Hash function ?

2. a) Discuss Digital Immune System approach to protect from virus attack. 8

   b) What is Man-in-the-middle attack and in which case this type of attack occurs ? 6

3. a) Encrypt the word "bomb" using the Hill cipher with the key $\begin{pmatrix} 9 & 4 \\ 5 & 7 \end{pmatrix}$. Show calculations and result. 8

   b) In DES encryption initial permutation of the plaintext is followed by 16 rounds. Input of each round is of 64 bits which is divided into left and right halves each of 32 bits. For the i^{th} round the relation between the output and input halves is as follows :

   $L_i = R_{i-1}$

   $R_i = L_{i-1} \oplus F(R_{i-1}, K_i)$

   Show with block diagram how $F(R_{i-1}, K_i)$ is obtained.

   6

4. a) How are the public and private keys in RSA algorithm generated ? 4

   b) Determine the ciphertext for the plaintext P = 5 using RSA algorithm for public key { 7, 187 } and private key { 23, 187 }. Also show how the receiver can obtain the plaintext. 3 + 3

   c) Comment on the security of RSA algorithm. 4

5. a) What are the requirements for Message Authentication Code ? 5

   b) What are the criteria a Hash Function should satisfy ? 5

   c) Comment on the security of Hash Functions and MACs. 4

6. a) Explain briefly the steps in MD5 Message Digest Algorithm. 7

   b) Discuss briefly the Digital Signature Algorithm. 7

7. Write short notes on any *two* : 7 + 7

   a) IPSec

   b) Kerberos

   c) Smatt Cards and security

   d) Biometric authentication.