Name : .....

Roll No. : .....

Invigilator's Signature : .....

CS/M.TECH(CSE)/SEM-2/MTCSE-21/2012

2012

INFORMATION 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.)

GRROUP - A

Answer any *five* questions from the following :

5 × 5 = 25

1. What is it important to sutdy the Feistel cipher ? What is the idea behind meet-in-middle attack ? 2 + 3

2. Briefly describe the Single round function and key generation of DES.

3. a) Find out the multiplicative inverse of { 95 }.

   b) $f(x) = x^6 + x^4 + x^2 + x + 1$ and $g(x) = x^7 + x + 1$.

   Find out $f(x) \cdot g(x)$, using the finite field GF (2^8), with the irreducible polynomial $m(x) = x^8 + x^4 + x^3 + x + 1$. 3 + 2

4. Briefly describe Key Distribution Centre (KDC) and Needham-Schroeder Protocol. 2 + 3

5. What are the requirements of a Mesaage Digest Algorithm ? What is a digital certificate ? 3 + 2

6. Why is SHA more secure than MD5 ? What is the difference between MAC and message digest ? 3 + 2

7. Briefly describe the working principle of a typical Samrt Card.

GRROUP - B

Answer any *three* questions from the following :

3 × 15 = 45

8. Briefly describe Kerberos protocol ? What are the five principal services provided by PGP ? How these principals were implemented in PGP protocol ? 8 + 3 + 4

9. Why is the SSL layer positioned between the application layer and transport layer ? What are the purpose of SSL handshake, record and alert protocol ? Who are the key participants in SET ? How SET protects payment information from merchant ? Outline the broad level steps in SET ?

2 + 6 + 2 + 2 + 3

10. What services are provided by IPSec ? Why does ESP include padding field ? What are the basic approaches to building SAs ? Describe the types of Biometrics ? What are the there main actions of a packet filter ? Why application gateway is called to be proxy Server ? 2 + 2 + 3 + 3 + 3 + 2

11. Briefly describe the Man-in-the-Middle attack in Diffie-Hellman Key Exchange algorithm. Mathematically prove that in Diffie-Hellman Key Exchange algorithm the same key is shared at the both end of the communication. Describe the basic functionalities of RSA algorithm. 6 + 4 + 5

12. How the length of the original message is appended with message in MD5 message digest algorithm ? Make a brief comparison of MD5 and SHA-1 algorithm. What are the changes done in SHA-512 with respect to SHA-1 ? How the length of the key is adjusted with the message block in HMAC algorithm ? 3 + 4 + 4 + 4