Roll No. .....

23078

M. Tech. 3rd Sem. (Computer Engg.)

Examination–January, 2013

Security of Information Systems

Paper-MTCE-707A(B)

Time : 3 hours ***Max. Marks : 100***

Before answering the questions, candidates should ensure that they have been supplied the correct and complete question paper. No complaint in this regard will be entertained after the examination.

Note : Attempt any **five** questions.

1. (a) Compare & contrast monalphabetic and polyaphabetic ciphers by giving examples. *10*

(b) Discuss crypto analysis of Caesar Cipher in detail by giving two examples. *10*

2. (a) Define and describe modular arithmetic. Discuss various properties of modular arithmetic by giving suitable examples. *10*

(b) State and prove Fermet's theorem. *10*

3. (a) What is relation between classes P and NP ? Discuss them by giving examples. *10*

(b) Discuss an algorithm used to compute inverse. Also give an example. *10*

4. (a) Discuss super increasing knapsacks in context of Merkle-Hellman algorithm in deail. *10*

(b) Explain DES by giving suitable example. Also write its advantages and disadvantages. *10*

5. (a) What is AES ? Explain various modes of AES in detail. *10*

(b) Give addition and multiplication tables for the integers Mod 5 and for the integers Mod 7. *10*

6. What is importance of hash functions ? Compare and contrast SHA_1 and SHA_2 hash functions by giving examples. Also write their merits and demerits. *20*

7. Describe the following in detail. *20*

   (a) Key management protocols

   (b) Security of networks from various attacks.

8. Write short note on the following : *20*

   (a) MD4

   (b) Substitution ciphers

   (c) Operating System Security

   (d) Public key encryption system characteristics.
