Total No. of Questions : 8] *[Total No. of Printed Pages : 2*

Roll No .....

MCIT-201

M.E./M.Tech., II Semester

Examination, June 2017

Information Security System

Time : Three Hours

Maximum Marks : 70

Note: i) Attempt any five questions.

ii) All questions carry equal marks.

1. a) What is fundamental difference between symmetric and asymmetric encryption.
   b) What is difference between digital signatures and digital certificates.

2. a) Write short notes on PKI.
   b) Explain the protocols used to provide secured communications.

3. The value of public key and private key are (N, E) = (33, 3) and (N, D) = (33, 7). Use RSA algorithm to encrypt the word "TECHNOLOGY" and also show how the word can be decrypted from its encrypted form.

4. a) Discuss MD5 with example.
   b) With suitable sketches, explain the working of DES algorithm.

5. a) Explain briefly about the ISO model list its limitations.
   b) Discuss challenge-response algorithms.

6. a) Describe the various categories of threats to information.
   b) Discuss any three cryptographic tools and their significance in information security.

7. a) Describe Diffie-Hellman problem.
   b) How does a network based IDPS differ from Host based IDPS?

8. Write short notes on:
   a) Blow Fish
   b) Zero knowledge protocol

******