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

Roll No .....

MCADD-803

M.C.A. (Integrated Course), VIII Semester

Examination, May 2019

Network Security

Time : Three Hours

Maximum Marks : 70

Note: i) Attempt any five questions.

ii) All questions carry equal marks.

1. a) Discuss the various principles Involved in private and public Key cryptography.

   b) Perform encryption for the plain text $m = 88$ using the RSA algorithm $p = 17$, $q = 11$ and the public component $e = 7$.

2. a) Explain Data Encryption Standard (DES) in detail.

   b) Explain Diffie-Hallman key exchange algorithm.

3. a) What is message authentication ? How is it different from message Integrity?

   b) State and describe Fermat's theorem.

4. a) Describe the process involved in digital signatures. Explain about different digital signatures?

   b) What are the requirement of Hash functions?

5. a) Discuss how firewalls help in the establishing a security framework for an organization?

   b) Classify the various security attacks and define them.

6. a) Give a brief note on x.509 authentication services.

   b) Describe IP security architecture.

7. a) Explain in detail about network based Intrusion detection system?

   b) List the transfer encoding used by S/MIME. What are the contents types provided by S/MIME?

8. Explain the following any two.

   i) Trusted systems

   ii) Secure socket layer

   iii) Combining security associations

******