

Roll No

MCADD-803

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

Examination, May 2023

Network Security

Time : Three Hours

Maximum Marks : 70

- Note :** i) Attempt any five questions.
ii) All questions carry equal marks.

1. a) What is Substitution encryption technique?
b) Differentiate between Traditional cryptography and Modern cryptography.
2. a) Explain simplified DES.
b) Using simplified DES encrypt the string (10100010) using the key (0111111101) by hand. Show intermediate results.
3. a) What is message authentication ? How is it different from message Integrity?
b) State and describe Fermat's theorem.
4. 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 $e = 7$.

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) What is Public key cryptography? Explain bring out the difference between conventional encryption and public key encryption.
b) Explain the classes of message authentication functions.
7. a) What are Intruders? Classify them.
b) Describe the operation of Virus.
8. a) What do you mean by firewall? When the system administrator trusts the internal users. What types of firewall is to be used? What are its advantages and disadvantages?
b) Briefly describe the types of viruses.
