No. of Printed Pages : **2**

21CSC3E1BL

Sl. No.

M.Sc. III Semester Degree Examination, April/May - 2024

COMPUTER SCIENCE

Cryptographic and amp ; Network Security

(NEP)

Time : 3 Hours Maximum Marks : 70

Note : *Answer* ***any five*** *of the following questions with Question No.* ***1 compulsory****.*

1. (a) What is the CIA Triad, and why is it important in the context of information security ? **7**

(b) Explain the Miller-Rabin algorithm, and use it to determine whether 61 is prime or not ? **7**

2. (a) Explain Symmetric Cipher model in detail. **7**

(b) Using the Playfair Cipher technique, how can we encrypt the plaintext "COMMUNICATE" with the key "COMPUTER" ? Please include all the rules and diagrams for encryption. **7**

3. (a) Explain the structure of AES with a clear diagram. **7**

(b) Discuss Double DES and Triple DES, and how do they work ? **7**

4. (a) Explain the principles of public key Cryptography. **7**

(b) Demonstrate encryption and decryption using the RSA algorithm with the example values p=3, q=5 and e=3. **7**

5. (a) What are the requirements for message authentication ? **7**

(b) What is a digital signature, and what are the essential elements of the digital signature process ? **7**

6. (a) Using the columnar transposition technique, demonstrate how encryption and decryption are done for the plaintext **"Attack postponed until two am"** with the key **"4312567"**. **7**

(b) Explain the Electronic Code Book (ECB) mode of block cipher. **7**

P.T.O.

7. (a) Explain the properties of cryptographic hash function. **7**

(b) Explain the concepts of attacks and forgeries in digital signatures. **7**

8. Write a short note on the following : **5+5+4**

(a) Feistel Structure

(b) RC4 Algorithm

(c) Network Security Model

- o 0 o -