



129768

62474

Reg. No.

Y 1 8 E B 2 2 S 12600

III Semester M.C.A. Degree Examination June/July - 2024

COMPUTER SCIENCE

Cryptography and Network Security (Elective)

(CBCS Y2k20 Scheme)

Time : 3 Hours

Maximum Marks : 70

*Instructions to Candidates :*

1. Answer any **Five** questions from Part-A. Each carries 6.
2. Answer any **Four** questions from Part-B. Each carries 10.

**PART - A**Answer any **FIVE** questions. Each question carries **SIX** marks.

(5×6=30)

1. Briefly explain the stream cipher with an example.
2. Draw a neat diagram of AES general structures and explain it.
3. Explain Diffie-Hellman Key exchange.
4. What are the properties a digital signature should have?
5. What four requirements were defined for Kerberos?
6. Explain the X.509 standard with a neat diagram.
7. What is the difference between SSL connection and SSL session?
8. Explain the concepts of Message Authentication code.

**PART - B**Answer any **FOUR** questions. Each question carries **TEN** marks.

(4×10=40)

9. Compare Cryptography and Steganography.
10. Explain the different types of Attacks on Encrypted Message.

[P.T.O.]



(2)

62474

10. a) Explain Fermat's and Euler's Theorem.  
b) Explain the Data Encryption Standard with a neat diagram. (5+5)
11. a) Explain the concept Chinese Remainder Theorem with an example.  
b) Describe the RSA Algorithm step by step. (5+5)
12. a) What is Message Authentication Code? Explain in detail.  
b) Explain the Elliptic curve cryptography. (5+5)
13. a) What are the roles of the public and private keys.  
b) What is Hash function? Explain in detail. (5+5)
14. a) Explain the various types of firewalls.  
b) What are the basic approaches of Security Association. (5+5)
-