62474

Reg. No. ☐☐☐☐☐☐☐☐

III Semester MCA Degree Examination, June/July - 2023
COMPUTER SCIENCE
Cryptography and Network Security (Elective)
(CBCS Scheme 2020-21) (Y2K20)

Time : 3 Hours   Maximum Marks : 70

Instructions to candidates:

1) Answer any **five** questions from section-A, each question carries **6** marks.

2) Answer any **four** questions from section-B, each question carries **10** marks.

SECTION-A

Answer any **Five** of the following questions. Each question carries 6 marks.   (5×6=30)

1. Explain different types of security attacks on data.
2. Briefly explain the symmetric cipher model.
3. Explain DES encryption algorithm.
4. Explain cipher block chaining mode.
5. Write a note on Fermat's and Euler's theorem.
6. Write a note on Elliptic curve arithmetic.
7. Explain any two authentication protocols.
8. Compare SSL and TLS.

SECTION - B

Answer any **Four** of the following questions. Each carries 10 marks.   (4×10=40)

9. Explain in detail different types of security services.
10. Explain different substitution techniques used for encryption.
11. Explain AES structure and encryption process with neat diagram.
12. Explain RSA algorithm with suitable example.
13. Explain different public keys distribution techniques.
14. Write short notes on
    a) Digital signature.
    b) Intrusion detection.   (5+5)