



62474

Reg. No. 

M	C	2	0	0	8	3	4
---	---	---	---	---	---	---	---

III Semester M.C.A. Degree Examination, April/May - 2022

COMPUTER SCIENCE

Cryptography and Network Security

(CBCS Scheme 2020-21)

Time : 3 Hours

Maximum Marks : 70

*Instructions to Candidates:*

- 1) Answer any **Five** questions from **Section-A**, each carries Six marks.
- 2) Any **Four** questions from **Section-B**, each carries Ten marks.

**SECTION - A****Answer any FIVE of the following questions. Each carries 6 Marks. (5×6=30)**

1. Briefly explain security mechanisms in cryptography.
2. With a neat diagram explain the model for network security.
3. Write a note on RC4.
4. Explain the steps involved in AES cipher.
5. With an example explain Euclidean algorithm.
6. Briefly explain Digital Signature.
7. Explain RSA algorithm.
8. Write a note on SSL and TLS.

**SECTION - B****Answer any FOUR of the following questions. Each carries 10 Marks. (4×10=40)**

9. Define Cryptography. Explain the types of attacks on encrypted messages.
10. a) Write the difference between substitution and transposition cipher. (5+5)  
b) Write a note on Ceaser Cipher.
11. Explain single round DES algorithm.
12. With a neat diagram explain the different block cipher modes of operation.

[P.T.O.]



(2)

62474

13. a) Explain Diffie-Hellman key exchange algorithm.
- b) Briefly explain Hash function.
14. Write a note on PKI and Malicious software.

(5+5)

(5+5)