QP CODE: 24800009 24800009 **Reg No** : ....

Name : ....

MCA DEGREE EXAMINATIONS, DECEMBER 2023

Third Semester

Master of Computer Application

Elective - MCA304ET2 - CRYPTOGRAPHY AND NETWORK SECURITY

2020 Admission Onwards

FA082D11

Time: 3 Hours Maximum: 75 Marks

Part A

*Answer any **ten** questions*

*Each question carries **3** marks*

1. Encrypt "hello world" using Caeser cipher with key=3.
2. What is modular arithmetics?
3. What is S-box in DES?
4. What is AES?
5. What is triple DES ?
6. Explain Fermat's theorem with example.
7. What are the characteristics of a secure hash function?
8. What is suppress-replay attack in authentication? Explain the protocol used to eliminate this attack.
9. Explain the X.509 certificate format.
10. Explain the concepts of Extensible Authentication Protocol.
11. What are the services provided by PGP?
12. What are the steps involved in the SSL record protocol transmission?

(10×3=30 marks)

Part B

*Answer **all** questions*

*Each question carries **9** marks*

13. a) Explain DES with a suitable diagram

OR

b) Explain single round of DES with a suitable diagram

14. a) Explain AES encrypton with a neat diagram.

OR

b) Given two prime numbers p=5 and q=11, and encryption key e=7 derive the decryption key d. Let the message be x=24. Perform the encryption and decryption using RSA algorithm.

15. a) Write a short note on digital signatures.

OR

b) Explain the digital signature algorithm DSA.

16. a) Explain key distribution techniques used in asymmetric encryption.

OR

b) Explain the IEEE802.1X Port-Based NAC Typical authentication progression.

17. a) Describe how the cryptographic keys and key rings used for the PGP message transfer.

OR

b) Explain the various protocols used in SSL.

(5×9=45 marks)