



QP CODE: 25024397



25024397

Reg No : .....

Name : .....

**M.Sc DEGREE (CSS) EXAMINATION, APRIL 2025**

**Fourth Semester**

**ELECTIVE - CA800402 - APPLIED CRYPTOGRAPHY**

M Sc COMPUTER SCIENCE, M Sc INFORMATION TECHNOLOGY

2019 ADMISSION ONWARDS

9A7DB883

Time: 3 Hours

Weightage: 30

**Part A (Short Answer Questions)**

*Answer any **eight** questions.*

*Weight 1 each.*

1. Define Substitution technique in Cryptography.
2. Which are the three critical aspects of block cipher design?
3. How we perform mix column transformation AES Algorithm?
4. Define TRNG.
5. Define hash function.
6. List the applications of cryptographic hash function.
7. What is Masquerade?
8. What is weak spots?
9. Is HMAC more secure than MAC?
10. Briefly describe the general format of X.509 certificates.

(8×1=8 weightage)

**Part B (Short Essay/Problems)**

*Answer any **six** questions.*

*Weight 2 each.*

11. Explain Stream Cipher in detail with the help of block diagram.
12. Explain DES Encryption algorithm.
13. Write the difference between AES and DES Algorithms.
14. Write the key formation of encryption and decryption of multiple DES algorithms.
15. Describe the requirements for public-key cryptography.





16. Explain the MAC algorithm that is treated as a concatenation of 64-bit blocks from the set of M messages.
17. Briefly explain the role of KDC in symmetric distribution.
18. Discuss the role of digital signature in secure data transfer.

(6×2=12 weightage)

**Part C (Essay Type Questions)**

*Answer any **two** questions.*

*Weight 5 each.*

19. Explain Transposition technique - Rail Fence , with the help of an example.
20. Explain true random number generators.
21. Explain Diffie-Hellman key exchange with example
22. Explain the role MAC when sender and receiver try to send their messages.

(2×5=10 weightage)

