



QP CODE: 26019130



26019130

Reg No :

Name :

M.Sc DEGREE (CSS) EXAMINATION, MARCH 2026

Fourth Semester

ELECTIVE - CA800402 - APPLIED CRYPTOGRAPHY

M Sc COMPUTER SCIENCE, M Sc INFORMATION TECHNOLOGY

2019 Admission Onwards

47D72242

Time: 3 Hours

Weightage: 30

Part A (Short Answer Questions)

*Answer any **eight** questions.*

Weight 1 each.

1. Define Block cipher.
2. What is the importance of the number of rounds in block cipher design?
3. What is a subbytes in AES Algorithm?
4. What is middle attack in DES Algorithm?
5. What is trap-door one-way function?
6. What is the use of a hash buffer in SHA-512?
7. Define the term message authentication code.
8. What is message encryption?
9. What is the security of HMAC?
10. What is hierarchical key control in symmetric key distribution using symmetric encryption?
(8×1=8 weightage)

Part B (Short Essay/Problems)

*Answer any **six** questions.*

Weight 2 each.

11. Explain Symmetric Encryption.
12. Explain DES Encryption algorithm.
13. What is the difference between ShiftRows and Rotword?
14. What are the parameters used in LCG?





15. Explain Cryptographic Hash Function.
16. Is it necessary to recover the secret key in order to attack a MAC algorithm?
17. Discuss about general format of X. 509 certificates.
18. Discuss about digital signature.

(6×2=12 weightage)

Part C (Essay Type Questions)

*Answer any **two** questions.*

Weight 5 each.

19. Explain any 3 Substitution Techniques in detail.
20. Write the role of RC4 in Network security.
21. Explain RSA algorithm with example.
22. Explain the purpose of message authentication function with diagram.

(2×5=10 weightage)

