



QP CODE: 25047644



Reg No :

Name :

M.Sc DEGREE (CSS) EXAMINATION, NOVEMBER 2025

Third Semester

MSc CYBER FORENSICS

Core Course - CF010301 - CRYPTOGRAPHY AND APPLICATIONS

2019 ADMISSION ONWARDS

61C4CDA2

Time: 3 Hours

Weightage: 30

Part A (Short Answer Questions)

*Answer any **eight** questions.*

Weight 1 each.

1. What is arbitrated protocol?
2. What is meant by bit commitment?
3. Explain time and cost estimates for brute-force attack.
4. Explain how long should a key be.
5. What is the major disadvantage of end-to-end encryption? Explain it?
6. Define hiding ciphertext in ciphertext.
7. Define entropy and uncertainty.
8. Explain key transformation in DES.
9. What is RSA?
10. What is Diffie Hellman Key exchange algorithm? Explain.

(8×1=8 weightage)

Part B (Short Essay/Problems)

*Answer any **six** questions.*

Weight 2 each.

11. Describe about algorithms and types of algorithms.
12. Explain compromised keys and destroying keys.
13. Explain cipher block chaining mode.
14. Differentiate block cipher modes.
15. Describe feedback with carry shift registers.





16. Explain N-Hash.
17. Explain pohlig-Hellman encryption scheme and Elliptic curve crypto system?
18. Describe KERBEROS.

(6×2=12 weightage)

Part C (Essay Type Questions)

*Answer any **two** questions.*

Weight 5 each.

19. Explain about Secret splitting and secret sharing.
20. Compare a) hardware encryption and software encryption b) File-level and Driver- level Encryption.
21. Explain double and triple encryption.
22. Explain GOST digital signature algorithm and Discrete Logarithm signature scheme.

(2×5=10 weightage)

