QP CODE: 25022617

25022617

Reg No : .....

Name : .....

M.Sc DEGREE (CSS) SPECIAL REAPPEARANCE EXAMINATION, APRIL 2025

Third Semester

M.Sc CYBER FORENSICS

CORE - CF010301 - CRYPTOGRAPHY AND APPLICATIONS

2019 ADMISSION ONWARDS

79322031

Time: 3 Hours Weightage: 30

Part A (Short Answer Questions)

*Answer any **eight** questions.*

*Weight **1** each.*

1. Define the terms a) Encryption and decryption b) Algorithm and key
2. Define one way function.
3. Explain about updating keys.
4. What is OFB mode?
5. What is the major disadvantage of end-to-end encryption? Explain it.
6. What is detecting encryption?
7. What is meant by strong primes?
8. What is RC4?
9. What is Fiat-Shamir signature scheme with example.
10. Describe KERBEROS.

(8×1=8 weightage)

Part B (Short Essay/Problems)

*Answer any **six** questions.*

*Weight **2** each.*

11. Describe subliminal channel.
12. Explain fair coin flips.
13. Explain compromised keys and destroying keys.

14. Write short note on compression, encoding and encryption.

15. Write a note on triple-encryption modes.

16. Describe MD5.

17. What is RSA? Write a note on RSA encryption.

18. Explain is Pohlig - Hellman encryption scheme.

(6×2=12 weightage)

Part C (Essay Type Questions)

*Answer any **two** questions.*

*Weight **5** each.*

19. Explain digital signatures with encryption.

20. Compare various classes of algorithms to CIA triad and key management.

21. Explain data encryption standard algorithm in detail.

22. Explain GOST digital signature algorithm and Discrete Logarithm signature scheme.

(2×5=10 weightage)