



25804047

QP CODE: 25804047

Reg No :

Name :

MCA DEGREE EXAMINATION, OCTOBER 2025

Third Semester

MASTER OF COMPUTER APPLICATION

ELECTIVE - MCA304ET2 - CRYPTOGRAPHY AND NETWORK SECURITY

2020 ADMISSION ONWARDS

5FD40198

Time: 3 Hours

Maximum: 75 Marks

Part A

*Answer any **ten** questions*

*Each question carries **3** marks*

1. Mention the mathematical tools for cryptography.
2. List out the parameters considered in the design of a feistel network.
3. What is the avalanche effect in DES?
4. What are the evaluation criteria for AES?
5. List the block cipher modes of operation.
6. Differentiate Symmetric and Asymmetric Key Cryptography.
7. Write a short note on Diffie-Hellman key exchange protocols.
8. How digital signature is implemented using RSA approach?
9. Explain the Mutual Authentication protocol.
10. Explain thr requirements of Kerberos.
11. Give the operational description of PGP?
12. Neatly sketch the generic transmission of a PGP message.

(10×3=30 marks)





Part B

Answer **all** questions

Each question carries **9** marks

13. a) What is polynomial arithmetics? Illustrate the euclidean algorithm to find the gcd of two polynomials.

OR

- b) Explain security attacks and security mechanisms with suitable diagrams.

14. a) Explain the block cipher modes of operation.

OR

- b) Explain and use the concepts of Fermat's theorem and find the remainder of $7^{2019} \text{ mod } 13$.

15. a) Explain key distribution in public key cryptosystem.

OR

- b) What is a hash function? What are the basic uses of hash functions?

16. a) Explain the working of Kerberos Version 4.

OR

- b) Explain the working and different methods of Extensible Authentication Protocol.

17. a) Discuss the electronic mail security in detail.

OR

- b) Explain the secure electronic payment systems concepts.

(5×9=45 marks)

