

Reg. No.

--	--	--	--	--	--	--	--

III Semester M.C.A. Degree Examination, April/May - 2026

COMPUTER SCIENCE

Cryptography and Network Security (Elective)

(CBCS Scheme 2020-2021 Onwards)

Time : 3 Hours

Maximum Marks : 70

Instructions to Candidates :

1. Answer **any Five** questions from **Section - A**.
2. Answer **any Four** questions from **Section - B**.

SECTION - A

Answer any Five of the following. Each question carries 6 marks.

(5×6=30)

1. Define Security Attacks and classify them with examples.
2. Explain the OSI Security Architecture and its components.
3. Describe the Symmetric Cipher Model with neat diagram.
4. Explain the working principle of the Data Encryption Standard (DES).
5. What is differential cryptanalysis? What are the applications of the same?
6. Explain Fermat's Theorem with an example.
7. Define Digital Signatures and list their properties.
8. Explain the role of firewalls in network security.

SECTION - B

Answer any Four of the following. Each question carries 10 marks.

(4×10=40)

9. Explain the model for Network Security. Discuss various security services and mechanisms in detail.
10. Demonstrate the working of classical encryption techniques using substitution and transposition methods.
11. Explain AES structure and its design principles. Compare it with DES.



12. Illustrate the RSA algorithm with a suitable numerical example.
 13. Explain Digital Signature Standard (DSS) and X.509 authentication service in detail.
 14. Discuss SSL/TLS protocols and explain how they provide secure communication over networks.
-