Printed Pages– 4 Roll No. 300012821095

C127573(022)

B. Tech. (Hon's) (Fifth Semester) Examination, Nov.-Dec. 2023

(Computer Science and Engg. Branch - Artificial Intelligence)

CRYPTOGRAPHY and NETWORK SECURITY

Time Allowed : Three hours

Maximum Marks : 100

Minimum Pass Marks : 35

***Note** : All questions are compulsory. Part (a) of each unit is compulsory and carries 4 marks. Attempt any **two** parts from (b), (c) and (d) and carries 8 marks each.*

Unit-I

1. (a) Define symmetric cipher model. 4

(b) Explain how steganography can be used to enhance security in communication. 8

(c) Discuss the Limitations of Perfect Secrecy. 8

(d) Describe Shannon's theorem and its significance in cryptography. 8

Unit-II

2. (a) What is modular arithmetic and give a simple example? 4

(b) How does prime factorization underpin the security of modern cryptographic methods? 8

(c) Explain discrete logarithms and their applications in cryptography. 8

(d) Describe computations in finite fields and their relevance to cryptography. 8

Unit-III

3. (a) Briefly explain what a pseudorandom function is. 4

(b) Summarize the DES encryption process. 8

(c) Describe different modes of operation in block ciphers. 8

(d) Discuss the vulnerabilities of DES and methods to increase its security. 8

Unit-IV

4. (a) Define public-key cryptography. 4

(b) Outline the Diffie-Hellman Key Agreement process. 8

(c) Explain the RSA algorithm and discuss its security. 8

(d) Compare and contrast private and public-key encryption. 8

Unit-V

5. (a) What is a hash function? 4

(b) Explain the concept of Collision-Resistant Hash Functions. 8

(c) Describe the role of Secure Message Authenticate Codes in network security. 8

(d) Discuss the SHA-512 hash algorithm and its advantages over its predecessors. 8