

JAWAHARLAL NEHRU TECHNOLOGICAL UNIVERSITY GURAJADA VIZIANAGARAM
IV B. Tech I Semester Advanced Supplementary Examinations March 2025

CRYPTOGRAPHY AND NETWORK SECURITY

(Open Elective)

Time: 3 hours

Max. Marks: 70

Answer any **FIVE** Questions. **ONE** Question from **Each unit**

All Questions Carry Equal Marks

UNIT-I

1. a) Summarize the key security goals? [7M]
b) Describe different types of cryptographic attacks? [7M]
(OR)
2. a) Define cryptographic services and mechanisms, and list their key types? [7M]
b) Explain the mathematics of cryptography in detail. [7M]

UNIT-II

3. a) What are the mathematical principles of symmetric key cryptography and show how they are applied in encryption and decryption? [7M]
b) Explain the introduction to Modern Symmetric Key Ciphers. [7M]
(OR)
4. a) Explain DES and different modes of operation in DES. State its advantages and disadvantages. [7M]
b) Describe AES and various operations used in its round function? [7M]

UNIT-III

5. a) Define the mathematics behind asymmetric key cryptography and list its key components? [7M]
b) Explain how asymmetric key cryptography works in detail. [7M]
(OR)
6. a) Perform decryption and encryption using RSA algorithm with $p=3, q=11, e=7, N=5$. [7M]
b) Explain RSA algorithm in detail. Identify the possible threats for RSA algorithm and list their counter measures? [7M]

UNIT-IV

7. a) Explain HASH function and its properties in cryptography. [7M]
b) Analyze digital signature algorithm? [7M]
(OR)
8. a) Explain the classes of message authentication function. [7M]
b) Differentiate between MAC and Hash function? [7M]

UNIT-V

9. a) Explain the operational description of PGP. [7M]
b) Describe a short note on S/MIME? [7M]
(OR)
10. a) Explain the architecture of IP security. [7M]
b) Describe a short notes on E-mail security? [7M]
