*R20 Regulation* *Subject code: 3E6GC*

# TKR COLLEGE OF ENGINEERING AND TECHNOLOGY

(Autonomous, Accredited by NAAC with 'A+' Grade)

**B.Tech VI Semester Supplementary Examinations, November 2025**

## CRYPTOGRAPHY

*(CSE(AI&ML))*

*Maximum Marks: 70* Date: 13.11.2025 Duration: 3 hours

**Note:** **1.This question paper contains two parts A and B.**
**2. Part A is compulsory which carries 20 marks. Answer all questions in Part A.**
**3. Part B consists of 5 Units. Answer any one full question from each unit.**
**4. Each question carries 10 marks and may have a, b, c, d as sub questions.**

Part-A

| | All the following questions carry equal marks (10X2M=20 Marks) | Marks | CO | BTL |
|---|---|---|---|---|
| 1 | Define Primality Test. | 2M | 1 | L1 |
| 2 | Specify the various types of authentication protocols? | 2M | 1 | L1 |
| 3 | Write about strength of DES algorithm. | 2M | 2 | L1 |
| 4 | What are the different modes of operation in DES? | 2M | 2 | L1 |
| 5 | What happens when two different messages are encrypted using the same keystream from a stream cipher? | 2M | 3 | L1 |
| 6 | Is LFSR asynchronous or synchronous? | 2M | 3 | L1 |
| 7 | State the Fermat's Theorem. | 2M | 4 | L1 |
| 8 | Define Primality Test. | 2M | 4 | L1 |
| 9 | Specify the various types of authentication protocols? | 2M | 5 | L1 |
| 10 | List out some hash algorithm. | 2M | 5 | L1 |

Part-B

| | Answer All the following questions. (5X10M=50Marks) | Marks | CO | BTL |
|---|---|---|---|---|
| 11 | a) Discuss briefly about Divisibility Algorithm with an example.<br>b) Compare Modular Arithmetic with Polynomial arithmetic. | 5M<br>5M | 1 | L2 |
| | OR | | | |
| 12 | Solve gcd (98, 56) using Extended Euclidean algorithm. Write the algorithm. | 10M | 1 | L2 |
| 13 | Define Caesar cipher and calculate the encryption and decryption for the following plain text P="COME TO MY HOME" by using caser cipher with Key k=3? | 10M | 2 | L2 |
| | OR | | | |
| 14 | a) Give an example to explain the concept of transposition ciphers in detail.<br>b) Compare and Contrast between Symmetric and Asymmetric key cryptography. | 5M<br>5M | 2 | L2 |
| 15 | Discuss in brief about Pseudo-Random-Sequence Generators with neat diagram. | 10M | 3 | L2 |
| | OR | | | |

| | | | | |
|---|---|---|---|---|
| 16 | Examine in brief about Linear Congruential Generators with neat diagram. | 10M | 3 | L2 |
| 17 | Discuss Elliptic Curve Cryptography in detail. | 10M | 4 | L2 |
| | OR | | | |
| 18 | Use Euler's theorem to find a number between 0 and 28 with congruent to 6 modulo 35. | 10M | 4 | L2 |
| 19 | a) What is the purpose of digital signature? Explain its properties and requirements.<br>b) Explain two different MACs based on block ciphers. | 5M<br>5M | 5 | L2 |
| | OR | | | |
| 20 | a) Explain the process involved in message digest generation and processing of single block in SHA-512.<br>b) What is Message Authentication code? Explain its functions and basic uses. | 5M<br>5M | 5 | L2 |