R20 Regulation *Subject code:3E6GC*

TKR COLLEGE OF ENGINEERING AND TECHNOLOGY

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

B.Tech VI Semester Supplementary Examinations, May 2025

CRYPTOGRAPHY

(CSE(AI&ML))

Maximum Marks: 70 Date: 23.06.2025 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	What is the number theory?	2M	1	L1
2	Find the number of trailing zeros in the 100!	2M	1	L1
3	Define Cipher Block Chaining (CBC) mode	2M	2	L1
4	Brief the strength of triple DES	2M	2	L1
5	What are the 2 main problems associated with pseudo random number generation?	2M	3	L1
6	What is stream cipher and pseudorandom functions?	2M	3	L1
7	State the Fermat's Theorem.	2M	4	L1
8	Define Primality Test.	2M	4	L1
9	List three approaches to Message Authentication.	2M	5	L1
10	What are the requirements of Authentication?	2M	5	L1

Part-B

Answer All the following questions. (5X10M=50Marks)		Marks	CO	BTL
11	Distinguish Groups, Rings and fields in detail.	10M	1	L2
	OR			
12	Solve gcd (98, 56) using Extended Euclidean algorithm. Write the algorithm.	10M	1	L2
13	Describe AES algorithm with all its round functions in detail.	10M	2	L2
	OR			
14	a) Explain the terminologies used in Encryption. b) What are the two basic functions used in encryption algorithms?	5M 5M	2	L2
15	a) Discuss in brief about Linear Congruential Generators with neat diagram. b) Elaborate the following: i)Linear Feedback Shift Registers ii) Design and analysis of stream ciphers	5M 5M	3	L2
	OR			

16	a) Discuss in brief about Pseudo-Random-Sequence Generators with neat diagram. b) Elaborate the following: i)RC 4 algorithm ii)Stream ciphers using LFSRs	5M 5M	3	L2
17	Discuss Elliptic Curve Cryptography in detail	10M	4	L2
	OR			
18	a) Explain the RSA algorithm. Compute cipher text for M=88, p=17 and q=11. b) Explain about the strength of RSA.	5M 5M	4	L2
19	a) What is message authentication? List the authentication requirements. b) Compare the principal characteristics of secure hash functions.	5M 5M	5	L2
	OR			
20	Describe the steps in message digest generation in Secure Hash Algorithm in detail.	10M	5	L2