R20 Regulation *Subject code:* **3E6GC**

TKR COLLEGE OF ENGINEERING AND TECHNOLOGY

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

B.Tech VI Semester Supplementary Examinations, December2024

CRYPTOGRAPHY

(CSE(AI&ML))

Maximum Marks: 70 Date:04.01.2025 Duration: 3 hours

	Part-A		
All the following questions carry equal marks	**(10X2M=20 Marks)**	CO	Bloom Tx
1	What are security mechanisms? Explain.	CO3	I
2	What is steganography?	CO3	I
3	Why Encryption is needed.	CO1	I
4	Write the operation of block cipher?	CO1	I
5	What are the advantages of stream cipher?	CO2	I
6	What is a linear congruential generator?	CO2	I
7	State Euler's theorem.	CO3,4	I
8	Define public key cryptosystem.	CO3,4	I
9	What are the requirements for message authentication?	CO5	I
10	How digital Signature differs from authentication protocols?	CO5	II
	Part-B		
Answer All the following questions.**(5X10M=50Marks)**			
11	a) List and briefly define categories of Security Services and attacks. [5M] b) How would you test a piece of cipher text to determine quickly if it was likely the result of a simple substitution? Explain. [5M]	CO3	III
	OR		
12	How is GCD calculated with Euclid's algorithm? Calculate the GCD of (270, 192). [10M]	CO3	IV
13	a) Summarize the public key cryptographic principles. Explain RSA algorithm for given example, where p = 3 and q = 11. [5M] b) Enumerate Diffie-Hellman Key exchange for encryption and decryption with suitable examples. [5M]	CO1	III
	OR		
14	Explain Fermat theorem and Euler's theorem with examples. [10M]	CO1	III
15	Stream ciphers work well for real time communication such as video streaming or online gaming. Discuss. Also add a note on the advantages and disadvantages of stream ciphers. [10M]	CO2	III
	OR		
16	Discuss the design and implementation of a 4-bit LFSR. [10M]	CO2	IV
17	a)Alice chooses 173 and 149 as two prime numbers and 3 as public key in RSA. Check whether the chosen prime numbers are valid or not? [5M]	CO3,4	IV

	b)Prove that Euler's Totient value of any prime number (p) is p-1 and the Euler's Totient value of the non-prime number (n) is (p-1) x (q-1) where p x q are prime factor of n. [5M]		
	OR		
18	a)Demonstrate the DH key exchange methodology using following key values: $p = 11$, $g = 2$, $X_A = 9$, $X_B = 4$. [6M] b)Diffie–Hellman key agreement is not limited to negotiating a key shared by only two participants. Any number of users can take part in an agreement by performing iterations of the agreement protocol and exchanging intermediate. Write the steps and formulas to be followed for DH key exchange between Alice, Bob, and Carol. [4M]	CO3,4	IV
19	Explain the MD5 processing of a single 512 bit block with suitable example and write its advantages. [10M]	CO5	III
	OR		
20	Discuss various Digital signatures and describe the digital signature algorithm and show how signing and verification is done using Digital signature standard. [10M]	CO5	III