R20 Regulation *Subject code: 3E6GC*

TKR COLLEGE OF ENGINEERING AND TECHNOLOGY

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

B.TechVI Semester Regular/Supplementary Examinations, July2024

CRYPTOGRAPHY

(CSE (AI & ML))

Maximum Marks: 70 Date:26.07.2024 Duration: 3 hours

Note:
1. **This question paper contains two parts A and B.**
2. **Part A is compulsory and carries 20 marks. Answer all questions in Part A.**
3. **Part B consists of 5 Units. Answer any one full question from each unit which carries 10M.**
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)		CO	Bloom Tx
1	Define field and ring in number theory.	CO1	I
2	Find GCD of (2740, 1760) using Euclidean Algorithm	CO1	III
3	List the entities that are to be kept secret in conventional encryption techniques.	CO2	I
4	Compare Substitution and Transposition techniques	CO2	II
5	Give the applications of pseudo random sequence generators.	CO3	I
6	List the properties of stream cipher.	CO3	I
7	Using Fermat's theorem, check whether 19 is prime or not? Consider 'a' as 7.	CO4	III
8	State the differences between private key and public key algorithm.	CO4	II
9	What is hash in cryptography?	CO5	I
10	State the requirements of digital signature.	CO5	I

Part-B

Answer All the following questions .(5X10M=50Marks)			
11	A. Demonstrate that the set of polynomials whose coefficients forms a field is a ring. [7M] B. In finite field arithmetic, $(x^6+x^4+x^2+x+1)+(x^7+x+1)=?$. [3M]	CO1	IV
	OR		
12	Discuss the properties that are to be satisfied by the Groups, Rings and Fields. [10M]	CO1	III
13	In the basic communication scenario there are two parties, A and B, who want to securely communicate with each other. A third party C is a potential eavesdropper. Classify the substitution techniques in which the message can be converted into an unintelligible format in such a way that C cannot read the message. [10M]	CO2	III
	OR		
14	Draw the functionality diagram (functionality in one round) of DES with number of bits in each flow of data. [10M]	CO2	III

15	What is stream cipher? Why LFSRs are used in stream ciphers and explain with examples? [10M]	CO2	IV
	OR		
16	Discuss the design and implementation of a 4-bit LFSR. [10M]	CO2	III
17	A Box contains gold coins. If the coins are equally divided among three friends, two coins are left over. If the coins are equally divided among five friends, three coins are left over. If the coins are equally divided among seven friends, two coins are left over. If the box holds smallest number of coins that meets these conditions, how many coins are there? (Use Chinese Remainder Theorem). [10M]	CO3,4	IV
	OR		
18	Discuss Diffie- Hellman key exchange algorithm in detail. [10M]	CO3,4	III
19	What is Hash algorithm and Compare the performance of MD5 algorithm and SHA-1 algorithm. [10M]	CO5	IV
	OR		
20	Explain the concepts of digital signature algorithm with key generation and verification in detail. [10M]	CO5	III