Register Number:……..

KUMARAGURU
college of technology
character is life

B.E./B.TECH. DEGREE EXAMINATIONS: APRIL / MAY 2023

(Regulation 2018)

Fourth Semester

COMMON TO ALL BRANCHES

U18CSR4012: Network Security and Cryptography

COURSE OUTCOMES

CO1: Analyze and select appropriate security mechanisms for designing various security services
CO2: Construct cryptographic algorithms from hard problems in mathematics
CO3: Identify appropriate algorithms for assuring message integrity and authentication
CO4: Discover how cryptographic algorithms are used to build network security protocols
CO5: Identify appropriate mechanisms for providing system security

Time: Three Hours **Maximum Marks: 100**

Answer all the Questions:-
PART A (10 x 2 = 20 Marks)
(Answer not more than 40 words)

1.	Outline the type of attacks possible on encrypted messages.	CO1	[K_2]
2.	Relate the terms: Security Attacks, Mechanisms and Services.	CO1	[K_2]
3.	Summarize the applications of Public-Key Cryptosystems.	CO2	[K_2]
4.	Illustrate the steps of Diffie-Hellman key exchange algorithm.	CO2	[K_2]
5.	Interpret the requirements that must be met by authentication.	CO3	[K_2]
6.	Classify the 3 different approaches to Message Authentication.	CO3	[K_2]
7.	Why is PGP popular?	CO4	[K_1]
8.	List out the functions in S/MIME.	CO4	[K_2]
9.	What is meant by non-malicious program errors?	CO5	[K_1]
10.	Define firewall and why do we need it uses.	CO5	[K_2]

Answer any FIVE Questions:-
PART B (5 x 16 = 80 Marks)
(Answer not more than 400 words)

11.		Illustrate the operation of AES algorithm, by clearly depicting all the intermediate stages.	16	CO1	[K_2]
12.	a)	Demonstrate the principle of Elliptic curve cryptography.	8	CO2	[K_2]
	b)	Explain RSA algorithm with an example and test for primality.	8	CO2	[K_2]

13.	a)	Explain HMAC algorithm with a relevant diagrams.	12	CO3	[K_2]
	b)	What are the advantages of HMAC?	4	CO3	[K_2]
14.		Illustrate how the messages are generated and received by PGP.	16	CO4	[K_2]
15.	a)	Outline the role of Intrusion detection system in securing networks.	6	CO5	[K_2]
	b)	Explain about types of firewall interms if system security.	10	CO5	[K_2]
16.		Summarize the requirements of digital signature and also discuss how digital signatures can be produced and verified.	16	CO3	[K_2]