KUMARAGURU
college of technology
character is life

B.E/B.TECH DEGREE EXAMINATIONS: NOV /DEC 2024

(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.	Construct a Playfair matrix with the key occurrence. Make a reasonable assumption about how to treat redundant letters in the key.	CO1	[K2]
2.	What is meant by non-repudiation?	CO1	[K1]
3.	How to find the multiplicative inverse of a number?	CO2	[K2]
4.	State the Euler's totient function. Mention its uses.	CO2	[K1]
5.	What are the requirements of the hash function?	CO3	[K1]
6.	How is HMAC code generated?	CO3	[K1]
7.	Explain the function of S/MIME.	CO4	[K1]
8.	Give the significance of Kerberos	CO4	[K1]
9.	What is meant by non-malicious program errors?	CO5	[K1]
10.	Define password protection.	CO5	[K1]

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

11.	a)	Discuss in detail about DES encryption algorithm and the key distribution	10	CO1	[K2]
	b)	Summarize on the various Attacks, Services and Mechanisms in cryptography	6	CO1	[K2]
12.	a)	Explain RSA algorithm with an example	8	CO2	[K2]
	b)	Describe the steps involved in Diffie-Hellman algorithm with an example	8	CO2	[K2]
13.		Enumerate on the different stages in the AES algorithm with neat sketches.	16	CO1	[K2]
14.	a)	Explain how problems related to digital signatures can be taken care of using an arbiter.	8	CO3	[K2]
	b)	Explain how hash functions are used in authentication using SHA-1 algorithm	8	CO3	[K2]
15.		Describe the PGP message generation process	16	CO4	[K2]
16.		Enumerate the need for using firewalls and explain the types of firewalls	16	CO5	[K2]

****