Register Number:……..

KUMARAGURU
college of technology
character is life

B.TECH DEGREE EXAMINATIONS: NOV/DEC 2023

(Regulation 2018)

Fifth Semester

INFORMATION TECHNOLOGY

U18ITT5002: Cryptography and Network Security

COURSE OUTCOMES

CO1: Explain security attacks and issues in computer systems and networks.
CO2: Apply the mathematics symmetric and asymmetric algorithms related to cryptography
CO3: Explain the purpose and working of authentication and system level security algorithms
CO4: Apply the appropriate security mechanism for different computing environment
CO5: Apply appropriate security methods to solve real life applications

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

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

1.	Find the shift row transformation used in AES for the following matrix. 45 3E 82 21 A7 59 94 4D 3A 1B 28 73 3F 2C 54 62	CO1	[K_3]
2.	Decrypt the following text using rail fence technique. sdioduaslanyhiy	CO1	[K_3]
3.	What is 'Meet-in-the-middle' attack?	CO2	[K_2]
4.	State Fermat's and Euler's theorem.	CO2	[K_2]
5.	List out the properties of digital signature.	CO3	[K_2]
6.	Specify the requirements for message authentication.	CO3	[K_2]
7.	Draw the X.509 certificate Format.	CO4	[K_2]
8.	Give the limitations of SMTP schemes in electronic mail security.	CO4	[K_2]
9.	How is honeypot used in intrusion detection?	CO5	[K_2]
10.	Define Biometric Authentication.	CO5	[K_2]

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

11.	a)	Give the detailed explanation about DES encryption algorithm.	12	CO1	[K_2]
	b)	Using playfair cipher i) Generate a key matrix using the keyword "DIAMOND" ii) encrypt the message "BIRMINGHAM"	4	CO1	[K_3]
12.	a)	Outline the concepts of digital signature algorithm with key generation and verification in detail.	10	CO3	[K_2]
	b)	Perform encryption and decryption using RSA algorithm with p=11, q=13, e=11, M=7.	6	CO2	[K_3]
13.	a)	Explain the concepts of SHA-1 in detail with their compression function.	10	CO3	[K_2]
	b)	Consider a Diffie Hellman scheme with the common prime q=23 and primitive root $\alpha = 9$ (1) If user A has private key $X_A = 4$, what is A's public key Y_A? (2) If user B has private key $X_B = 3$, what is B's public key Y_B? (3) What is the shared secret key K?	6	CO2	[K_3]
14.		How the authentication is ensured using Kerberos? Explain in detail about the dialogue exchanges between server and workstation.	16	CO4	[K_2]
15.		How does PGP provide confidentiality and authentication service for e-mail and storage applications? Draw the block diagram and explain its components.	16	CO4	[K_2]
16.		What is a firewall? Explain about different types of firewalls with its merits and demerits.	16	CO5	[K_2]

****