Register Number:……..

KUMARAGURU
college of technology
character is life

B.E DEGREE EXAMINATIONS: NOV/DEC 2023

(Regulation 2018)

Seventh Semester

ELECTRONICS AND COMMUNICATION ENGINEERING

U18ECE0023: Network security

COURSE OUTCOMES

CO1: Apply block cipher and stream cipher algorithms.
CO2: Employ Public key cryptographic techniques.
CO3: Explain the authentication and hash algorithms.
CO4: Analyze the digital signature concepts and applications.
CO5: Apply the Network and System level security measures.

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

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

1.	Differentiate cryptography and cryptanalysis	CO1	[K_2]
2.	State the significance of S box and P box in cipher design.	CO1	[K_2]
3.	What is the main problem with the asymmetric encryption?	CO2	[K_2]
4.	Why ECC is more secure than RSA?Justify	CO2	[K_2]
5.	Mention the requirements of MAC functions.	CO3	[K_1]
6.	Differentiate SHA 256 and RIPEMD-160.	CO3	[K_2]
7.	How can electronic signatures benefit organizations?	CO4	[K_2]
8.	A digital signature is a mathematical technique which validates the authenticity, non-repudiation and integrity of a message.T/F	CO4	[K_1]
9.	List the features of Encapsulating Security Payload (ESP)	CO5	[K_1]
10.	Compare worm and virus.	CO5	[K_2]

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

11.	a)	Summarize the security attaches and services defined by OSI security architecture.	8	CO1	[K_2]

	b)	Using Hill cipher, perform encryption and decryption: plain-text : 'ACT' (n = 3),Key $\begin{bmatrix} 1 & 2 \\ 3 & 4 \end{bmatrix}$: Analyse its security strength.	8	CO1	[K_3]
12.	a)	What requirements must a public key cryptosystems fulfill to be a secure algorithm? In an RSA system, the public key of a given user is e=5, n=35. Find the plaintext if the cipher text intercepted is C=100.	8	CO2	[K_3]
	b)	In the Diffie-Hellman protocol a=7,p=23,X_A=3,X_B=5 .a) What is the value of the symmetric key? b) What is the value of Y_A ad Y_B? c) What happens if X_A and X_B have the same value? Comment on the security strength of Diffie – Hellman proltocol.	8	CO2	[K_3]
13.	a)	Describe the three main concerns with the use of passwords for authentication. Enumerate the security requirements and properties of Hash function	8	CO3	[K_3]
	b)	Illustrate the requirements, functions and properties of MAC.	8	CO3	[K_3]
14.	a)	What is a digital signature? Explain the role of certifying authority (CA) with suitable example.	8	CO4	[K_2]
	b)	Explain the working on The ElGamal Signature Schemes and compare with Schnorr scheme.	8	CO4	[K_3]
15.	a)	Explain the salient features of Secure Electronic Transaction (SET) with neat block diagram.	8	CO5	[K_2]
	b)	Outline three design goals for a firewall and explain any one type firewall used to control access and enforce a security policy.	8	CO5	[K_3]
16.	a)	For each of the following elements of DES, indicate the comparable elements in AES or explain why it is not needed in AES.(a) XOR of the subkey material with the input of the f function.(b) XOR of the f function output with the left half of the block.(c) The f function.(d) Permutation P.(e) Swapping of halves of the block. Which of these elements of the algorithm accomplish confusion and diffusion?	8	CO1	[K_4]
	b)	In IPSec, what parameters identify a security Association and what parameters characterize the nature of a particular security association? Discuss how IPsec can be used to provide both confidentiality and authentication.	8	CO5	[K_2]

****