Register Number:……………..

KUMARAGURU
college of technology
character is life

B.E DEGREE EXAMINATIONS: NOV/DEC 2024

(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. Apply Caesar cipher with key of 5 to encrypt the Plain text "Security". CO1 [K_3]

2. Compare the block cipher and stream cipher. CO1 [K_3]

3. Determine the Euler's Totient function φ (21). CO2 [K_3]

4. List the salient features of elliptic curve cryptography. CO2 [K_2]

5. Distinguish between MAC and Hash functions CO3 [K_2]

6. Classify the attacks possible on Message authentication codes. CO3 [K_2]

7. List the various applications of digital Signature. CO4 [K_2]

8. Compare one way and mutual authentication CO4 [K_2]

9. Interpret the key components involved in a secure electronic transaction. CO5 [K_2]

10. Specify the different types of viruses. CO5 [K_1]

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

11. a) Illustrate the various security attacks and security services defined in OSI architecture standard X.800. 10 CO1 [K_2]

b) Using the keyword "Assessment" encrypt the message "NETWORK SECURITY" using PlayFair cipher technique. 6 CO1 [K_3]

12.		Elaborate the various asymmetric encryption algorithms widely used in data protection. Discuss the process of generation of a RSA key pair generation, encryption and decryption algorithms. Using RSA algorithm encrypt the message M = 5 for the values of p = 3, q = 11, e = 7.	16	CO2	[K$_3$]
13.	a)	Prioritize the requirements for a Hash function. Explain the various ways in which Hash code can be used to provide authentication	8	CO3	[K$_2$]
	b)	Explain in detail about Hash-based Message Authentication Code (HMAC)	8	CO3	[K$_2$]
14.	a)	Elaborate the signature creation and verification scheme in Digital Signature Standard with neat diagrams	8	CO4	[K$_2$]
	b)	Outline the working principle of Elagmal and compare with schnorr protocol	8	CO4	[K$_2$]
15.		A network administrator wants to provide a secure internal network for an e-commerce company handling sensitive customer data. Justify the use of firewall for establishing a secure network and discuss its types and functions in detail.	16	CO5	[K$_3$]
16.	a)	Illustrate the concept of Data Encryption Standard with neat diagram elaborating on the functionalities of fiestal structure used in single round.	8	CO1	[K$_2$]
	b)	Summarize the various key distribution methods and elaborate any one scheme in detail.	8	CO2	[K$_2$]

****