Register No : _____

THE KAVERY ENGINEERING COLLEGE

(An Autonomous Institution)

B.E/B.TECH DEGREE END SEMESTER THEORY EXAMINATIONS, NOV/DEC 2025

Fifth Semester

Computer Science and Engineering

CB3491 - Cryptography and Cybersecurity

Regulations - 2021

Duration : 3 Hrs *Maximum : 100 Marks*

*PART – A (ANSWER ALL QUESTIONS) (Marks 10*2=20)*

Q.No	*Questions*	*BLT*	*CO*	*Marks*
1.	Define computer security and its importance in today's digital world.	L1	1	2
2.	Summarize the foundations of modern cryptography.	L2	1	2
3.	What is the Euclidean algorithm and how is it applied in cryptography?	L1	2	2
4.	Compare differential and linear cryptanalysis in the context of block ciphers.	L2	2	2
5.	State Euler's totient function and its importance in cryptography.	L2	3	2
6.	What is elliptic curve cryptography?	L1	3	2
7.	Define a Message Authentication Code (MAC) and its purpose.	L1	4	2
8.	How do biometrics enhance entity authentication?	L1	4	2
9.	Describe the method of password cracking and its implications for security.	L2	5	2
10.	What are the primary challenges associated with web security?	L1	5	2

*PART – B (ANSWER ALL QUESTIONS) (Marks 5*16 = 80)*

Q.No			*Questions*	*BLT*	*CO*	*Marks*
11.	a	i	Explain the key concepts of "Security Services" and "Security Mechanisms" in the context of computer security.	L2	1	8
		ii	Discuss the OSI Security Architecture and its relevance to modern network security.	L2	1	8
			Or			
	b	i	Explain the concepts of substitution techniques and transposition techniques in classical encryption. Provide examples of each technique.	L2	1	8
		ii	Define steganography and discuss its role in data security.	L2	1	8
12.	a		Describe the structure and functioning of the Data Encryption Standard (DES).	L2	2	16
			Or			
	b		Explain the importance of key distribution in symmetric key ciphers and describe the main methods used for key distribution.	L2	2	16
13.	a		Provide a step-by-step example of how you would apply Chinese Remainder Theorem to improve the efficiency of decryption operations in RSA.	L3	3	16
			Or			

	b	Utilize the Diffie-Hellman key exchange method in the following context: i. Plan the steps Carol and David should take to securely establish a shared secret key, including the selection of public parameters and the calculation of their private and public keys. ii. Experiment with identifying vulnerabilities in the Diffie-Hellman process and propose solutions to mitigate these risks.	L3	3	16
14.	a	Plan the steps required for generating and verifying a digital signature for a document, including the role of hash functions in the process. Use an example to illustrate your explanation.	L3	4	16
		Or			
	b	Construct a model that illustrates how public and private keys will be used to securely distribute symmetric keys.	L3	4	16
15.	a	Classify cybercrimes and discuss at least three different types of cyber-attacks, including their impact and examples.	L2	5	16
		Or			
	b	Describe security measures that organizations can implement to protect against cyber threats focusing on cloud security and web security.	L2	5	16