Register No : _____

THE KAVERY ENGINEERING COLLEGE

(An Autonomous Institution)

B.E/B.TECH DEGREE END SEMESTER THEORY EXAMINATIONS, NOV /DEC 2024

Fifth Semester

Artificial Intelligence and Data Science

CW3551 - Data and Information Security

Regulations - 2021

Duration : 3 Hrs *Maximum : 100 Marks*

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

Q.No	*Questions*	*BLT*	*CO*	*Marks*
1.	What is information security?	RE	1	2
2.	Give the critical characteristics of information.	RE	1	2
3.	Why is security essential in information systems?	RE	2	2
4.	What is the function of an access control matrix?	UN	2	2
5.	Define digital signature.	RE	3	2
6.	Define Kerberos, and what does it provide.	RE	3	2
7.	What is the primary purpose of PGP in email security?	UN	4	2
8.	What does S/MIME stand for, and what is its role in email security?	RE	4	2
9.	State the primary requirements for web security.	UN	5	2
10.	Explain the primary function of SSL.	UN	5	2

*PART – B (ANSWER ALL QUESTIONS) (Marks 5*13 = 65)*

Q.No			*Questions*	*BLT*	*CO*	*Marks*
11.	a	i	Analyze how the three critical characteristics interact with each other in a secure information system.	AN	1	7
		ii	Analyze the consequences of a failure in one of these characteristics.	AN	1	6
			Or			
	b		Illustrate briefly about SDLC methodology and analyze its relation in respect to information security.	AN	1	13
12.	a	i	Describe the fundamental reasons for the need for security in business and computing environments.	UN	2	7
		ii	List and explain key elements in the overview of computer security.	UN	2	6
			Or			
	b		Apply the concept of the access control matrix to a business scenario involving internal threats and attacks. Explain how you would implement the matrix to mitigate these risks and protect sensitive data.	UN	2	13

13.	a	Analyze the concept of digital signatures and explain the different digital signature schemes and their variants. Provide examples for the same.	AN	3	13
		Or			
	b i	Analyze the role of authentication protocols in maintaining secure communication in distributed systems.	AN	3	7
	ii	Discuss potential vulnerabilities and weaknesses in protocols such as Kerberos or X.509.	AN	3	6
14.	a	Analyze the operational description of PGP in email security, focusing on its key management and trust model also explain what a security association is in IPSec.	AN	4	13
		Or			
	b	Analyze the roles of the ESP and AH protocols in IPSec. Also discuss the advantages and disadvantages of each protocol.	AN	4	13
15.	a	Describe the SSL architecture in detail and analyze how it helps in maintaining secure end-to-end Communication.	AN	5	13
		Or			
	b	Analyze a secure online payment system for a business by integrating both SSL and SET protocols. Explain how SSL will handle secure communication, and how SET will ensure the secure processing of electronic transactions, including DS verification.	AN	5	13

*PART – C (Marks 1*15 = 15)*

Q.No		*Questions*	*BLT*	*CO*	*Marks*
16.	a	Analyze the relationship between confidentiality, integrity, and availability in ensuring the security of information and create a scenario where these characteristics are compromised and propose a security framework to mitigate such risks.	CR	1	15
		Or			
	b	Create a secure communication system for an organization using both S/MIME for email security and IPSec for securing network traffic. Provide a step-by-step explanation of how these two protocols will work together to ensure confidentiality, integrity, and authentication.	CR	4	15