Register No : _____

THE KAVERY ENGINEERING COLLEGE

(An Autonomous Institution)

UG/PG DEGREE END SEMESTER THEORY EXAMINATIONS, APRIL/MAY 2026

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*	*BTL*	*CO*	*Marks*
1.	Define Information Security.	L1	1	2
2.	List any two critical characteristics of information.	L2	1	2
3.	Define Access Control Matrix in computer security.	L1	2	2
4.	List any two legal or ethical issues related to computer security.	L2	2	2
5.	List any two requirements of an authentication system.	L2	3	2
6.	What is the use of Kerberos?	L1	3	2
7.	State any two functions of Security Association in IPsec.	L2	4	2
8.	Expand S/MIME and mention its primary use.	L1	4	2
9.	What is the primary function of the Secure Sockets Layer (SSL)?	L1	5	2
10.	Differentiate between SSL and Transport Layer Security.	L2	5	2

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

Q.No		*Questions*	*BLT*	*CO*	*Marks*
11.	a	Explain the NSTISSC Security Model and also describe how it supports confidentiality, integrity, and availability in an information system.	L2	1	16
		Or			
	b	Explain the steps of the Security SDLC and evaluate how it helps in balancing security and access during the development of an information system.	L2	1	16
12.	a	Explain various types of security policies (security, confidentiality, integrity, and hybrid) and analyze their role in protecting information assets.	L2	2	16
		Or			
	b i	Discuss the need for security in business organizations.	L2	2	8
	ii	Explain how different types of threats and attacks can impact business operations.	L3	2	8

13.	a	i	Explain the working mechanism of a Digital Signature Scheme with a neat diagram.	L3	3	8
		ii	Compare different Digital Signature Standards and analyze their security features.	L3	3	8
			Or			
	b	i	Evaluate the role of Kerberos in providing secure authentication in a networked environment.	L4	3	8
		ii	Design an authentication protocol using *X.509* Directory Services and justify its advantages over traditional methods.	L4	3	8
14.	a	i	Explain the architecture and operational steps of PGP in securing electronic mail with a neat diagram.	L2	4	8
		ii	Analyze the IPsec architecture, describing how ESP and AH protocols work together to provide confidentiality, integrity, and authentication.	L4	4	8
			Or			
	b	i	Evaluate the effectiveness of key management and trust models in S/MIME and PGP, highlighting their advantages and limitations.	L5	4	8
		ii	Design a secure e-mail system using IPsec modes (Transport and Tunnel) and justify the choice of protocols and key-management techniques.	L4	4	8
15.	a	i	Describe the objectives and layers of SSL.	L3	5	8
		ii	Explain how SSL provides secure communication over the web.	L3	5	8
			Or			
	b		Evaluate the components and processing steps of a Secure Electronic Transaction (SET), highlighting the role of DS verification.	L5	5	16