Register No : _____

THE KAVERY ENGINEERING COLLEGE

(An Autonomous Institution)

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

Fifth Semester

Computer Science and Engineering

CB3491 – CRYPTOGRAPHY AND CYBER 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.	Distinguish between attack and threat.	U	1	2
2.	Define Steganography.	R	1	2
3.	Find GCD (1970,1066) using Euclid's Algorithm.	U	2	2
4.	Compare Block cipher and Stream cipher.	U	2	2
5.	State Fermat's little theorem.	R	3	2
6.	Compare public key and private key.	U	3	2
7.	Define the term Message Digest.	R	4	2
8.	Identify 4 requirements defined by Kerberos.	U	4	2
9.	Define Cybercrime.	R	5	2
10.	List the key principles and practices of cloud security.	R	5	2

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

Q.No			*Questions*	*BLT*	*CO*	*Marks*
11.	a		Explain about OSI Architure model with suitable example.	U	1	16
			Or			
	b		Discuss the rules to be followed in Playfair method. Encrypt the word "Networksecurity" with the keyword "cypto" using Playfair method.	U	1	16
12.	a		Explain the overall structure and round structure of DES with neat sketch.	U	2	16
			Or			
	b		Explain Block cipher mode of operation with neat sketch.	U	2	16
13.	a		Perform encryption and decryption using RSA algorithm for the following: p=7 q=11, e=7, M=9.	AP	3	16
			Or			
	b		Find the secret key shared between user A and user B using Diffie- Hellman algorithm for the following q=353; α (primitive root)=3, XA=45 and XB=50	AP	3	16
14.	a		Create the process of deriving eighty 64-bit words from 1024 bits for processing Of a single blocks and also discuss single round function in SHA-512 algorithm. Show the values of W16, W17, W18 and W19. (15)	CR	4	16
			Or			
	b	i	Elaborate the way how the limitations of Kerberos version 4 is overcome in the environmental shortcomings and technical deficiencies.	CR	4	8
		ii	Elaborate how the encryption is key generated from password in Kerberos.	CR	4	8
15.	a		Discuss the security risk associated with public key Wi-Fi networks and the best practices for ensuring the wireless security on personal devices.	U	5	16
			Or			
	b		Describe how spyware functions and its impact on privacy and data security. What steps can individuals and organizations take to detect and prevent spyware infections?	U	5	16