Register No : _____

THE KAVERY ENGINEERING COLLEGE

(An Autonomous Institution)

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

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.	Differentiate interruption and interception based on their characteristics.	AN	1	2
2.	Define threat.	RE	1	2
3.	List any four operating modes of block cipher.	RE	2	2
4.	Indicate the need for Avalanche effect in block cipher.	UN	2	2
5.	Check whether 2 is a primitive root of mod 5 & 4 is a primitive root of mod 5.	AN	3	2
6.	Define man-in-the-middle attack.	RE	3	2
7.	Compare MAC and Hash function based on their characteristics.	AN	4	2
8.	Identify the entities that constitute a full service in Kerberos environment.	UN	4	2
9.	Define keylogger.	RE	5	2
10.	Write down any four security considerations used for web security.	UE	5	2

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

Q.No			*Questions*	*BLT*	*CO*	*Marks*
11.	a	i	Explain OSI security architecture model with neat diagram.	UN	1	7
		ii	Encrypt the message “this is an exercise” using additive cipher with key = 20. Ignore the space between words. Decrypt the message to get the original plaintext.	AP	1	6
			Or			
	b	i	Illustrate the network security model and its important parameters with a neat block diagram.	UN	1	7
		ii	Encrypt the word “Network security” with the keyword “crypto” using play fair method.	AP	1	6
12.	a	i	Explain the key generation, encryption and decryption of SDES algorithm in detail.	UN	2	8
		ii	Specify how Triple –DES enhances the data protection with its large key size.	AN	2	5
			Or			

	b	i	Diagrammatically illustrate the structure of AES and describe the steps in AES encryption process with example.	UN	2	8
		ii	Assess whether the set of residue classes (mod 3) form a group or not.	AN	2	5
13.	a		Use Chinese remainder theorem and find X for the given set of congruent equations using CRT X = 2 (mod 3) X = 3 (mod 5) X = 2 (mod 7)	AP	3	13
			Or			
	b		Apply RSA algorithm, perform encryption and decryption to the system with p=7, q=11, e=17, M=8.	AP	3	13
14.	a	i	Suggest and explain about an authentication scheme for mutual authentication between the user and the server which relies on symmetric encryption.	AP	4	9
		ii	Show how SHA is more secure than MD5.	AN	4	4
			Or			
	b	i	With neat diagram specify the certificate parameters of X.509 and show how it is helpful in key distribution of public keys in a secure way.	AP	4	9
		ii	Analyze how digital signatures differ from authenticator protocols.	AN	4	4
15.	a		Describe in detail about the classification of cybercrimes.	UN	5	13
			Or			
	b		Explain in detail about the password cracking and types of attacks in password cracking.	UN	5	13

*PART – C (Marks 1*15 = 15)*

Q.No			*Questions*	*BLT*	*CO*	*Marks*
16.	a	i	Explain the following in detail: a) Linear cryptanalysis b) Differential cryptanalysis	UN	2	8
		ii	Solve GCD (98,56) using extended Euclidean algorithm. Also, write the algorithm.	AP	2	7
			Or			
	b	i	With a neat sketch explain the elliptic curve cryptography with an example.	UN	3	8
		ii	Users Alice and Bob use the Diffie-Hellman key exchange technique with a common prime q=83 and a primitive root α=5. a) If Alice has a private key XA=6, what is Alice‟s public key YA? b) If Bob has a private key XB=10, what is Bob‟s public key YB? c) Compute the shared secret key.	AP	3	7