

THE KAVERY ENGINEERING COLLEGE*(An Autonomous Institution)***B.E/B.TECH DEGREE END SEMESTER THEORY EXAMINATIONS, APRIL-MAY 2025***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.	Define computer security.	L1	1	2
2.	Differentiate between substitution and transposition techniques.	L2	1	2
3.	What is modular arithmetic?	L1	2	2
4.	Compare block cipher and stream cipher.	L2	2	2
5.	Find the remainder when 7^{23} is divided by 11 using Fermat's little theorem.	L1	3	2
6.	Explain data encryption standard.	L2	3	2
7.	List any two authentication protocols.	L1	4	2
8.	Differentiate between HMAC and CMAC.	L2	4	2
9.	Define cyber crime.	L1	5	2
10.	Explain SQL injection with an example.	L2	5	2

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

Q.No	Questions	BLT	CO	Marks
11.	a Apply the OSI Security Architecture model to explain how it addresses different security services and mechanisms.	L3	1	16
	Or			
	b Demonstrate classical encryption techniques with symmetric cipher model.	L3	1	16
12.	a Explain the overall structure and round structure of DES with neat sketch and write its strengths and weaknesses.	L2	2	16
	Or			
	b i Discuss the use of pseudorandom number generators in symmetric key cryptography.	L2	2	8
	i Explain about RC4 algorithm.	L2	2	8

- | | | | | | |
|-----|---|---|----|---|----|
| 13. | a | Analyze the working of RSA algorithm with an example. Show key generation, encryption, and decryption steps. | L4 | 3 | 16 |
| | | Or | | | |
| | b | Examine the role of elliptic curve arithmetic in enhancing security in modern cryptographic systems. | L4 | 3 | 16 |
| 14. | a | Describe the working of digital signature schemes like DSS and ElGamal. | L2 | 4 | 16 |
| | | Or | | | |
| | b | Discuss mutual trust and the use of X.509 certificates in public key infrastructure. | L2 | 4 | 16 |
| 15. | a | Assess the importance of web, wireless, and cloud security in today's digital world. | L5 | 5 | 16 |
| | | Or | | | |
| | b | Critically evaluate various tools and methods used in cybercrimes like key loggers, spyware, and password cracking tools. | L5 | 5 | 16 |