Roll No. □□□□□□□□□□

ANNA UNIVERSITY :: CHENNAI

B.E(FT) END SEMESTER EXAMINATIONS–DEC/JAN 2025

Computer Science and Engineering
Seventh Semester
CS6008-. CRYPTOGRAPHY AND NETWORK SECURITY
(Regulation 2018-RUSA)

COURSE OUTCOMES:
CO1: Present the exploitation present in the security.
CO2: Discuss various types of attacks and their characteristics.
CO3: Illustrate the basic concept of encryption and decryption for secure data transmission.
CO4: Develop solutions for security problems.
CO5: Analyze various cryptography techniques and its applications

Bloom's Taxonomy Level:
L1-Remember, L2-Understand, L3-Apply, L4-Analyze, L5-Evaluate, L6-Create

	PART - A (10 x 2 = 20 Marks) **(Answer All Questions)**	**CO**	**BL**
1.	What assembly constructs might indicate the presence of a constant table (e.g., S-box or key schedule) in cryptographic code?	CO1	L1
2.	Why is secure memory allocation important in cryptography?	CO1	L1
3.	How can buffer overflows affect cryptographic security?	CO2	L1
4.	What is the primary cause of format string vulnerabilities?	CO2	L1
5.	Define SQL Injection.	CO3	L1
6.	What are the three main types of ELF file headers?	CO3	L1
7.	What is the primary purpose of hashing in data security?	CO4	L1
8.	How does fuzzing help in identifying software vulnerabilities?	CO4	L1
9.	Why is key management important in cryptography?	CO5	L1
10.	What is a block cipher?	CO5	L1

	PART – B (8 x 8 = 64 marks) **(Answer any 8 questions)**	**CO**	**BL**
11.	Explain the key features of GDB that make it useful for reverse engineering cryptographic algorithms.	CO1	L4
12.	Describe how shellcode can be injected into a cryptographic application. What precautions can be taken to prevent such injections?	CO1	L4
13.	Describe the fundamental concepts of Return-Oriented Programming and how it can be used to bypass security mechanisms in cryptographic applications.	CO2	L3
14.	Explain how attackers use port scanning to bypass encryption or authentication mechanisms.	CO2	L3
15.	Discuss the importance of Discrete Logarithms in public-key cryptography.	CO3	L4
16.	Discuss the concept of a field extension in the context of finite fields. How is this concept applied to enhance security in cryptographic protocols?	CO3	L3
17.	Explain the concept of modes of operation in block ciphers. Why are they necessary in modern cryptography?	CO4	L3
18.	Explain how a MAC is used to verify both the integrity and authenticity of a message	CO4	L3
19.	Explain the concept of a certificate authority (CA) in the context of digital signatures. How does a CA contribute to the trustworthiness of digital signatures?	CO4	L4
20.	Discuss the importance of key management in PKI systems. What strategies are employed to protect private keys and ensure their secure use?	CO5	L3
21.	Explain how the Greatest Common Divisors (GCD) is related to the security of cryptographic systems, particularly in the context of algorithms like RSA or ECC.	CO3	L4
22.	Explain the Chinese Remainder Theorem (CRT) and discuss its importance in modern cryptographic systems.	CO3	L3

	PART–C(2x8=16marks) **Answer All Questions**	**CO**	**BL**
23.	Compare RSA encryption to other cryptographic algorithms, such as elliptic curve cryptography (ECC).. What are the advantages and disadvantages of using RSA in modern cryptography, and in what situations might it be more or less appropriate?	CO4	L5
24.	Consider the field $GF(2^4)$, with $P(x) = x^4 + x + 1$ being the irreducible polynomial. Find the inverses of $A(x) = x$ and $B(x) = x^2 + x$.	CO3	L3