

Reg. No. :

--	--	--	--	--	--	--	--	--	--	--	--	--	--	--

Question Paper Code : 90374

B.E./B.Tech. DEGREE EXAMINATIONS, APRIL/MAY 2025.

Fifth Semester

Computer Science and Engineering

CB 3491 – CRYPTOGRAPHY AND CYBER SECURITY

(Common to : Computer Science and Engineering (Artificial Intelligence and Machine Learning)/Computer and Communication Engineering)

(Regulations 2021)

Time : Three hours

Maximum : 100 marks

Answer ALL questions.

PART A — (10 × 2 = 20 marks)

1. Mention the significance of Steganography.
2. What is Cryptanalysis?
3. List the advantages of Euclid's algorithm.
4. How can algebraic structures be exploited to design efficient and secure cryptographic protocols?
5. Mention the properties of Euler's totient function.
6. List the most recent applications of Elliptic Curve Arithmetic.
7. Define MAC.
8. Mention the key components of an X.509 certificate.
9. Mention the types of SQL injection attacks.
10. Narrate the key measures to be implemented to ensure Wireless Security.

PART B — (5 × 13 = 65 marks)

11. (a) Demonstrate the role of the OSI Security Architecture in providing a systematic approach for securing network communications.

Or

- (b) Illustrate the various Classical Encryption techniques with examples.

12. (a) Describe the way the Feistel network structure contributes to the security of DES.

Or

- (b) Describe the row shifting and column mixing design, key generation and working of AES.

13. (a) Describe the working of RSA algorithm with an illustration on possible ways to attack it.

Or

- (b) Describe the process of key distribution and management in Asymmetric ciphers with example.

14. (a) Consider a large-scale e-commerce platform that processes millions of transactions daily. The platform employs digital signatures to ensure authenticity, integrity, and non-repudiation of these transactions. Discuss the specific scenarios within the e-commerce platform where digital signatures can be applied, their potential benefits in these contexts, including reduced fraud, increased trust, and streamlined processes.

Deliberate the possible use of common digital signature algorithms, their core principles, security challenges and possible countermeasures.

Or

- (b) Explain the basic architecture of a Kerberos system, including authentication process, roles of the Key Distribution Center (KDC), Authentication Server (AS), and Ticket Granting Server (TGS).

15. (a) Describe the motivation, impact and classification of Cyber Crimes.

Or

- (b) Describe the key components, types and implementation of a NAC system.

PART C — (1 × 15 = 15 marks)

16. (a) Consider a hash function H that is widely used in various cryptographic applications. Suppose a malicious attacker discovers a collision for H , i.e., two distinct inputs x and y such that $H(x) = H(y)$.

Demonstrate the possibility of this collision being exploited to compromise the security of a cryptographic system that relies on H , and highlight the possible countermeasures to mitigate such attacks.

Or

- (b) You are tasked with designing a secure communication system for a small organization using ElGamal cryptosystem, which relies on the difficulty of the discrete logarithm problem. Choose a suitable finite field F_p and a primitive root g for the system demonstrating the factors to consider when selecting these parameters and the process involved in generation of public and private keys.
-

