

Reg. No. :

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

Question Paper Code : 80386

B.E./B.Tech. DEGREE EXAMINATIONS, NOVEMBER/DECEMBER 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 — ($10 \times 2 = 20$ marks)

1. Differentiate between Authentication and Access Control.
2. List the steps in Cryptanalysis.
3. What conditions must be met for two matrices to be considered congruent?
4. Mention the mathematical principles upon which the correctness of Euclid's algorithm relies on.
5. State the Chinese Remainder Theorem and its significance in cryptography.
6. Define primitive root with an example.
7. What are the requirements of a digital signature.
8. Define collision.
9. What is a Spyware?
10. Mention the need for network access control.

PART B — ($5 \times 13 = 65$ marks)

11. (a) Describe the working, strengths and weaknesses of substitution encryption techniques.

Or

- (b) Illustrate the significance of the "Defense in Depth" strategy within the network security model and the distinct layers of security that contribute to this strategy with example.

12. (a) Illustrate the design principles and features of DES that contributed to its initial strength and the limitations that eventually led to its obsolescence.

Or

- (b) Demonstrate the factors that contribute to AES's performance with variable key sizes in hardware and software implementations.

13. (a) Illustrate the properties of Euler's Totient Function $\phi(n)$ function, including its multiplicative property, its significance and applications in number theory, modular arithmetic and cryptography with examples.

Or

- (b) Demonstrate the mathematical principles, the process of key generation, encryption and decryption, practical considerations and limitations of RSA algorithm.

14. (a) The secure distribution and management of public and private key pairs ensure effectiveness of asymmetric cryptography. Discuss in detail the challenges and various methods associated with distributing public keys securely and ensuring the confidentiality of private keys.

Or

- (b) Demonstrate on how HMAC helps to verify the integrity of the message, authenticate the sender of the message and protect against common attacks that might be effective against plain hash functions.

15. (a) Illustrate the range of potential negative consequences that a successful SQL injection attack can have on an application and its underlying database, including data modification, data deletion, and potential system compromise and possible countermeasures.

Or

- (b) Demonstrate the primary classification of Cybercrimes providing examples of specific types of cybercrimes that belong to each category.

PART C — (1 × 15 = 15 marks)

16. (a) A small business owner sets up a new Wi-Fi network for their shop. They want to ensure the security of their customer and business data transmitted over this network. Recommend the most appropriate Wireless Network Security protocol they should implement for their new network, justifying the choice by demonstrating its key security features and why that is superior to other alternatives in providing protection against common wireless threats.

Or

- (b) A Government agency plans to securely distribute important policy documents to its departments. They want to ensure both the authenticity of the document's origin and integrity of its content. Articulate on how the agency can utilize digital signatures and authentication mechanisms to meet the requirements.
-

