Reg. No. : □□□□□□□□□□□□

Question Paper Code : 40374

B.E./B.Tech. DEGREE EXAMINATIONS, NOVEMBER/DECEMBER 2024.

Fourth/Fifth Semester

Computer Science and Engineering

CB 3491 — CRYPTOGRAPHY AND CYBER SECURITY

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

(Regulations 2021)

Time : Three hours

Maximum : 100 marks

Answer ALL questions.

PART A — (10 × 2 = 20 marks)

1. Mention the three key objectives that are at the heart of Computer Security.
2. Define Non-repudiation.
3. Calculate gcd(568, 8)using Euclidean algorithm.
4. Compare linear and differential cryptanalysis.
5. Find 8^{-1} mod 173.
6. Mention the advantages of elliptic curve cryptography.
7. Why do we need Hash function?
8. Write the challenges in Key distribution.
9. What is a key logger?
10. How are Cyber crimes classified?

PART B — (5 × 13 = 65 marks)

11. (a) Discuss on the attack surfaces, attack trees and the model for network Security.

Or

(b) Describe the various Classical encryption techniques with illustrations.

12. (a) Illustrate the core principles behind Euclid's algorithm and extended euclidean and explain its functionality.

Or

(b) Describe the detailed structure of AES and reveal the significance of transformation function.

13. (a) Illustrate the core ideology behind Fermat's and Euler's Theorems and explain its applications. Give an example for each.

Or

(b) Discuss the working principle behind RSA algorithm with an example.

14. (a) Explain the need for authentication function and discuss a digital signature based scheme.

Or

(b) Describe the performance of Symmetric Key Distribution using Asymmetric Encryption.

15. (a) Describe the implementation of Network Access Control in Cloud using EAP.

Or

(b) Illustrate the services and phases of operation in IEEE 802.11i.

PART C — (1 × 15 = 15 marks)

16. (a) Digital India has led to an increase in the usage of cashless transactions, digital money. Data breaches are a serious problem in the banking sector. A weak cyber security system can cause their customer base to undergo cyber security threats. When a bank's data is breached, recovering from this data breach can be time-consuming and stressful.

Devise a solution to preserve the banking system from Cyber threats.

Or

(b) Devise a solution to automate the threat detection system and provide protection against potential threats, in a Cloud environment.

———————