Reg. No. : □□□□□□□□□□□□

Question Paper Code : 50356

B.E./B.Tech. DEGREE EXAMINATIONS, APRIL/MAY 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. Distinguish between attack and threat.

2. Define steganography.

3. Find GCD(1970,1066) using Euclid's algorithm.

4. Compare block cipher and stream cipher.

5. Find the remainder when 7^23 is divided by 11 using Fermat's Little Theorem.

6. How does the Chinese Remainder Theorem contribute to efficient modular arithmetic in encryption and decryption processes?

7. Define Digital signature. What are the properties of Digital Signature?

8. Write a simple authentication dialogue used in Kerberos.

9. Define cybercrime and explain why it poses significant challenges to individuals, organizations and society.

10. Write the key principles and practices of cloud security.

PART B — (5 × 13 = 65 marks)

11. (a) Show your calculations and the result to encrypt the message "meet me at the usual place at ten rather than eight o clock" using the Hill cipher with the key $\begin{pmatrix} 7 & 3 \\ 2 & 5 \end{pmatrix}$.

Or

(b) Explain about OSI Security architecture model with suitable example.

12. (a) (i) Solve the following using RC4 stream cipher algorithm. Assume the state vector is 8 bits. (8)

Key : [1 0 0 2]

Plaintext : [6 1 5 4]

(ii) Illustrate any one pseudo random number generator algorithm. (5)

Or

(b) Explain the overall structure and round structure of DES with neat sketch.

13. (a) You are given two prime numbers, p=13 and q=17. Calculate the following:

- Compute n, the modulus for the RSA cryptosystem. (3)
- Calculate $\varphi(n)$, Euler's Totient Function of n, which represents the count of positive integers less than n that are relatively prime to n. (4)
- Find the public exponent (e) for the RSA cryptosystem. (3)
- Calculate the private exponent (d) for the RSA cryptosystem. (3)

Or

(b) (i) Consider a Diffie-Hellman scheme with a common prime q = 11 and a primitive root a = 2. (8)

- If user A has public key YA = 9, what is A's private key XA?
- If user B has public key YB = 3, what is the secret key K shared with A?

(ii) How man in middle attack can be performed in Diffie Hellman algorithm? (5)

14. (a) With neat diagram, explain the steps involved in SHA algorithm for encrypting the message with maximum length of less than 2^{128} bits and produces as a output of message digest 512.

Or

(b) Describe Digital Signature Algorithm and show how signing and verification is done using DSS.

15. (a) Describe how spyware functions and its impact on privacy and data security. What steps can individuals and organizations take to detect and prevent spyware infections?

Or

(b) Discuss the security risks associated with public Wi-Fi networks and the best practices for ensuring wireless security on personal devices.

PART C — (1 × 15 = 15 marks)

16. (a) You work as an information technology administrator for a multinational firm. Describe how you would utilize Kerberos to improve network security and simplify user authentication and authorization. What components and processes would you need to put in place to do this?

Or

(b) Your company is implementing Network Access Control (NAC) to improve network security. Outline the implementation process, including policy development, authentication techniques, and enforcement.