Reg. No. : □□□□□□□□□□□□

Question Paper Code : 30460

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

Sixth / Seventh Semester

Computer Science and Engineering

CS 8792 — CRYPTOGRAPHY AND NETWORK SECURITY

(Common to : Computer and Communication Engineering / Electronics and Communication Engineering / Electronics and Telecommunication Engineering / Information Technology)

(Regulations 2017)

Time : Three hours Maximum : 100 marks

Answer ALL questions.

PART A — (10 × 2 = 20 marks)

1. Write the difference between cryptography and cryptanalysis.
2. What is notarization in network security?
3. When is a cryptographic algorithm considered to be unconditionally secure?
4. Compare linear and differential cryptanalysis.
5. Calculate the value of $\Phi(49)$ using Euler's Totient Function.
6. What is prime curve over Zp?
7. Compare any two SHA algorithms.
8. Write X.509 certificate format.
9. What are the MIME content types?
10. Mention the role of firewall in network security.

PART B — (5 × 13 = 65 marks)

11. (a) (i) Given the message "AES" and the key "MPIMNHJKV", encrypt the message using the Hill cipher, and then decrypt the ciphertext. (9)

(ii) Discuss various security services. (4)

Or

(b) (i) Encrypt the given plaintext "QUANTUM" using the Playfair cipher with the key "PSEUDORANDOMNESS". (5)

(ii) Encrypt the given plaintext "SPREADLOVEEVERYWHERE" using single columnar and double columnar transposition methods with the key "614352". (8)

12. (a) (i) Explain the concept of block cipher modes of operation and compare it. (8)

(ii) Determine the gcd(2589, 534) using the extended Euclidean algorithm. (5)

Or

(b) (i) Describe the structure and operation of the AES algorithm. (8)

(ii) Discuss the strengths and weaknesses of RC4 in cryptographic applications. (5)

13. (a) (i) State Fermat's Theorem and calculate 1718^7 mod 7. (5)

(ii) Describe the principles of elliptic curve cryptography and its advantages compared to RSA and other asymmetric key algorithms. (8)

Or

(b) (i) Compute the value of X using the Chinese remainder problem with the given congruences. (8)

$X \equiv 8 \pmod 9$

$X \equiv 5 \pmod 7$

$X \equiv 11 \pmod{13}$

(ii) Describe the challenges associated with key distribution and key management in asymmetric key cryptography. (5)

14. (a) (i) Discuss various cryptographic techniques used in authentication functions. (8)

(ii) Explain the concept of digital signatures and their role in authentication. (5)

Or

(b) (i) Describe the components of a Kerberos authentication system and also discusses the advantages and limitations of Kerberos in network authentication. (8)

(ii) Describe common use cases and scenarios where Kerberos and X.509 are used together to provide secure authentication and communication. (5)

15. (a) (i) Describe the components of the SET framework and their respective roles. (8)

(ii) Describe the two main modes of operation in IPSec. (5)

Or

(b) (i) Discuss the various categories of malicious software. (8)

(ii) Elaborate the approaches used in detecting intrusions. (5)

PART C — (1 × 15 = 15 marks)

16. (a) Describe RSA algorithm. Calculate the public and private keys, and perform encryption and decryption operations using the RSA algorithm for the given input : (15)

$p = 17; q = 13; e = 5; M = 678$

Or

(b) Elaborate Diffie-Hellman algorithm. Compute the public key of user A and the public key of user B, along with the shared secret key between them, using the Diffie-Hellman algorithm for the given scenario. (15)

$q = 887;$ $\alpha = 5$ (primitive root), $X_A = 98$ and $X_B = 345$