Reg. No. : | | | | | | | | | | | | |

Question Paper Code : 70451

B.E./B.Tech. DEGREE EXAMINATIONS, NOVEMBER/DECEMBER 2023.

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. Compare passive and active attack.

2. List the advantages and disadvantages of one-time pad cipher.

3. Mention the purpose of cryptanalysis.

4. What is meant by avalanche effect?

5. Find the value of $\phi(59)$ using Euler's totient function.

6. What is a primitive root of a number? Give an example.

7. Compare Hash and MAC.

8. What is Kerberos realm?

9. List the difference between PGP and S/MIME.

10. What is tunnel mode in IPSec?

PART B — (5 × 13 = 65 marks)

11. (a) (i) Describe various security mechanisms. (5)

(ii) With suitable example, explain playfair cipher. (4)

(iii) Encrypt the following using double columnar transposition. (4)

Plaintext : HAPPINESSWITHINOURSELF

Key : 256413

Or

(b) (i) Compare vulnerability, threats and attack. (5)

(ii) Consider ESC as plain text and BWVQRSUFN as key. Encipher and decipher using Hill cipher. (8)

12. (a) (i) How does RC4 work? Explain it. (5)

(ii) Find gcd(8976, 345) using extended Euclidean algorithm. (8)

Or

(b) (i) Explain electronic code book and cipher block chaining. (8)

(ii) Find multiplicative inverse of 438 in mod 2567. (5)

13. (a) (i) State Fermat's Theorem. Solve the 67^{83} mod 83 and 89^{78} mod 79 using it. (8)

(ii) Write a short note on elliptic curve cryptography. (5)

Or

(b) (i) Find the value of X using Chinese remainder problem. (8)

$X \equiv 5 (\text{mod } 23)$

$X \equiv 6 (\text{mod } 27)$

$X \equiv 5 (\text{mod } 31)$

(ii) Why do we need discrete logarithms? Explain it with example. (5)

14. (a) Discuss about various authentication protocols. (13)

Or

(b) What is an X.509? How does it work? Discuss in detail. (13)

15. (a) (i) Discuss about S/MIME. (8)

(ii) Write short notes on SSL. (5)

Or

(b) (i) Describe the approaches used for intrusion detection. (8)

(ii) Explain various types of viruses. (5)

PART C — (1 × 15 = 15 marks)

16. (a) Write Diffie-Hellman algorithm. Find the secret key shared between user A and user B using Diffie-Hellman algorithm for the following.

$q = 673$; $\alpha = 5$; $X_A = 418$ and $X_B = 59$. (15)

Or

(b) Solve the following: $p = 31$; $q = 67$; $e = 7$; $M = 413$ using RSA algorithm. Find public key and private key and perform encryption and decryption. (15)