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

Question Paper Code : 50439

B.E./B.Tech. DEGREE EXAMINATIONS, APRIL/MAY 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 attacks.

2. Perform encryption for the plain text "CRYPTOGRAPHYANDSTEGANOGRAPHY" using double columnar transposition technique and the key is 341562.

3. Find gcd(68,8) using Euclidean algorithm.

4. Compare the AES and DES.

5. Find the value of 7^8 mod 15 Using Euler's theorem.

6. Find $\Phi(21)$.

7. Compare MAC and hash function.

8. Mention the importance of ElGamal cryptosystem.

9. What are the various types of firewall?

10. What are key loggers?

PART B — (5 × 13 = 65 marks)

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

(ii) Encrypt the following Using playfair cipher. (4)

Plaintext : PRESERVE

Key : AGRICULTURE

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

Plaintext : CYBERSECURITYISIMPORTANT

Key : 5137462

Or

(b) (i) Discuss about various types of attacks. (5)

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

12. (a) (i) Find multiplicative inverse of 313 in mod 67. (5)

(ii) Elaborate on AES encryption and decryption. How will you evaluate the AES algorithm? (8)

Or

(b) (i) Discuss about various block mode of operation. (8)

(ii) Find gcd(6432,768) using extended Euclidean algorithm. (5)

13. (a) (i) Explain about elliptic curve cryptography. (10)

(ii) Find $\Phi(519)$. (3)

Or

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

$X = 10 \pmod{12}$

$X = 7 \pmod{9}$

$X = 3 \pmod{5}$

(ii) Find $103^{27} \bmod 467$. (5)

14. (a) Elaborate the Kerberos. (13)

Or

(b) Explain the various authentication protocols with an example. (13)

15. (a) (i) Discuss about various PGP services. (8)

(ii) Describe the various approaches used for intrusion detection. (5)

Or

(b) (i) Elaborate on SET in detail. (8)

(ii) Describe IPSec services. (5)

PART C — (1 × 15 = 15 marks)

16. (a) Users A and B use the Diffie Hellman key exchange technique, $q = 139$; g(primitive root)=3 (i) If user A has private key X_A=56. What is A's public key Y_A? (ii) If user B has private key X_B=115. What is B's public key Y_B? (iii) What is the shared secret key? Also write the algorithm. (15)

Or

(b) Explain RSA algorithm. Perform decryption and encryption using RSA algorithm with p=31, q=47, e=7 and M=69. (15)

———————