Reg. No. : □□□□□□□□□□□□

Question Paper Code : 80455

B.E./B.Tech. DEGREE EXAMINATIONS, APRIL/MAY 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. Find the cipher text using transposition technique, if the message is = "anna university", key = 3.

2. In crypt analysis, what is meant by di-gram and tri-gram?

3. Compute GCD (65,20) using Euclid Algorithm.

4. List any two strengths of AES.

5. Using Euler Totient Function, φ (35) =?

6. How to test the given number is prime or not using Fermat's algorithm?

7. In RSA algorithm, the encrypted text will be decrypted, and it will return the original message. Is it possible in SHA? Justify your answer.

8. List any two real time applications of digital signature.

9. Which security device helps to filter the incoming traffic? Discuss briefly about it.

10. Differentiate malicious software vs virus.

PART B — (5 × 13 = 65 marks)

11. (a) Discuss Confidentiality, Integrity, Authentication, Availability and Nonrepudiation with technical key factors.

Or

(b) Explain any three types of substitution techniques with proper examples.

12. (a) Explore in detail about the one round process of DES encryption and its functionalities.

Or

(b) Discuss the four major key operations of AES with its major technical factors.

13. (a) Alice and Bob communicate each other using secured chat system. Propose a Diffie Hellman (DH) based key exchange with proper flow diagram. Also discuss, how the Man in the middle attacks affects the DH key exchange?

Or

(b) Describe: Chinese Remainder theorem and its application in cyber security.

14. (a) Write brief notes about the MAC on message authentication, message authentication with confidentiality process. Also discuss the security aspects of MAC.

Or

(b) Demonstrate: The technical operations of SHA.

15. (a) Consider that you are a web designer and developed your own web site. Discuss the various types of attacks which will affects the web site and provide its prevention methodology.

Or

(b) Our email communication has several possible attacks. How these attacks will be secured using PGP. Write your answer with technical factors.

PART C — (1 × 15 = 15 marks)

16. (a) Find the cipher text of the message = "hi" using RSA algorithm. Use the following data for computation: p=3, q=11, ascii(h)=104.

Or

(b) Using Elliptic curve encryption/decryption scheme, key exchange between users Alice and Bob is accomplished. Compute from the following ECC data, Alice wishes to encrypt the message Pm = (10,9) and chooses the random value K=3. Determine the ciphertext Cm, and compute Bob's public key PB.

ECC Data: Ellyptic group of points E11 (1,6) and point G on the elliptic curve is G = (2,7). B's secret key is nB = 7.