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

Question Paper Code : 40404

B.E./B.Tech. DEGREE EXAMINATIONS, NOVEMBER/DECEMBER 2021.

Sixth/Seventh Semester

Computer Science Engineering

CS 8792 – CRYPTOGRAPHY AND NETWORK SECURITY

(Common to B.E. Computer and Communication Engineering/B.E. Electronics and Communication Engineering/B.E. Electronics and Telecommunication Engineering/B.Tech. Information Technology)

(Regulations 2017)

Time : Three hours | Maximum : 100 marks

Answer ALL questions.

PART A — (10 × 2 = 20 marks)

1. What is meant by Denial of Service attack? Is it Active Attack or Passive Attack?

2. Let message = “Anna”, and k = 3, find the ciphertext using Caesar.

3. Find Residues of 6 when n = 8.

4. Find gcd(2740, 1760) using Euclidean Algorithm.

5. Using Fermat’s theorem, check whether 19 is prime or not? Consider a is 7.

6. Find atleast two points lies in the elliptic curve $y^2 = x^3 + 2x + 3 (\text{mod}\, 5)$.

7. What is meant by padding? And, why padding is required?

8. Draw functional diagram of RSA based Digital Signature.

9. Explain the process of Radix 64 conversion.

10. Write short notes on Spammers and Key loggers.

PART B — (5 × 13 = 65 marks)

11. (a) (i) Let message = "graduate", Key = "word", find ciphertext using playfair cipher. (8)

(ii) List out any two di-gram, two tri-gram. Shortly describe the application of di-gram and tri-gram in cryptography. (5)

Or

(b) Demonstrate encryption and decryption process in hill cipher. Consider m = "sh" and key = hill". (4 + 9)

12. (a) (i) Draw the functionality diagram (functionality in one round) of DES with number of bits in each flow of data. (8)

(ii) Explain the bitwise XOR operation which involved in RC4. (5)

Or

(b) (i) Explain with sample data: Four transformations in AES. (10)

(ii) In finite field arithmetic, $\left(x^6 + x^4 + x^2 + x + 1\right) + \left(x^7 + x + 1\right) = ?$. (3)

13. (a) (i) Demonstrate the DH key exchange methodology using following key values : $p = 11$, $g = 2$, $X_A = 9$, $X_B = 4$. (7)

(ii) Diffie–Hellman key agreement is not limited to negotiating a key shared by only two participants. Any number of users can take part in an agreement by performing iterations of the agreement protocol and exchanging intermediate, Write the steps and formulas to be followed for DH key exchange between Alice, Bob, and Carol. (6)

Or

(b) (i) In a public-key system using RSA, you intercept the ciphertext C = 20 sent to a user whose public key is e = 13, n = 77. What is the plaintext M? (7)

(ii) In an RSA system, the public key of a given user is e = 65, n = 2881, What is the private key of this user? (6)

14. (a) Write the steps involved in the Generation of Message Digest. (13)

Or

(b) (i) Discuss the four requirements of Kerberos. (4)

(ii) Shortly describe about the elements of X509 Certificate. (9)

15. (a) Discuss the seven types of MIME content type.

Or

(b) Draw IPSec Authentication Header and write short notes on each element of the Header.

PART C — (1 × 15 = 15 marks)

16. (a) A Box contains gold coins. If the coins are equally divided among three friends, two coins are left over, If the coins are equally divided among five friends, three coins are left over If the coins are equally divided among seven friends, two coins are left over. If the box holds smallest number of coins that meets these conditions, how many coins are there? (Hint : Use Chinese Remainder Theorem).

Or

(b) (i) Alice chooses 173 and 149 as two prime numbers and 3 as public key in RSA. Check whether the chosen prime numbers are valid or not? (5)

(ii) Prove that Euler's Totient value of any prime number (p) is $p-1$ and the Euler's Totient value of the non-prime number (n) is $(p-1)\times(q-1)$ where $p\times q$ are prime factor of n. (5)

(iii) Mr. Ram chooses RSA for encryption, and he chooses 3 and 7 are two prime numbers. He encrypt the given message (message given in English alphabets) by mapping A = 1, B = 2, C = 3.., Z = 26. Find atleast two problems in his implementation. (5)

———————