Roll No											

PRESIDENCY UNIVERSITY
BENGALURU

SET - B

SCHOOL OF ENGINEERING
END TERM EXAMINATION - JUN 2023

Semester : Semester IV - 2021
Course Code : CSE3078
Course Name : Sem IV - CSE3078 - Cryptography and Network Security
Program : B.Tech - All Programs

Date : 22-JUN-2023
Time : 9.30AM - 12.30PM
Max Marks : 100
Weightage : 50%

Instructions:
(i) Read all questions carefully and answer accordingly.
(ii) Question paper consists of 3 parts.
(iii) Scientific and non-programmable calculator are permitted.
(iv) Do not write any information on the question paper other than Roll Number.

PART A

ANSWER ALL THE QUESTIONS **(10 X 2 = 20M)**

1. Mention two scenarios where you need to have filler characters in playfair cipher.
(CO1) [Knowledge]

2. List the parameters (block size, key size and no. of rounds) for the three AES versions.
(CO2) [Knowledge]

3. What are the design parameters of Feistel cipher network?
(CO1) [Knowledge]

4. Define public key cryptography?
(CO3) [Knowledge]

5. State Fermat's Theorem.
(CO2) [Knowledge]

6. What are the benefits of IP Security?
(CO4) [Knowledge]

7. Define symmetric and Asymmetric key cryptography. Give an example for each.
(CO1) [Knowledge]

8. Define Man-in-middle attack.
(CO3) [Knowledge]

9. Prove that 301 and 500 are relatively prime or not.
(CO2) [Knowledge]

10. What are the keys used by PGP?
(CO4) [Knowledge]

PART B

ANSWER ALL THE QUESTIONS **(5 X 10 = 50M)**

11. Discuss various requirements of Message authentication code?

(CO3) [Comprehension]

12. Explain Kerberos authentication mechanism in detail with suitable diagram.

(CO4) [Comprehension]

13. Give the structure of HMAC. Explain the overall operation of HMAC.

(CO3) [Comprehension]

14. Using Vignere cipher encrypt the text “Today is the final exam all the best” using the key “ENGINEERING”.

(CO1) [Comprehension]

15. How GCD calculated with Euclid’s algorithm? Calculate the GCD(270,192) and GCD(125,20)?

(CO2) [Comprehension]

PART C

ANSWER ALL THE QUESTIONS **(2 X 15 = 30M)**

16. Explain RSA algorithm. Two users ‘A’ and ‘B’ are willing to establish secure connection using RSA Algorithm. Following inputs are givenTwo primes: 11 and 29.
Select ‘e’ more than 20
Plaintext: 18
Calculate the Encryption and Decryption keys? Perform Encryption and Decryption for given plaintext.

(CO3) [Application]

17. State chinese remainder theorem and Using Chinese Remainder Theorem find the value of x for the given set of congruent equations.
$x \equiv 3 \pmod 5$
$x \equiv 1 \pmod 7$
$x \equiv 6 \pmod 8$

(CO2) [Application]