Roll No											

PRESIDENCY UNIVERSITY
BENGALURU

SET - A

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.	What is meant by denial of service attack? Is it active or passive attack?	(CO1) [Knowledge]
2.	List out the requirements of Kerberos.	(CO4) [Knowledge]
3.	What is the condition to select the public key in RSA?	(CO3) [Knowledge]
4.	What are the two general approaches to attacking a cipher?	(CO1) [Knowledge]
5.	List out any 4 security mechanisms defined by OSI security architecture.	(CO1) [Knowledge]
6.	Find out the prime factorization of number 1560.	(CO2) [Knowledge]
7.	List the operations used in DES.	(CO2) [Knowledge]
8.	What are the benefits of IP Security?	(CO4) [Knowledge]
9.	List out attacks are addressed by digital signature?	(CO3) [Knowledge]
10.	Define Commutative group in number theory.	(CO2) [Knowledge]

PART B

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

11. Using Miller Rabins primality testing. Use the same to test the primality of 271, 341 by considering base 2.

(CO2) [Comprehension]

12. Encrypt the message “COE” using Hill cipher with the following key matrix.

$$K = \begin{matrix} 17 & 17 & 5 \\ 21 & 18 & 21 \\ 2 & 2 & 19 \end{matrix}$$

(CO1) [Comprehension]

13. 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?

(CO3) [Comprehension]

14. Define Digital Signature. Which key is used to derive and verify the Digital Signature? Explain NIST Digital Signature Algorithm.

(CO3) [Comprehension]

15. What are the services provided by IPSec? Implement the IPSec architecture using Encapsulating security payload with neat diagram.

(CO4) [Comprehension]

PART C

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

16. Define primitive root? Consider the following inputs with respect to Diffie-Hellman key exchange Algorithm.Prime Number = 11
Sender’s Private Key = 6
Receiver’s Private Key = 8
Consider any primitive root less than 6.
Calculate the shared key for the given inputs.

(CO3) [Application]

17. Using Chinese Remainder Theorem find the value of x for the given set of congruent equations.
$x \equiv 1 \pmod 5$
$x \equiv 2 \pmod 7$
$x \equiv 3 \pmod 9$
$x \equiv 4 \pmod{11}$

(CO2) [Application]