Roll No											

PRESIDENCY UNIVERSITY
BENGALURU

SCHOOL OF ENGINEERING
MID TERM EXAMINATION - APR 2023

Semester : Semester VI -2020
Course Code : CSE3078
Course Name : Sem VI - CSE3078 - Cryptography and Network Security
Program : All Program

Date : 18-APR-2023
Time : 11:30AM - 1PM
Max Marks : 60
Weightage : 30%

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 **(5 X 2 = 10M)**

1. Differentiate between the active attacks and passive attacks
(CO1) [Knowledge]

2. Define Euler totient function with an example.
(CO2) [Knowledge]

3. What is the purpose of S-Boxes in DES algorithm
(CO2) [Knowledge]

4. List the operations used in AES Round structure
(CO2) [Knowledge]

5. Define cryptanalysis.
(CO1) [Knowledge]

PART B

ANSWER ALL THE QUESTIONS **(4 X 5 = 20M)**

6. Explain the network security model and its important parameters with a neat block diagram
(CO1) [Comprehension]

7. List and explain the security mechanisms defined by X.800
(CO1) [Comprehension]

8. Calculate 61^-1 mod 7465 using Extended Euclidean algorithm
(CO2) [Comprehension]

9. Consider the following state and perform mix column operation on this and derive only the firstelement

FF	DB	B7	93
0E	2A	46	62
ED	C9	A5	81
1C	38	54	70

(CO2) [Comprehension]

PART C

ANSWER ALL THE QUESTIONS **(3 X 10 = 30M)**

10. a) Explain Fermat's theorem for primality testing.
b) prove that fermat's little theorem is valid for p = 13, a = 7
c)Using fermat's theorem, check whether 19 is prime or not by considering a is 6

(CO2) [Application]

11. Describe the rules of playfair cipher? Using those rules decrypt the following message withthe key: "secret key"
Message: VCHTPNCSQCGCXBCELBYVEAVMGXCTRFED

(CO1) [Application]

12. Explain the feistel cipher structure with neat diagram and explain its design parameters?

(CO2,CO1) [Application]