Roll No											

PRESIDENCY UNIVERSITY
BENGALURU

SCHOOL OF ENGINEERING
MID TERM EXAMINATION - MAY 2023

Semester : Semester IV - B.Tech CSE - 2021
Course Code : CSE3078
Course Name : Sem IV - CSE3078 - Cryptography and Network Security
Program : B.Tech. Computer Science and Engineering

Date : 19-MAY-2023
Time : 2.00 PM - 3.30 PM
Max Marks : 50
Weightage : 25%

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. Define Cryptography.
(CO1) [Knowledge]
2. Find the value of Ø(100) and Ø(80)
(CO2) [Knowledge]
3. How fermat's little theorem and euler's theorem are related each other?
(CO2) [Knowledge]
4. Difference between block cipher and stream cipher
(CO1) [Knowledge]
5. **What is meant by relative prime? Give an example.**
(CO2) [Knowledge]

PART B

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

6. Explain the usage of gatekeeper function in model of network access security with neat diagram.
(CO1) [Comprehension]

7. Write the equations of DES round structure. How many sub keys are needed in DES and explain the sub key generation algorithm.

(CO2) [Comprehension]

8. Consider an automated cash deposit machine in which users provide a card or an account number to deposit cash. what are all the security services involved in the given scenario.Justify your answer

(CO1) [Comprehension]

9. Use Vignere Cipher with key HEALTH to encrypt the message “Life is full of surprises”

(CO1) [Comprehension]

PART C

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

10. Explain the key expansion algorithm in AES with neat diagram.

(CO2) [Application]

11. compare the vignere cipher and one time pad encryption process. Explain both algorithms with suitable examples.

(CO1) [Application]