Roll No.												

PRESIDENCY UNIVERSITY
BENGALURU

Department of Research & Development
Mid - Term Examinations - SEPTEMBER 2024

Odd Semester: Ph.D. Course Work	**Date**: 27 /09/2024
Course Code: CSE859	**Time**: 10:00am – 11:30am
Course Name: Cryptography and Network Security	**Max Marks**: 50
Department: SoCSE	**Weightage**: 25%

Instructions:

(i) Read all questions carefully and answer accordingly.

(ii) Do not write anything on the question paper other than roll number.

Part A

Answer ALL the Questions. Each question carries 5 marks.		**4Qx5M=20M**
1	S-Boxes inputs are S1(010010) & S2(000010) using Data Encryption Standard. Find the outputs.	**5 Marks**
2	Construct a **Playfair** matrix with the key "Security". Make a reasonable assumption about how to treat redundant letters in the key. Decrypt this message: "FUOQMPXNSPHQ "	**5 Marks**
3	Encrypt the following using **single columnar transposition**. PlainText is CYBERSECURITYISIMPORTAN and Key is 5137462	**5 Marks**
4	Using the **Extended Euclidean algorithm**, find the multiplicative inverse of 550 mod 1769.	**5 Marks**

Part B

Answer ALL Questions. Each question carries 15 marks.		**2QX15M=30M**
5	Consider **PEN** as the plain text and **ACTIVATED** as key. Encipher and decipher using **Hill cipher**.	**15 Marks**
6	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**).	**15 Marks**