Lab 3: Block Ciphers and RSA

Objectives:

- To implement/attack block cipher and RSA crypto systems

Submission:

- Checkpoints and a report explaining the approaches taken.

Instruction:

In this lab, we are going to implement Hill-cipher and RSA encryption. Report when you've completed any task.

Checkpoint – 1 (Marks 6)

Apply Hill-cipher to the supplied message. Use the supplied key matrix as the key for encryption. Show the encrypted text.

Checkpoint – 2 (Marks 7 + 7)

We're going to encrypt a message using RSA. For this, we may assume, a=1, b=2, c=2, and so on. The whole text will only contain lowercase alphabets.

Now, you're given n = 670726081 and d = 12345.

Task 1: Find e

Task 2 : Apply encryption to the supplied text