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 attack Vigenere cipher and RSA encryption. Report when you've completed any task.

Checkpoint – 1 (Marks 7)

You are given a cipher text. We have used 4 byte sized block for encrypting the text using Vigenere cipher. Find the plain text and key set. You are also given a cipher text containing spces and punctuations for you convenience.

Checkpoint – 2 (Marks 5 + 8)

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.

Suppose, you know the public keys, n = 80780754611 and e = 12345713

Task 1 Find private key

Task 2 : Apply encryption to the decrypted text of the previous task. Also, verify the correctness of your cipher text by deciphering it to the same plain text.
[The encrypted text might be some large numbers, don't be afraid]