Department of ECE

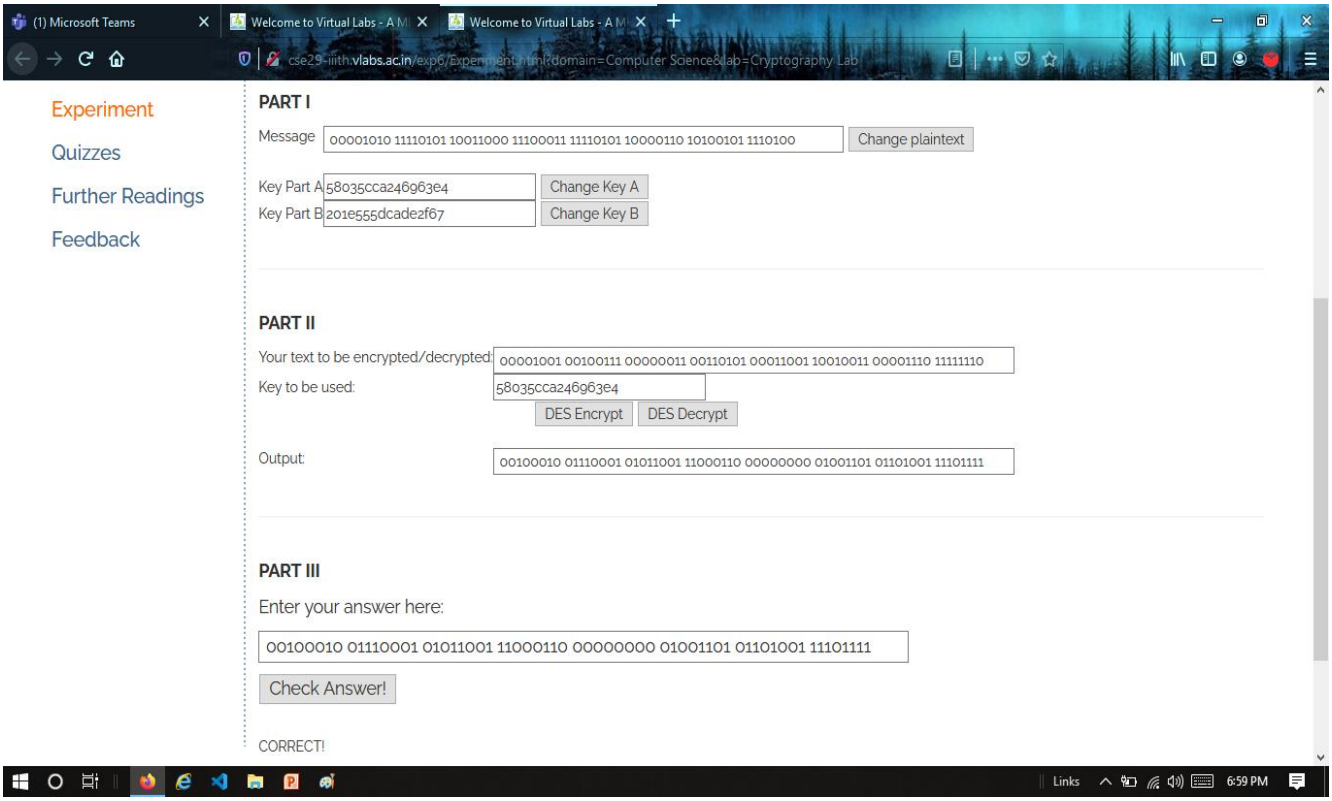
Vasavi college of Engineering

Hyderabad

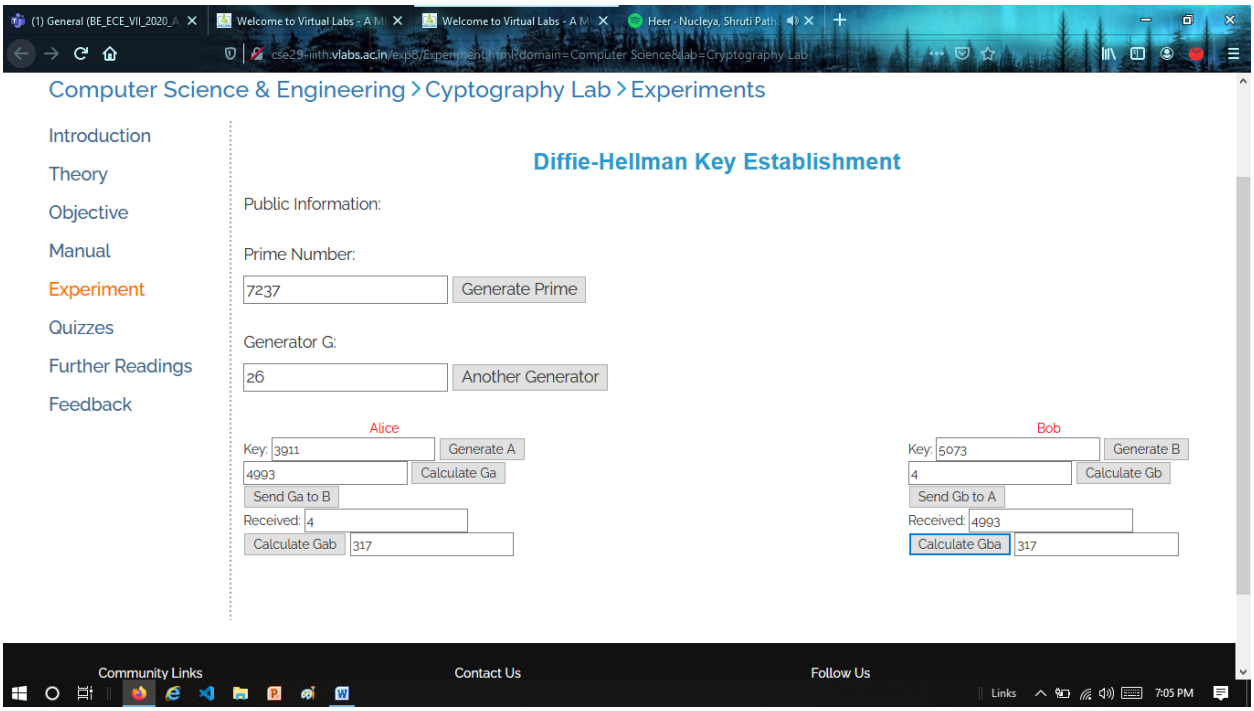
Virtual labs-Network security

4/4 B.E VII semester

1. DES Implementation:



2.Deffie Hellman algorithm:



3. RSA implementation:

Public-Key Cryptosystems (PKCSv1.5)

Plaintext (string):

hemanthreddy

encrypt

Ciphertext (hex):

796a51f8f4ae5b42c5505f8c8bba9ce4cd7a1782e908c6bf4f1cef958260238d
0148da8333706 9a4c6263f39eb18fb8f6a2f7dc2d50d6b764dab4af12dc79feb

decrypt

Decrypted Plaintext (string):

hemanthreddy

Status:

Decryption Time: 7ms

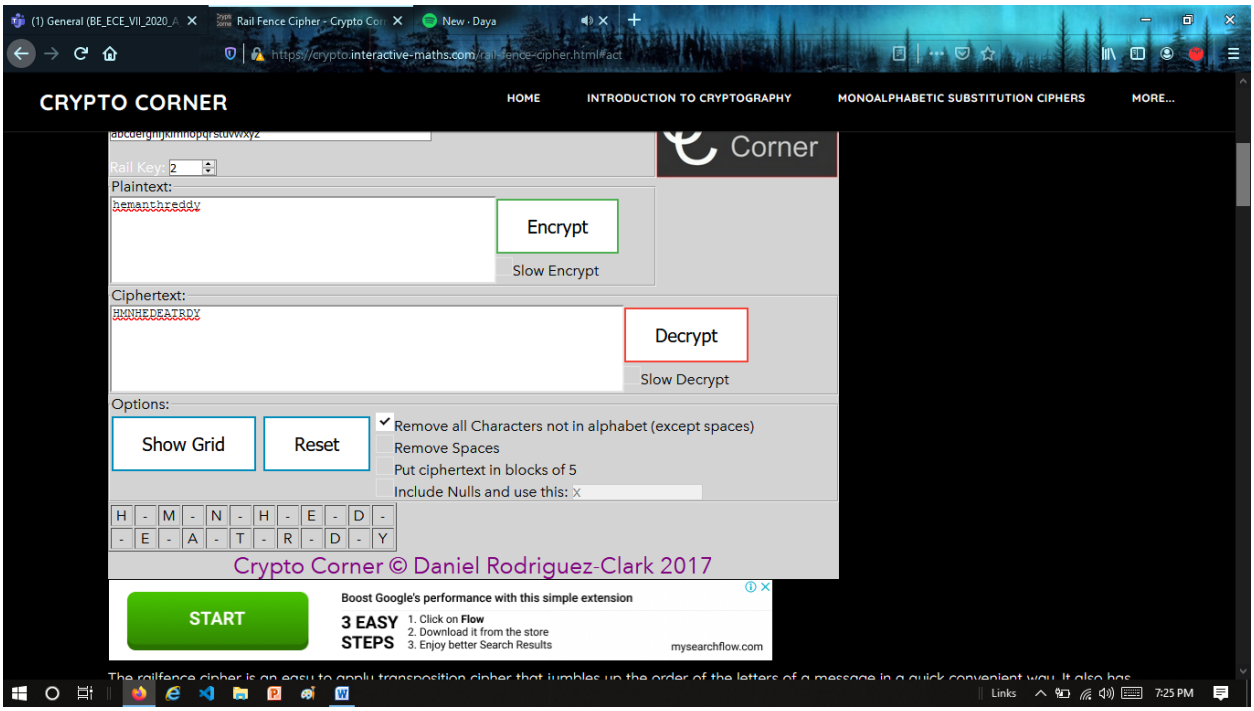
RSA private key

1024 bit | 1024 bit (e=3) | 512 bit | 512 bit (e=3) | Generate | bits = 512

Modulus (hex):

C4E3F7212602E1E396C0B6623CF11D26204ACE3E7D26685E037AD2507DCE82FC
28F2D5F8A67FC3AFAB89A6D818D1F4C28CFA548418BD9F8E7426789A67E73E41

4.Railfence cipher:



5.Playfaircipher:

Encrypt

Translate the letter J into I

☑ Encode double letters (down and right one spot)

Alphabet Key: ABCDEFGHIJKLMNOPQRSTUVWXYZ - Show Keymaker

Tableau Used:

```
A B C D E
F G H I K
L M N O P
Q R S T U
V W X Y Z
```

Your message:

hemanthreddy

Add Spaces - Adds a space after every other letter (only A-Z count) so you can see the letter pairs.
Only Letters - Removes all non-letters from the text.

This is your encoded or decoded text:

kclbosgsaeid

6.Caesar Cipher:

Plaintext

hemanth reddy

shift: 5

v Encrypt v | ^ Decrypt ^

Ciphertext

mjrfsym wjiid

7.Breaking the shift cipher:

PART III

Plaintext:

attack at dawn

shift: 7

v Encrypt v | ^ Decrypt ^

Ciphertext

haahjr ha khdu

PART IV

Enter your solution Plaintext and shift key here:

attack at dawn

Key 7

Check my answer!

CORRECT!!

S. Aruna Deepthi
Assistant Professor,
Department of ECE,
Mail ID: sadeepthi@staff.vce.ac.in
Phone No:9676772232