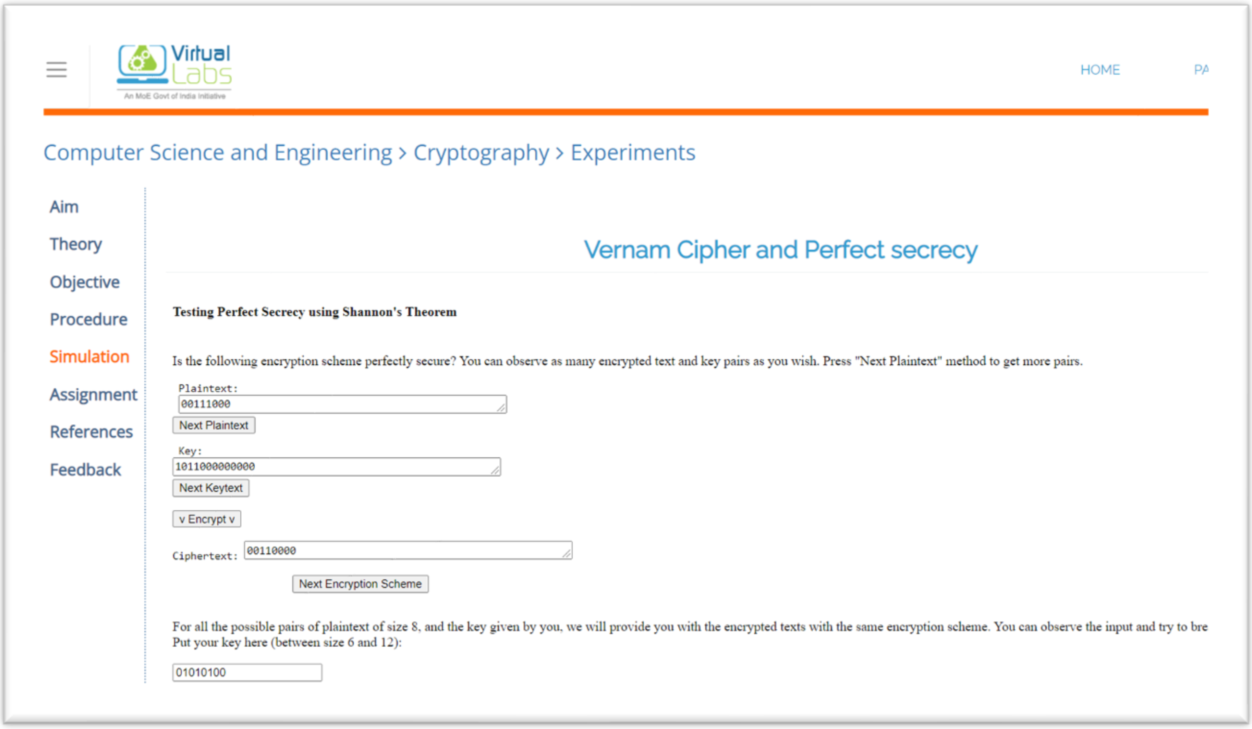
Omkar Gurav

8048

ICS Vlab session for Cryptography Lab

Exp 3 :



Vernam Cipher and Perfect secrecy

Testing Perfect Secrecy using Shannon's Theorem

Is the following encryption scheme perfectly secure? You can observe as many encrypted text and key pairs as you wish. Press "Next Plaintext" method to get more pairs.

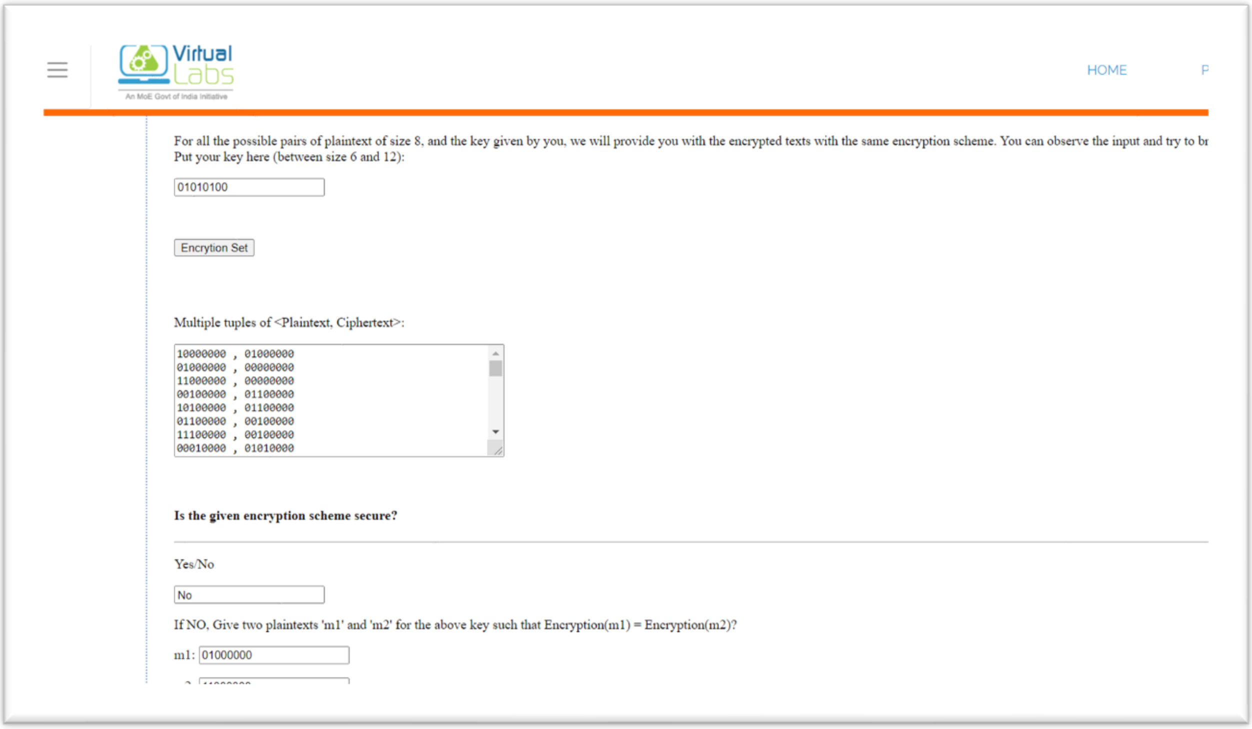
Plaintext: 00111000

Key: 1011000000000

Ciphertext: 00110000

For all the possible pairs of plaintext of size 8, and the key given by you, we will provide you with the encrypted texts with the same encryption scheme. You can observe the input and try to bre
Put your key here (between size 6 and 12):

01010100



For all the possible pairs of plaintext of size 8, and the key given by you, we will provide you with the encrypted texts with the same encryption scheme. You can observe the input and try to br
Put your key here (between size 6 and 12):

01010100

Multiple tuples of <Plaintext, Ciphertext>:

```
10000000 , 01000000
01000000 , 00000000
11000000 , 00000000
00100000 , 01100000
10100000 , 01100000
01100000 , 00100000
11100000 , 00100000
00010000 , 01010000
```

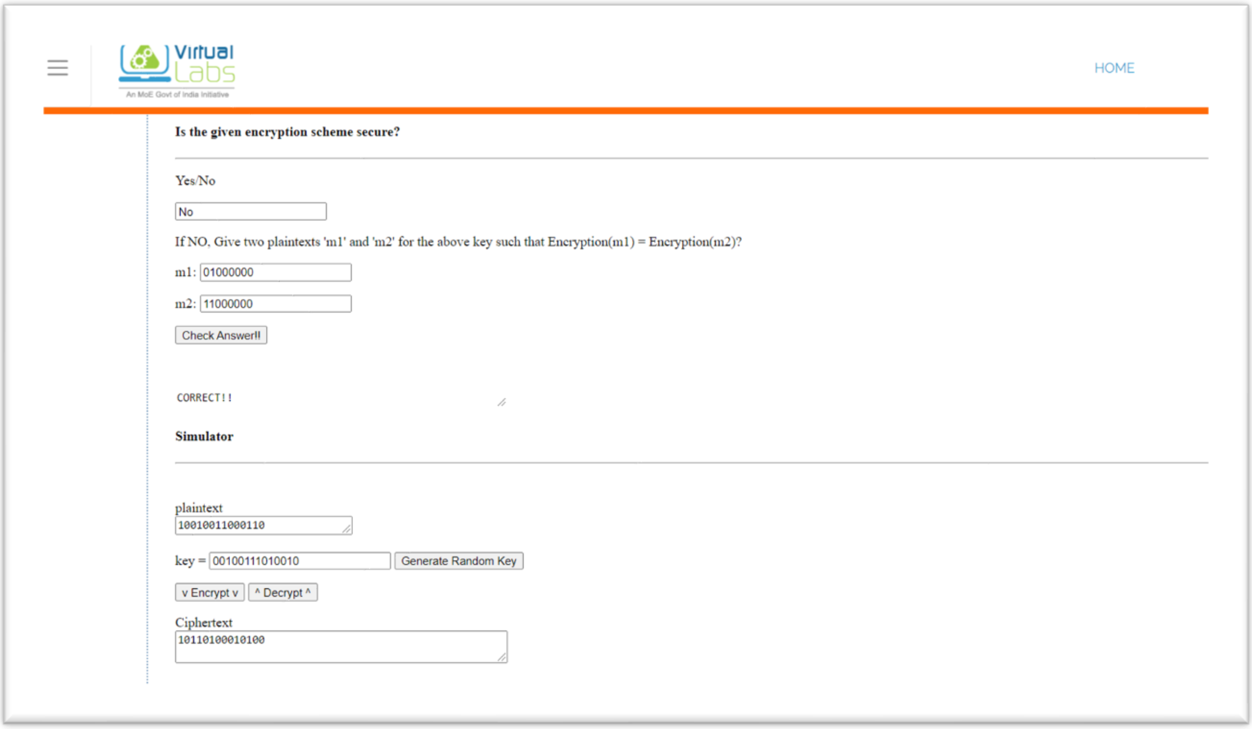
Is the given encryption scheme secure?

Yes/No

No

If NO, Give two plaintexts 'm1' and 'm2' for the above key such that Encryption(m1) = Encryption(m2)?

m1: 01000000



Is the given encryption scheme secure?

Yes/No

No

If NO, Give two plaintexts 'm1' and 'm2' for the above key such that Encryption(m1) = Encryption(m2)?

m1: 01000000

m2: 11000000

```
CORRECT!!
```

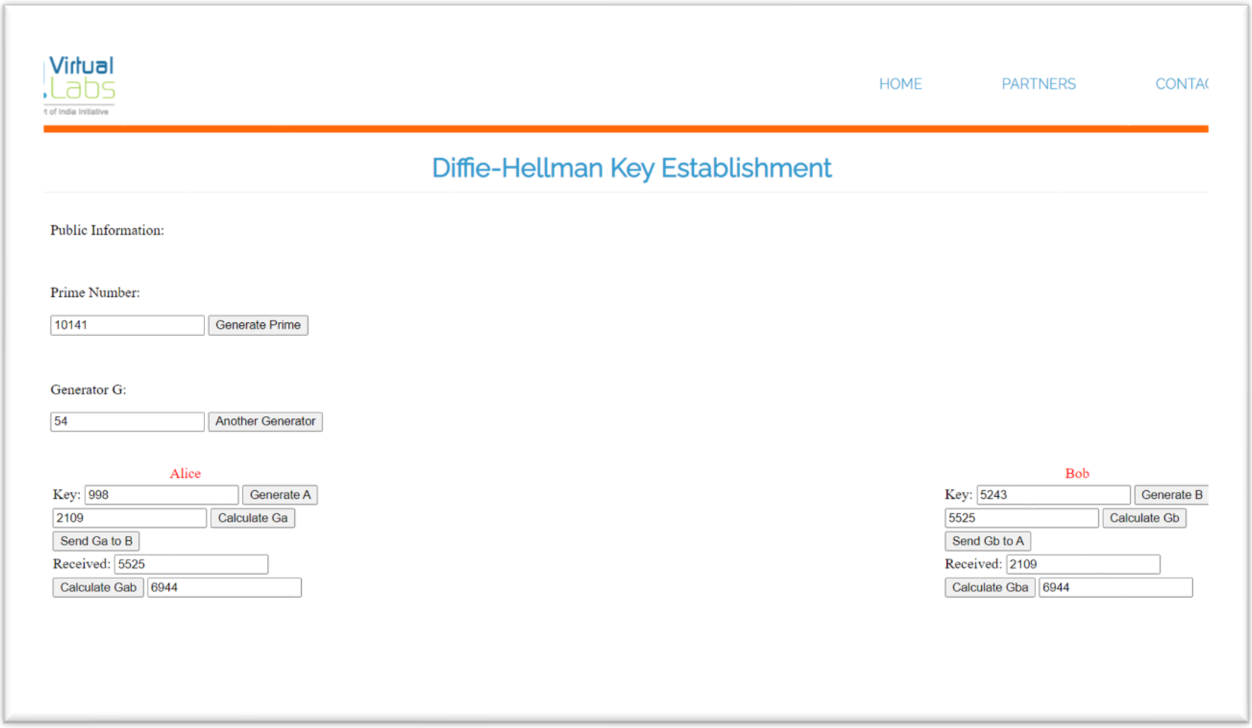
Simulator

plaintext
10010011000110

key = 00100111010010

Ciphertext
10110100010100

Exp 8 :



Diffie-Hellman Key Establishment

Public Information:

Prime Number: 10141

Generator G: 54

Alice

Key: 998

2109

Received: 5525

6944

Bob

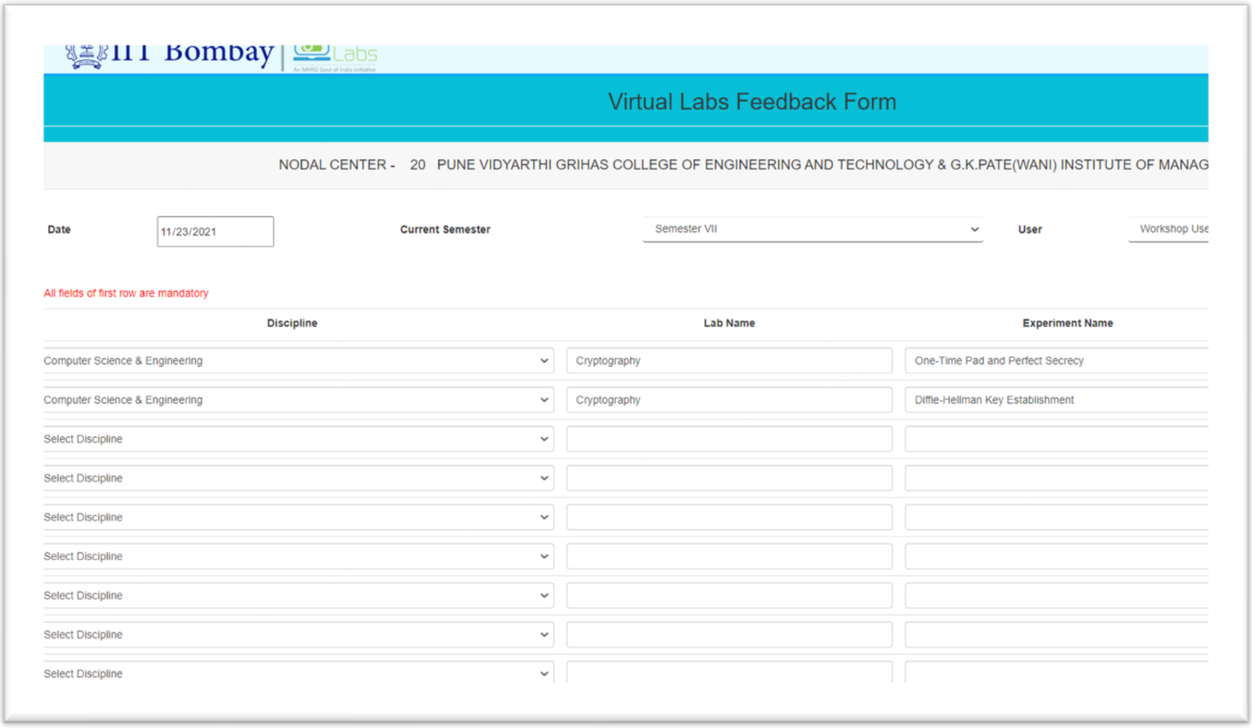
Key: 5243

5525

Received: 2109

6944

Feedback form :



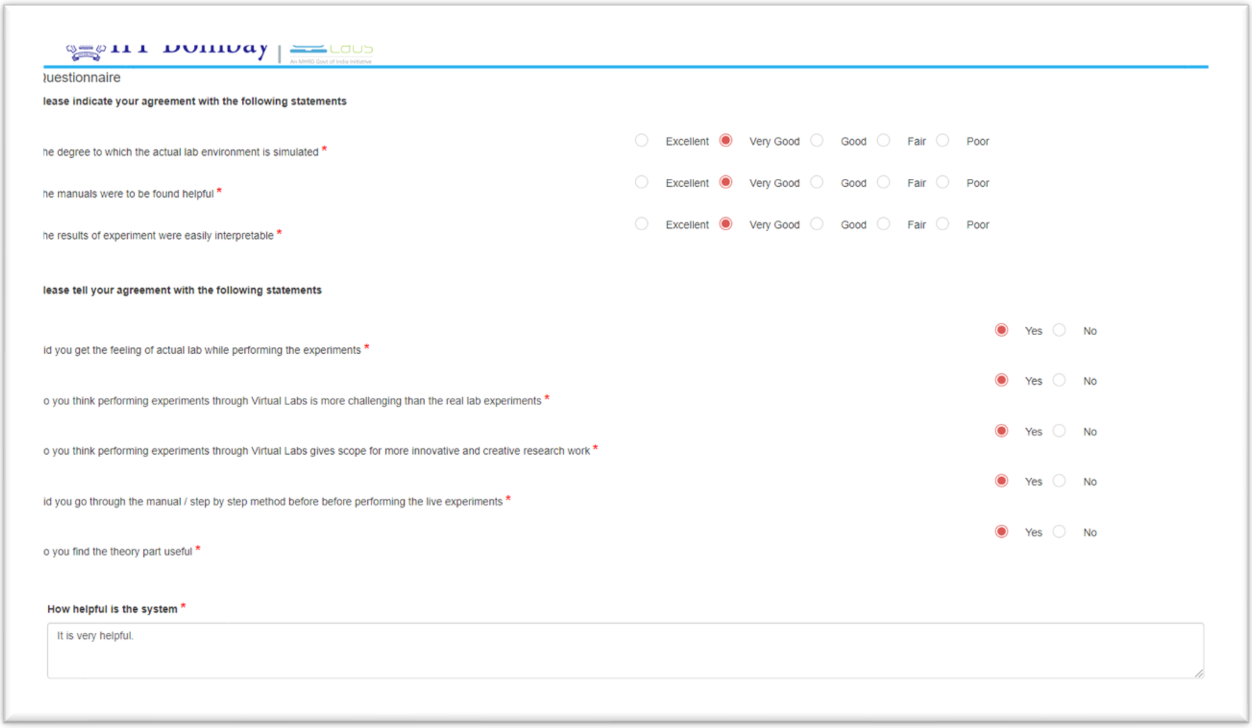
Virtual Labs Feedback Form

NODAL CENTER - 20 PUNE VIDYARTHI GRIHAS COLLEGE OF ENGINEERING AND TECHNOLOGY & G.K.PATE(WANI) INSTITUTE OF MANAG

Date 11/23/2021 Current Semester Semester VII User Workshop Use

All fields of first row are mandatory

Discipline	Lab Name	Experiment Name
Computer Science & Engineering	Cryptography	One-Time Pad and Perfect Secrecy
Computer Science & Engineering	Cryptography	Diffie-Hellman Key Establishment
Select Discipline		
Select Discipline		
Select Discipline		
Select Discipline		
Select Discipline		
Select Discipline		
Select Discipline		



uestionnaire

lease indicate your agreement with the following statements

he degree to which the actual lab environment is simulated * ○ Excellent ● Very Good ○ Good ○ Fair ○ Poor

he manuals were to be found helpful * ○ Excellent ● Very Good ○ Good ○ Fair ○ Poor

he results of experiment were easily interpretable * ○ Excellent ● Very Good ○ Good ○ Fair ○ Poor

lease tell your agreement with the following statements

id you get the feeling of actual lab while performing the experiments * ● Yes ○ No

o you think performing experiments through Virtual Labs is more challenging than the real lab experiments * ● Yes ○ No

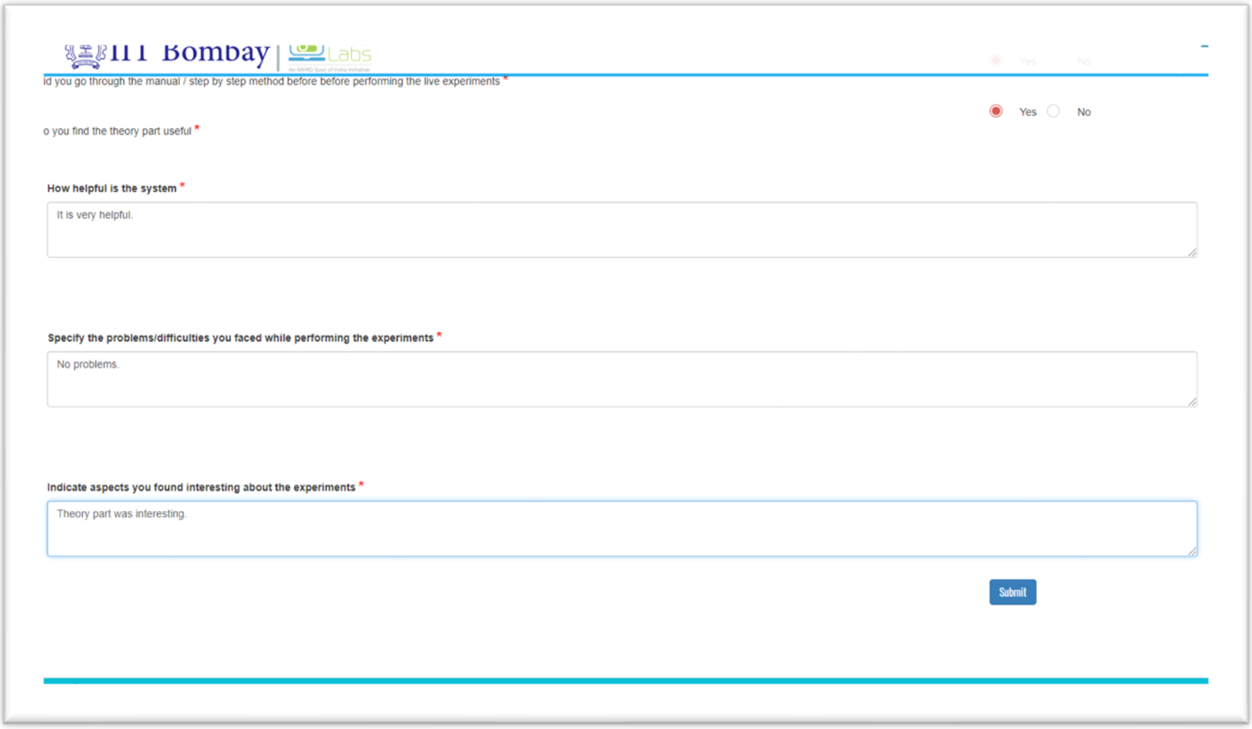
o you think performing experiments through Virtual Labs gives scope for more innovative and creative research work * ● Yes ○ No

id you go through the manual / step by step method before before performing the live experiments * ● Yes ○ No

o you find the theory part useful * ● Yes ○ No

How helpful is the system *

It is very helpful.



id you go through the manual / step by step method before before performing the live experiments *

o you find the theory part useful * ● Yes ○ No

How helpful is the system *

It is very helpful.

Specify the problems/difficulties you faced while performing the experiments *

No problems.

Indicate aspects you found interesting about the experiments *

Theory part was interesting.