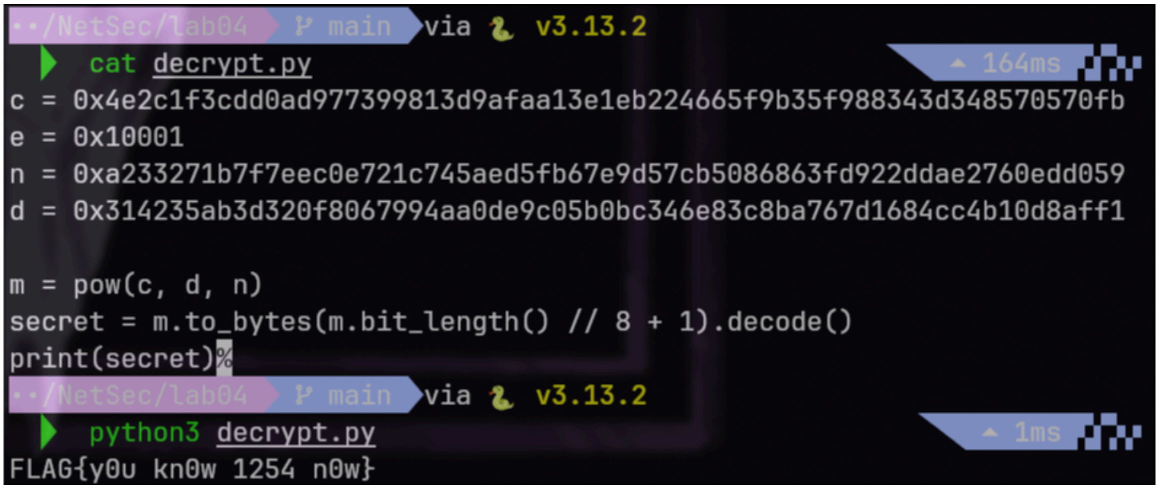
Lab 4 Report

Name: 林靖昀 Student ID: B12902116

1. Page 8: two questions

   Alice wants to send you a message, the encrypted cypher is:
   c = 0x4e2c1f3cdd0ad977399813d9afaa13e1eb224665f9b35f988343d348570570fb
   Both Alice and Eve have your public key:
   e = 0x10001
   n = 0xa233271b7f7eec0e721c745aed5fb67e9d57cb5086863fd922ddae2760edd059
   HW - Q1: Can Eve know the message from cypher?
   A1: Unless Eve can factor the extremely large n, and produce the private key, she won't be able to decrypt the cipher text.

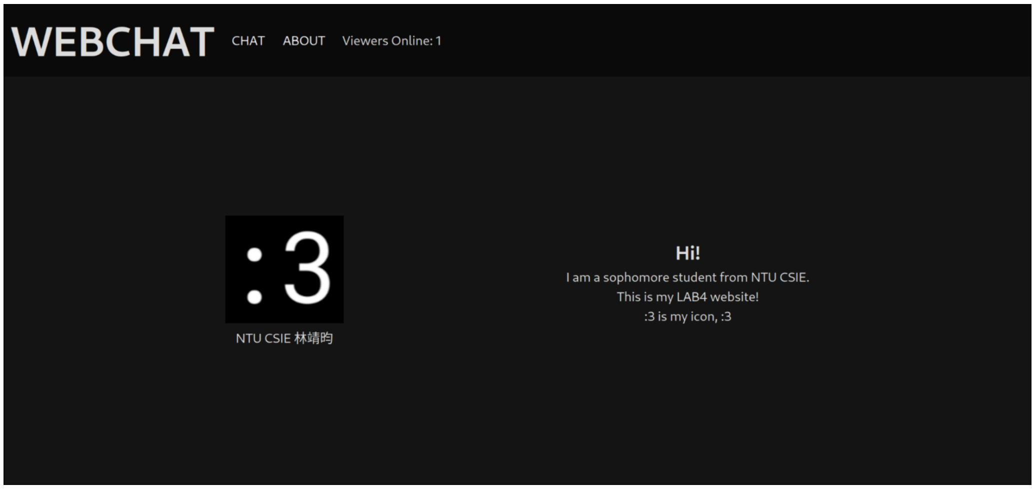
   You have the private key
   d = 0x314235ab3d320f8067994aa0de9c05b0bc346e83c8ba767d1684cc4b10d8aff1
   n is the same
   HW - Q2: What's the message? (the message is in the form: FLAG{...})
   A2: FLAG{y0u kn0w 1254 n0w}



```
··/NetSec/lab04  main via 🐍 v3.13.2
  ▶ cat decrypt.py                                         ▲ 164ms
c = 0x4e2c1f3cdd0ad977399813d9afaa13e1eb224665f9b35f988343d348570570fb
e = 0x10001
n = 0xa233271b7f7eec0e721c745aed5fb67e9d57cb5086863fd922ddae2760edd059
d = 0x314235ab3d320f8067994aa0de9c05b0bc346e83c8ba767d1684cc4b10d8aff1

m = pow(c, d, n)
secret = m.to_bytes(m.bit_length() // 8 + 1).decode()
print(secret)%
··/NetSec/lab04  main via 🐍 v3.13.2
  ▶ python3 decrypt.py                                       ▲ 1ms
FLAG{y0u kn0w 1254 n0w}
```

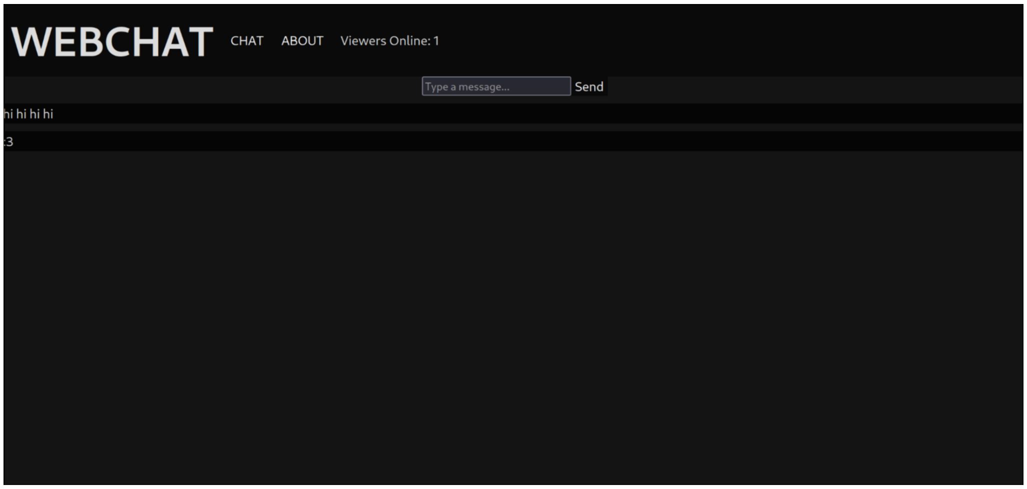
2. Create a website and deploy to GitHub
   Your URL Link:
   https://lexicalerror.github.io/webchat/
   Your Website Screenshot:



NTU CSIE 林靖昀

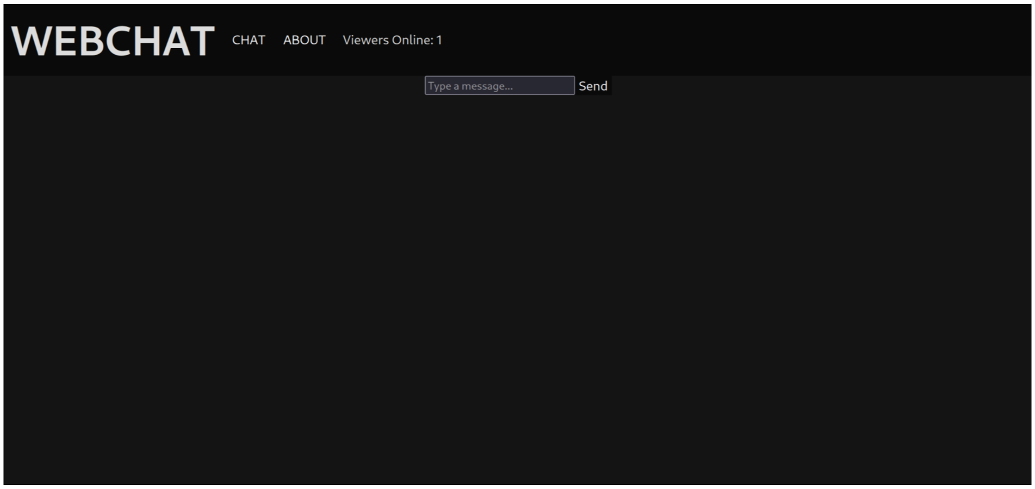
Hi!

I am a sophomore student from NTU CSIE.
This is my LAB4 website!
:3 is my icon, :3



hi hi hi hi

:3



3. Simply introduce yourself in the website.