Isaac Flores
CruzID: **isgflore**
Prof. Miller
CSE13S
November 6, 2022

WRITEUP for ASGN 5: Public Key Cryptography

encryptthis.txt
~/cse13s/asgn5

```
When I look at you
Oh, I don't know what's real
Once in a while
And you make me laugh
And I'll see you tomorrow
And it won't be long
Once in a while
Then you take me down
Then you walk away

When you said 'I do'
Oh, I don't believe you
I can't forget it, no
When you sleep tomorrow
And it won't be long
Once in a while
When you make me smile
And you turn your long blond hair

When I look at you
Oh, I don't know what's real
Once in a while
And you make me laugh
And I'll see you tomorrow
And it won't be long
Once in a while
Then you take me down
Then you walk away
```

This is the text that I want to encrypt. It's just the lyrics to a song I like.

```
isaac@isaac-VirtualBox:~/cse13s/asgn5$ ./keygen -b 256 -i 100 -n pubkey.txt -d privkey.txt -v
username: isaac
user signature (253 bits): 101784074811436380155986580196012934746676549454066088217665305628525523884 04
p (135 bits): 43554813737884338407734193814201031467007
q (121 bits): 2658446484190027802632339966899781631
n - modulus (256 bits): 115788141451030142587378140387123126827046650304572482208238051557027881148417
e - public exponent (254 bits): 16411441575120958572037935366182109205495391845582301778593460715456323826573
d - private exponent (255 bits): 44516794715936813081983718308770982949925150840797383808640699623566702357717
```

I have already run my Makefile for all three programs. I run keygen and store the public key data in pubkey.txt and the private key data in privkey.txt.

pubkey.txt
~/cse13s/asgn5

encrypted_data.txt | decrypted_text.txt | pubkey.txt | privkey.txt

```
fffdc40077e00040203ff6c0420a7fc006f90057f0007fe00fff6011ff7fe001
24488bf85223d4835cf3cec06309a30fabda7cbf8215dc99f6909c8a8a9ab38d
1680c6445525d3ffeab0a6a1e5f71e628d87ced3552a2cec2cecfb24d9bf2f34
isaac
```

This is the data stored in the public key file.

```
fffdc40077e00040203ff6c0420a7fc006f90057f0007fe00fff6011ff7fe001
626b9ce7b142852d6b04092036042906450 8ca37b90d8867ef07dc86a3c92cd5
```

This is the data stored in the private key file. The public modulus in this file matches the public modulus stored in the public key file.

```
isaac@isaac-VirtualBox:~/cse13s/asgn5$ ./encrypt -i encryptthis.txt -o encrypted_data.txt -n pubkey.txt -v
username: isaac
user signature (253 bits): 101784074811436380155986580196012934746676549454066088217665305628525523884 04
n - modulus (256 bits): 115788141451030142587378140387123126827046650304572482208238051557027881148417
e - public exponent (254 bits): 164114415751209585720379353661821092054953918455823017785934607154563238265 73
```

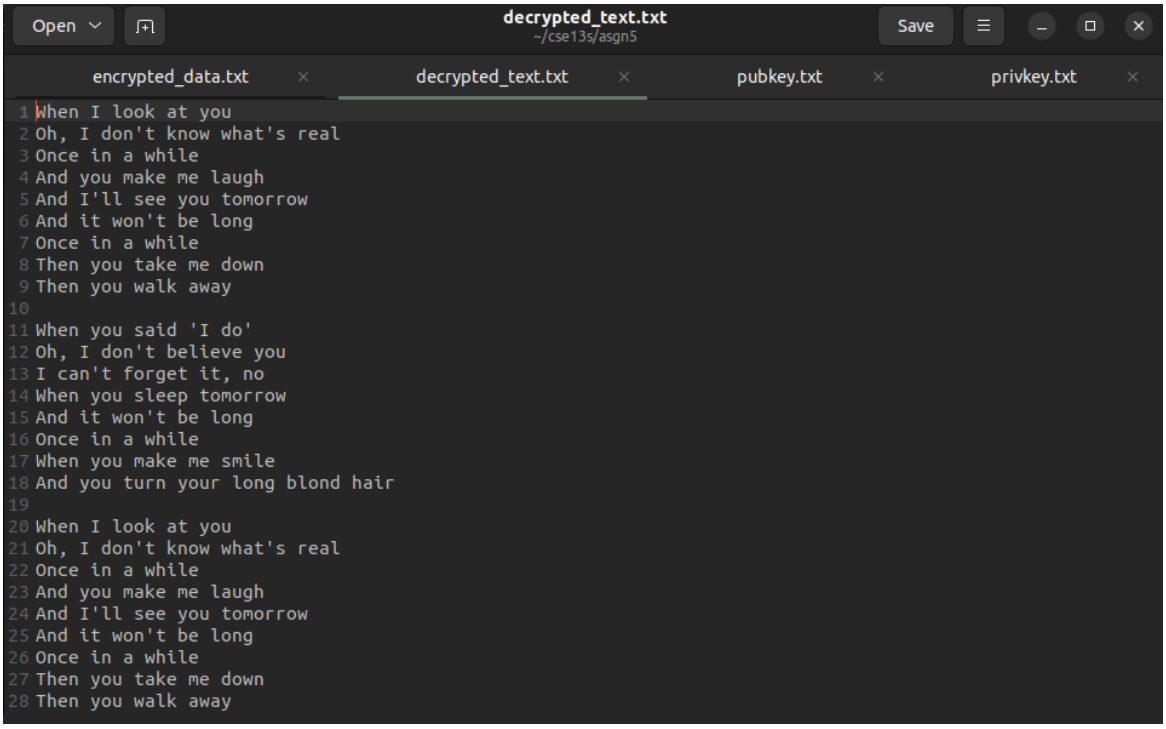
I run encrypt with the input being the lyrics I want to encrypt, the output is stored in encrypted_data.txt, and the public key data stored is in pubkey.txt.

```
bd0f3616df7893c986af0fae196a3cc2628ca4eb6c8c24d71f179103a768ff32
d567c7fc9a1b5c795af1dd2525ede310eaae1cdfc6ce57ca1786d62cb6f3cc88
2f6fdfac184f676e483bc463dafc1f93a19641e7d86f03f0310b041ca8e6c011
5e89c00f416f22beb996e6d2eda0e70d911e546dbfb7aad3739982378203df37
93399725876db109a69fdb019186566738824c9dbff72fd036b74a03dc53a3b2
7048f28a5edf4884e0786504e4292af4abfc302854d7ff7d1d4a69dd33c91639
99a4e376818976f88dab22897a6bbeb4a4495079d3a848902d589df39e600297
ebc866001639689bcf8935beaa6aeb7b3108d1349b7612750ba51f30c70f812e
c816a43997e4fb57b5840c8930f5516614ada4360ef49b4e80179c9f8944cca3
ba80fe6e4a65611d597473fc5eb8b9211919f9278c9d8d57dd34d8ee84476b3
148258154a271b6e4c0fff741e4589138a2c06917f82eef12193469a9d595176
cda56bc18f38b1b1ba3d0c5c5fd7c77e0c3d3e79622065de24393f9ca49964ef
65c0719b2d68c5baa67e9ae71cdf268b6b9dd5cafb5d8258520e6c4060b55376
53d69040fb387776c78371494592642dfa5daa09c8598cebfa4a7e159d0e5085
55ede54802f03a31e57fd3e9199b21b1629099c8ea27cff05eebe842eb86761
5ee17eb68cb6f0573474508ebea2c15cee24047b50b0bea53ccd19778cbe121a
28db1ab75c103296d9dd7b45b5f4816f30dbf86d0361bf6e256e684eb26b1f41
22358118c14b9f5f2926bbff92abee970912afb275f784f9ecc7874abca10c6b
db436f6258ae6b3c56efb7013c43ce4f65dc918d337ca6482854017f8371ce03
```

This is the encrypted data I got from running encrypt.

```
isaac@isaac-VirtualBox:~/cse13s/asgn5$ ./decrypt -i encrypted_data.txt -o decrypted_text.txt -n privkey.txt -v
n - modulus (256 bits): 115788141451030142587378140387123126827046650304572482208238051557027881148417
d - private exponent (255 bits): 44516794715936813081983718308770982949925150840797383808640699623566702357717
```

I run decrypt with the encrypted data I got from running encrypt, the output is stored in decrypted_text.txt, and the private key data is in privkey.txt.



This is the output of decrypt which is the exact same as the data I wanted to encrypt. This means my three programs work since they successfully produced public and private key data, encrypted a file with the public key data, and decrypted the encrypted data with the private key data. The result was the text I wanted to encrypt.