**Assignment description:**

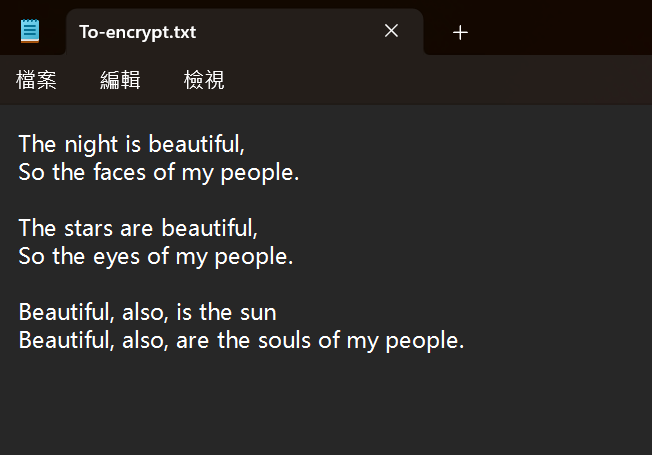
Using Python to build an RSA system. Try to encrypt a text file with a few hundreds words and save the encrypt version. Then read the encrypted file and try to decrypt it.

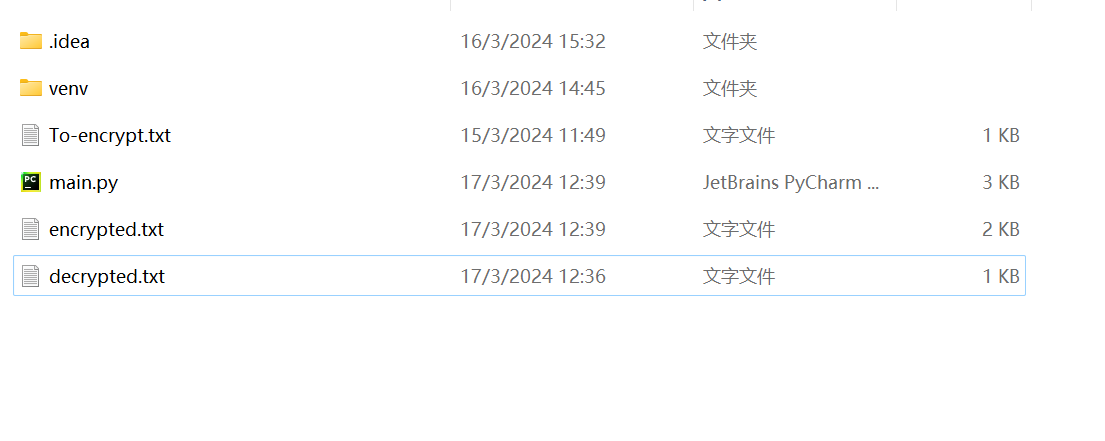
**Function and requirements breakdown:**

1. Generate public and secret key
   1. Function to generate large prime number
2. Encryption and create encrypted file
   1. Function to encrypt the original message
3. Decryption and create decrypted file
   1. Function to decrypt the encrypted message
4. File input and output handling

**Presentation of the program:**

1. Prerequisite, put the To-encrypt.txt file in the same directory with the main.py. The other 2 txt file will be generated afterwards.





1. There are 2 modes : encryption and decryption. Encryption mode produces the Keys and generates the encrypted.txt file.

*Remember to save the Private key or the file can not be decrypted afterwards.*

The message to encrypt should be named "To-encrypt.txt", while the file to decrypt should be named "encrypted.txt".

Enter 'e' for encryption or 'd' for decryption: *e*

Public key: (65537, 861103)

Private key: (775889, 861103)

Encryption completed. The encrypted file 'encrypted.txt' is created.

1. Decryption: Run the program again and enter ‘d’ this time to enter decryption mode.

Please make sure the files are in the correct directory.

The message to encrypt should be named "To-encrypt.txt", while the file to decrypt should be named "encrypted.txt".

Enter 'e' for encryption or 'd' for decryption: *d*

Enter the private key (d): 775889

Enter the modulus (n): 861103

Decryption completed. The decrypted file 'decrypted.txt' is created.