

# project

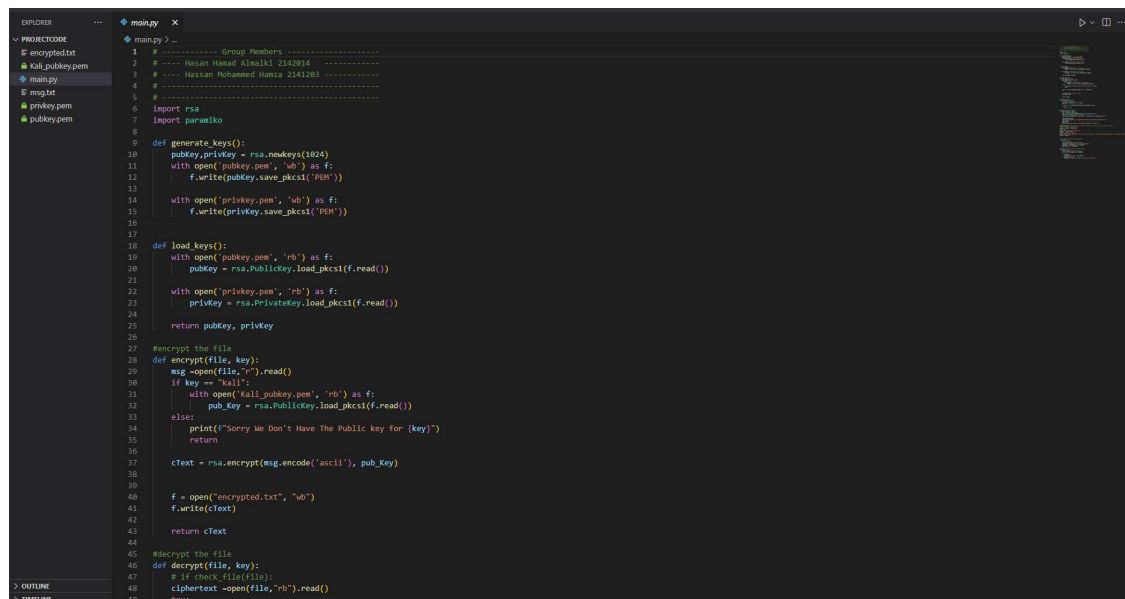
## Secure File Transfer using RSA Encryption

Team Members:

Name: Hasan Hamad Almalki ID: 2142014

Name: Hassan Mohammed Hamza ID: 2141203

## Output of Code



```
1 # ----- Group Members -----
2 # --- Hasan Hamad Almalki 2142014 ---
3 # --- Hassan Mohammed Hamza 2141203 ---
4 # -----
5
6 import rsa
7 import paramiko
8
9 def generate_keys():
10     pubkey, privkey = rsa.newkeys(1024)
11     with open('pubkey.pem', 'wb') as f:
12         f.write(pubkey.save_pkcs1('PEM'))
13     with open('privkey.pem', 'wb') as f:
14         f.write(privkey.save_pkcs1('PEM'))
15
16 def load_keys():
17     with open('pubkey.pem', 'rb') as f:
18         pubkey = rsa.PublicKey.load_pkcs1(f.read())
19     with open('privkey.pem', 'rb') as f:
20         privkey = rsa.PrivateKey.load_pkcs1(f.read())
21     return pubkey, privkey
22
23 #encrypt the file
24 def encrypt(file, key):
25     msg = open(file, 'r').read()
26     if key == 'kali':
27         with open('kali_pubkey.pem', 'rb') as f:
28             pub_key = rsa.PublicKey.load_pkcs1(f.read())
29     else:
30         print("Sorry We Don't Have The Public key for {key}")
31         return
32     ctext = rsa.encrypt(msg.encode('ascii'), pub_key)
33
34     f = open('encrypted.txt', 'wb')
35     f.write(ctext)
36     return ctext
37
38 #decrypt the file
39 def decrypt(file, key):
40     # if check file:
41     ciphertext = open(file, 'rb').read()
42     try:
```

I put the receiver named **kali** and file named **msg.txt**, which will be encrypted using Kali's public key.

```
PS C:\Users\CP\Desktop\projectCode> python main.py
Please choose an option:
1. Send A File
2. Decrypt A File
Please enter the name of the file you wish to open, including the file extension. For example, myfile.txt
1
Enter a File name:msg.txt
Enter the recipient name:kali
The File msg.txt Was Uploaded Successfully to kali
PS C:\Users\CP\Desktop\projectCode> 
```

Once the encrypted file is sent to Kali, it can be decrypted using Kali's private key.

Please choose option 2, then enter the name of the file that was sent to you, and you want to decrypt.

```
(kali㉿kali)-[~/Desktop/projectCCCY312]
$ ls
encrypted.txt  main.py  privkey.pem  pubkey.pem

(kali㉿kali)-[~/Desktop/projectCCCY312]
$ python3 main.py
Please choose an option:
1. Send A File
2. Decrypt A File
Please enter the name of the file you wish to open, including the file extension. For example, myfile.txt
2
Enter a File name:encrypted.txt
Plain text: Hi Dr. Naif,
This message contains sensitive data and has been encrypted using RSA encryption.
```

The decrypted message is.

```
Plain text: Hi Dr. Naif,
This message contains sensitive data and has been encrypted using RSA encryption.
```