EXPERIMENT NO.10

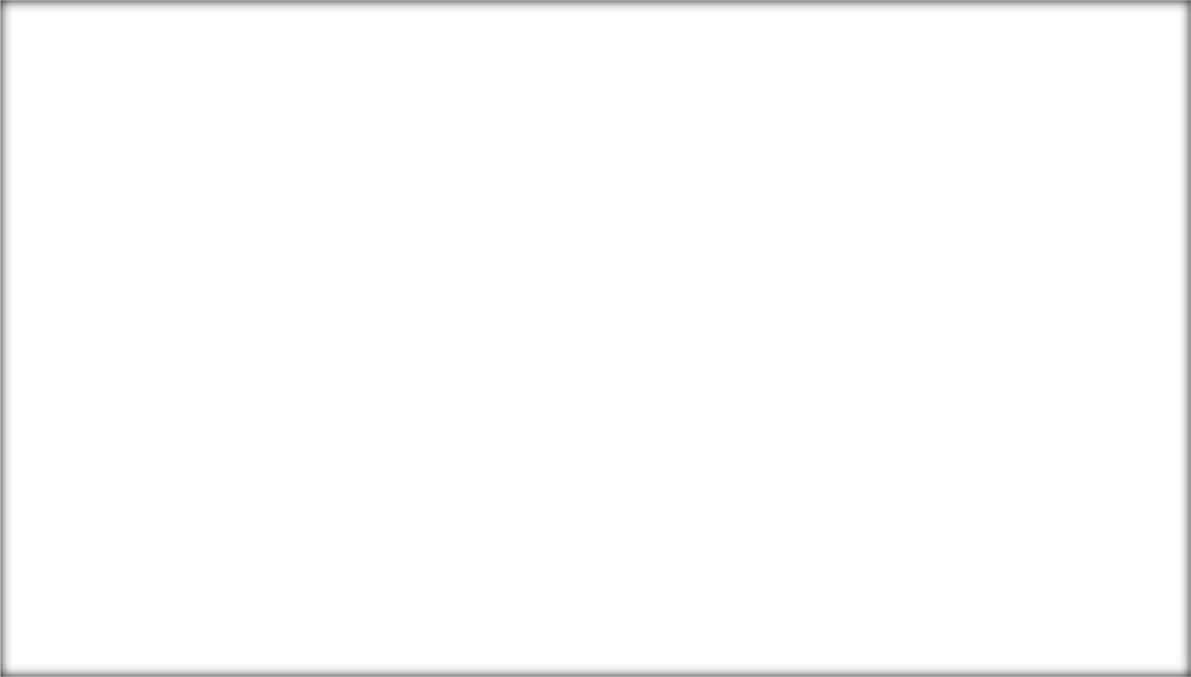
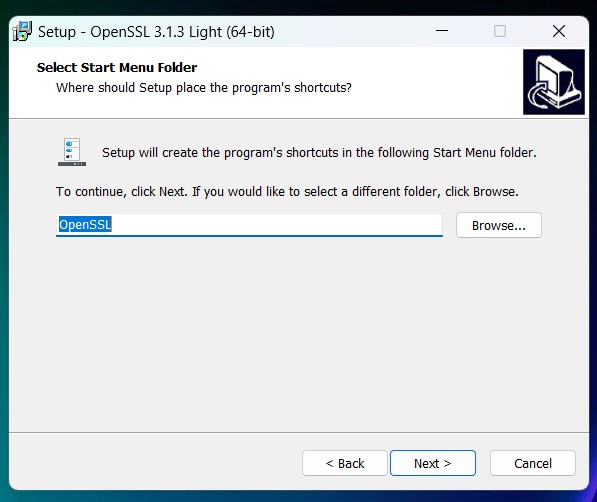
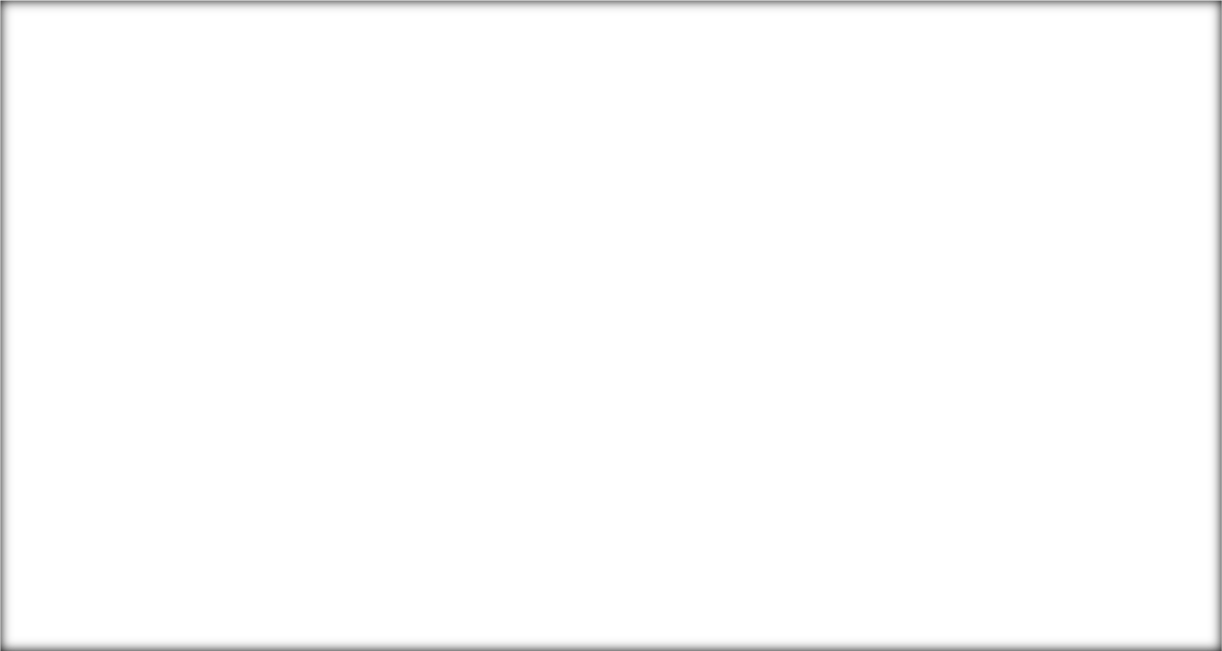
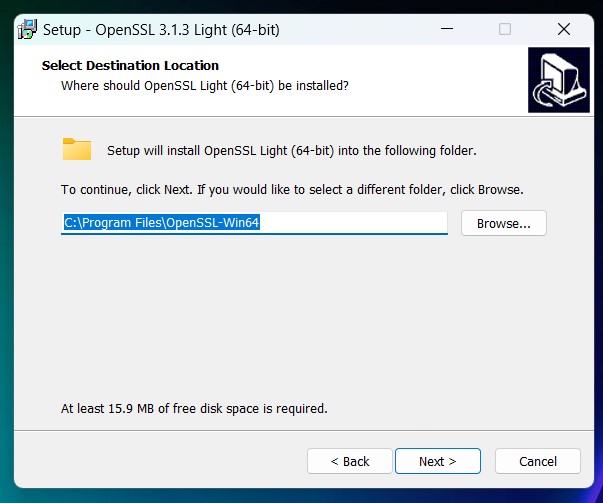
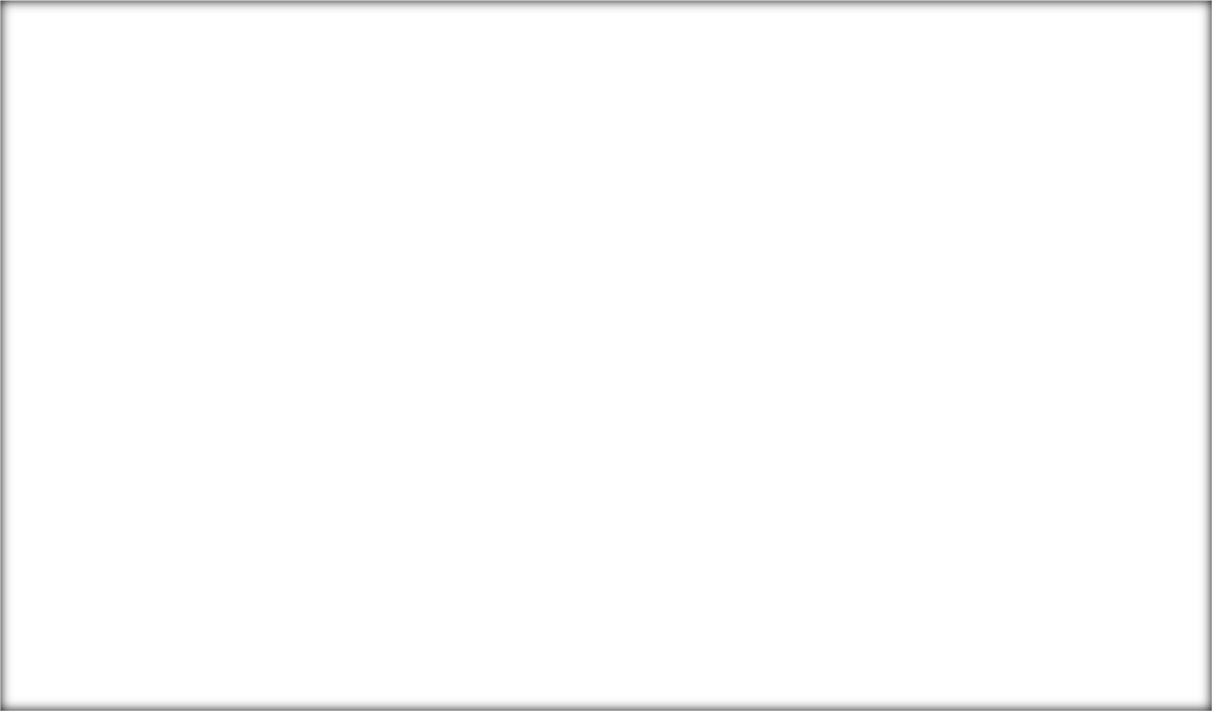
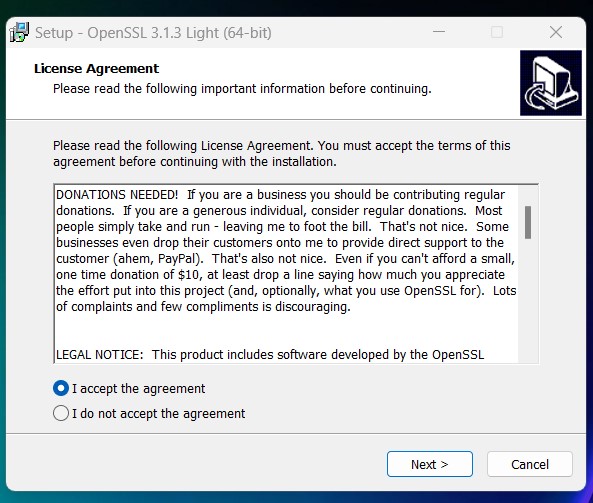
Perform a case study on roll of Private & Public Key.

Title: Perform a case study on roll of Private & Public Key.

Objective: Students will be able to implement a case study on roll of Private & Public Key.

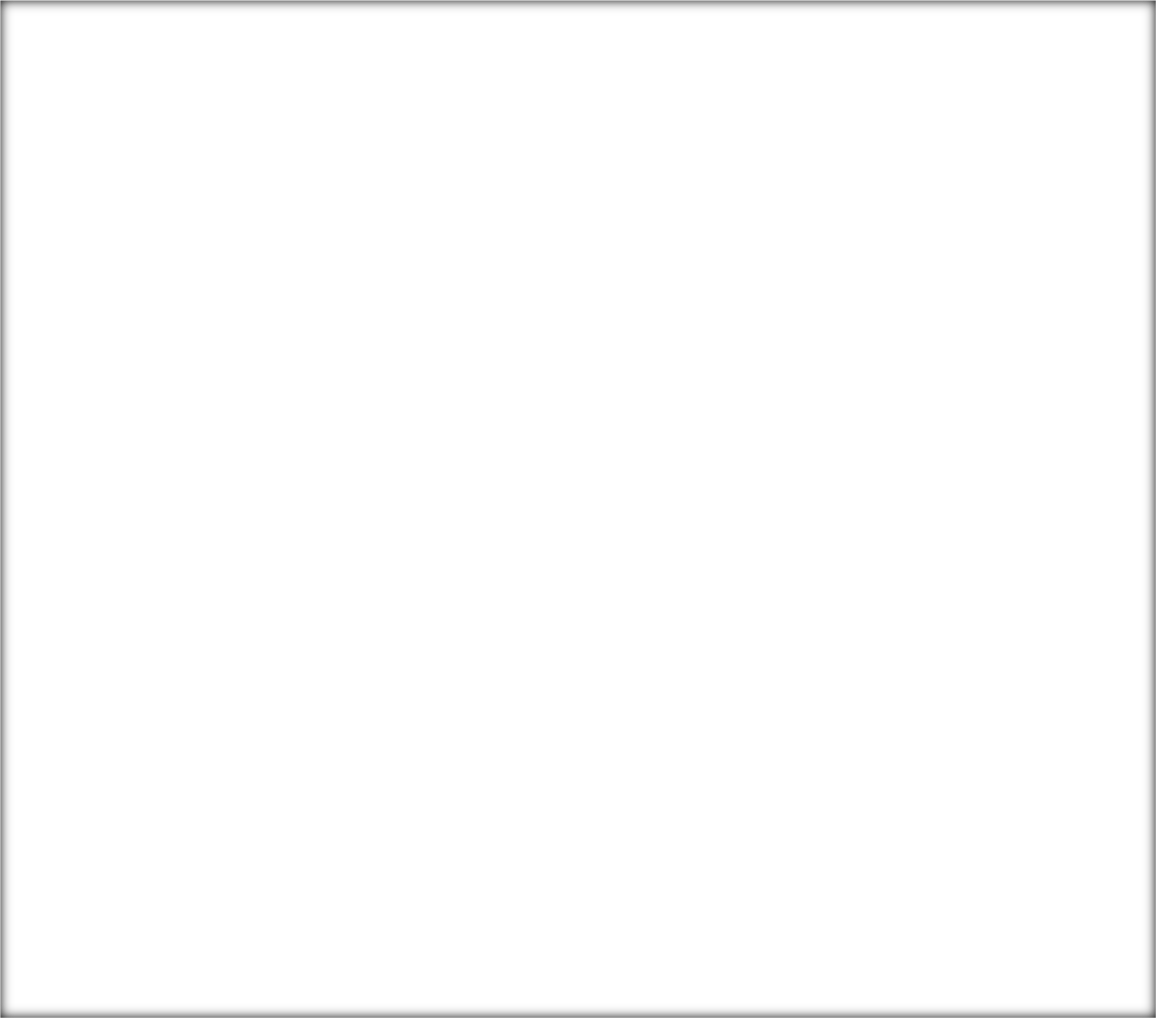
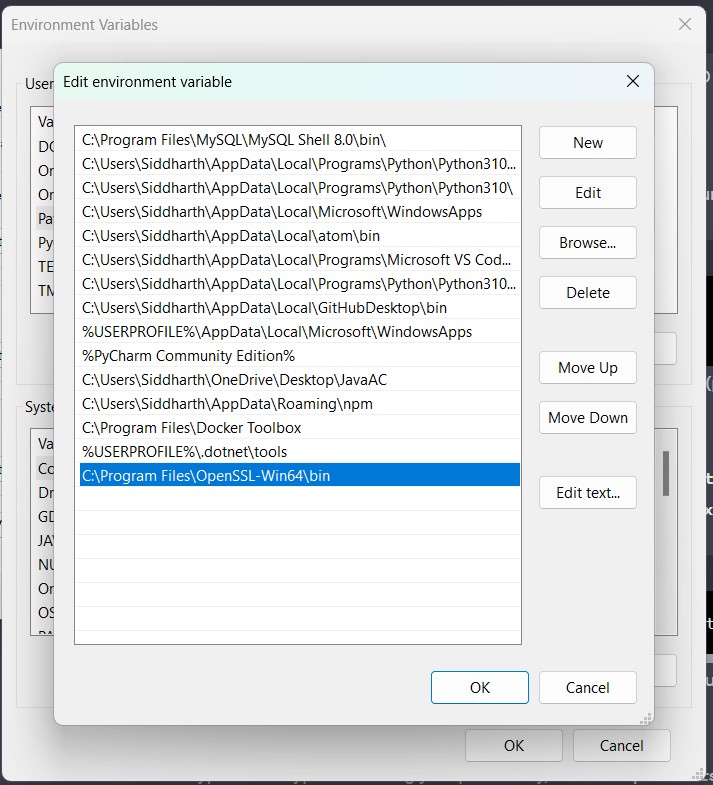
Step 1:

Download the Openssl



Installed step.

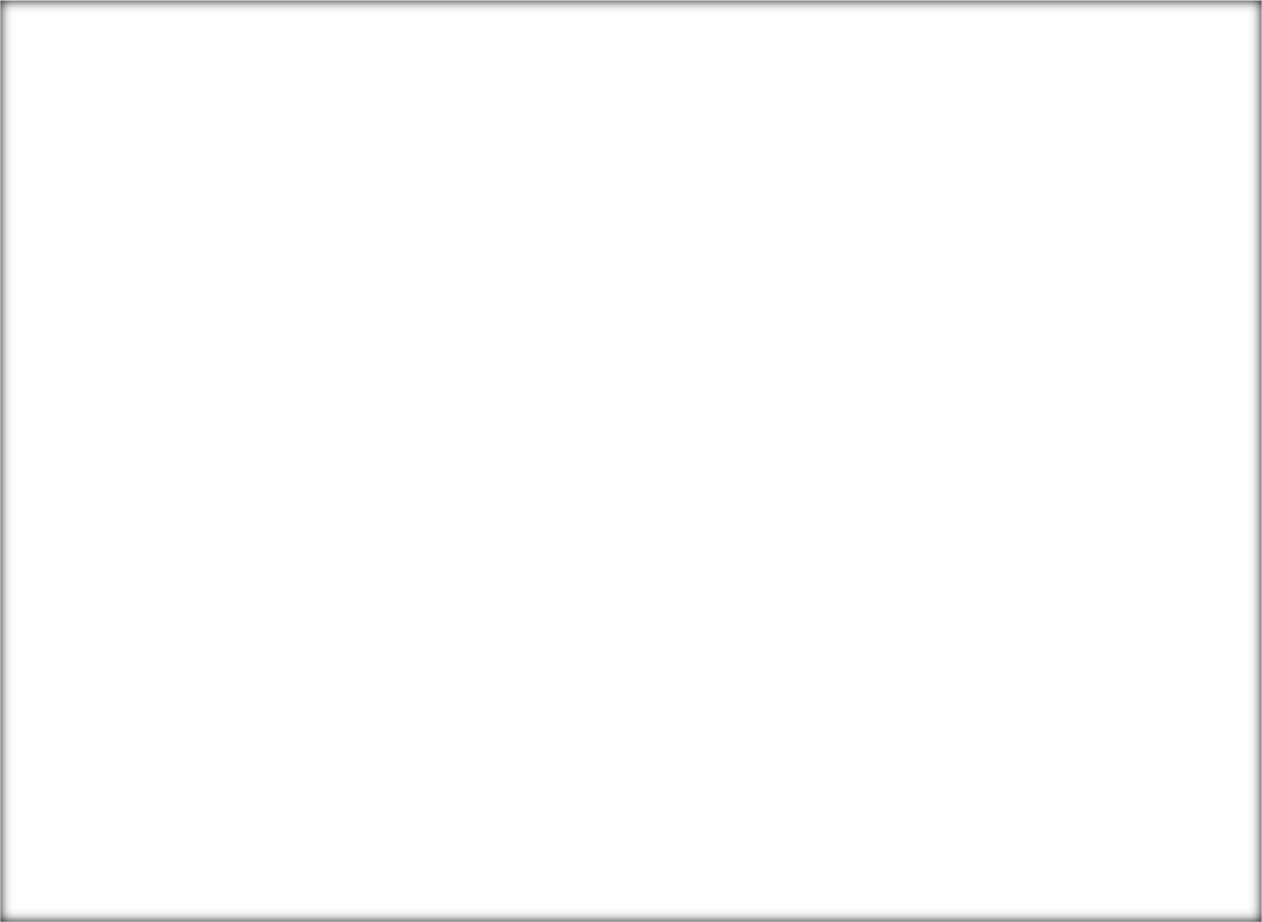
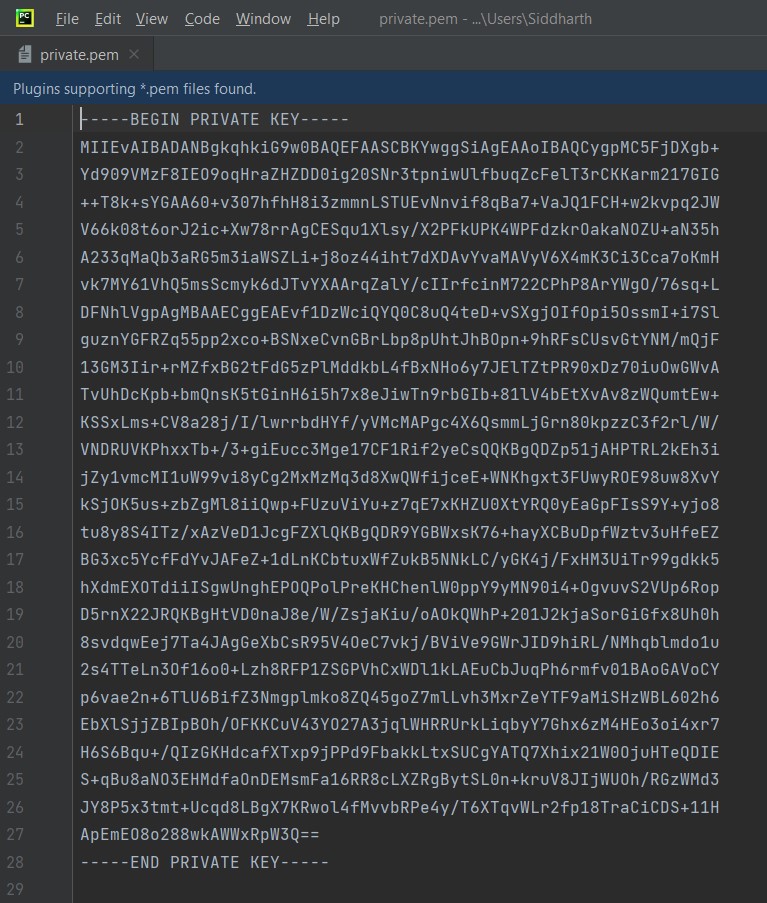
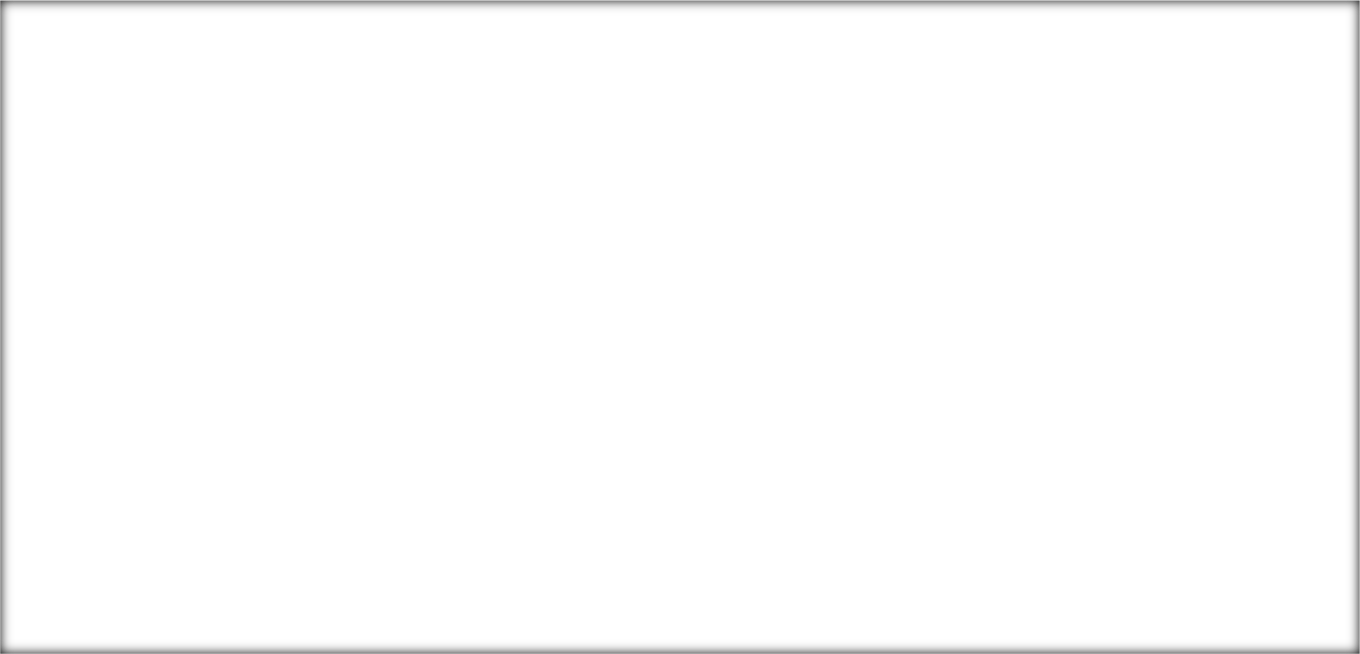
1. Edit in system environment variable



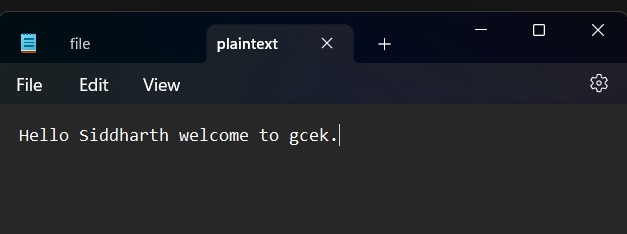
1. Check openssl version command & Create the private key.

Private key created as private.pem

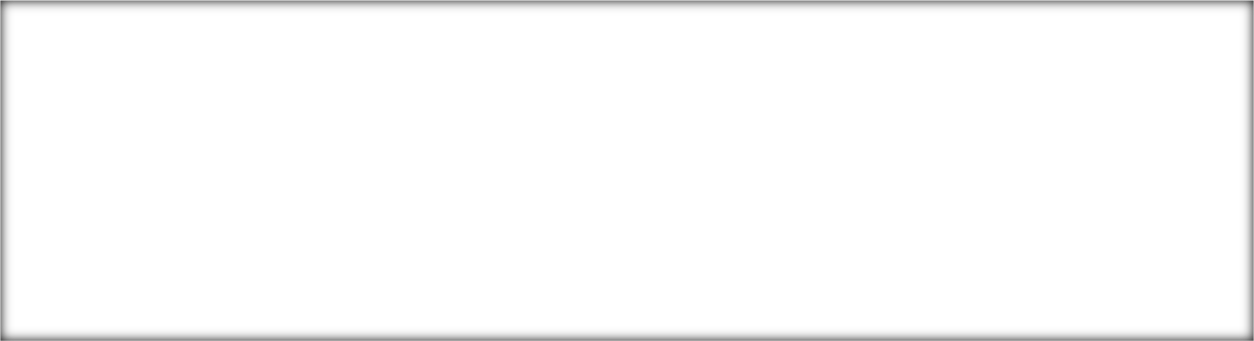
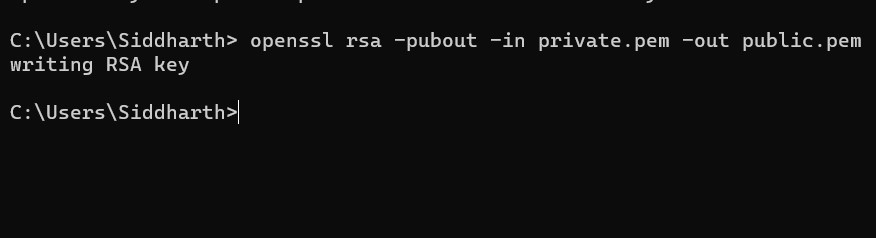
Private key created:



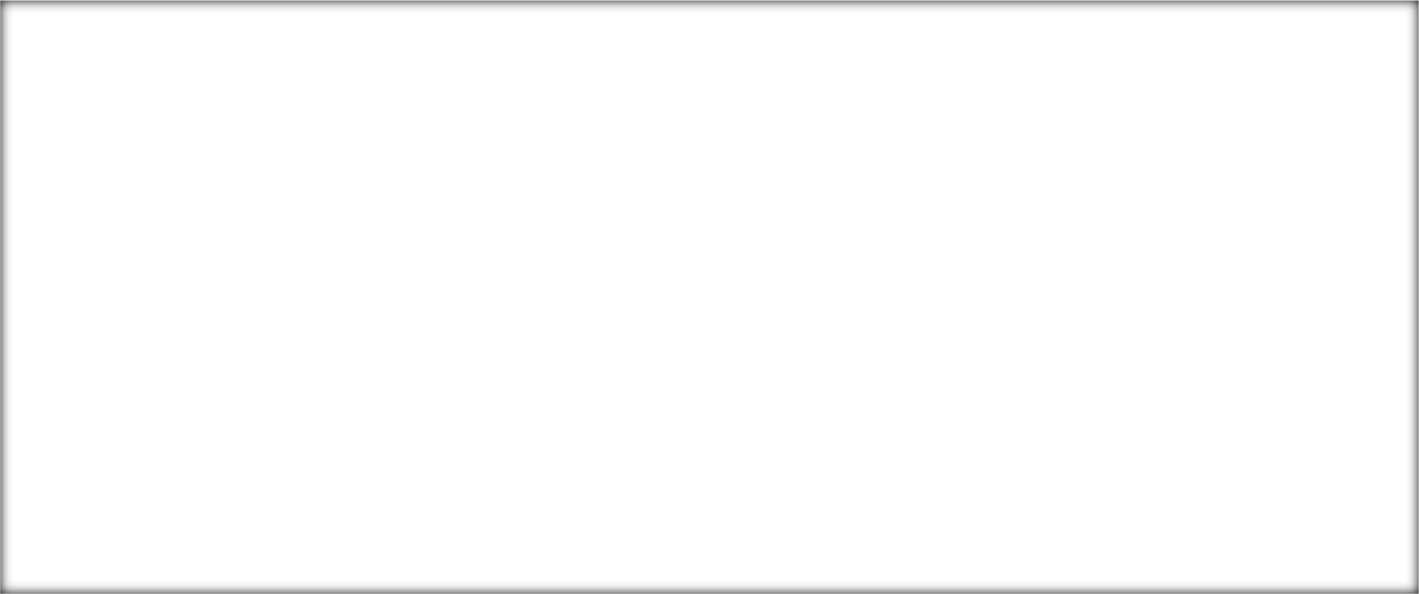
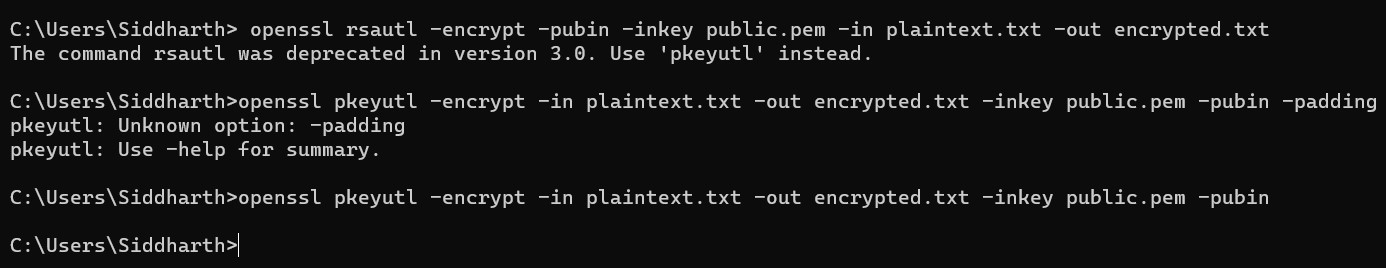
1. Plaintext file - plaintext.txt



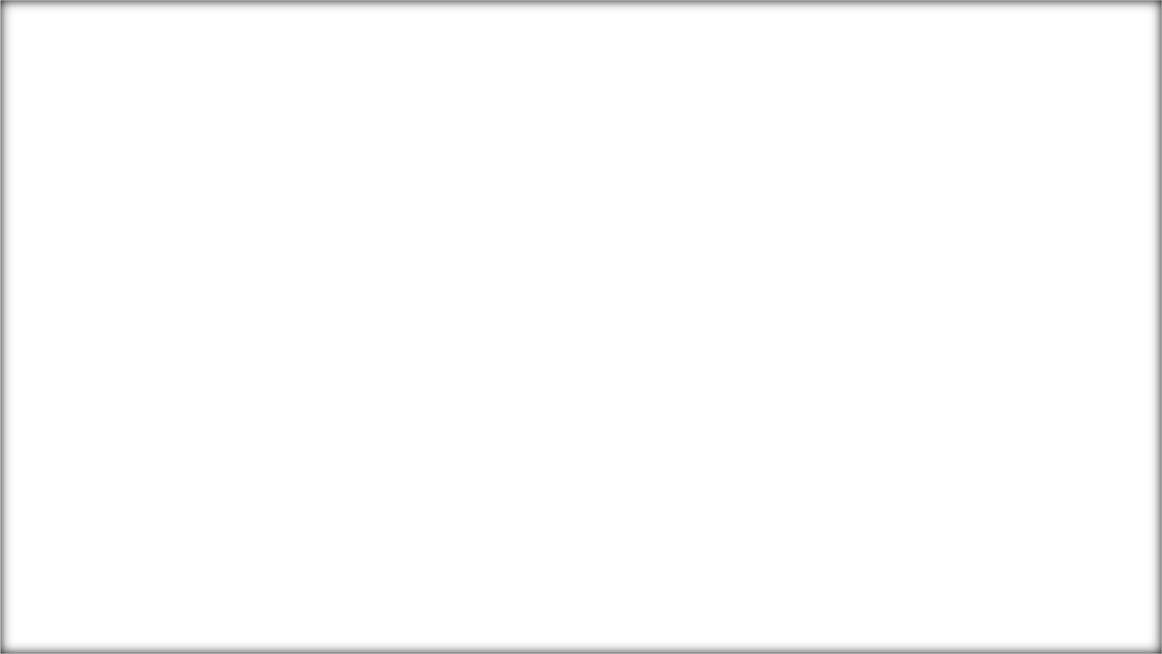
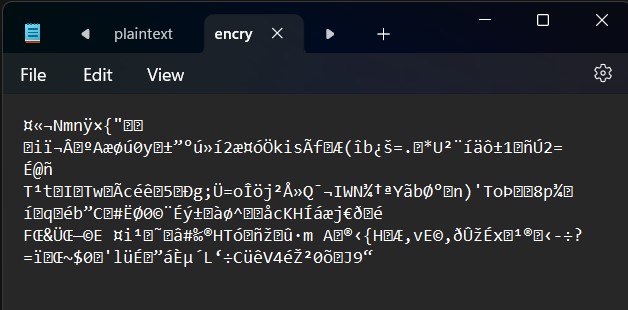
1. Extract the public key (public.pem) from it.



1. Encryption: To encrypt a message using the recipient's public key, use the pkeyutl command. Replace public.pem with the recipient's public key file and plaintext.txt with the file



1. Encrypted file –



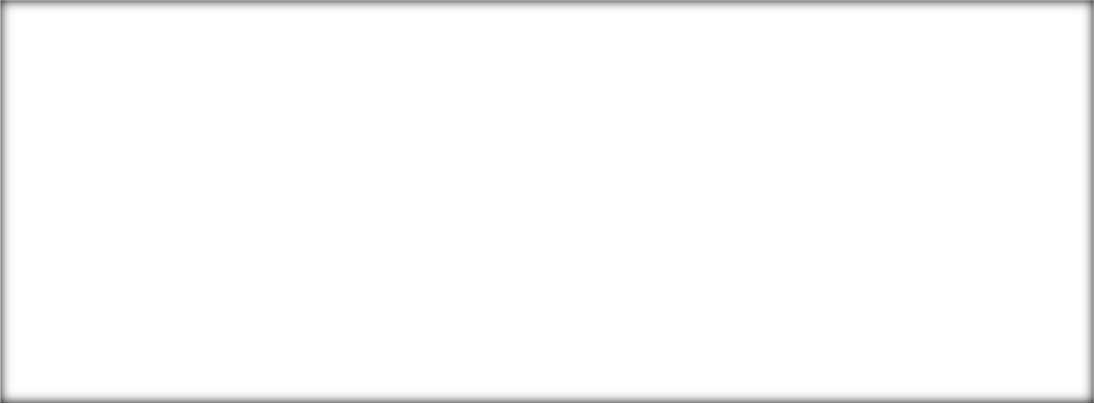
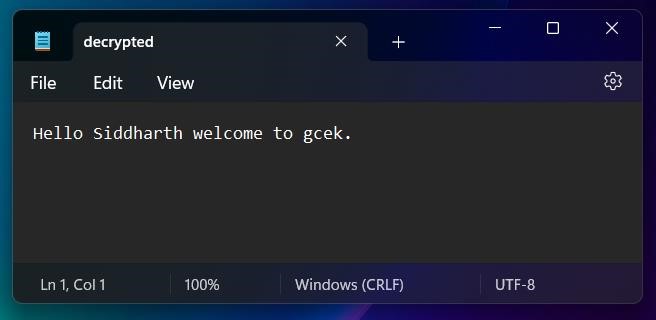
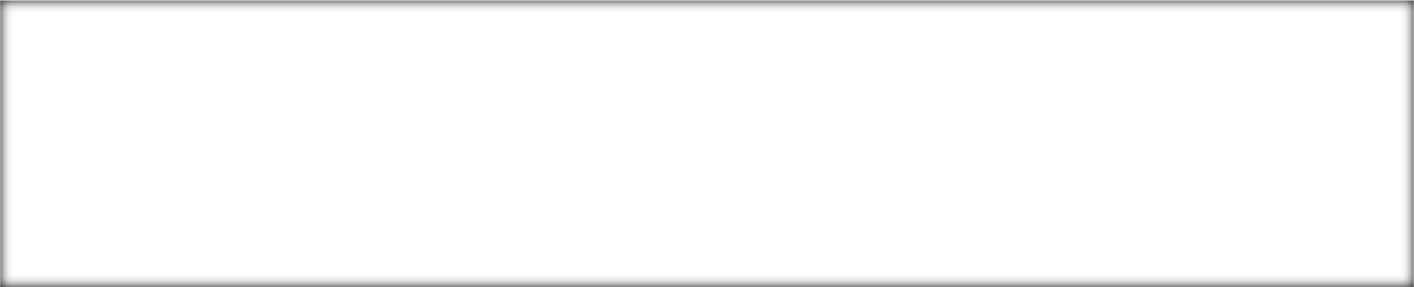
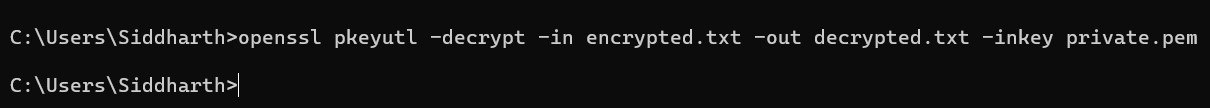
1. Decryption-

To decrypt the encrypted message using your private key, use the pkeyutl command again. Replace private.pem with your private key file and encrypted.txt with the file.

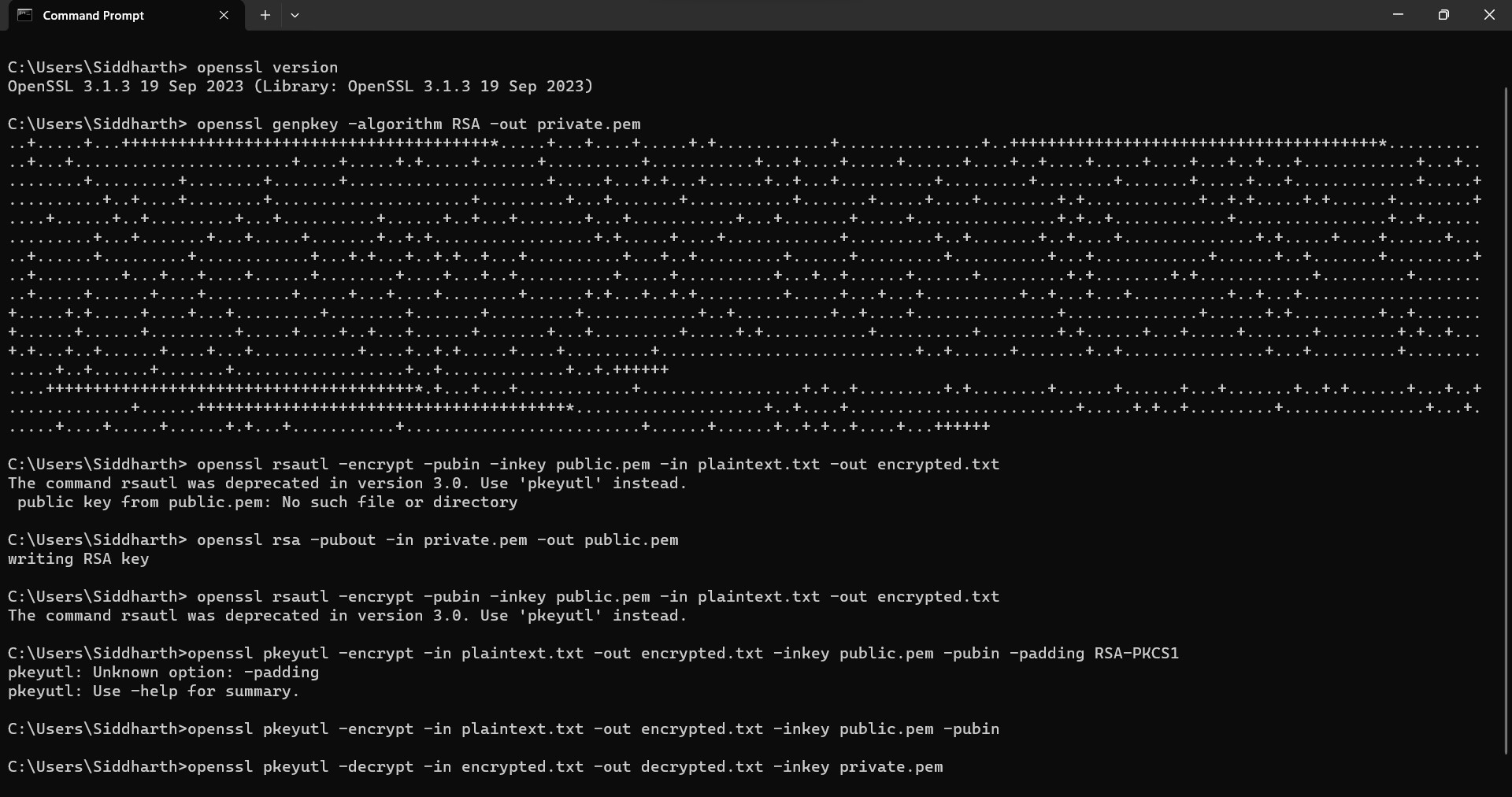
9

. Decrypted file

–



Complete commands:



Microsoft Windows [Version 10.0.22621.2428] (c) Microsoft Corporation. All rights reserved.

C:\Users\Siddharth> openssl version

OpenSSL 3.1.3 19 Sep 2023 (Library: OpenSSL 3.1.3 19 Sep 2023)

C:\Users\Siddharth> openssl genpkey -algorithm RSA -out private.pem

..+.....+...+++++++++++++++++++++++++++++++++++++++\*.....+...+....+.....+.

+............+...............+..+++++++++++++++++++++++++++++++++++++++\*.......

.....+...+.......................+....+.....+.+.....+......+..........+...........+...+....+.....+......+....+..+. ...+.....+....+...+..+...+............+...+..........+.........+........+.......+.....................+.....+...+.

+...+......+..+...+..........+.........+........+.......+.....+...+.............+.....+..........+..+....+........ +.....................+.........+...+.......+...........+.......+.....+....+........+.+............+..+.+.....+.+.

.....+........+....+......+..+.........+...+..........+......+..+...+.......+...+...........+...+.......+.....+.

..............+.+..+............+................+..+...............+...+.......+...+.....+.......+..+.+............ .....+.+.....+....+............+.........+..+.......+..+....+..............+.+.....+....+......+.....+......+... ......+............+...+.+...+..+.+..+...+..........+...+..+.........+......+.........+..........+...+.......... ..+......+..+.......+.........+..+.........+...+...+....+......+........+....+...+..+..........+.....+.......... +...+..+......+......+.........+.+........+.+............+.........+.........+.....+......+....+.........+.....+

...+....+........+......+.+...+..+.+.........+.....+...+...+..........+..+...+...+..........+..+...+.......... .........+.....+.+.....+....+...+.........+........+.......+.........+............+..+..........+..+....+.......... .....+..............+......+.+.........+..+.......+......+......+.........+.....+....+..+...+......+.......+...+ .........+.....+.+...........+..........+........+.+......+...+.....+.......+........+.+..+...+.+...+..+......

+....+...+...........+....+..+.+.....+....+.........+...........................+..+......+.......+..+.............

..+...+.........+.............+..+......+.......+..................+..+.............+..+.++++++

....+++++++++++++++++++++++++++++++++++++++\*.+...+...+............+...........

......+.+..+.........+.+........+......+......+...+.......+..+.+......+...+..+.............+......+++++++

++++++++++++++++++++++++++++++++\*....................+..+....+........................+

.....+.+..+.........+...............+...+......+....+.....+......+.+...+...........+.........................+......

+......+..+.+..+....+...++++++

C:\Users\Siddharth> openssl rsautl -encrypt -pubin -inkey public.pem -in plaintext.txt -out encrypted.txt

The command rsautl was deprecated in version 3.0. Use 'pkeyutl' instead. public key from public.pem: No such file or directory

C:\Users\Siddharth> openssl rsa -pubout -in private.pem -out public.pem writing RSA key

C:\Users\Siddharth> openssl rsautl -encrypt -pubin -inkey public.pem -in plaintext.txt -out encrypted.txt

The command rsautl was deprecated in version 3.0. Use 'pkeyutl' instead.

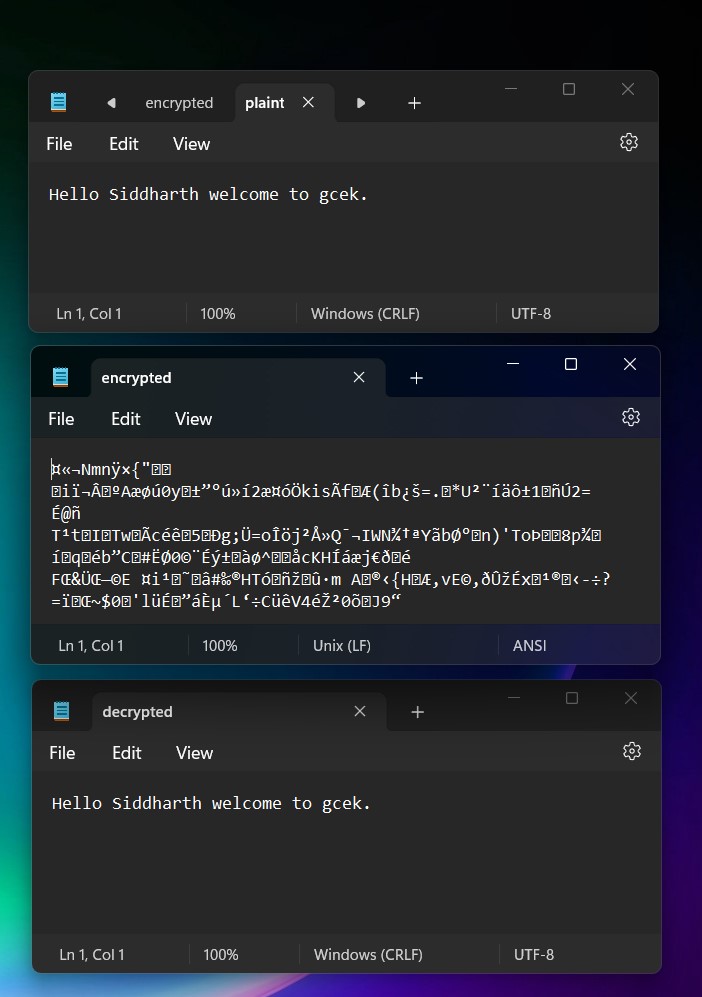
C:\Users\Siddharth>openssl pkeyutl -encrypt -in plaintext.txt -out encrypted.txt -inkey public.pem -pubin -padding RSA-PKCS1 pkeyutl: Unknown option: -padding pkeyutl: Use -help for summary.

C:\Users\Siddharth>openssl pkeyutl -encrypt -in plaintext.txt -out encrypted.txt -inkey public.pem -pubin

C:\Users\Siddharth>openssl pkeyutl -decrypt -in encrypted.txt -out decrypted.txt -inkey private.pem

C:\Users\Siddharth>

Output:

Sender File

Encrypted File

Receiver/Decrypted

File

Conclusion:

In this case study, I have studied and implemented roll of Private & Public Key.