ISC ASSIGNMENT -08_part2

ROLL NO: U21CS052

NAME : PANCHAL GUNGUN PARESH

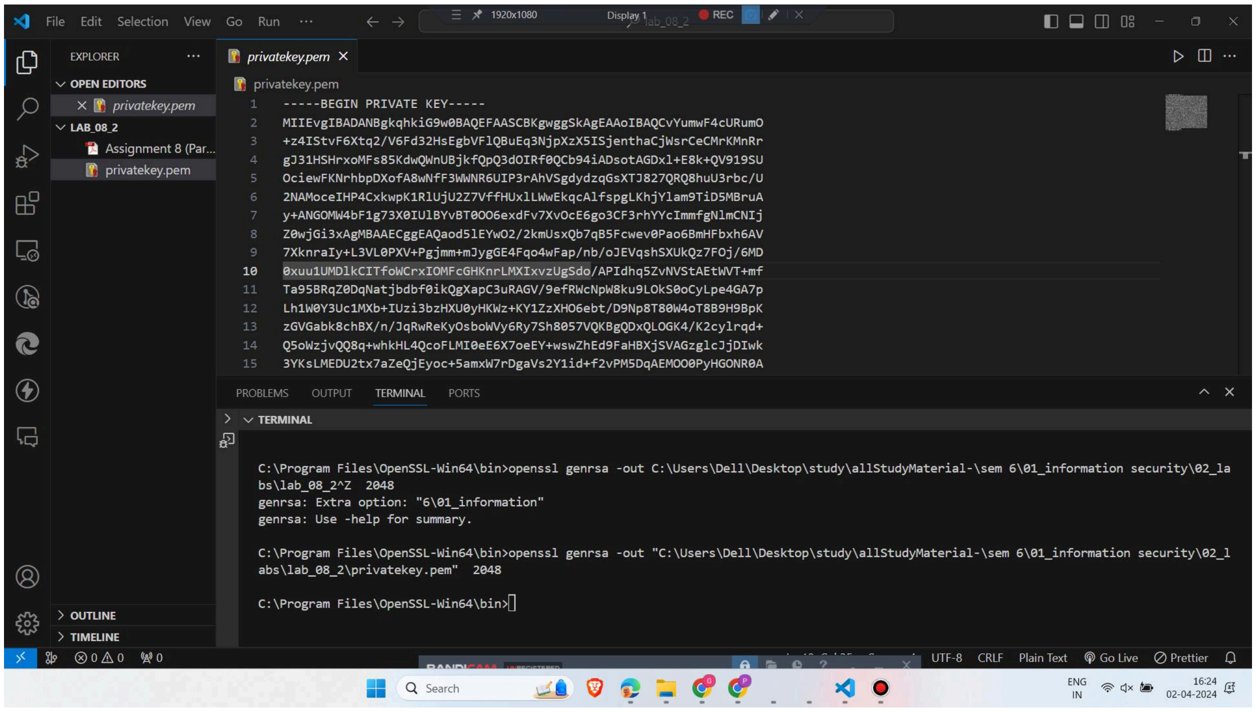
OpenSSL Library commands.

Task 3: Perform the following instructions to digitally sign a document and verify it.

a) Generate a private key using RSA asymmetric cryptography technique.

Private Key Generation:

openssl genrsa -out privatekey.pem 2048



privatekey.pem

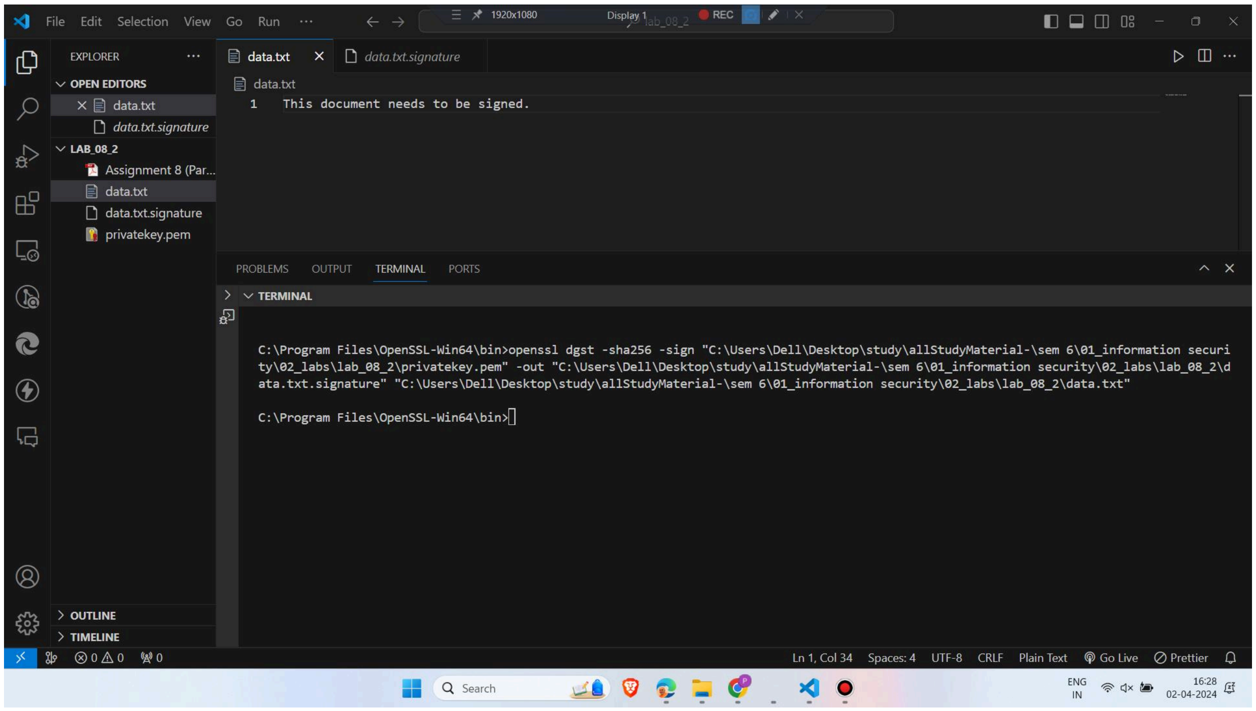
```
-----BEGIN PRIVATE KEY-----
MIIEvgIBADANBgkqhkiG9w0BAQEFAASCBKgwggSkAgEAAoIBAQCvYumwF4cURumO
+z4IStvF6Xtq2/V6Fd32HsEgbVFlQBuEq3NjpXzX5ISjenthaCjWsrCeCMrKMnRr
gJ31HSHrxoMFs85KdwQWnUBjkfQpQ3dOIRf0QCb94iADsotAGDxl+E8k+QV919SU
OciewFKNrhbpDXofA8wNfF3WWNR6UIP3rAhVSgdydzqGsXTJ827QRQ8huU3rbc/U
2NAMoceIHP4CxkwpK1RlUjU2Z7VffHUxlLWwEkqcAlfspgLKhjYlam9TiD5MBruA
y+ANGOMW4bF1g73X0IUlBYvBT0OO6exdFv7XvOcE6go3CF3rhYYcImmfgNlmCNIj
Z0wjGi3xAgMBAAECggEAQaod5lEYwO2/2kmUsxQb7qB5Fcwev0Pao6BmHFbxh6AV
7XknraIy+L3VL0PXV+Pgjmm+mJygGE4Fqo4wFap/nb/oJEVqshSXUkQz7FOj/6MD
0xuu1UMDlkCITfoWCrxIOMFcGHKnrLMXIxvzUgSdo/APIdhq5ZvNVStAEtWVT+mf
Ta95BRqZ0DqNatjbdbf0ikQgXapC3uRAGV/9efRWcNpW8ku9LOkS0oCyLpe4GA7p
Lh1W0Y3Uc1MXb+IUzi3bzHXU0yHKWz+KY1ZzXHO6ebt/D9Np8T80W4oT8B9H9BpK
zGVGabk8chBX/n/JqRwReKyOsboWVy6Ry7Sh8057VQKBgQDxQLOGK4/K2cylrqd+
Q5oWzjvQQ8q+whkHL4QcoFLMI0eE6X7oeEY+wswZhEd9FaHBXjSVAGzglcJjDIwk
3YKsLMEDU2tx7aZeQjEyoc+5amxW7rDgaVs2Y1id+f2vPM5DqAEMOO0PyHGONR0A
```

TERMINAL

```
C:\Program Files\OpenSSL-Win64\bin>openssl genrsa -out C:\Users\Dell\Desktop\study\allStudyMaterial-\sem 6\01_information security\02_la
bs\lab_08_2^Z  2048
genrsa: Extra option: "6\01_information"
genrsa: Use -help for summary.

C:\Program Files\OpenSSL-Win64\bin>openssl genrsa -out "C:\Users\Dell\Desktop\study\allStudyMaterial-\sem 6\01_information security\02_l
abs\lab_08_2\privatekey.pem"  2048

C:\Program Files\OpenSSL-Win64\bin>
```

b) Digitally Sign a document data.txt.

openssl dgst -sha256 -sign privatekey.pem -out data.txt.signature data.txt



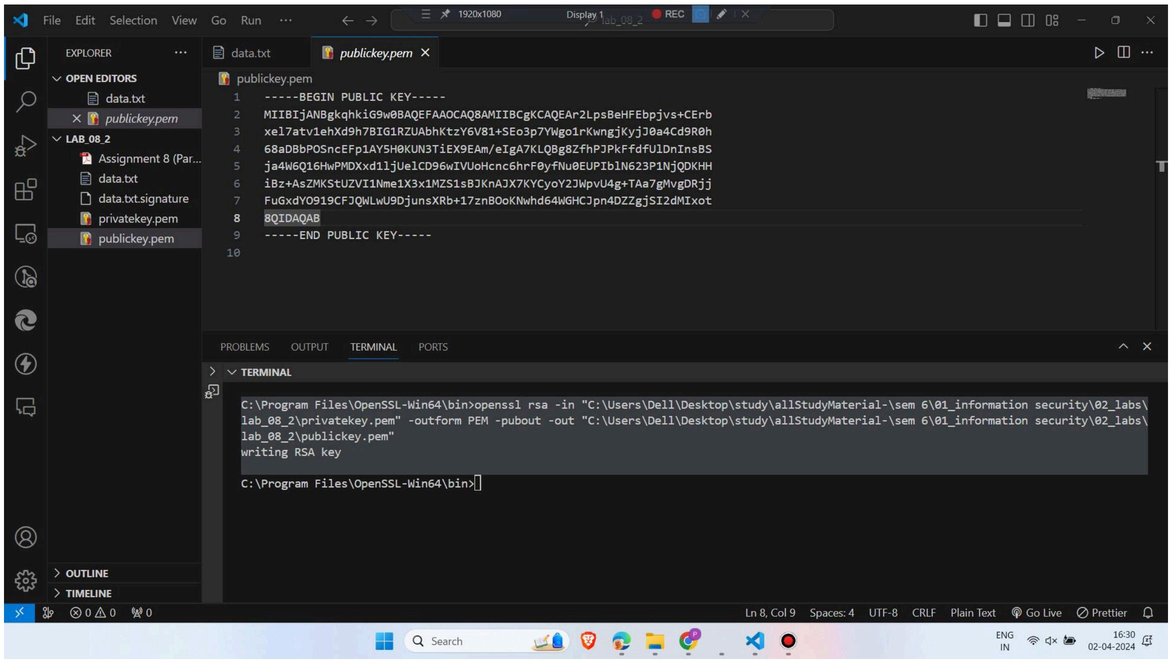
```
This document needs to be signed.
```

```
C:\Program Files\OpenSSL-Win64\bin>openssl dgst -sha256 -sign "C:\Users\Dell\Desktop\study\allStudyMaterial-\sem 6\01_information securi
ty\02_labs\lab_08_2\privatekey.pem" -out "C:\Users\Dell\Desktop\study\allStudyMaterial-\sem 6\01_information security\02_labs\lab_08_2\d
ata.txt.signature" "C:\Users\Dell\Desktop\study\allStudyMaterial-\sem 6\01_information security\02_labs\lab_08_2\data.txt"

C:\Program Files\OpenSSL-Win64\bin>
```

c) Generate a public key using RSA asymmetric cryptography technique to verify the document data.txt.signature.

Public Key Generation:

openssl rsa -in privatekey.pem -outform PEM -pubout -out publickey.pem

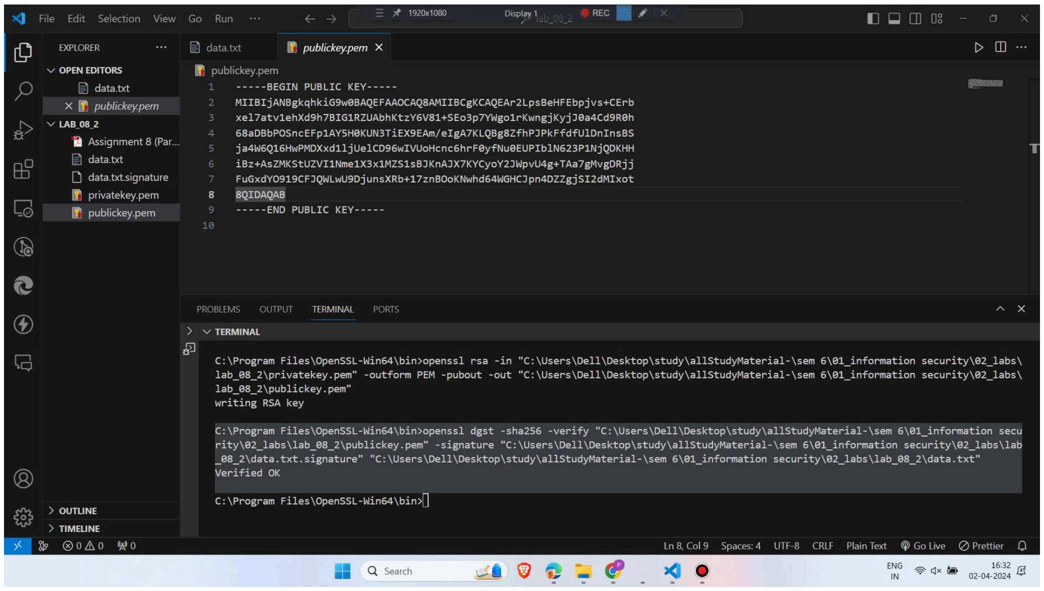


```
-----BEGIN PUBLIC KEY-----
MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAr2LpsBeHFEbpjvs+CErb
xel7atv1ehXd9h7BIG1RZUAbhKtzY6V81+SEo3p7YWgo1rKwngjKyjJ0a4Cd9R0h
68aDBbPOSncEFp1AY5H0KUN3TiEX9EAm/eIgA7KLQBg8ZfhPJPkFfdfUlDnInsBS
ja4W6Q16HwPMDXxd1ljUelCD96wIVUoHcnc6hrF0yfNu0EUPIblN623P1NjQDKHH
iBz+AsZMKStUZVI1Nme1X3x1MZS1sBJKnAJX7KYCyoY2JWpvU4g+TAa7gMvgDRjj
FuGxdYO919CFJQWLwU9DjunsXRb+17znBOoKNwhd64WGHCJpn4DZZgjSI2dMIxot
8QIDAQAB
-----END PUBLIC KEY-----
```

```
C:\Program Files\OpenSSL-Win64\bin>openssl rsa -in "C:\Users\Dell\Desktop\study\allStudyMaterial-\sem 6\01_information security\02_labs\
lab_08_2\privatekey.pem" -outform PEM -pubout -out "C:\Users\Dell\Desktop\study\allStudyMaterial-\sem 6\01_information security\02_labs\
lab_08_2\publickey.pem"
writing RSA key

C:\Program Files\OpenSSL-Win64\bin>
```

Verification:

openssl dgst -sha256 -verify publickey.pem -signature data.txt.signature data.txt



```
-----BEGIN PUBLIC KEY-----
MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAr2LpsBeHFEbpjvs+CErb
xel7atv1ehXd9h7BIG1RZUAbhKtzY6V81+SEo3p7YWgo1rKwngjKyjJ0a4Cd9R0h
68aDBbPOSncEFp1AY5H0KUN3TiEX9EAm/eIgA7KLQBg8ZfhPJPkFfdfUlDnInsBS
ja4W6Q16HwPMDXxd1ljUelCD96wIVUoHcnc6hrF0yfNu0EUPIblN623P1NjQDKHH
iBz+AsZMKStUZVI1Nme1X3x1MZS1sBJKnAJX7KYCyoY2JWpvU4g+TAa7gMvgDRjj
FuGxdYO919CFJQWLwU9DjunsXRb+17znBOoKNwhd64WGHCJpn4DZZgjSI2dMIxot
8QIDAQAB
-----END PUBLIC KEY-----
```

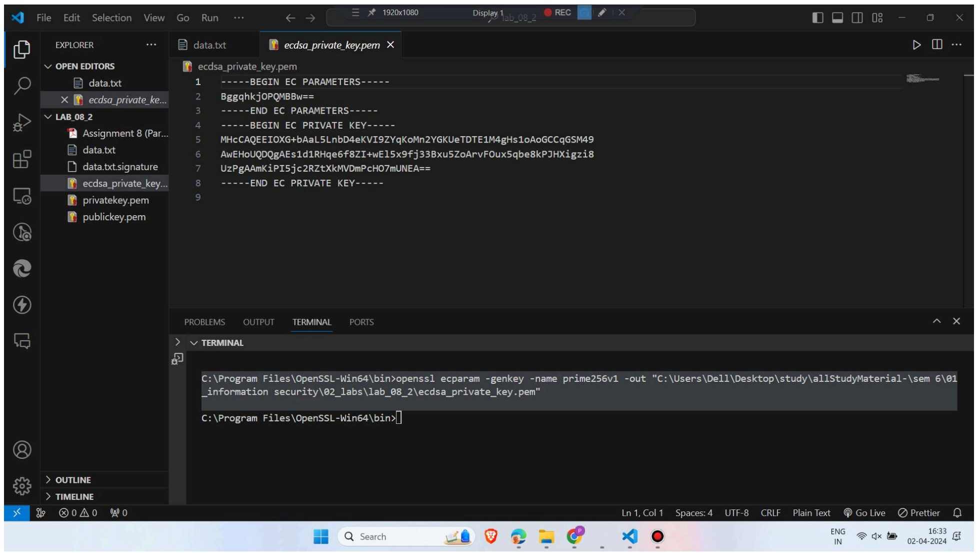
```
C:\Program Files\OpenSSL-Win64\bin>openssl rsa -in "C:\Users\Dell\Desktop\study\allStudyMaterial-\sem 6\01_information security\02_labs\
lab_08_2\privatekey.pem" -outform PEM -pubout -out "C:\Users\Dell\Desktop\study\allStudyMaterial-\sem 6\01_information security\02_labs\
lab_08_2\publickey.pem"
writing RSA key

C:\Program Files\OpenSSL-Win64\bin>openssl dgst -sha256 -verify "C:\Users\Dell\Desktop\study\allStudyMaterial-\sem 6\01_information secu
rity\02_labs\lab_08_2\publickey.pem" -signature "C:\Users\Dell\Desktop\study\allStudyMaterial-\sem 6\01_information security\02_labs\lab
_08_2\data.txt.signature" "C:\Users\Dell\Desktop\study\allStudyMaterial-\sem 6\01_information security\02_labs\lab_08_2\data.txt"
Verified OK

C:\Program Files\OpenSSL-Win64\bin>
```

Task 4:

To perform ECDSA (Elliptic Curve Digital Signature Algorithm) digital signature generation and verification follow these steps. ECDSA is based on elliptic curve cryptography and is commonly used for digital signatures.

a) Generate ECDSA Private Key

openssl ecparam -genkey -name prime256v1 -out ecdsa_private_key.pem

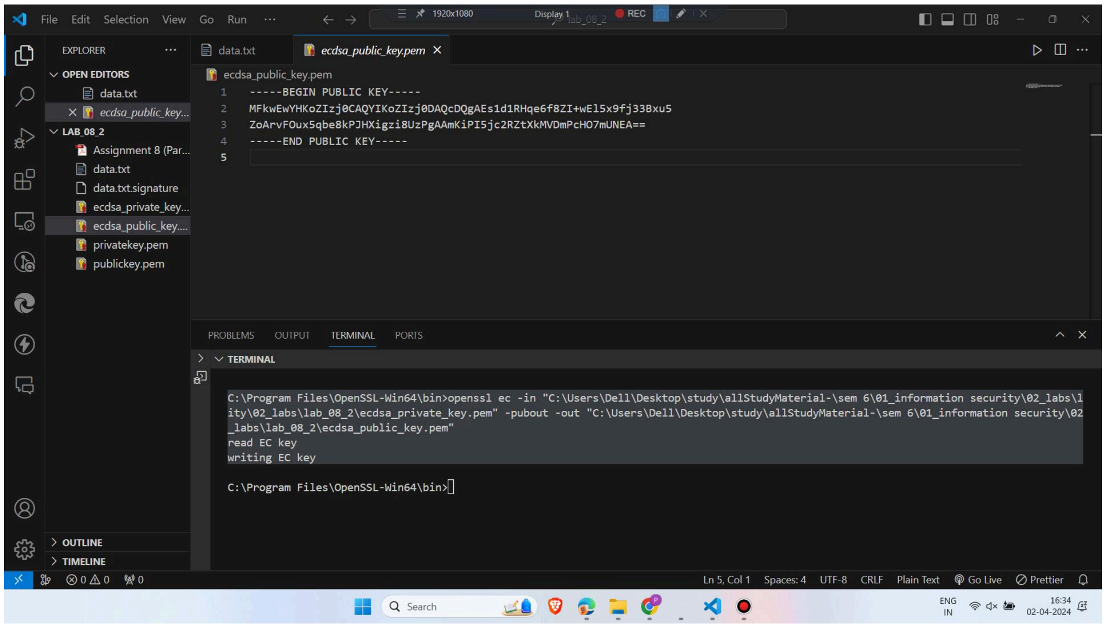


```
-----BEGIN EC PARAMETERS-----
BggqhkjOPQMBBw==
-----END EC PARAMETERS-----
-----BEGIN EC PRIVATE KEY-----
MHcCAQEEIOXG+bAaL5LnbD4eKVI9ZYqKoMn2YGKUeTDTE1M4gHs1oAoGCCqGSM49
AwEHoUQDQgAEs1d1RHqe6f8ZI+wEl5x9fj33Bxu5ZoArvFOux5qbe8kPJHXigzi8
UzPgAAmKiPI5jc2RZtXkMVDmPcHO7mUNEA==
-----END EC PRIVATE KEY-----
```

```
C:\Program Files\OpenSSL-Win64\bin>openssl ecparam -genkey -name prime256v1 -out "C:\Users\Dell\Desktop\study\allStudyMaterial-\sem 6\01
_information security\02_labs\lab_08_2\ecdsa_private_key.pem"

C:\Program Files\OpenSSL-Win64\bin>
```

b) Extract ECDSA Public Key

openssl ec -in ecdsa_private_key.pem -pubout -out ecdsa_public_key.pem



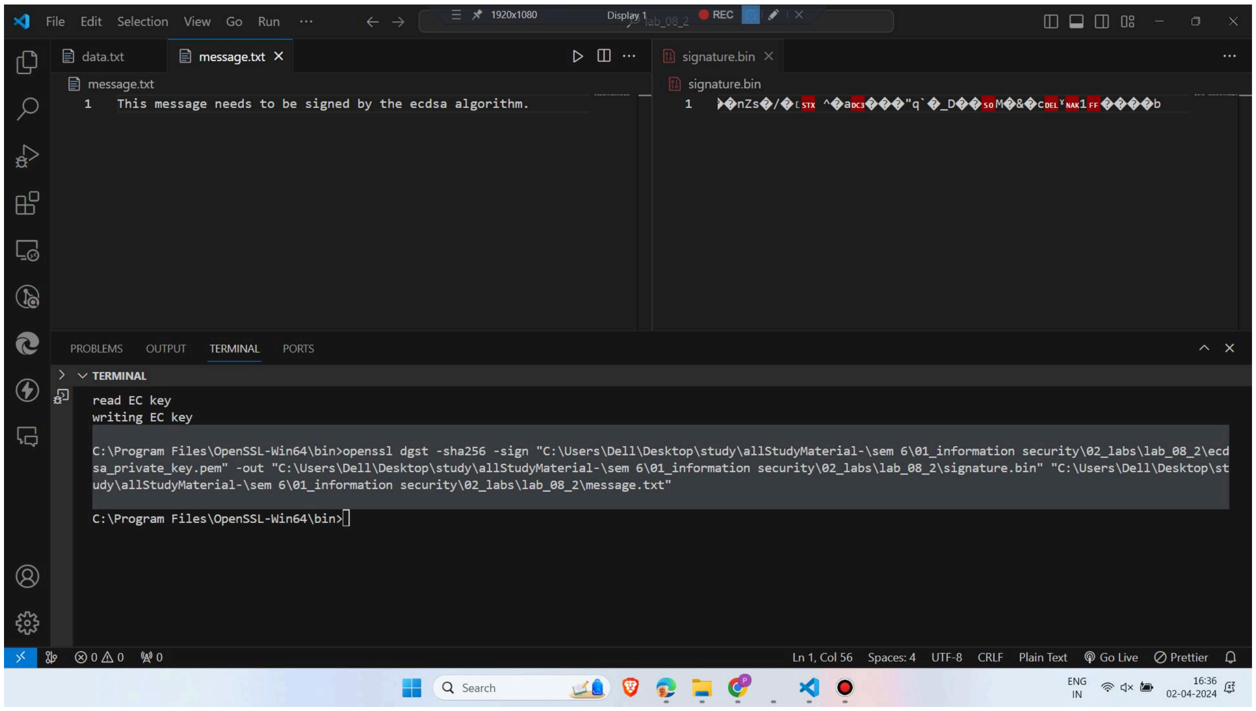
ecdsa_public_key.pem

```
-----BEGIN PUBLIC KEY-----
MFkwEwYHKoZIzj0CAQYIKoZIzj0DAQcDQgAEs1d1RHqe6f8ZI+wEl5x9fj33Bxu5
ZoArvFOux5qbe8kPJHXigzi8UzPgAAmKiPI5jc2RZtXkMVDmPcHO7mUNEA==
-----END PUBLIC KEY-----
```

```
C:\Program Files\OpenSSL-Win64\bin>openssl ec -in "C:\Users\Dell\Desktop\study\allStudyMaterial-\sem 6\01_information security\02_labs\l
ity\02_labs\lab_08_2\ecdsa_private_key.pem" -pubout -out "C:\Users\Dell\Desktop\study\allStudyMaterial-\sem 6\01_information security\02
_labs\lab_08_2\ecdsa_public_key.pem"
read EC key
writing EC key

C:\Program Files\OpenSSL-Win64\bin>
```

c) Sign Data data.txt with ECDSA Private Key

openssl dgst -sha256 -sign ecdsa_private_key.pem -out signature.bin message.txt



message.txt

```
This message needs to be signed by the ecdsa algorithm.
```

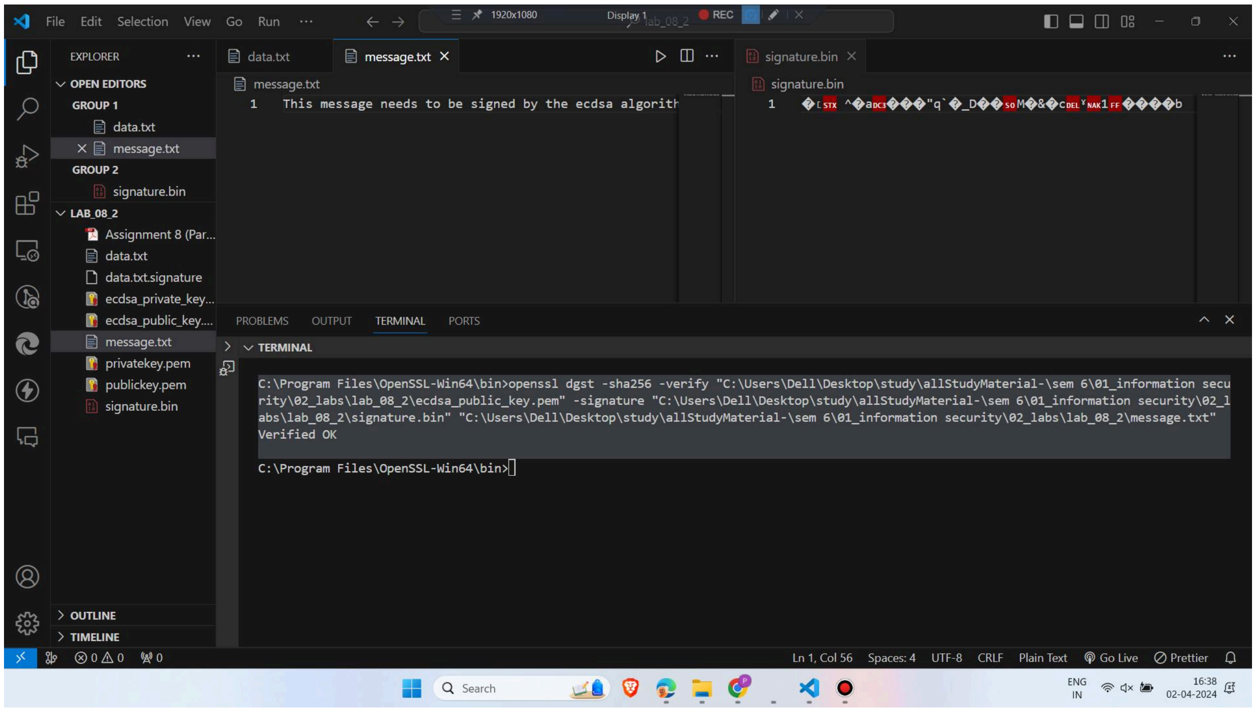
signature.bin

```
�nZs�/�STX ^�aDC3���"q`�_D��SOM�&�CDEL NAK1 FF ����b
```

```
read EC key
writing EC key

C:\Program Files\OpenSSL-Win64\bin>openssl dgst -sha256 -sign "C:\Users\Dell\Desktop\study\allStudyMaterial-\sem 6\01_information security\02_labs\lab_08_2\ecd
sa_private_key.pem" -out "C:\Users\Dell\Desktop\study\allStudyMaterial-\sem 6\01_information security\02_labs\lab_08_2\signature.bin" "C:\Users\Dell\Desktop\st
udy\allStudyMaterial-\sem 6\01_information security\02_labs\lab_08_2\message.txt"

C:\Program Files\OpenSSL-Win64\bin>
```

d) Verify Signature with ECDSA Public Key

openssl dgst -sha256 -verify ecdsa_public_key.pem -signature signature.bin message.txt



```
message.txt
This message needs to be signed by the ecdsa algorith
```

```
C:\Program Files\OpenSSL-Win64\bin>openssl dgst -sha256 -verify "C:\Users\Dell\Desktop\study\allStudyMaterial-\sem 6\01_information secu
rity\02_labs\lab_08_2\ecdsa_public_key.pem" -signature "C:\Users\Dell\Desktop\study\allStudyMaterial-\sem 6\01_information security\02_l
abs\lab_08_2\signature.bin" "C:\Users\Dell\Desktop\study\allStudyMaterial-\sem 6\01_information security\02_labs\lab_08_2\message.txt"
Verified OK

C:\Program Files\OpenSSL-Win64\bin>
```