ISC ASSIGNMENT -08

ROLL NO: U21CS052
NAME : PANCHAL GUNGUN PARESH

AES

Install OpenSSL Win64 OpenSSL v3.2.1 to your computer using the following site:
https://slproweb.com/products/Win32OpenSSL.html

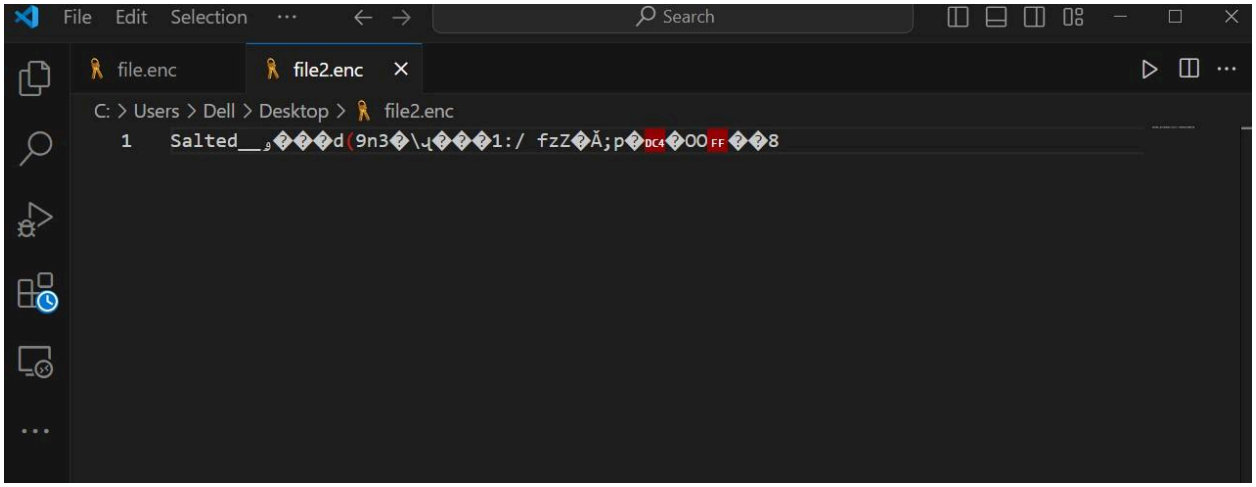
Task 1:
Perform encryption and decryption of the file using OpenSSL commands.
a) Use AES symmetric encryption technique to encrypt and decrypt the file using the following commands.

Encryption:
openssl enc -aes-256-cbc -salt -in file.txt -out file.enc -k key

Decryption :
openssl enc -d -aes-256-cbc -in file.enc -out file.txt -k key

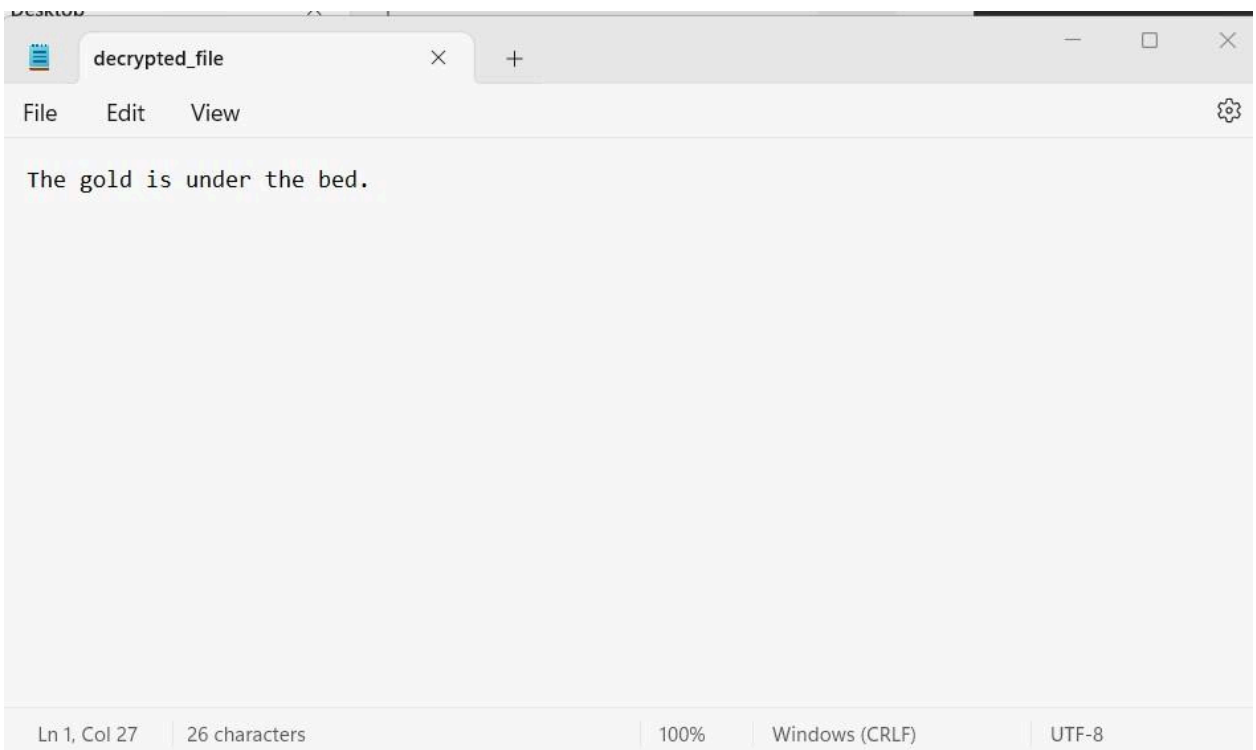
```
C:\Program Files\OpenSSL-Win64\bin>openssl enc -aes-256-cbc -salt -in "C:\Users\Dell\Desktop\study\allStudyMaterial-\sem
 6\01_information security\02_labs\lab_08\file.txt" -out "C:\Users\Dell\Desktop\file2.enc" -k key -pbkdf2

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




```
C:\Program Files\OpenSSL-Win64\bin>openssl enc -d -aes-256-cbc -in "C:\Users\Dell\Desktop\file2.enc" -out "C:\Users\Dell\Desktop\decrypted_file.txt" -pbkdf2
enter AES-256-CBC decryption password:

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



b) Use RSA public encryption technique to encrypt and decrypt the file using following commands.

Generate a public and private key pairs using following commands:

```
C:\Program Files\OpenSSL-Win64\bin>openssl genrsa -out "C:\Users\Dell\Desktop\isc_ass\private.key" 512

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

private.key

C: > Users > Dell > Desktop > isc_ass > private.key


```
-----BEGIN PRIVATE KEY-----
MIIBVQIBADANBgkqhkiG9w0BAQEFAASCAT8wggE7AgEAAkEA1hmlglsAY3N0de3x
XLt+6HK5ejCg/Yiy6UM6+bwzbo+rrpDeaoCwd/zUt6fKfun2bK7sB8bJ6HPH+Mb5
fsLO4wIDAQABAkEAw+kJ4yNkUpx2J+dIIcPL1+YKxL20wuqQVBRZ5eWJ5pLSQn/p
Iq56PAf2+GQqE0KJlmgJSQPaP93ETwJOBQF9aQIhAO+vFQUS9GUs8f3vUK9kNtdX
vdL0K8G3WmDxhuP71CEtAiEA5Ky48T/ZUVcHSqNkgP3u9F853dDdjpXr38qZjzlm
Gk8CIFmWZ5Tt8MugcRMpUE8+dgEnmpwvB+vwTKfPn0u35SJBAiAVzssMZtRox23w
lkh9bLofH/26w7J9aJrICuA+InE0TQIhAOAlTppJ5qUT8ZX4W3pQlKASdsiWXO2N
I9w+9deBf45N
-----END PRIVATE KEY-----
```


```
C:\Program Files\OpenSSL-Win64\bin>openssl genrsa -out "C:\Users\Dell\Desktop\isc_ass\private.key" 512

C:\Program Files\OpenSSL-Win64\bin>openssl rsa -in "C:\Users\Dell\Desktop\isc_ass\private.key" -pubout -out "C:\Users\De
ll\Desktop\isc_ass\public.key"
writing RSA key

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

private.key public.key

C: > Users > Dell > Desktop > isc_ass > public.key


```
-----BEGIN PUBLIC KEY-----
MFwwDQYJKoZIhvcNAQEBBQADSwAwSAJBANYZpYJbAGNzdHXt8Vy7fuhyuXowoP2I
sulDOvm8M26Pq66Q3mqAsHf81Lenyn7p9myu7AfGyehzx/jG+X7CzuMCAwEAAQ==
-----END PUBLIC KEY-----
```


Encryption:

```
C:\Program Files\OpenSSL-Win64\bin>openssl pkeyutl -encrypt -inkey "C:\Users\Dell\Desktop\isc_ass\public.key" -pubin -in
 "C:\Users\Dell\Desktop\isc_ass\file.txt" -out "C:\Users\Dell\Desktop\isc_ass\encrpted_file.enc"

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

Rsautl is deprecated so use the **pkeyutl** instead.

Decryption:

```
C:\Program Files\OpenSSL-Win64\bin>openssl pkeyutl -decrypt -inkey "C:\Users\Dell\Desktop\isc_ass\private.key" -in "C:\U
sers\Dell\Desktop\isc_ass\encrypted_file.enc" -out "C:\Users\Dell\Desktop\isc_ass\decrypted_file.txt"

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

The gold is under the bed. decrypted_file

File Edit View

The gold is under the bed.

c) Use ECC-ElGamal public encryption technique to encrypt and decrypt the file using following commands.

Generate ECC Private Key:

```
C:\Program Files\OpenSSL-Win64\bin>openssl ecparam -genkey -name prime256v1 -out "C:\Users\Dell\Desktop\isc_ass\ecc_priv
ate_key.pem"

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

private.key | public.key | ecc_private_key.pem

C: > Users > Dell > Desktop > isc_ass > ecc_private_key.pem

```
-----BEGIN EC PARAMETERS-----
BggqhkjOPQMBBw==
-----END EC PARAMETERS-----
-----BEGIN EC PRIVATE KEY-----
MHcCAQEEIEcEstTKVPM+oo9DwR4ZJbEu6jegDincIVjYGsHkGDNBoAoGCCqGSM49
AwEHoUQDQgAEdtsU00FP3fhgiVW81Mq3tgKjX7HDTMKwkuzEYpfUGhC0FSHyU/+L
i+Y1UNPAJl6IW3BdPqaVc9gRRsN+KtKT9Q==
-----END EC PRIVATE KEY-----
```

```
C:\Program Files\OpenSSL-Win64\bin>openssl ecparam -genkey -name prime256v1 -out "C:\Users\Dell\Desktop\isc_ass\ecc_priv
ate_key.pem"

C:\Program Files\OpenSSL-Win64\bin>openssl ec -in "C:\Users\Dell\Desktop\isc_ass\ecc_private_key.pem" -pubout -out "C:\U
sers\Dell\Desktop\isc_ass\ecc_public_key.pem"
read EC key
writing EC key

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

private.key | public.key | ecc_private_key.pem | ecc_public_key.pem

C: > Users > Dell > Desktop > isc_ass > ecc_public_key.pem

```
-----BEGIN PUBLIC KEY-----
MFkwEwYHKoZIzj0CAQYIKoZIzj0DAQcDQgAEdtsU00FP3fhgiVW81Mq3tgKjX7HD
TMKwkuzEYpfUGhC0FSHyU/+Li+Y1UNPAJl6IW3BdPqaVc9gRRsN+KtKT9Q==
-----END PUBLIC KEY-----
```

Generate Random Session Key:

Command Prompt

```
C:\Program Files\OpenSSL-Win64\bin>openssl rand -out "C:\Users\Dell\Desktop\isc_ass\session_key.bin" 32

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

File Edit Selection View ··· Search

private.key | public.key | ecc_private_key.pem | ecc_public_key.pem | session_key.bin

C: > Users > Dell > Desktop > isc_ass > session_key.bin

```
e9T7:zGI+9fu J
,F wFS
```

Encrypt Session Key with ECC Public Key:

```
C:\Program Files\OpenSSL-Win64\bin>openssl pkeyutl -derive -inkey "C:\Users\Dell\Desktop\isc_ass\ecc_private_key.pem" -p
eerkey "C:\Users\Dell\Desktop\isc_ass\ecc_public_key.pem" -out "C:\Users\Dell\Desktop\isc_ass\shared_secret.bin"

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

Encrypt Data with AES using the Session Key:

```
C:\Program Files\OpenSSL-Win64\bin>openssl enc -aes-256-cbc -salt -in "C:\Users\Dell\Desktop\isc_ass\ssn_key.bin" -out "C:\Users\Dell\
Desktop\isc_ass\encrypted_ssn_key.bin" -pass file:"C:\Users\Dell\Desktop\isc_ass\ssn_key.bin" -pbkdf2

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

ECC ElGamal Decryption =>
Decrypt Session Key with ECC Private Key:

Decrypt Data with AES using the Decrypted Session Key:

Task 2: Generate Hash of the given text using OpenSSL commands.

a) Get a list of supported cryptographic hash functions

openssl list --digest-commands

b) Create one text file data.txt and generate a message digest using md5, sha1, sha256, and sha512 hash functions using the following command

```
Command Prompt

C:\Program Files\OpenSSL-Win64\bin>openssl list --digest-commands
blake2b512        blake2s256        md5               rmd160
sha1              sha224            sha256            sha3-224
sha3-256          sha3-384          sha3-512          sha384
sha512            sha512-224        sha512-256        shake128
shake256          sm3

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

openssl dgst -sha256 data.txt

To write result to a file, use -out option:

openssl dgst -sha256 -out data.sha256 data.txt

```
Command Prompt

C:\Program Files\OpenSSL-Win64\bin>openssl dgst -md5 "C:\Users\Dell\Desktop\isc_ass\data.txt"
MD5(C:\Users\Dell\Desktop\isc_ass\data.txt)= b726579e62eda2e5cef756201fb64df4

C:\Program Files\OpenSSL-Win64\bin>openssl dgst -sha1 "C:\Users\Dell\Desktop\isc_ass\data.txt"
SHA1(C:\Users\Dell\Desktop\isc_ass\data.txt)= 64a812d2a0becc78defc4212ea67c7c0fa4ff0db

C:\Program Files\OpenSSL-Win64\bin>openssl dgst -sha256 "C:\Users\Dell\Desktop\isc_ass\data.txt"
SHA2-256(C:\Users\Dell\Desktop\isc_ass\data.txt)= b7af8a319172abb9a086be2dbb73c365880b4bb0998e241c12caf8f2b026f9f2

C:\Program Files\OpenSSL-Win64\bin>openssl dgst -sha512 "C:\Users\Dell\Desktop\isc_ass\data.txt"
SHA2-512(C:\Users\Dell\Desktop\isc_ass\data.txt)= e5fe64f3573382154a4cc4399a9abeda3c625fa07ea19340a2b8b3073b5d58c210aff9
a0c050fffe59d18622cfb942fdcb1b3e010a7dc2c406927a43fa4d6de1

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