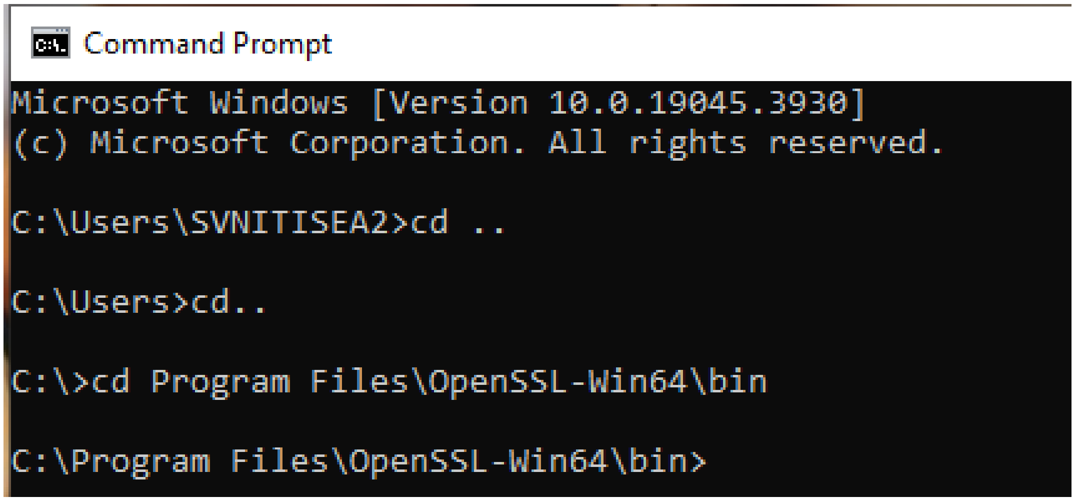
Sardar Vallabhbhai National Institute of Technology (SVNIT), Surat
Department of Computer Science and Engineering
B.Tech III (Semester VI)
Information Security and Cryptography- CS302
Lab Assignment 8

This assignment is about exploring the OpenSSL library. Follow the below instructions:

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

Run the .exe file and install OpenSSL in the system.
Open the command prompt (cmd) and redirect the path to the bin folder.



```
Microsoft Windows [Version 10.0.19045.3930]
(c) Microsoft Corporation. All rights reserved.

C:\Users\SVNITISEA2>cd ..

C:\Users>cd..

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

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

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 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
```

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:

```
openssl genrsa -out private.key 512
```

```
openssl rsa -in private.key -pubout -out public.key
```

Encryption:

```
openssl rsautl -encrypt -inkey public.key -pubin -in file.txt -out file.enc
```

Decryption:

```
openssl rsautl -decrypt -inkey private.key -in file.enc -out file.dec
```

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

Generate ECC Private Key:

```
openssl ecparam -genkey -name prime256v1 -out ecc_private_key.pem
```

Extract ECC Public Key from Private Key:

```
openssl ec -in ecc_private_key.pem -pubout -out ecc_public_key.pem
```

ECC ElGamal Encryption

Generate Random Session Key:

```
openssl rand -out session_key.bin 32
```

Encrypt Session Key with ECC Public Key:

```
openssl pkeyutl -encrypt -pubin -inkey ecc_public_key.pem -in
session_key.bin -out encrypted_session_key.bin
```

Encrypt Data with AES using the Session Key:

```
openssl enc -aes-256-cbc -salt -in plaintext.txt -out encrypted_data.enc -pass file:session_key.bin
```

ECC ElGamal Decryption

Decrypt Session Key with ECC Private Key:

```
openssl pkeyutl -decrypt -inkey ecc_private_key.pem -in encrypted_session_key.bin -out decrypted_session_key.bin
```

Decrypt Data with AES using the Decrypted Session Key:

```
openssl enc -d -aes-256-cbc -in encrypted_data.enc -out decrypted_data.txt -pass file:decrypted_session_key.bin
```

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

```
openssl dgst -sha256 data.txt
```

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

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