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:

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
```

b) Digitally Sign a document *data.txt*.

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

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
```

Verification:

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

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
```

b) Extract ECDSA Public Key

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

c) Sign Data *data.txt* with ECDSA Private Key

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

d) Verify Signature with ECDSA Public Key

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