openSSL Assignment

```
mkdir alice bob
```

Confidentiality

```
1)  openssl rand 128 > symm.key

2)  cat > plain.txt

3)  openssl enc -aes-256-cbc -pass file:symm.key -in plain.txt -out cipher.txt

4)  openssl genrsa -out alicepriv.key 2048

5)  openssl rsa -in alicepriv.key -pubout > alicepub.key

6)  openssl genrsa -out bobpriv.key 2048     openssl rsa -in bobpriv.key -pubout > bobpub.key


7)  cp cipher.txt ../bob/

8)  openssl enc -aes-256-cbc -pass file:../bob/bobpub.key -in symm.key -out symm.enc.key

9)  openssl enc -aes-256-cbc -pass file:../bob/bobpriv.key -d -in symm.enc.key -out symm.dec.key

10) openssl enc -aes-256-cbc -pass file:symm.dec.key -d -in ../bob/cipher.txt -out cipher.dec.txt
```

output of cipher.dec.txt is same as plain.txt file

INTEGRITY

```
11) openssl dgst -out hash.txt -sha512 plain.txt
```

```
12)  openssl dgst -out hash1.txt -sha512 plain.txt
     diff hash.txt hash1.txt
     output: no ouput as no difference in file
```

```
13) vim plain.txt
     openssl dgst -out hash1.txt -sha512 plain.txt
     diff hash.txt hash1.txt
    After changing the content of plain.txt file, output will change.
```

Authentication

```
14) openssl dgst -sha512 -hmac -in plain.txt > plain.mac  openssl dgst -sha512 -sign
    alicepriv.key -out alicemac.sign plain.txt  => signing the file.
15) openssl dgst -sha512 -verify alicepub.key -signature alicemac.sign plain.txt
    output: verified OK
```

```
16) vim plain.txt
    After editing the file.
    openssl dgst -sha512 -verify alicepub.key -signature alicemac.sign plain.txt
output: verification failure
```

DigitalSignature

```
17) openssl dgst -sha512 -sign alicepriv.key -out hash.sign plain.txt
```

```
18) cp plain.txt ../bob/
    cp hash.sign ../bob/
```

```
19) openssl dgst -sha512 -verify alicepub.key -signature ../bob/hash.sign
    ../bob/plain.txt       output : verified OK
```

```
20) vim plain.txt
```

After editing file.if we verify the signature using openssl dgst -sha512 -verify alicepub.key -signature ../bob/hash.sign ../bob/plain.txt output: Verification fails.