openSSL Assignment 1851: Khushboo Shetkar

Creating the directories

```
khush@khush: ~/Documents/CNS/labWork

(base) khush@khush: ~/Documents/CNS/labWork$ mkdir alice
(base) khush@khush: ~/Documents/CNS/labWork$ mkdir bob
(base) khush@khush: ~/Documents/CNS/labWork$ ls
alice bob
(base) khush@khush: ~/Documents/CNS/labWork$
```

Confidentiality

1. Creating a random key of size 128 bits (stored in symm.key)

2. Creating a file with dummy data (plain.txt)

```
khush@khush: ~/Documents/CNS/labWork/alice

(base) khush@khush: ~/Documents/CNS/labWork/alice$ cat > plain.txt

1851: Khushboo Shetkar

CNS lab assignment
openssl

thank you!
(base) khush@khush: ~/Documents/CNS/labWork/alice$ cat plain.txt

1851: Khushboo Shetkar

CNS lab assignment
openssl

thank you!
(base) khush@khush: ~/Documents/CNS/labWork/alice$
```

3. Encrypting the contents of plain.txt to cipher.txt using AES-128 algorithm in CBC mode, using symm.key

```
FI.
                               khush@khush: ~/Documents/CNS/labWork/alice
(base) khush@khush:~/Documents/CNS/labWork/alice$ man enc
(base) khush@khush:~/Documents/CNS/labWork/alice$ openssl enc -list
Supported ciphers:
-aes-128-cbc
                         -aes-128-cfb
                                                    -aes-128-cfb1
-aes-128-cfb8
                        -aes-128-ctr
                                                    -aes-128-ecb
                        -aes-192-cbc
-aes-128-ofb
                                                    -aes-192-cfb
                        -aes-192-cfb8
-aes-192-cfb1
                                                   -aes-192-ctr
-aes-192-ecb
                         -aes-192-ofb
                                                   -aes-256-cbc
-aes-256-cfb
                         -aes-256-cfb1
                                                    -aes-256-cfb8
                                                    -aes-256-ofb
-aes-256-ctr
                         -aes-256-ecb
                         -aes128-wrap
                                                    -aes192
-aes128
-aes192-wrap
                                                    -aes256-wrap
                         -aes256
-aria-128-cbc
                         -aria-128-cfb
                                                    -aria-128-cfb1
-aria-128-cfb8
                         -aria-128-ctr
                                                    -aria-128-ecb
-aria-128-ofb
                          -aria-192-cbc
                                                    -aria-192-cfb
-aria-192-cfb1
                         -aria-192-cfb8
                                                    -aria-192-ctr
-aria-192-ecb
                         -aria-192-ofb
                                                    -aria-256-cbc
-aria-256-cfb
                         -aria-256-cfb1
                                                    -aria-256-cfb8
-aria-256-ctr
                         -aria-256-ecb
                                                    -aria-256-ofb
                         -aria192
-aria128
                                                    -aria256
-bf
                         -bf-cbc
                                                    -bf-cfb
-bf-ecb
                         -bf-ofb
                                                    -blowfish
-camellia-128-cbc
                         -camellia-128-cfb
                                                    -camellia-128-cfb1
-camellia-128-cfb8
                         -camellia-128-ctr
                                                    -camellia-128-ecb
-camellia-128-ofb
                         -camellia-192-cbc
                                                    -camellia-192-cfb
-camellia-192-cfb1
                         -camellia-192-cfb8
                                                    -camellia-192-ctr
-camellia-192-ecb
                         -camellia-192-ofb
                                                    -camellia-256-cbc
-camellia-256-cfb
                         -camellia-256-cfb1
                                                    -camellia-256-cfb8
-camellia-256-ctr
                         -camellia-256-ecb
                                                    -camellia-256-ofb
-camellia128
                         -camellia192
                                                    -camellia256
                                                    -cast5-cbc
-cast
                         -cast-cbc
                         -cast5-ecb
-cast5-cfb
                                                    -cast5-ofb
-chacha20
                         -des
                                                    -des-cbc
-des-cfb
                         -des-cfb1
                                                    -des-cfb8
                         -des-ede
-des-ecb
                                                    -des-ede-cbc
des-ede-cfb
                         -des-ede-ecb
                                                    -des-ede-ofb
                         -des-ede3-cbc
                                                    -des-ede3-cfb
des-ede3
des-ede3-cfb1
                         -des-ede3-cfb8
                                                    -des-ede3-ecb
-des-ede3-ofb
                         -des-ofb
                                                    -des3
-des3-wrap
                          -desx
                                                    -desx-cbc
                          -id-aes128-wrap-pad
-id-aes128-wrap
                                                    -id-aes192-wrap
-id-aes192-wrap-pad
                          -id-aes256-wrap
                                                    -id-aes256-wrap-pad
                                                    -idea-cbc
-id-smime-alg-CMS3DESwrap -idea
                          -idea-ecb
                                                    -idea-ofb
-idea-cfb
                                                    -rc2-40
-rc2
                          -rc2-128
-rc2-40-cbc
                          -rc2-64
                                                    -rc2-64-cbc
-rc2-cbc
                          -rc2-cfb
                                                    -rc2-ecb
-rc2-ofb
                          -rc4
                                                    -rc4-40
-seed
                          -seed-cbc
                                                    -seed-cfb
-seed-ecb
                          -seed-ofb
-sm4-cbc
                          -sm4-cfb
                                                    -sm4-ctr
-sm4-ecb
                          -sm4-ofb
(base) khush@khush:~/Documents/CNS/labWork/alice$
```

```
khush@khush: ~/Documents/CNS/labWork/alice

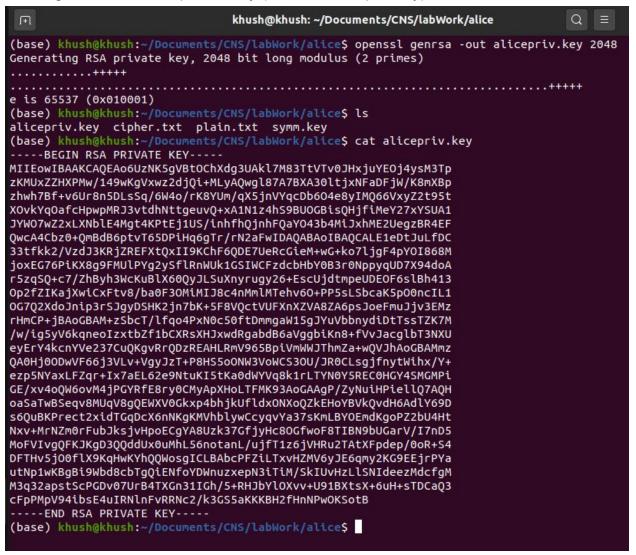
(base) khush@khush: ~/Documents/CNS/labWork/alice$ openssl enc -aes-128-cbc -in cipher.txt -out cipher.txt -kfile symm.key

*** WARNING: deprecated key derivation used.
Using -iter or -pbkdf2 would be better.
(base) khush@khush: ~/Documents/CNS/labWork/alice$ cat cipher.txt

Salted_d; *WLNB***Occuments/CNS/labWork/alice$ *

*t(base) khush@khush: ~/Documents/CNS/labWork/alice$
```

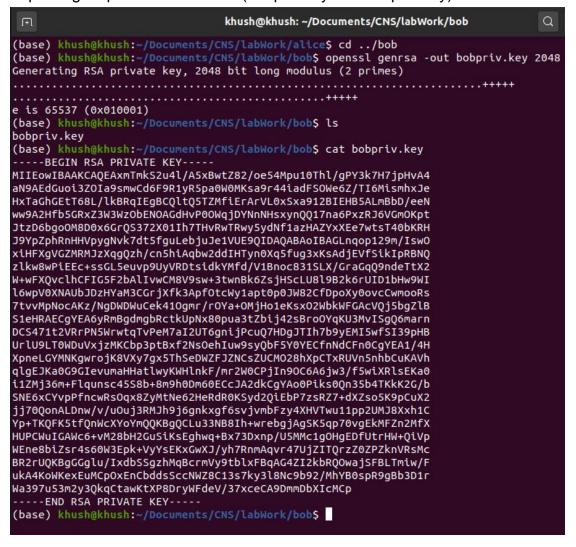
Creating a 2048 bit RSA private key (stored in alicepriv.key)



Extracting the public key from alicepriv.key and storing in file alicepub.key

```
khush@khush: ~/Documents/CNS/labWork/alice Q = - □ (base) khush@khush: ~/Documents/CNS/labWork/alice openssl rsa -in alicepriv.key -pubout > alicepub.key writing RSA key (base) khush@khush: ~/Documents/CNS/labWork/alice ls alicepriv.key alicepub.key cipher.txt plain.txt symm.key (base) khush@khush: ~/Documents/CNS/labWork/alice cat alicepub.key cat alicepub.key
```

6. Repeating steps 4 and 5 for Bob (bobpriv.key and bobpub.key)



```
khush@khush: ~/Documents/CNS/labWork/bob$ openssl rsa -in bobpriv.key -pubout > bobpub.key writing RSA key
(base) khush@khush: ~/Documents/CNS/labWork/bob$ ls
bobpriv.key bobpub.key
(base) khush@khush: ~/Documents/CNS/labWork/bob$ cat bobpub.key
-----BEGIN PUBLIC KEY-----
MIIBIJANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAxmTmkS2u4l/A5xBwtZ82
/oe54Mpu10Thl/gPY3k7H7jpHvA4aN9AEdGuoi3ZOIa9smwCd6F9R1yR5pa0W0MK
sa9r44iadFSOWe6Z/TI6MismhxJeHxTaGhGEtT68L/lkBRqIEgBCQltQ5TZMfiEr
ArvL0xSxa912BIEHB5ALmBbD/eeNww9A2Hfb5GRxZ3W3Wz0bENOAGdHvP00WqjDY
NnNHsxynQQ17na6PxzRJ6VGmOKptJtzD6bgoOM8D0x6GrQS372X01Ih7THvRwTRw
y5ydMf1azHAZYxXEe7wtsT40bKRHJ9YpZphRnHHVpygNvk7dt5fguLebjuJe1VUE
9QIDAQAB
-----END PUBLIC KEY-----
(base) khush@khush: ~/Documents/CNS/labWork/bob$
```

Alice and Bob exchange their public keys

```
khush@khush: ~/Documents/CNS/labWork/bob$ cp bobpub.key ../alice/bobpub.key (base) khush@khush: ~/Documents/CNS/labWork/bob$ ls ../alice/alicepriv.key alicepub.key bobpub.key cipher.txt plain.txt symm.key (base) khush@khush: ~/Documents/CNS/labWork/bob$ (base) khush@khush: ~/Documents/CNS/labWork/bob$ (base) khush@khush: ~/Documents/CNS/labWork/bob$ (base) khush@khush: ~/Documents/CNS/labWork/bob$ cd ../alice (base) khush@khush: ~/Documents/CNS/labWork/bob$ cd ../alice (base) khush@khush: ~/Documents/CNS/labWork/alice$ cp alicepub.key ../bob/alicepub.key (base) khush@khush: ~/Documents/CNS/labWork/alice$ ls ../bob/alicepub.key bobpriv.key bobpub.key (base) khush@khush: ~/Documents/CNS/labWork/alice$
```

7. Alice sends cipher.txt to Bob

```
khush@khush: ~/Documents/CNS/labWork/bob

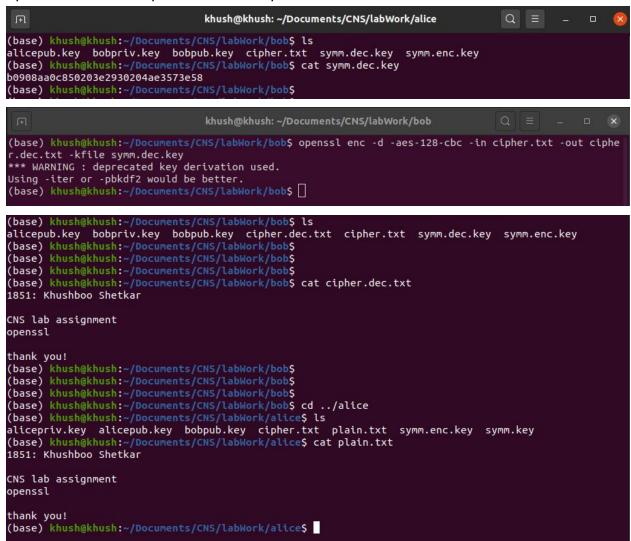
(base) khush@khush: ~/Documents/CNS/labWork/alice$ cp cipher.txt ../bob/cipher.txt
(base) khush@khush: ~/Documents/CNS/labWork/alice$ cd ../bob
(base) khush@khush: ~/Documents/CNS/labWork/bob$ ls
alicepub.key bobpriv.key bobpub.key cipher.txt
(base) khush@khush: ~/Documents/CNS/labWork/bob$
```

8. Alice encrypts symm.key using the public key of Bob (stored in symm.enc.key)

Bob decrypts symm.enc.key using his private key and stores the output in symm.dec.key

```
khush@khush: ~/Documents/CNS/labWork/bob Q = - □ (base) khush@khush: ~/Documents/CNS/labWork/alice$ cp symm.enc.key ../bob/symm.enc.key (base) khush@khush: ~/Documents/CNS/labWork/alice$ cd ../bob (base) khush@khush: ~/Documents/CNS/labWork/bob$ ls alicepub.key bobpriv.key bobpub.key cipher.txt symm.enc.key (base) khush@khush: ~/Documents/CNS/labWork/bob$ openssl rsautl -decrypt -in symm.enc.key -out symm.de c.key -inkey bobpriv.key bobpriv.key bobpriv.key bobpriv.key bobpriv.key symm.enc.key symm.enc.key (base) khush@khush: ~/Documents/CNS/labWork/bob$ ls alicepub.key bobpriv.key bobpub.key cipher.txt symm.dec.key symm.enc.key (base) khush@khush: ~/Documents/CNS/labWork/bob$ cat symm.dec.key bo908aa0c850203e2930204ae3573e58 (base) khush@khush: ~/Documents/CNS/labWork/bob$
```

10. Bob decrypts cipher.txt using symm.dec.key and stores the output in cipher.dec.txt. The cipher.dec.txt and plain.txt has same contents.



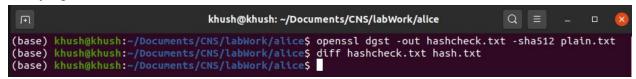
Integrity Check

11. Compute sha-512 hash on plain.txt and store in hash.txt.

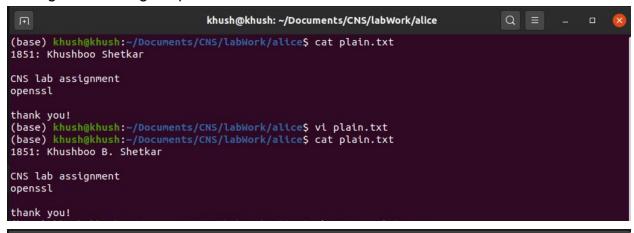
```
khush@khush: ~/Documents/CNS/labWork/alice

(base) khush@khush: ~/Documents/CNS/labWork/alice$ man dgst
(base) khush@khush: ~/Documents/CNS/labWork/alice$ openssl dgst -out hash.txt -sha512 plain.txt
(base) khush@khush: ~/Documents/CNS/labWork/alice$ ls
alicepriv.key alicepub.key bobpub.key cipher.txt hash.txt plain.txt symm.enc.key symm.key
(base) khush@khush: ~/Documents/CNS/labWork/alice$ cat hash.txt
SHA512(plain.txt)= 30fd40e7f554b40b6804dee4d39d58facb0ba2f94cd7d7b0a71b428dfc01e76bcd9fd27ef0c833b073
037e48d7a9f9fe43e780ae95d7664d2aab0447640d3f82
(base) khush@khush: ~/Documents/CNS/labWork/alice$
```

12. Verifying the hash



13. Making some change in plain.txt to see the verification fail



```
khush@khush: ~/Documents/CNS/labWork/alice Q = - □ X

(base) khush@khush: ~/Documents/CNS/labWork/alice$ openssl dgst -out hashcheck.txt -sha512 plain.txt (base) khush@khush: ~/Documents/CNS/labWork/alice$ diff hashcheck.txt hash.txt

1c1

< SHA512(plain.txt)= 56f91163cb7e63a8555a609c75830d9658dfe208baeab047451480b2cad52fd2f32ac9a5ef93c5bc 9d87198fcab3d3b5a944c3230bfba58ab7b6ed020711cac5

---

> SHA512(plain.txt)= 30fd40e7f554b40b6804dee4d39d58facb0ba2f94cd7d7b0a71b428dfc01e76bcd9fd27ef0c833b0 73037e48d7a9f9fe43e780ae95d7664d2aab0447640d3f82 (base) khush@khush: ~/Documents/CNS/labWork/alice$ 

[]
```

Authentication Check

14. Computing MAC on plain.txt using sha-512 and store in plain.mac

```
khush@khush:~/Documents/CNS/labWork/alice$ openssl dgst -out plain.mac -hmac -sha512 plain.txt (base) khush@khush:~/Documents/CNS/labWork/alice$ cat plain.mac
HMAC-SHA256(plain.txt) = 2964c32b8faab856769f97d4c31137b5de3de42bd072bfcbfbbd5923323ad079
(base) khush@khush:~/Documents/CNS/labWork/alice$ ls
alicepriv.key alicesign.sign cipher1.txt hashcheck.txt plain.mac symm.enc.key
alicepub.key bobpub.key cipher1.txt hash.txt plain.txt symm.key
(base) khush@khush:~/Documents/CNS/labWork/alice$ openssl dgst -sha512 -sign alicepriv.key -out alice
macsign.sign plain.txt
(base) khush@khush:~/Documents/CNS/labWork/alice$
```

15. Verifying the MAC

```
khush@khush: ~/Documents/CNS/labWork/alice Q = - □ & (base) khush@khush: ~/Documents/CNS/labWork/alice$ openssl dgst -sha512 -verify alicepub.key -signature alicemacsign.sign plain.txt

Verified OK (base) khush@khush: ~/Documents/CNS/labWork/alice$
```

16. Making some change in plain.txt to see the verification fail

```
khush@khush: ~/Documents/CNS/labWork/alice
(base) khush@khush:~/Documents/CNS/labWork/alice$ cat plain.txt
1851: Khushboo B. Shetkar
CNS lab assignment
openssl
thank you!
(base) khush@khush:~/Documents/CNS/labWork/alice$ vi plain.txt
(base) khush@khush:~/Documents/CNS/labWork/alice$ cat plain.txt
1851: Khushboo Shetkar
CNS lab assignment
openssl
thank you!
(base) khush@khush:~/Documents/CNS/labWork/alice$ openssl dgst -sha512 -verify alicepub.key -signatur
e alicemacsign.sign plain.txt
Verification Failure
(base) khush@khush:~/Documents/CNS/labWork/alice$
```

Digital Signature

17. Alice creates sha-512 hash on plain.txt and signs it using her private key. Store signed hash in file hash.sign

```
khush@khush: ~/Documents/CNS/labWork/alice

(base) khush@khush: ~/Documents/CNS/labWork/alice

(base) khush@khush: ~/Documents/CNS/labWork/alice

(base) khush@khush: ~/Documents/CNS/labWork/alice

(base) khush@khush: ~/Documents/CNS/labWork/alice

alicemacsign.sign alicepub.key bobpub.key hashcheck.txt hash.txt plain.txt symm.key

alicepriv.key alicesign.sign cipher.txt hash.sign plain.mac symm.enc.key

(base) khush@khush: ~/Documents/CNS/labWork/alice

(base) khush@khush: ~/Documents/CNS/labWork/alice
```

18. Alice sends plain.txt and hash.sign to Bob

```
khush@khush: ~/Documents/CNS/labWork/bob

(base) khush@khush: ~/Documents/CNS/labWork/alice$ cp plain.txt ../bob/plain.txt (base) khush@khush: ~/Documents/CNS/labWork/alice$ cp hash.sign ../bob/hash.sign (base) khush@khush: ~/Documents/CNS/labWork/alice$ cd ../bob (base) khush@khush: ~/Documents/CNS/labWork/bob$ ls alicepub.key bobpub.key cipher.txt plain.txt symm.enc.key bobpriv.key cipher.dec.txt hash.sign symm.dec.key (base) khush@khush: ~/Documents/CNS/labWork/bob$
```

19. Bob verifies the signature using the public key of Alice

```
khush@khush:~/Documents/CNS/labWork/bob

Q = - □ 

(base) khush@khush:~/Documents/CNS/labWork/bob$ openssl dgst -sha512 -verify ../alice/alicepub.key -s ignature hash.sign plain.txt

Verified OK (base) khush@khush:~/Documents/CNS/labWork/bob$
```

20. Check that the verification fails if the file plain.txt is modified

