

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)

```
khush@khush: ~/Documents/CNS/labWork/alice
(base) khush@khush:~/Documents/CNS/labWork/alice$ man rand
(base) khush@khush:~/Documents/CNS/labWork/alice$ openssl rand -hex 16
c5b1ed64a31de09a33e8595c4657a2f5
(base) khush@khush:~/Documents/CNS/labWork/alice$ openssl rand -hex 16
3fb69e9754b256b59be5d10bbe0286c1
(base) khush@khush:~/Documents/CNS/labWork/alice$ openssl rand -out symm.key -hex 16
(base) khush@khush:~/Documents/CNS/labWork/alice$ ls
symm.key
(base) khush@khush:~/Documents/CNS/labWork/alice$ cat symm.key
b0908aa0c850203e2930204ae3573e58
(base) khush@khush:~/Documents/CNS/labWork/alice$
```

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

```
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-128-ofb          -aes-192-cbc          -aes-192-cfb
-aes-192-cfb1         -aes-192-cfb8         -aes-192-ctr
-aes-192-ecb          -aes-192-ofb          -aes-256-cbc
-aes-256-cfb          -aes-256-cfb1         -aes-256-cfb8
-aes-256-ctr          -aes-256-ecb          -aes-256-ofb
-aes128               -aes128-wrap          -aes192
-aes192-wrap          -aes256               -aes256-wrap
-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
-aria128              -aria192              -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
-cast                 -cast-cbc             -cast5-cbc
-cast5-cfb           -cast5-ecb            -cast5-ofb
-chacha20             -des                  -des-cbc
-des-cfb              -des-cfb1             -des-cfb8
-des-ecb              -des-ede              -des-ede-cbc
-des-ede-cfb          -des-ede-ecb          -des-ede-ofb
-des-ede3             -des-ede3-cbc         -des-ede3-cfb
-des-ede3-cfb1        -des-ede3-cfb8        -des-ede3-ecb
-des-ede3-ofb         -des-ofb              -des3
-des3-wrap            -desx                 -desx-cbc
-id-aes128-wrap        -id-aes128-wrap-pad   -id-aes192-wrap
-id-aes192-wrap-pad   -id-aes256-wrap       -id-aes256-wrap-pad
-id-smime-alg-CMS3DESwrap -idea                -idea-cbc
-idea-cfb             -idea-ecb             -idea-ofb
-rc2                  -rc2-128              -rc2-40
-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
-sm4-cbc              -sm4-cfb              -sm4-ctr
-sm4-ecb              -sm4-ofb
```



```
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;ϖWLNBoϖϖϖC6ϖRϖ
ϖt(base) khush@khush:~/Documents/CNS/labWork/alice$
```

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

```
khush@khush: ~/Documents/CNS/labWork/alice
(base) khush@khush:~/Documents/CNS/labWork/alice$ openssl genrsa -out alicepriv.key 2048
Generating RSA private key, 2048 bit long modulus (2 primes)
.....+++++
.....+++++
e is 65537 (0x010001)
(base) khush@khush:~/Documents/CNS/labWork/alice$ ls
alicepriv.key cipher.txt plain.txt symm.key
(base) khush@khush:~/Documents/CNS/labWork/alice$ cat alicepriv.key
-----BEGIN RSA PRIVATE KEY-----
MIIIEowIBAAKCAQEAo6UzNK5gVBt0ChXdg3UAkl7M83TtVTv0JHxjuVE0j4ysM3Tp
zKMUXZZHXPMw/149wKgVxwz2djQi+MLyAQwgl87A7BXA30ltjxNFaDFjW/K8mXBp
zhwh7Bf+v6Ur8n5DLsSq/6W4o/rK8YUm/qX5jnVYqCDB604e8yIMQ66VxyZ2t95t
XOvkYqOafCHpwpMRJ3vtdhNttgeuvQ+xA1N1z4hS9BU0GBisQHjfiMeY27xYSUA1
JYW07wZ2xLXNblE4Mgt4KPtEj1US/inhfHQjnhFQaY043b4MiJxhME2UegzBR4EF
QwCA4Cbz0+QmBdB6ptvT65DPiHq6gTr/rN2aFwIDAQABaoIBAQCALE1eDtJulfDC
33tfkk2/VzdJ3KRjZREFxtQxII9KChF6QDE7UeRcGieM+wG+ko7ljgF4pY0I868M
joxEG76PiKX8g9FMULPYg2ysfLrnWuk1GSIWCFzdcBhY0B3r0NppyqUD7X94doA
r5zqSQ+c7/ZhByh3WcKuBlX60QyJLSuXnyrugy26+EscUjdtmpeUDE0F6s1Bh413
Op2fZIKajXwiCxftv8/ba0F30MiMIJ8c4nMmLMtehv60+PP5sLSbcaK5p00ncIL1
OG7Q2XdoJnlp3rSJgyDSHK2jn7bK+5F8VQctVUFXnXZVA8ZA6psJoeFmuJjv3EMz
rHmCP+jBAoGBAM+zSbcT/lfqo4PxN0c50ftDmmgaW15gJYUvbbnydiDtTssTZK7M
/w/ig5yV6kqneoIzxtbZf1bCXRsXHJxwdRgabdB6aVggbiKn8+fVvJacglbT3NXU
eyErY4kcnYVe237CuQKgvRrQDzREAHLRmV965BpiVmwWJThmZa+wQVJhAoGBAMmZ
QA0Hj00DwVF66j3VLv+VgyJzT+P8HS5o0NW3VoWCS30U/JR0CLsgjfnytwihx/Y+
ezp5NYaxLFZqr+Ix7aEL62e9NtuKI5tKa0dWYVq8k1rLTYN0Y5REC0HGY4SMGMPi
GE/xv4oQW6ovM4jPGYRfE8ry0CMYApXHoLTFMK93AoGAAGP/ZyNuiHPiellQ7AQH
oaSaTwBSeqv8MUqV8gQEWXV0Gkxp4bhjkUfldxONXoQZKEHoYBVkQvdH6AdLY69D
s6QuBKPrect2xidTGqDcX6nNKgKMVhblYwCcyqvYa37sKmlBY0EmdKgoPZ2bU4Ht
Nxv+MrNZm0rFubJksjvHpoECgYA8Uzk37GfjyHc80GfwoF8TIBN9bUGarV/I7nD5
MoFVIvgQFKJKgD3QQddUx0uMhL56notanL/ujfT1z6jVHRu2TAtXFpdep/0oR+S4
DFTHv5j00fLX9KqHwKYhQQWosgICLBAbcPFZiLTxvHZMV6yJE6qmy2KG9EEjrPYa
utNp1wKBgBi9Wbd8cbTgQiENFoYDwnuzxepN3itiM/SkIUvHzLlSNideezMdcfgM
M3q32apstScPGDv07UrB4TXGn31IGh/5+RHJbYlOXvv+U91BXtsX+6uH+sTDCaQ3
cFpPmPV94ibsE4uIRNlnFvRRNc2/k3GS5aKKKBH2fHnNPwOKSotB
-----END RSA PRIVATE KEY-----
(base) khush@khush:~/Documents/CNS/labWork/alice$
```


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

```
khush@khush: ~/Documents/CNS/labWork/alice
(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
-----BEGIN PUBLIC KEY-----
MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAo6UzNK5gVBtOChXdg3UA
kl7M83TtTv0JHxjuYE0j4ysM3TpzKMUXZZHXPMw/149wKgVxwz2dJQi+MLyAQwg
l87A7BXA30ltjxNFaDFjW/K8mXBpzhwh7Bf+v6Ur8n5DLsSq/6W4o/rK8YUm/qX5
jnvYqcDb604e8yIMQ66VxyZ2t95tXOvkYq0afCHpwpMRJ3vtdhNttgeuvQ+xA1N1
z4hS9BU0GBisQhJfiMeY27xYSUA1JYW07wZ2xLXNbLE4Mgt4KPtEj1US/inhfhQj
nhFQaY043b4MlJxhME2UegzBR4EFQwcA4Cbz0+QmBdB6ptvT65DPiHq6gTr/rN2a
FwIDAQAB
-----END PUBLIC KEY-----
(base) khush@khush:~/Documents/CNS/labWork/alice$
```

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

```
khush@khush: ~/Documents/CNS/labWork/bob
(base) khush@khush:~/Documents/CNS/labWork/alice$ cd ../bob
(base) khush@khush:~/Documents/CNS/labWork/bob$ openssl genrsa -out bobpriv.key 2048
Generating RSA private key, 2048 bit long modulus (2 primes)
.....+++++
.....+++++
e is 65537 (0x010001)
(base) khush@khush:~/Documents/CNS/labWork/bob$ ls
bobpriv.key
(base) khush@khush:~/Documents/CNS/labWork/bob$ cat bobpriv.key
-----BEGIN RSA PRIVATE KEY-----
MIIEowIBAAKCAQEAxmTmKS2u4L/A5xBwtZ82/oe54Mpu10ThL/gPY3k7H7jpHvA4
aN9AEdGuoi3ZOIa9smwCd6F9R1yR5pa0W0MKsa9r44iadFS0We6Z/TI6MismhxJe
HxTaGhGtT68L/lkBRqIEgBCqltQ5TZMfiErArVL0xSxa912BIEHB5ALmBbD/eeN
ww9A2Hfb5GRxZ3W3WzObENOAGdHvP00WqjDYNNHsxynQQ17na6PxzRJ6VGmOKpt
JtD6bgo0M8D0x6GrQS372X01Ih7THvRwTRwy5ydnf1azHAZYxxEe7wtsT40bKRH
J9YpZphRnHHVpygNvk7dt5fgULebjuJe1VUE9QIDAQBAoIBAGLnqop129m/IsW0
xiHFxgVGZMRMJzXqgQzh/cn5hiAqbw2ddIHTyn0Xq5fug3xKsAdjEVfSikIprBNQ
zlkW8wPiEEC+ssGLSeuVp9UyVRDtsidkYmfd/V1Bnoc831SLX/GraGqQ9ndeTtX2
W+wFXQvcLhCFIG5F2bAlIvwCM8V9sw+3twnBk6ZsJHScLU8L9B2k6rUID1bHw9WI
l6wpV0XNAUBJDzHYaM3CGrjXfk3Apf0tcWy1apt0p0JW82CfDpoXy0ovcCwmooRs
7tvvMpNocAKz/ngDWDWuCek410gmr/r0Ya+0MjHo1eKsx02WbkWFGAcVQj5bgZLB
S1eHRAECgYEA6yRmBgdmgbRctkUpNx80pua3tZbij42sBro0YqKU3MvISgQ6marn
DCS471t2VRrPN5WrwqtVPeM7aI2UT6gniJpCuQ7HDgJTIh7b9yEMI5wFSI39pHB
UrLU9LT0WduVxjzMKCb3ptBxf2Ns0ehIuw9syQbF5Y0YECfnNdCFn0CgYEA1/4H
XpneLGYMNKGwrojk8VXy7gx5ThSeDWZFJZNCsZUCM028hXpCTxRUvN5nhbCuKAVh
qlgEJka0G9GIEvumaHHatLwyKWHlnkF/mr2W0CPjIn90C6A6jw3/f5wiXRlsEka0
i1ZMj36m+FLqunsc45S8b+8m9h0Dm60EccJA2dkCgYAAoPiks0Qn35b4TKkK2G/b
SNE6xCYvpPfcwRs0qx8ZYmtNe62HerDR0KSyd2QIEbP7zsRZ7+dXZso5K9pCuX2
jj70QonALDnw/v/u0uj3RMJh9j6gnkxgf6svjvmbFzy4XHVtwu11pp2UMJ8Xxh1C
Yp+TKQFK5tFqnWcXYoYmQQKBgQClu33NB8Ih+wrebgjAgSK5qp70vgEkMFZn2MfX
HUPCWuIGAWc6+vM28bH2GuSiKsEghwq+Bx73Dxnp/U5MMC1g0HgEDfutrHW+QiVp
WEnE8biZsr4s60W3EpK+VyYsEKXGwXJ/yh7RnmAqvr47UjZITQrzZ0ZPZknVRsMc
BR2rUQKBgGglu/IxdbSSgzHmQBCrmV9tBlxqBqAG4ZI2kbrQ0wajSFBLTmlw/F
uka4KowKexEuMCPoxEnCbddsScCNWZ8C13s7ky3l8Nc9b92/MhYB0spr9gBb3D1r
wa397u53m2y3QkqCtawKtXP8DryWFdev/37xceCA9DmDbXICMCP
-----END RSA PRIVATE KEY-----
(base) khush@khush:~/Documents/CNS/labWork/bob$
```


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

```
khush@khush: ~/Documents/CNS/labWork/bob
(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.dec
c.key -inkey bobpriv.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
b0908aa0c850203e2930204ae3573e58
(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.

```
khush@khush: ~/Documents/CNS/labWork/alice
(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
b0908aa0c850203e2930204ae3573e58
(base) khush@khush:~/Documents/CNS/labWork/bob$
```

```
khush@khush: ~/Documents/CNS/labWork/bob
(base) khush@khush:~/Documents/CNS/labWork/bob$ openssl enc -d -aes-128-cbc -in cipher.txt -out cipe
r.dec.txt -kfile symm.dec.key
*** WARNING : deprecated key derivation used.
Using -iter or -pbkdf2 would be better.
(base) khush@khush:~/Documents/CNS/labWork/bob$
```

```
(base) khush@khush:~/Documents/CNS/labWork/bob$ ls
alicepub.key bobpriv.key bobpub.key cipher.dec.txt cipher.txt symm.dec.key symm.enc.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$ cat cipher.dec.txt
1851: Khushboo Shetkar

CNS lab assignment
openssl

thank you!
(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/alice$ ls
alicepriv.key alicepub.key bobpub.key cipher.txt plain.txt symm.enc.key symm.key
(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$
```

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

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

13. 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 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 B. Shetkar

CNS lab assignment
openssl

thank you!

khush@khush: ~/Documents/CNS/labWork/alice
(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
(base) 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)= 2964c32b8faab856769f97d4c31137b5de3de42bd072bfcfbdbd5923323ad079
(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     cipher.txt   hash.txt       plain.txt  symm.key
(base) khush@khush:~/Documents/CNS/labWork/alice$ openssl dgst -sha512 -sign alicepriv.key -out alicemacsign.sign plain.txt
(base) khush@khush:~/Documents/CNS/labWork/alice$
```

15. Verifying the MAC

```
khush@khush: ~/Documents/CNS/labWork/alice
(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 -signature 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$ openssl dgst -out hash.sign -sign alicepriv.key -sha512 plain.txt
(base) khush@khush:~/Documents/CNS/labWork/alice$ ls
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$ cat hash.sign
K5+++++rMc++8Nr&TJ++^p^h^N+++
z++l_ hV~+Iie+sqr,++^+/fac1J++P{+ "[a++?{+++V++++!++++WV]h+++S+++++si,@+8Jt
+B+++M$+z++++z:4+++_bon+++rB++c?@ed[+B++8+v++>+bX[!o+?&?q+V++o,A+ M++d-+
z>+e+++8++?I++++++('++++++7{P+$+MjS(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
(base) khush@khush:~/Documents/CNS/labWork/bob$ openssl dgst -sha512 -verify ../alice/alicepub.key -signature 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

```
khush@khush: ~/Documents/CNS/labWork/bob
(base) khush@khush:~/Documents/CNS/labWork/bob$ cat plain.txt
1851: Khushboo Shetkar

CNS lab assignment
openssl

thank you!
(base) khush@khush:~/Documents/CNS/labWork/bob$ vi plain.txt
(base) khush@khush:~/Documents/CNS/labWork/bob$ cat plain.txt
1851: Khushboo Shetkar

CNS lab assignment
openSSL

thank you!
(base) khush@khush:~/Documents/CNS/labWork/bob$ openssl dgst -sha512 -verify ../alice/alicepub.key -s
signature hash.sign plain.txt
Verification Failure
(base) khush@khush:~/Documents/CNS/labWork/bob$
```