Assignment-1

1. OpenSSL usage :

Install openssl (or ensure it is installed). Syntax:
openssl command [options] [arguments] In this lab, we will use the following commands:
passwd, enc, genrsa, x509, dgst, req, verify.

2. Encoding with base64 Definition:

Base64 is an encoding scheme which uses 65 printable characters (26 lower-case letters, 26 upper-case letters, 10 digits, characters '+' and '/', and special character '='). Base64 allows to exchange data with limited encoding problems.

Syntax: To encode with base64, the following command is used:
openssl enc -base64 -in input-file -out output-file

```
tanishqkakkar@Tanishqs-Macbook-Pro LAB-1 % openssl enc -base64 -in plain.txt -ou
t encode.txt
tanishqkakkar@Tanishqs-Macbook-Pro LAB-1 % cat plain.txt
Hello, I am Tanishq%
tanishqkakkar@Tanishqs-Macbook-Pro LAB-1 % cat encode.txt
SGVsbG8sIEkgYW0gVGFuaXNocQ==
tanishqkakkar@Tanishqs-Macbook-Pro LAB-1 %
```

4. Encryption

Syntax: To encrypt, we can use command enc. To decrypt, we can use command enc with option -d. To use DES, we can use option -des. To use triple-DES, we can use option -des3. We will also use option -nosalt in the following.

- Encrypt an arbitrary file and decrypt it using the good password (with DES and no salt).

```
tanishqkakkar@Tanishqs-Macbook-Pro LAB-1 % openssl enc -des -in plain.txt -out d
es_enc.txt
enter des-cbc encryption password:
Verifying - enter des-cbc encryption password:
*** WARNING : deprecated key derivation used.
Using -iter or -pbkdf2 would be better.
tanishqkakkar@Tanishqs-Macbook-Pro LAB-1 % cat plain.txt
Hello, I am Tanishq%
tanishqkakkar@Tanishqs-Macbook-Pro LAB-1 % cat des_enc.txt
Salted__?C??$"cx?/?ȝ??kj?zk>D6?%7?%
tanishqkakkar@Tanishqs-Macbook-Pro LAB-1 %
```

- Encrypt an arbitrary file and try to decrypt it using a wrong password. Remark: openssl detects that the password was wrong. We will try to see how openssl could detect it.

```
tanishqkakkar@Tanishqs-Macbook-Pro LAB-1 % openssl enc -des -d -nosalt -in des_e
nc.txt -out des_dec.txt
enter des-cbc decryption password:
*** WARNING : deprecated key derivation used.
Using -iter or -pbkdf2 would be better.
bad decrypt
8158591616:error:06065064:digital envelope routines:EVP_DecryptFinal_ex:bad decr
ypt:crypto/evp/evp_enc.c:612:
tanishqkakkar@Tanishqs-Macbook-Pro LAB-1 %
```

- With an hexadecimal editor (such as tool xxd), study the difference between plaintext nopad. Explain the differences.

```
tanishqkakkar@Tanishqs-Macbook-Pro LAB-1 % xxd plain.txt
00000000: 4865 6c6c 6f2c 2049 2061 6d20 5461 6e69  Hello, I am Tani
00000010: 7368 71                                  shq
tanishqkakkar@Tanishqs-Macbook-Pro LAB-1 % xxd des_dec.txt
00000000: 314d ba6a a3fe e4f5 50f0 fed1 c970 5fa5  1M.j....P....p_.
00000010: 071d 058f 427f 1b8d 7507 b1ca a10f 75d8  ....B...u.....u.
tanishqkakkar@Tanishqs-Macbook-Pro LAB-1 %
```

5. Encryption with RSA Key generation Syntax:

(a) The key generation is performed using: *openssl genrsa -out key.pem size*

```
tanishqkakkar@Tanishqs-Macbook-Pro LAB-1 % openssl genrsa -out key.pem 1024
Generating RSA private key, 1024 bit long modulus (2 primes)
.......................................+++++
.......+++++
e is 65537 (0x010001)
tanishqkakkar@Tanishqs-Macbook-Pro LAB-1 % cat key.pem
-----BEGIN RSA PRIVATE KEY-----
MIICXQIBAAKBgQCw1n0XlRG5sNo5CNrWLC3Nj74PshS7FnoG7mfbbSX0GOYLzTRz
zksrvstfHsObKppxfXHKVBjcUlnINy5XOhV66UDxmAAGrlAxilqMcPgmp9Ng2fzE
zdJNHQ8nJlS9vIP7+us30axcj+rv4L2YQekuo6HamuV8hbvSGyQBXaJ9wIDAQAB
AoGBAK1ZVT7szndtOj52w673l97Obc4ND+1mVzC8O+sJ0A686aXf/u8W5vF3Ev2n
trBAzy05f3aLgeNYhtKR5Ud0lOBKANCpj7/D4kvGTG44Czl7w5aKj+gO0ijCJRG4
C4q+a2Lmz6s7wH69Iu436pmVRtogBuDgtFjiIcFKm0ny3VxBAkEA40l+0n+Fp+5z
G47OYdSehKjZ0IwK/6Dc2yr3y7yB2jazOs/EPkLvZzeuIeTBI66fBsm5VBN81kQU
6OazSDqbDwJBAMctdKy7E0z8AU+6v8dXvhyUNhrWEqv2dwvZniizKPz5xfXUAPJO
poaFkAGV6eEjNrxbI+fgWzLkpLx2VdIqQpkCQQDPgjhRgq/KRD+/d0AhvXcEcwx6
BIG+JWW+i5o03mRHkA1OsoXeuknMmN9Yfnt/UlxKXD3h7vDYxsu4X3hrh2YtAkAN
uZAkpu95ipP8jn3Qmrc6+OuRhdbbiqxBYMmJPG9Cn2OIwQcfq1PGSUXXFiF7phWL
fSxIOimOpDrF0dGwHcFhAkBCa4lCx8X1YMHWRllwLq9XFhh0ylMFibN25rVTFfhn
o/d9YKc7fQZppcro05TOOuoEpRyUpi4MJzmVmZO+l2WK
-----END RSA PRIVATE KEY-----
tanishqkakkar@Tanishqs-Macbook-Pro LAB-1 %
```

(b) Syntax: To obtain information on a key, we can use:
openssl rsa -in key.pem -text -noout

- Crack your own RSA key by factorizing the modulus. Why could you crack it? Syntax: In order to save the key in a safe way, a symmetric encryption algorithm (such as triple-DES) can be used: *openssl genrsa -des3 -out private-key size*

```
tanishqkakkar@Tanishqs-Macbook-Pro LAB-1 % openssl genrsa -des3 -out key.pem 102
4
Generating RSA private key, 1024 bit long modulus (2 primes)
....+++++
............+++++
e is 65537 (0x010001)
Enter pass phrase for key.pem:
Verifying - Enter pass phrase for key.pem:
tanishqkakkar@Tanishqs-Macbook-Pro LAB-1 % cat key.pem
-----BEGIN RSA PRIVATE KEY-----
Proc-Type: 4,ENCRYPTED
DEK-Info: DES-EDE3-CBC,ECA8E3D6C7134D28

QWH1Xk2DvxJ3gJ2Q4sQKHmMVlHegqYZUy7i3QbFF5ucDBNNwypqeBxWSNzFSZdf6
GBGPjzAGCv/KeHPgn8aacVCTjVCQ7lwOkNKgT7BT/rDDI1csjKJ0fNxSp8qBcc2j
kfWnBVPx24dSUHb8NBcYS/GM1BDHFS3LHNBN+k3G4rlJ6DrGWv2Q9RPKNtCO47SF
CQ83gm9U7ItCfzxoIB/ZKO7cKsXwhlzjh9Ou6ehjCCxHKDSFsdxDGktZDOV7wMkr
8uhzgpQfKw9CfDYroHD9h1jr/ykrrzQucK/NhROZzaPJNT/sHh2LJoHH6ThA4B7i
iaLs6vIAbk/6eFuDOJ7oKi7KOP9A3N6yHHTuBWjLXWm5s8GN6B+UUs4m/zw3RdPV
rJeC1UEm5PF1n78/absVITauZx0sB49Ia/rlE6NxFDiI9i/2W1c1RfFyGXInOcZC
a8XL+Nyt6D5mxlzQToT0kZAalqXPLrnUpX5hoq+LZGKGlw/7G5bYG/wyRpT/nEh4
rqinmItLGFuS2eFboddVtAsMPbWHAVoe9RDwn+iEC7R5jPe8OQ6WqkKG88r6eslD
qQpzXMaf/sHiEVEpJWvkadCdMehqbq3fTpA7AMciaiMgB7pudqZdD2d3gPQK0BiM
C2cPClIuNS0tMQNkkgqcnyvTeOj2eSJKOyKbcWNtK3JWI7jmAIRRC3nwuGMd7ZAL
10Q8eo4iD0/qI5XUONTdpRTXA7StADjRQ1w30ANEyXbuRkNuYcGa1nDl2gvOP8Vv
qykQmwI6ChDtOiLvsm05iYc2bW1crv2Ag+N2vTBbcIXqJo2ZHDW/qQ==
-----END RSA PRIVATE KEY-----
tanishqkakkar@Tanishqs-Macbook-Pro LAB-1 %
```

Signatures

Syntax: To hash a file, we use:

a) openssl dgst -md5 -out hash file

```
tanishqkakkar@Tanishqs-Macbook-Pro LAB-1 % openssl dgst -md5 -out hash.txt plain
.txt
tanishqkakkar@Tanishqs-Macbook-Pro LAB-1 % cat plain.txt
Hello, I am Tanishq%
tanishqkakkar@Tanishqs-Macbook-Pro LAB-1 % cat hash.txt
MD5(plain.txt)= f3a5db16cbacf90e4c1da19040f57d77
tanishqkakkar@Tanishqs-Macbook-Pro LAB-1 %
```

Syntax: To sign a hash, we use:

openssl rsautl -sign -in hash -inkey key -out signature

```
tanishqkakkar@Tanishqs-Macbook-Pro LAB-1 % openssl rsautl -sign -in hash.txt -in
key key.pem -out signature.txt
Enter pass phrase for key.pem:
tanishqkakkar@Tanishqs-Macbook-Pro LAB-1 % cat signature.txt
?Ll}&"???kS??x?H??}??jo??a??n?h?"A?????4dm????
                                        ??;?/p?Γ2?9Kk@?N???Y?w]?[-????????
#????7?¡?XP?4?R2?@???d?4?m?%
tanishqkakkar@Tanishqs-Macbook-Pro LAB-1 %
```

6. Certificates

Certificate generation

a) Syntax: To generate a certificate, a request has to be created first:
openssl req -new -key key -out request

Final Assignment on OpenSSL

Generate two files like in the following.

file.txt

000000000000000
111111111111111
222222222222222
000000000000000
111111111111111
222222222222222
000000000000000
111111111111111 222222222222222

modified_file.txt (only one DIGIT

change)

000000000000000
111111111111111
222222222222222
000000010000000

111111111111111
222222222222222
000000000000000
111111111111111
222222222222222

Use AES encryption and mode of operation ECB and CBC to analyze the cipher text.

Use syntax like in the following
$ *openssl aes-256-ecb -e -in file.txt -out cipher_ecb.bin -nosalt*

```
tanishqkakkar@Tanishqs-Macbook-Pro LAB-1 % cat file1.txt
000000000000000
111111111111111
222222222222222
000000000000000
111111111111111
222222222222222
000000000000000
111111111111111
222222222222222 %
tanishqkakkar@Tanishqs-Macbook-Pro LAB-1 % cat modified_file.txt
000000000000000
111111111111111
222222222222222
000000010000000
111111111111111
222222222222222
000000000000000
111111111111111
222222222222222%
tanishqkakkar@Tanishqs-Macbook-Pro LAB-1 % openssl aes-256-ecb -e -in file1.txt
-out cipher_ecb.bin -nosalt
enter aes-256-ecb encryption password:
Verifying - enter aes-256-ecb encryption password:
*** WARNING : deprecated key derivation used.
Using -iter or -pbkdf2 would be better.
tanishqkakkar@Tanishqs-Macbook-Pro LAB-1 % cat cipher_ecb.bin
A\??m?ゐ?ej??[??k}?
                  ~dYo&?l89s??? ?D?p?J?ŦA\??m?ゐ?ej??[??k}?
                                                      ~dYo&?l89s??? ?D?p?J?Ŧ
A\??m?ゐ?ej??[??k}?
                  ~dYo&?l89U?}1#^???.

                                      n??0?b"??N2?N??_e%
tanishqkakkar@Tanishqs-Macbook-Pro LAB-1 %
```

After use
$xxd cipher_cbc.bin

```
tanishqkakkar@Tanishqs-Macbook-Pro LAB-1 % xxd cipher_ecb.bin
00000000: 415c f6a4 6ddc dcac e265 6a9a 0f83 5b91  A\..m....ej...[.
00000010: d26b 7d9c 0b7e 6410 596f 26aa 6c38 3917  .k}..~d.Yo&.l89.
00000020: 73bf b413 cb20 c744 c470 9b4a e01c d3bb  s.... .D.p.J....
00000030: 415c f6a4 6ddc dcac e265 6a9a 0f83 5b91  A\..m....ej...[.
00000040: d26b 7d9c 0b7e 6410 596f 26aa 6c38 3917  .k}..~d.Yo&.l89.
00000050: 73bf b413 cb20 c744 c470 9b4a e01c d3bb  s.... .D.p.J....
00000060: 415c f6a4 6ddc dcac e265 6a9a 0f83 5b91  A\..m....ej...[.
00000070: d26b 7d9c 0b7e 6410 596f 26aa 6c38 3917  .k}..~d.Yo&.l89.
00000080: 1955 e9af 7d31 235e dac1 1894 2e0b 0b6e  .U..}1#^.......n
00000090: e9f9 30ec 6222 98d0 4e32 ae4e abc0 5f65  ..0.b"..N2.N.._e
tanishqkakkar@Tanishqs-Macbook-Pro LAB-1 %
```