

LAB-5

The lab is on familiarization with the OpenSSL utility and its various options.

1. Encoding a text file's contents in Base64 format

```
gurusaran@guru: ~/Desktop/ECS
File Actions Edit View Help
gurusaran@guru:~/Desktop$ cd ECS/
gurusaran@guru:~/Desktop/ECS$ ls
msg.txt
gurusaran@guru:~/Desktop/ECS$ cat msg.txt
Hi, My name is GuruSaran
gurusaran@guru:~/Desktop/ECS$ openssl base64 -in msg.txt -out base64
gurusaran@guru:~/Desktop/ECS$ ls
base64 msg.txt
gurusaran@guru:~/Desktop/ECS$ cat base64
SGksIE15IG5hbWUgaXMgR3VydVNhcmFuCg==
gurusaran@guru:~/Desktop/ECS$
```

2. Encrypting a file with DES, with no salt used and decrypting the encrypted file

```
gurusaran@guru: ~/Desktop/ECS
File Actions Edit View Help
gurusaran@guru:~/Desktop$ cd ECS/
gurusaran@guru:~/Desktop/ECS$ ls
base64 msg.txt
gurusaran@guru:~/Desktop/ECS$ openssl des -in msg.txt -out msgEncryptDes => Encryption
enter des-cbc encryption password:
Verifying - enter des-cbc encryption password:
*** WARNING : deprecated key derivation used.
Using -iter or -pbkdf2 would be better.
gurusaran@guru:~/Desktop/ECS$ ls
base64 msgEncryptDes msg.txt
gurusaran@guru:~/Desktop/ECS$ openssl des -d -in msgEncryptDes -out msgDecryptDes => Decryption
enter des-cbc decryption password:
*** WARNING : deprecated key derivation used.
Using -iter or -pbkdf2 would be better.
gurusaran@guru:~/Desktop/ECS$ ls
base64 msgDecryptDes msgEncryptDes msg.txt
gurusaran@guru:~/Desktop/ECS$ cat msgDecryptDes
Hi, My name is GuruSaran => Decrypted msg
gurusaran@guru:~/Desktop/ECS$
```

3. Testing encryption by encrypting a file with DES and then attempting to decrypt it using a wrong password

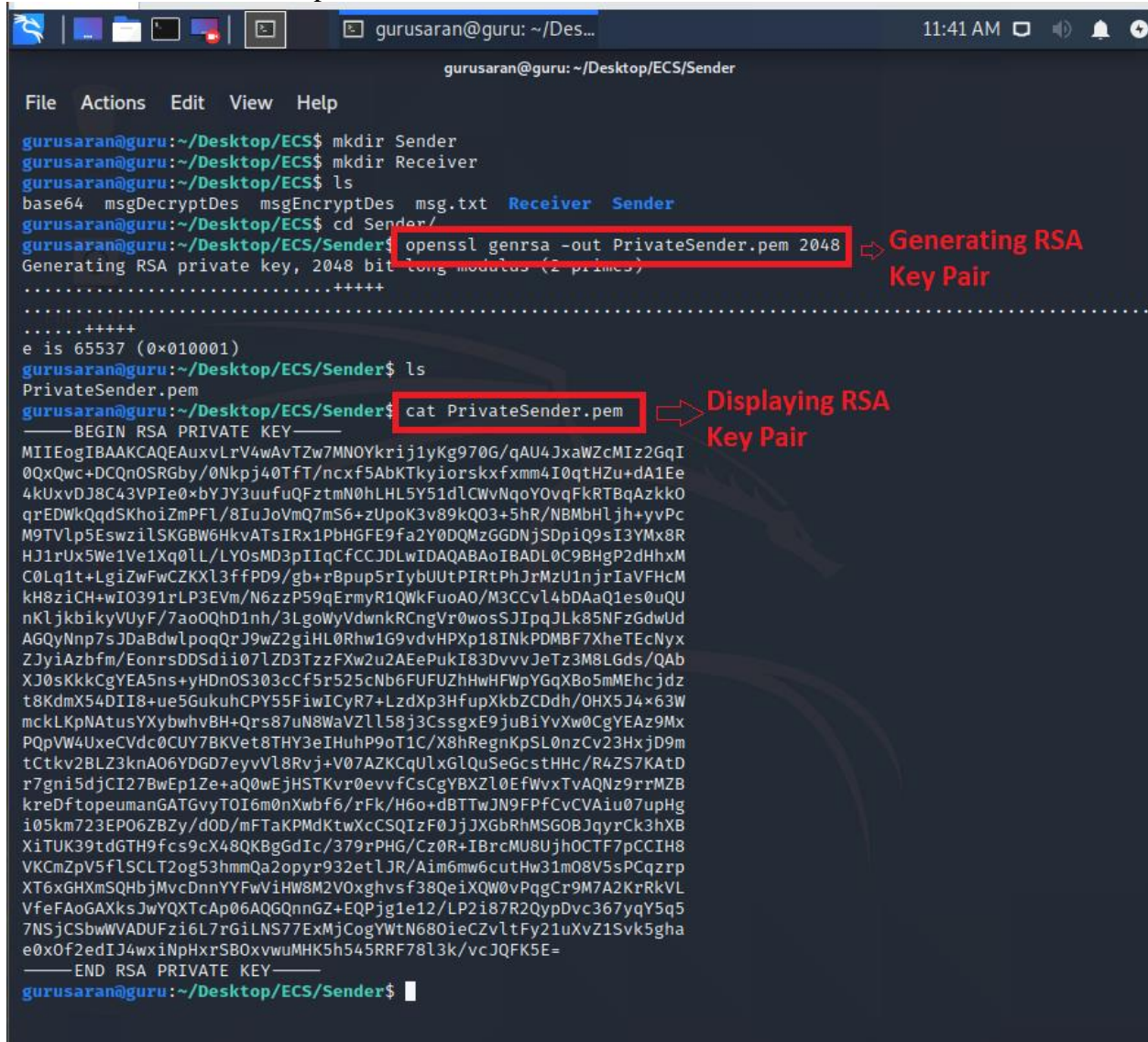
```
gurusaran@guru:~/Desktop/ECS$ ls
base64 msgDecryptDes msgEncryptDes msg.txt
gurusaran@guru:~/Desktop/ECS$ openssl des -d -in msgEncryptDes -out msgDecryptDes
enter des-cbc decryption password:
*** WARNING : deprecated key derivation used.
Using -iter or -pbkdf2 would be better.
bad decrypt
139706344146240:error:06065064:digital envelope routines:EVP_DecryptFinal_ex:bad decrypt:../crypto/evp/evp_enc.c:583:
gurusaran@guru:~/Desktop/ECS$
```

4. Generating an RSA key pair

Openssl genrsa -out PrivateSender.pem 2048

5. Displaying the key pair and the related information of the generated RSA key Pair

Cat PrivateSender.pem



The screenshot shows a terminal window with the following commands and output:

```
gurusaran@guru: ~/Desktop/ECS/Sender
File Actions Edit View Help

gurusaran@guru:~/Desktop/ECS$ mkdir Sender
gurusaran@guru:~/Desktop/ECS$ mkdir Receiver
gurusaran@guru:~/Desktop/ECS$ ls
base64 msgDecryptDes msgEncryptDes msg.txt Receiver Sender
gurusaran@guru:~/Desktop/ECS$ cd Sender/
gurusaran@guru:~/Desktop/ECS/Sender$ openssl genrsa -out PrivateSender.pem 2048
Generating RSA private key, 2048 bit long modulus (2 primes)
.....+++++
.....+++++
e is 65537 (0x010001)
gurusaran@guru:~/Desktop/ECS/Sender$ ls
PrivateSender.pem
gurusaran@guru:~/Desktop/ECS/Sender$ cat PrivateSender.pem
-----BEGIN RSA PRIVATE KEY-----
MIIEogIBAAKCAQEAuxvLrV4wAvTZw7MNOYkrij1yKg970G/qAU4JxaWZcMIz2GqI
0QxQwc+DCqnOSRGby/0Nkpj40FT/ncxf5AbKTkyiorskxfxmm4I0qthZu+dA1Ee
4kUxvDj8C43VPie0xbYJY3uufuQFztmN0hLHL5Y51dLCWvNqoY0vqFkRTBqAzkk0
qrEDWkQdSKhoizmPFL/8IuJoVmQ7mS6+zUpoK3v89kQ03+5hR/NBmbHLjh+yvPc
M9TVlp5EswziLSKGBW6HkvATsIRx1PbHGFE9fa2Y0DQMzGGDNjSDpiQ9sI3YMx8R
HJlrUx5We1Ve1Xq0LL/LYOsMD3pIIqCfCCJDLwIDAQABAoIBADL0C9BHgP2dHhXm
C0Lq1t+LgiZwFwCZKXl3ffPD9/gb+rBpup5rIybUUtPIRtPhJrMzU1njrIaVFHcM
kH8ziCH+wI0391rLP3EVm/N6zzP59qErmyR1QWKfuoAO/M3CCvL4bDAaQ1es0uQU
nKljbikyVUyF/7ao0QhD1nh/3LgoWyVdwnkRCngVr0wosSJIpqJLk85NFzGdwUd
AGQyNnp7sJDABdwlpooQrJ9wZ2giHL0Rhw1G9vdvHPXp18INkPDMBF7XheTECNyx
ZJyiAzbfm/EonrsDDSDii07LZD3TzzFXw2u2AEePukI83DvvvJeTz3M8LGds/QAb
XJ0sKkkCgYEA5ns+yHDnOS303cCf5r525cNb6FUFUZHhWFwPYGqXBo5mMEhcjdz
t8KdmX54DII8+ue5GukuhCPY55FiwICyR7+LzdXp3HfupXkbZCDdh/OHX5J4x63W
mckLKpNatusYXybwhvBH+Qrs87uN8WaVZll58j3CsgxE9juBiYvXw0CgYEAz9Mx
PqVW4UxeCvdc0CUY7BKVet8THY3eIHuhP9oT1C/X8hRegnKpSL0nzCv23HxjD9m
tCtkv2BLZ3knA06YDGD7eyvVl8Rvj+V07AZKCqULxG1QuSeGcstHhc/R4ZS7KAtD
r7gni5djCI27BwEp1Ze+aQ0wEjHSTKvr0evvfCsCgYBXZL0EfWvxTvAQnz9rrMZB
kreDftopeumanGATGvyTOI6m0nXwbF6/rFk/H6o+dBTTwJN9FPfCvCVAiu07upHg
i05km723EP06ZBzy/dOD/mFTaKPMdKtwXcCSQIzF0JjJXGbrHMSGOBjQyrCk3hXB
XiTUK39tdGTH9fcs9cX48QKBgGdIc/379rPHG/Cz0R+IBrcMU8Ujh0CTF7pCCIH8
VKCmZpV5fLSCLT2og53hmmQa2opyr932etlJR/Aim6mw6cutHw31m08V5sPCqzrp
XT6xGHXmSQHbjMvcdnnYYFwViHW8M2V0xghvsf38QeIXQW0vPqgCr9M7A2KrKvL
VfeFAoGAXksJwYQTCaP06AQGQnnGZ+EQPjg1e12/LP2i87R2QypDvc367yqY5q5
7NSjCSbwWVADUFzi6L7rGiLNS77ExMjCogYwTn680ieCZvltFy21uXvZ1Svk5gha
e0x0f2edIJ4wxinPhxrSB0xvwuMHK5h545RRF78L3k/vcJQFK5E=
-----END RSA PRIVATE KEY-----
gurusaran@guru:~/Desktop/ECS/Sender$
```

Annotations in the image:

- A red box highlights the command `openssl genrsa -out PrivateSender.pem 2048` with an arrow pointing to the text "Generating RSA Key Pair".
- A red box highlights the command `cat PrivateSender.pem` with an arrow pointing to the text "Displaying RSA Key Pair".

6. Generating the public RSA keyfile from the RSA key pair generated before and displaying the contents of the public RSA keyfile

```
gurusaran@guru:~/Desktop/ECS/Sender$ openssl rsa -in PrivateSender.pem -pubout -out PublicSender.pem
writing RSA key
gurusaran@guru:~/Desktop/ECS/Sender$ ls
PrivateSender.pem PublicSender.pem
gurusaran@guru:~/Desktop/ECS/Sender$ cat PublicSender.pem
-----BEGIN PUBLIC KEY-----
MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAuxvLrV4wAvTZw7MNOYkr
ij1yKg970G/qAU4JxaWZcMIz2GqIQXQwc+DCQnOSRGby/0Nkpj40TfT/ncxf5Ab
KTkyiorskxfxmm4I0qthZu+dA1Ee4kUxvDJ8C43VPiE0xYJY3uufuQFztmN0hLH
L5Y51dLCWvNqoY0vqFkRTBqAzkkOqrEDWkQqdSKhoiZmPFL/8IuJoVmQ7mS6+zUp
oK3v89kQ03+5hR/NBMBhljh+yvPcM9TVlp5EswzilSKGBW6HkvATsIRx1PbHGF9
fa2Y0DQMzGGDNjSDpIQ9sI3YMx8RHJ1rUx5We1Ve1Xq0LL/LYQsMD3pIIqCfCCJD
LwIDAQAB
-----END PUBLIC KEY-----
gurusaran@guru:~/Desktop/ECS/Sender$
```

Generating and Displaying the public RSA file

7. Encrypting a sample text file with the public key generated earlier

Generating RSA private and public Keypairs for A(Sender) and B(Receiver)

```
gurusaran@guru:~/Desktop/ECS$ cd A/
gurusaran@guru:~/Desktop/ECS/A$ openssl genrsa -out keypairA.pem 2048
Generating RSA private key, 2048 bit long modulus (2 primes)
.....+++++
.....+++++
e is 65537 (0x010001)
gurusaran@guru:~/Desktop/ECS/A$ cat keypairA.pem
-----BEGIN RSA PRIVATE KEY-----
MIIEowIBAAKCAQEAxRg/1M/Hjx38evC2tTsElmsLKHcZiyeqavMAWLR4bw08qma
2btGrfXhXk+fmechLT86TcCwLlFv3xWBQU390dI9NPTSWPOFv90QHj7EGeU8M4n
+4KWYbGoFupltKSuVv3YUbcvWQYVNe+VLLN11WPHZk1wyHJM04RFZEiI+rr2fhfO
ydo0p8Gdfjh3m33PyngRjP9CiZLBGr1G+5QjaCt0dcVEWE/jpbUsya6uyqyj/iF
/xwF/S+rgVYw2Bp8En3ATwXs2TSPE8q5JekXJ0WxKBg/lfbRBxi8zNFcuQhjAtyU
k1PF7ByFeBEXRicFwxCnjpZauIAVzZbzJWYXkwIDAQABAoIBAeyJPMEf1loYpX18
+kKY2r9/UuEivZGEXafEBTYD5NuQq90zeUjggKxALjZNC5L1HGVljvldf1A5eJ2
p5mSiMHqY00xuk+vuqLDL9g4r75CF0IPJMSg9j7Vf1FYvgyZkiff/iqJymtcEMT
mrMfS/+AE+S1ruFgS3AQ09Z/Zfp7Uvpo1k5VZ48K3yUsBihR0bBspSExcQCLltC9
6HxDpCE6hp+P64mbPANucPebxpp7Srt1S7iizEBREp5KT3lutfboJzIK9eyV6fx
kd5nkrY819xHP0ZvqpcXCfUmpa/+fPDMvhx1ueQebECrNNZLRhtlJME5i39zM3x
csmwJkCgYEA1ePR1WtoN3Jhz1KXohdJNu9MKdatN+av3QRBUKETusE++i6zY8Uw
q7uZRTAwYzvtynagojvKrYFC0DeRVVDZp2Ik3ql7xJUyrsIAkmJUD5Iscbc9WV
2RafnZlaIMweDatSsHcKgmOMjRaemM7vPgsvHHHwRHYtT8ZLojBqBcCgYEA0/rA
eZGLZwrv02BqdZv3U9q2fVS6UPrL/o5FWH6d16/5uhQ1YBvpB/LVImEWw3ms1ae4
5LJa88rAeJu0RrDLve8Ji5fZqaiZEdJdIcJuvDFpxhFFUpYS7msiDnMTmf/g1lBAG
i7gW8vvhfrLRxc6JHntg8s/sko5inqoGn9bu/eUCgYEAAnX0bqEF88nQtNGVkylop
91qpAp0Z5/DVvSmIu0YYM/5V0e3EIZEDhygOaDRVddRnc/I5PKZ5CUP86o/SD8/4
Ue3dwFMLG5yu9p5AAw8HG1E6ykP8HYU5ThmtXmKpSKN4TC+2K1k2AnEHEEYh5L5W
F2fJmlA38B5m20i4TN03UfKcGYBi1IbGZyRAY4GzAEHDA39FZjQs7MLNHJDDRsG1
B8hZlh8NjXzZKu0VQKbzL2aAjosJNeBb6cu3ESuNpHvX2AuVnMR1SNTGWca9h18
+ui7DrPcJ/saDG9XM+NAxPQ/0Z7pQDecTKD0ghyI86fvXGLKxHFH4679iUrrhIQA
I648DQKBGdGdfwiqoRDakszLFZSp51u0IRSK0uBj56D7m9Ti8XTYrBGyhlB36aHN
3LI7iB38GikJVs2KH3myTOImoGvRemhzWAM9n9J9anRLgLDXetnGuKgyuKJeTae
72Yee7cIayRJM1/SBfaxuU30ftwqb6IaaDNWZidGOWYjLaUTRB
-----END RSA PRIVATE KEY-----
gurusaran@guru:~/Desktop/ECS/A$ openssl rsa -in keypairA.pem -pubout -out publicA.pem
writing RSA key
gurusaran@guru:~/Desktop/ECS/A$ cat publicA.pem
-----BEGIN PUBLIC KEY-----
MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAxRg/1M/Hjx38evC2tTs
ElmsLKHcZiyeqavMAWLR4bw08qma2btGrfXhXk+fmechLT86TcCwLlFv3xWBQU3
90dI9NPTSWPOFv90QHj7EGeU8M4n+4KWYbGoFupltKSuVv3YUbcvWQYVNe+VLLN1
1WPHZk1wyHJM04RFZEiI+rr2fhfOydo0p8Gdfjh3m33PyngRjP9CiZLBGr1G+5Q
jaCt0dcVEWE/jpbUsya6uyqyj/iF/xwF/S+rgVYw2Bp8En3ATwXs2TSPE8q5JekX
J0WxKBg/lfbRBxi8zNFcuQhjAtyUk1PF7ByFeBEXRicFwxCnjpZauIAVzZbzJWYX
kwIDAQAB
-----END PUBLIC KEY-----
gurusaran@guru:~/Desktop/ECS/A$
```

```
gurusaran@guru: ~/Desktop/ECS/B
File Actions Edit View Help
gurusaran@guru:~/Desktop/ECS$ cd B/
gurusaran@guru:~/Desktop/ECS/B$ openssl genrsa -out keypairB.pem 2048
Generating RSA private key, 2048 bit long modulus (2 primes)
.....+++++
.....+++++
e is 65537 (0x010001)
gurusaran@guru:~/Desktop/ECS/B$ cat keypairB.pem
-----BEGIN RSA PRIVATE KEY-----
MIIEowIBAAKCAQEAx08i1GL7jBSemecQ+jLY/2meFyaFY2M8BzFQFSWTEWZMTGU
AzEJOR3rY55jIW244mMas/ldgH3obHi5DEW9hdiTbFENRUwhp7JuqRSOuXrzEuf1
ZS0zYLEs1xHIFGKc0iGAR6twMA0wCLM4DVYy7y17X39WP9R8AEQqtwm3XtXbcHo1
EGwA64eJYRudjq1s0QLCLsUKLeAH7Y8Z/GtbXKLd77DBCLrW5BFyZ/wI6pIWvkAT
9EPai3otcDqzFG3UPPL2HbFTIAzjaMZorHt/4y/LEK5bwz5aIfFwsA3hxn/f6zdx
2RpAFjKvMIIZ5nvJClwYDlf4gc+mJ0kI9GHI fQIDAQAABaoIBAF/fj/34wd+b5QuX
1/fjSnA65YyjhnaQSBEGjpH5UejF3XqRSyJfDSigqssssHr/+1DGhGFUJGDhAZi
0eiFyABKgTnaGGQXpTJ39OZgdrEJ1ZM/Fsjc6jMoCkFurEULq4c0uuZiAMiWEGc
mKL1UW5pKZn5F3+a95fNv7LNXtJUHCQ/h7AY370Et+e0k13utq1Hb2DCSUHCwpLL
Y3llv0+wyfCHWSdas4MtDiboQPxAf14Dr7n0aTGAa21hcZki/iA1Ks8/WS4iF351
4NNzn2rkfNpZCQTFPGHbSdIMVvk2XtBkhhvSGATnkFPWkpNxx0aZ/DJcKEM44Mnhp
mVtb1wECgYEA9M/iMvpfe/N5Cfn51BVjrU7dUBCTI271qqERWpTEitQHucy3c6A
kuL+c55eMEgYd3VN64tZEe+0KvEw6QLaTqws+6vNA+cnRJNA3/mdkdwN+ANA3kYJ
715qWLCOpiOjyxMTZjxKx83ecNWqok/39euAI9HZt3Xy7bHBH4D1sMECgYEAzPj1
o8VuVCAzMFj5Nura8RA4/d1jaznzrofelD+vwOiyMF/G9/PVH0LSFpQ3lTXkpQKc
g99oiyF/rNpg1wKAXloJ8Cous4vEsi4uqDGLonGqG0e6RyWzU8/uQE5aKnVQXTF6
bqRvdSMDrNNQAgeOIImnqpeoJo8dCLHV0LP0Gyr0CgYBb4a3+/hNaPR4fjW+jlseL
Yz8S7rWapemU0dF+krLVdZDUdAw2TWvaNVHU6QpmypHlIUJWdj1eyv1u5Ik72vM+
dbzGMkvG/Dmzt1Syk0hLVyC1J+Ux6ltpM6Fswg+f8V5n0GiehWB3rx+eb8MUGjlx
VgsI5pj1D1K2vXFDNq5/wQKBgQC12Aw3z6wGtApYYmiDOXRWxAYmKha15DNEW75
MtvMFMF20/30ncitbGYCwECKj8uWeUulzYF+P9/ykRCs4XThAQGYqncSeDGOkfix
cbfGhfVQkhHBYqdlJ+YuOtGRt+BgGeYeLvsh8+6A10WgpyX6G1Hr/NMpxi4USniT
wa56tQKBgGj5WVvQNCw58I/l6tzQeLEQYHrxygYhRbcEPeS6WXRwPMgjlaLWjFdY
wFhQLg/vRIqpe5oAkY8ajSdSRmLIqoG5tqg2X4N+DjgKBcXRHia3kvI9Ycm8d26q
Jx0jmr2LTv6ZF241V6oQ4n2sHiB7VQYqyPak6E/NJpAy3msKJtPt
-----END RSA PRIVATE KEY-----
gurusaran@guru:~/Desktop/ECS/B$ openssl rsa -in keypairB.pem -pubout -out publicB.pem
writing RSA key
gurusaran@guru:~/Desktop/ECS/B$ cat publicB.pem
-----BEGIN PUBLIC KEY-----
MIIBIjANBgkqhkiG9w0BAQEFAAOCQA8AMIIBCgKCAQEAx08i1GL7jBSemecQ+jL
Y/2meFyaFY2M8BzFQFSWTEWZMTGUazEJOR3rY55jIW244mMas/ldgH3obHi5DEW9
hdiTbFENRUwhp7JuqRSOuXrzEuf1ZS0zYLEs1xHIFGKc0iGAR6twMA0wCLM4DVYy
7y17X39WP9R8AEQqtwm3XtXbcHo1EGwA64eJYRudjq1s0QLCLsUKLeAH7Y8Z/Gtb
XKLd77DBCLrW5BFyZ/wI6pIWvkAT9EPai3otcDqzFG3UPPL2HbFTIAzjaMZorHt/
4y/LEK5bwz5aIfFwsA3hxn/f6zdx2RpAFjKvMIIZ5nvJClwYDlf4gc+mJ0kI9GHI
fQIDAQAAB
-----END PUBLIC KEY-----
gurusaran@guru:~/Desktop/ECS/B$
```

Sharing public keypairs of A and B

```
-----END PUBLIC KEY-----
gurusaran@guru:~/Desktop/ECS/B$ cp publicB.pem ~/Desktop/ECS/A/
gurusaran@guru:~/Desktop/ECS/B$ cd ..
gurusaran@guru:~/Desktop/ECS$ cd A/
gurusaran@guru:~/Desktop/ECS/A$ ls
keypairA.pem publicA.pem publicB.pem
gurusaran@guru:~/Desktop/ECS/A$ cp publicA.pem ~/Desktop/ECS/B/
gurusaran@guru:~/Desktop/ECS/A$ cd ..
gurusaran@guru:~/Desktop/ECS$ cd B/
gurusaran@guru:~/Desktop/ECS/B$ ls
keypairB.pem publicA.pem publicB.pem
gurusaran@guru:~/Desktop/ECS/B$
```



```
gurusaran@guru:~/Desktop/ECS/B$ cd ..  
gurusaran@guru:~/Desktop/ECS$ cd A/  
gurusaran@guru:~/Desktop/ECS/A$ ls  
keypairA.pem publicA.pem publicB.pem  
gurusaran@guru:~/Desktop/ECS/A$ echo 'Hi, How are u?' > msg.txt ➡ Creating sample msg  
gurusaran@guru:~/Desktop/ECS/A$ ls  
keypairA.pem msg.txt publicA.pem publicB.pem  
gurusaran@guru:~/Desktop/ECS/A$ cat msg.txt  
Hi, How are u?  
gurusaran@guru:~/Desktop/ECS/A$ openssl rsautl -encrypt -in msg.txt -out encrypt -inkey publicB.pem -pubin ➡ Encryption  
gurusaran@guru:~/Desktop/ECS/A$ ls  
encrypt keypairA.pem msg.txt publicA.pem publicB.pem  
gurusaran@guru:~/Desktop/ECS/A$ cat encrypt  
000000z0dk[000]0-[v20000k+0000000000080  
00 ;0IKZm)8,C[00"0200000+000J000U0u000js900=0000[00'0Ik0<b0  
r0j20090d0 h=rn000000au0S060K000000000:00;u00  
-w0u0000-000  
M00I00/W-0W0  
%j0DAkfSJ'%040000000F'060
```

Decryption

```
gurusaran@guru:~/Desktop/ECS/A$ cp encrypt ~/Desktop/ECS/B
gurusaran@guru:~/Desktop/ECS/A$ cd ..
gurusaran@guru:~/Desktop/ECS$ cd B/
gurusaran@guru:~/Desktop/ECS/B$ ls
encrypt  keypairB.pem  publicA.pem  publicB.pem
gurusaran@guru:~/Desktop/ECS/B$ openssl rsautl -decrypt -in encrypt -out Decrypt -inkey keypairB.pem
Invalid command 'rsault'; type "help" for a list
gurusaran@guru:~/Desktop/ECS/B$ openssl rsautl -decrypt -in encrypt -out Decrypt -inkey keypairB.pem
gurusaran@guru:~/Desktop/ECS/B$ ls
Decrypt  encrypt  keypairB.pem  publicA.pem  publicB.pem
gurusaran@guru:~/Desktop/ECS/B$ cat Decrypt
Hi, How are u?
```

Decrypted msg

Decryption

9. Testing encryption and decryption using a symmetric cipher method (AES-256-CBC or any other symmetric cipher)

Encryption (AES)

```
File Actions Edit View Help
gurusaran@guru:~/Desktop$ cd S
bash: cd: S: No such file or directory
gurusaran@guru:~/Desktop$ cd Sender/
gurusaran@guru:~/Desktop/Sender$ echo Hi, Iam GuruSaran >msg.txt
gurusaran@guru:~/Desktop/Sender$ ls
msg.txt
gurusaran@guru:~/Desktop/Sender$ cat msg.txt
Hi, Iam GuruSaran
gurusaran@guru:~/Desktop/Sender$ openssl enc -aes-256-cbc -base64 -in msg.txt -out encMsg
enter aes-256-cbc encryption password:
Verifying - enter aes-256-cbc encryption password:
*** WARNING : deprecated key derivation used.
Using -iter or -pbkdf2 would be better.
gurusaran@guru:~/Desktop/Sender$ ls
encMsg msg.txt
gurusaran@guru:~/Desktop/Sender$ cat encMsg
U2FsdGVkX18n80lLMnbKWZTXEZYFX4437prjT0C7Ru0jyWNT8DiRFfkaFM5fXRhy
gurusaran@guru:~/Desktop/Sender$ cp encMsg ~/D
Desktop/ Documents/ Downloads/
gurusaran@guru:~/Desktop/Sender$ cp encMsg ~/Desktop/Receiver/
gurusaran@guru:~/Desktop/Sender$ ls
encMsg msg.txt
gurusaran@guru:~/Desktop/Sender$
```

Encryption

Encrypted msg

Decryption (AES)

```
File Actions Edit View Help
gurusaran@guru:~/Desktop/Receiver$ ls
encMsg
gurusaran@guru:~/Desktop/Receiver$ cat encMsg
U2FsdGVkX18n80lLMnbKWZTXEZYFX4437prjT0C7Ru0jyWNT8DiRFfkaFM5fXRhy
gurusaran@guru:~/Desktop/Receiver$ openssl enc -aes-256-cbc -d -base64 -in encMsg -out decMsg
enter aes-256-cbc decryption password:
*** WARNING : deprecated key derivation used.
Using -iter or -pbkdf2 would be better.
bad decrypt
140247999132992:error:06065064:digital envelope routines:EVP_DecryptFinal_ex:bad decrypt:../crypto/evp/evp_enc.c:5
83:
gurusaran@guru:~/Desktop/Receiver$ openssl enc -aes-256-cbc -d -base64 -in encMsg -out decMsg
enter aes-256-cbc decryption password:
*** WARNING : deprecated key derivation used.
Using -iter or -pbkdf2 would be better.
gurusaran@guru:~/Desktop/Receiver$ ls
decMsg encMsg
gurusaran@guru:~/Desktop/Receiver$ cat decMsg
Hi, Iam GuruSaran
gurusaran@guru:~/Desktop/Receiver$
```

Decrypting with wrong password

Decrypting with correct password

Decrypted Msg

```
File Actions Edit View Help
gurusaran@guru: ~/Desktop/ECS
gurusaran@guru:~/Desktop$ cd ECS/
gurusaran@guru:~/Desktop/ECS$ ls
A B base64 msgDecryptDes msgEncryptDes msg.txt
gurusaran@guru:~/Desktop/ECS$ cat msg.txt
Hi.. Mv name is Gurusaran
gurusaran@guru:~/Desktop/ECS$ md5sum msg.txt
21677152f7de58b8e0e7def73909a781 msg.txt
gurusaran@guru:~/Desktop/ECS$
```

➡ Generating Md5 hash

[illegible]

12. Generating a new certificate signing request with the RSA key pair generated earlier

```
openssl req -new -key private.pem -out certificate
```

13. View the contents of the certificate signing request

Cat certificate

```
Verified OK
gurusaran@guru:~/Desktop/ECS/sign$ ls
msg private.pem public.pem signed
gurusaran@guru:~/Desktop/ECS/sign$ openssl req -new -key private.pem -out certificate
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.

Country Name (2 letter code) [AU]:IN
State or Province Name (full name) [Some-State]:guru
Locality Name (eg, city) []:vizag
Organization Name (eg, company) [Internet Widgits Pty Ltd]:amrita
Organizational Unit Name (eg, section) []:cyber
Common Name (e.g. server FQDN or YOUR name) []:guru
Email Address []:gurusarand@gmail.com

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:1234
An optional company name []:
gurusaran@guru:~/Desktop/ECS/sign$ ls
certificate msg private.pem public.pem signed
gurusaran@guru:~/Desktop/ECS/sign$ cat certificate
-----BEGIN CERTIFICATE REQUEST-----
MIIC3DCCACQCAwAwYEXCzAJBgNVBAYTAklOMQ0wCwYDVQQIDARndXJ1MQ4wDAYD
VQQHDAV2aXphZ2EPMA0GA1UECgwGYW1yaXRhMQ4wDAYDVQQIDAVjeWJlcjENMAAsG
A1UEAwwEZ3VydTEjMCEGCSqGSIb3DQEJARYUz3VydXNhcmFuZEBnbWFPbC5jb20w
ggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQAuX4deusw47RglzXa6GF4
+rLkpFrIb+N4YnooHf7A9hfxvs+tr5jxngriXe/FuMcwTmd5E611kf4qINosYqp
CYP10Lk9gOXmkMouZmLikemhX9Xcr/QfbZx3zc4rwdwaRUt4pwcqzsoQi+oh+VKS
unh/tu0bYuah/LH5Ih0LtEChndHNM5U9Mycgj+bmFXhtQkAh1AbNWRuU3WLCmCOM
hydbbsMwUQtVQXZUTIZkiZBTDP4wR4HNg/S1AhJHe9h+BiQ1PsJ/LE5dmSFeZG2L
FCxL5Rdfzjresgfne643e4HZbmXG+qigQbiIo3X0Qg+JkRx2fLIYgUB31eHvP0B5
AgMBAAGFTATBgqhkiG9w0BCQcxBgwEMTIzNDANBgkqhkiG9w0BAQsFAAOCAQEAF
5ZgFsCohNFR686ZbSjZCjGNNoEDsWmjQfxtBShHh2XmGTkvGi/D9v/j17bAFya/
/LIYqcyoCuoH2F0fQZNhzVZN4me03OgxF/kJtuTPoH4FwKFRlQEUE8Tulm+p6UG
5jlF6Pf8103UPE4BkPojvgLshq7fGwGykBUqSftHM4R6c4Rfwv1fShhDj0y7XPvq
ek7IZt0DgEDY5eMeETuQna0vcDSzkLX6+eHe2iYBJUuYxVEed1vK63yoYjcU9Yjv
H+UMJmCs0pnF7MQpXIg5YbTMk2U9jB8rsAgwXUM3p1o070IjAVhAzPIEUyOvKwMD
3I1ke3Id0kcUw1f0Z9sHWA=
-----END CERTIFICATE REQUEST-----
```

Generating a new certificate signing request

Content of certificate signing request

14. Automatically signing a certificate request and create the a self-signed Certificate

Openssl x509 -req -in certificate -signkey private.pem -out certone

15. View the content of certificate

Cat certone

```
-----BEGIN CERTIFICATE REQUEST-----
gurusaran@guru:~/Desktop/ECS/sign$ openssl x509 -req -in certificate -signkey private.pem -out certone
Signature ok
subject=C = IN, ST = guru, L = vizag, O = amrita, OU = cyber, CN = guru, emailAddress = gurusarand@gmail.com
Getting Private key
gurusaran@guru:~/Desktop/ECS/sign$ ls
certificate certone msg private.pem public.pem signed
gurusaran@guru:~/Desktop/ECS/sign$ cat certone
-----BEGIN CERTIFICATE-----
MIIDizCCANMCF9facrLVxUv6sRPs+wGnM146yGiMA0GCSqGSIb3DQEBCwUAMIGB
MQswCQYDVQQGEwJJTjENMAsGA1UECAwEZ3VydTEOMAwGA1UEBwwFdml6YWcxZDZAN
BgNVBAoMBmFtcm0YTEOMAwGA1UECwwFY3liZXIxDALBgNVBAMMBGd1cnUxIzAh
BgkqhkiG9w0BCQEFQg1cnVzYXJhbmRAZ21haWwY29tMB4XDTEwMTAyNDE2MzU1
Nl0XDTEwMTEyMzE2MzU1Nl0wYExCZAJBgNVBAYTAk0MQ0wCwYDVQQIDARndXJ1
MQ4wDAYDVQQHDAV2aXphZzEPMA0GA1UECgwGYW1yaXRhMQ4wDAYDVQQLEDAVjeWJl
cjENMAsGA1UEAwEZ3VydTEjMCEGCSqGSIb3DQEJARYUZ3VydXNhcmFuZEBnbWFP
bC5jb20wggiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQAuX4deusw47Rg
lzXa6GF4+rLkpFrIb+N4YnooHf7A9hfxvs+tr5jxngrIXe/FuMwTmd5E611kfm4
qINosYqpCYP10Lk9g0XmkMOuZmLikemhX9Xcr/QfbZx3zc4rvdwaRUt4pwcqzsoQ
i+oh+VkSunh/tu0bYuah/LH5Ih0LtEChndHNMsU9Mycgj+bmFXhtQkAh1AbNWRuU
3WLCmCOMhydbbsMwUqtVQXZUTIZkiZBTDp4wR4HNg/S1AhJHe9h+BiQ1PsJ/LE5d
mSFeZG2LFCxL5Rdfzjresgfne643e4HZbmXG+qigQbiIo3X0Qg+JkRx2fLIYgUB3
1eHvP0B5AgMBAAEwDQYJKoZIhvcNAQELBQADggEBAakoXSUqkRmR3ccsCv4oUD6N
XIT3iFj6cSuT5c/mlbvmeD3M7208rNrlCWbjIYHGUAQzkX9zcM+XVrm+8CdFit3X
fELOQU6ZmfHlhzkymzRq/ge+tjed/0hNqT2rCenja0y3DVYFL2UqXs/ige+hC58n
MoQMnFc103v0P7XtgFEm7eN3SNQxZEX29LjoQHnV4R8nE/aSVxJ4Tr96EiaJ/kbC
OX8rLJA95CyWjlgm502dgyC7szbRbRaUXY0M1mHsWk486Z0hxEEh37600p5oWbk2
gZhhQPeflCA7YwBkmVdXnwXRXWTNufw1Sme3vXiba5wEL93s27w9rIBtrXZ3Yoc=
-----END CERTIFICATE-----
gurusaran@guru:~/Desktop/ECS/sign$
```