ECE PARIS
ÉCOLE D'INGÉNIEURS

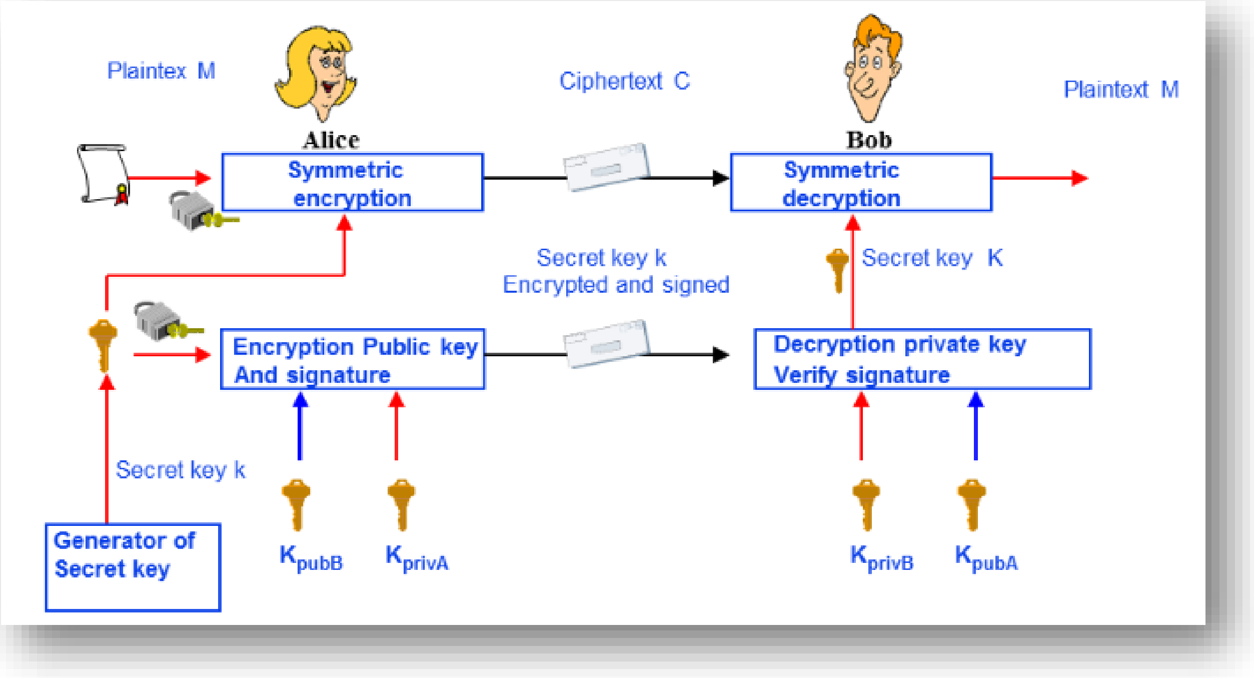
CRYPTOGRAPHY LAB

SUBMITTED BY-

DEVYANSHI TIWARI

SOURADEEP BANERJEE

Q.1) Explain the Scenario:

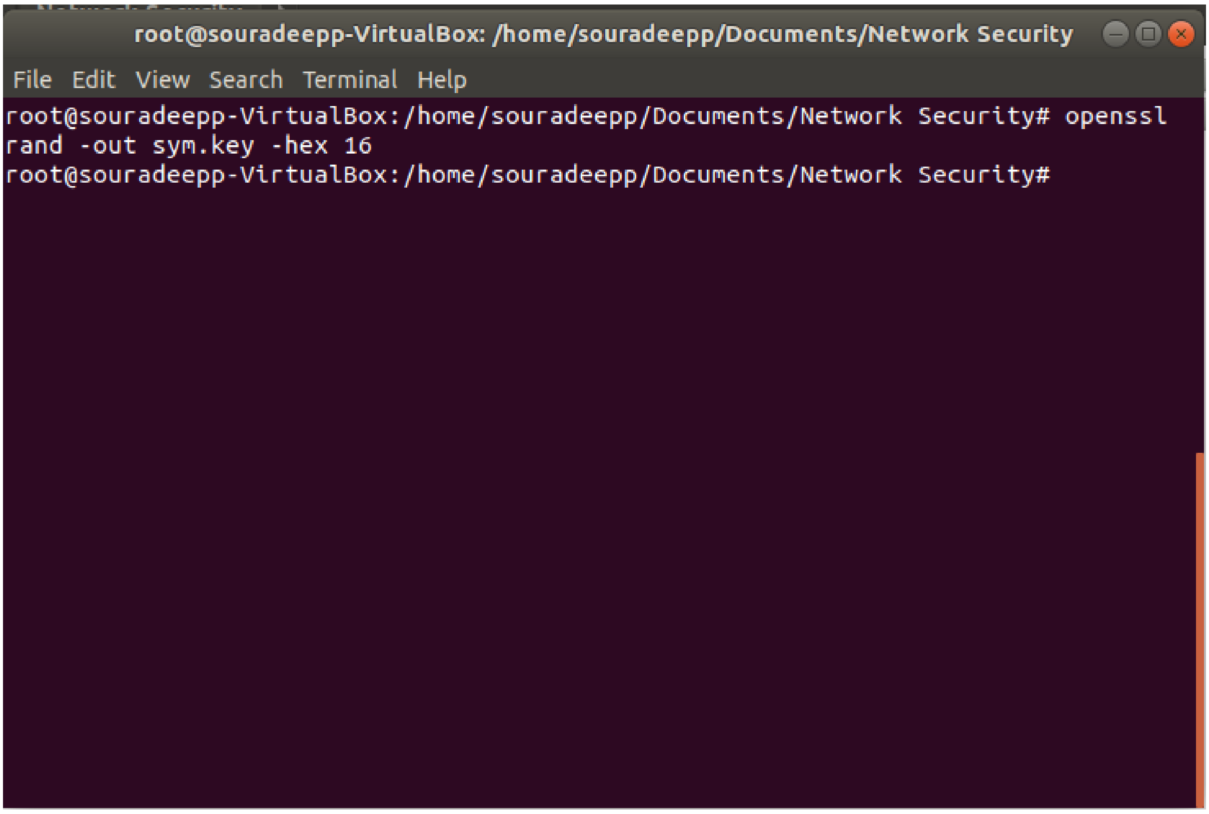


In the above scenario, Alice is sending a file named Plaintext to Bob. For the same, Alice uses symmetric encryption to encrypt the file and send the encrypted file Ciphertext to Bob. Alice uses a symmetric key called secret key to do the symmetric encryption. She uses asymmetric encryption in order to do the encryption and for this she uses the public key of Bob in order to encrypt the file. She also uses her digital signature to sign the encrypted secret key.

Bob on the other hand on receiving the encrypted key, decrypts the same with his private key and verifies the signature of Alice. He then uses the decrypted secret key to decrypt the Ciphertext that Alice sent him and gets the original file which was Plaintext.

Q.2) Generate the symmetric key sym.key with the length of **128** bits; use the rand command and encode the key in **hex**.

Ans: To do the same we use the command→openssl rand -out sym.key -hex 16



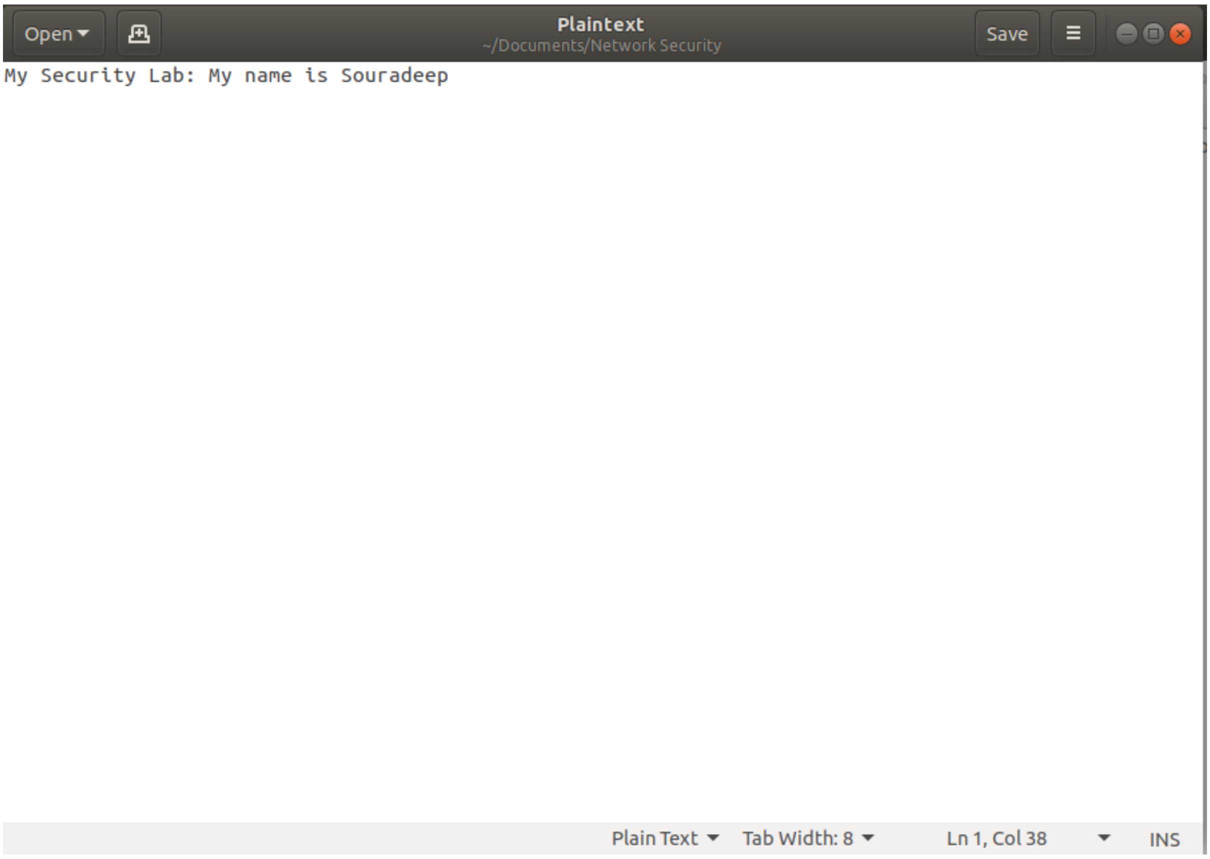
root@souradeepp-VirtualBox: /home/souradeepp/Documents/Network Security
File Edit View Search Terminal Help

```
root@souradeepp-VirtualBox:/home/souradeepp/Documents/Network Security# openssl
rand -out sym.key -hex 16
root@souradeepp-VirtualBox:/home/souradeepp/Documents/Network Security#
```

Q.3) Realize the above scenario and by exchanging a safe way the symmetric key with your colleague:

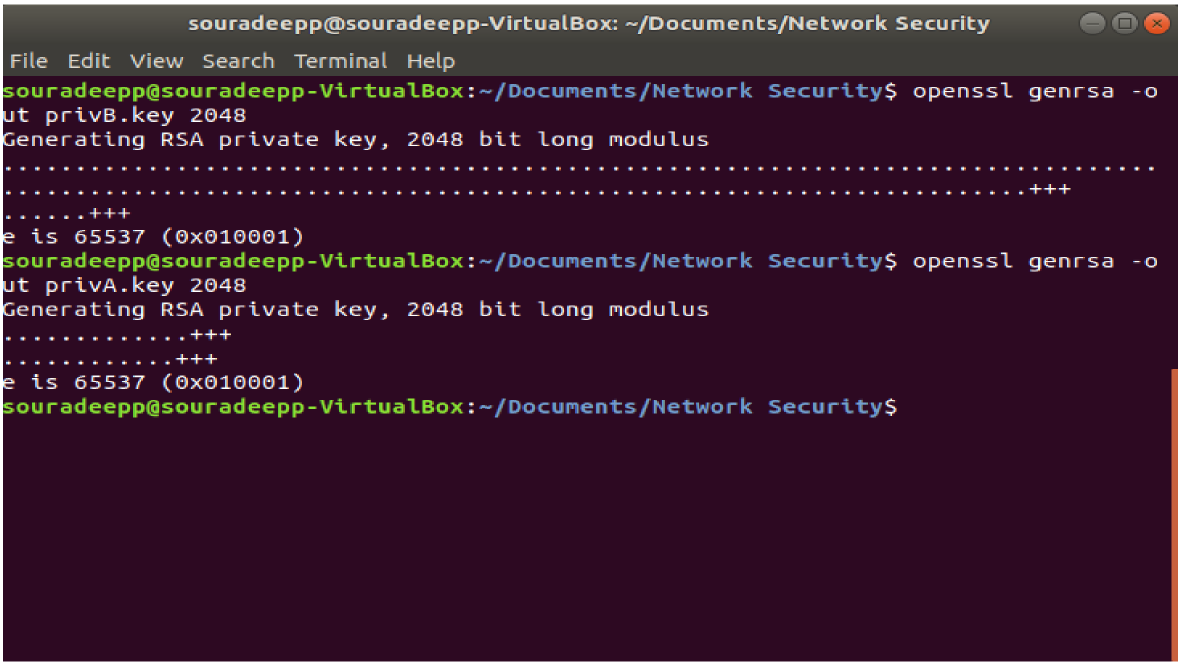
a) Create Plaintext.txt contain: My security lab: My name is <your_name>.

Ans:



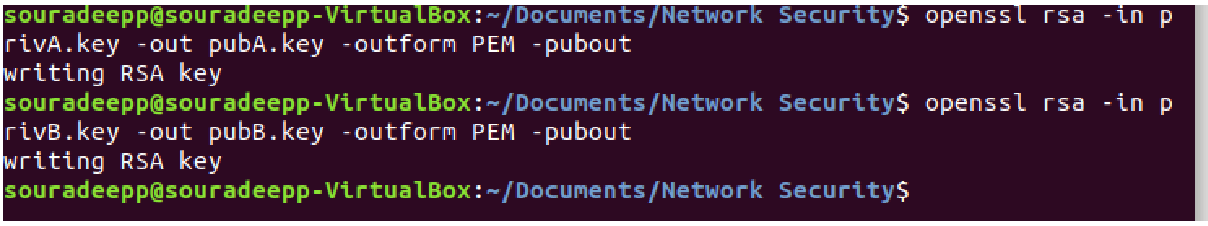
```
My Security Lab: My name is Souradeep
```

b) Generate RSA keys which are 2048bits long: named privA.key, privB.key, pubA.key, pub.key.



souradeepp@souradeepp-VirtualBox: ~/Documents/Network Security
File Edit View Search Terminal Help

```
souradeepp@souradeepp-VirtualBox:~/Documents/Network Security$ openssl genrsa -o
ut privB.key 2048
Generating RSA private key, 2048 bit long modulus
................................................................................
.........................................................................+++
......+++
e is 65537 (0x010001)
souradeepp@souradeepp-VirtualBox:~/Documents/Network Security$ openssl genrsa -o
ut privA.key 2048
Generating RSA private key, 2048 bit long modulus
.............+++
............+++
e is 65537 (0x010001)
souradeepp@souradeepp-VirtualBox:~/Documents/Network Security$
```

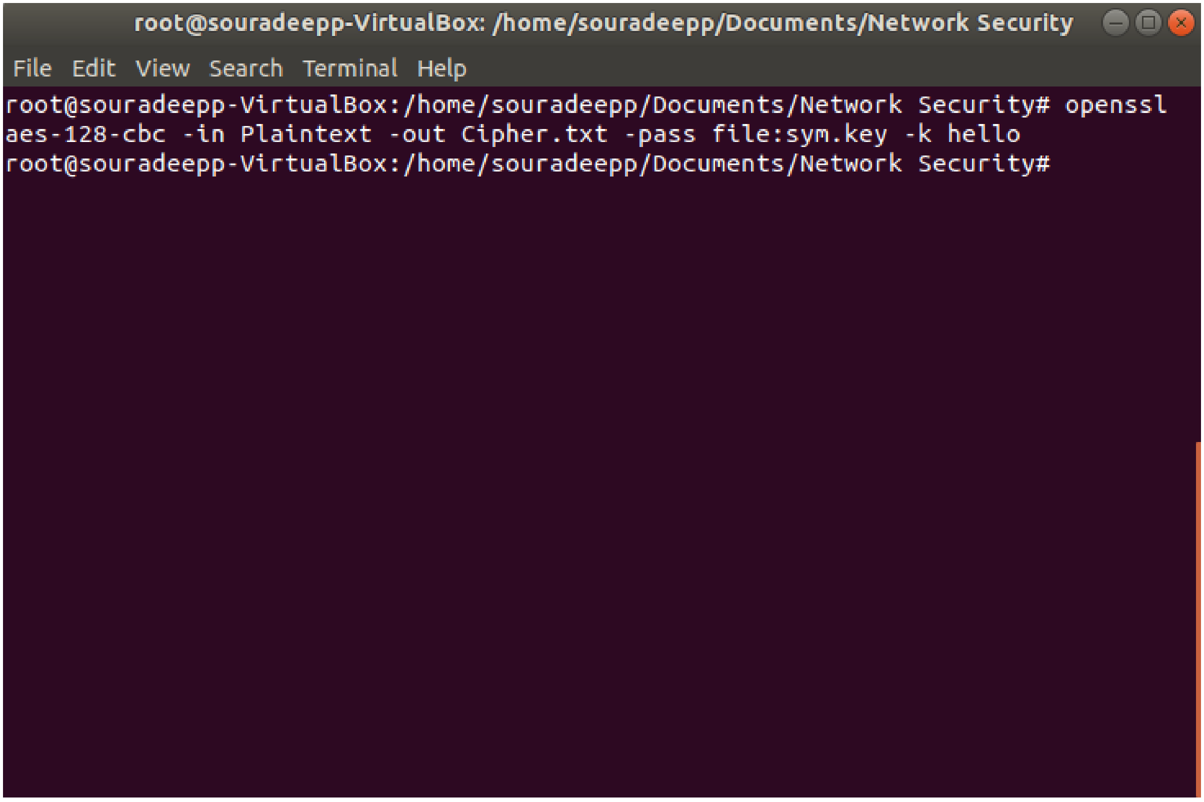


```
souradeepp@souradeepp-VirtualBox:~/Documents/Network Security$ openssl rsa -in p
rivA.key -out pubA.key -outform PEM -pubout
writing RSA key
souradeepp@souradeepp-VirtualBox:~/Documents/Network Security$ openssl rsa -in p
rivB.key -out pubB.key -outform PEM -pubout
writing RSA key
souradeepp@souradeepp-VirtualBox:~/Documents/Network Security$
```

c) Exchange the public keys.

d) Encrypt the PlaintextM.txt using symmetric algorithm (-aes-128-cbc): Ciphertext.txt (use the key generated in this task), use the option -kfile for password and -base64.

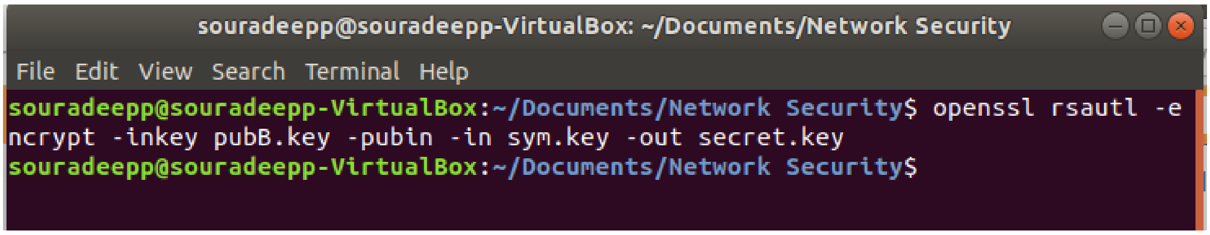
Ans: To the task we use the command→ openssl aes-128-cbc -in Plaintext -out Cipher.txt -pass file:sym.key -k hello


root@souradeepp-VirtualBox: /home/souradeepp/Documents/Network Security
File Edit View Search Terminal Help

```
root@souradeepp-VirtualBox:/home/souradeepp/Documents/Network Security# openssl
aes-128-cbc -in Plaintext -out Cipher.txt -pass file:sym.key -k hello
root@souradeepp-VirtualBox:/home/souradeepp/Documents/Network Security#
```

e) Encrypt the symmetric key using asymmetric algorithm (generate the encrypted file: secret.key)

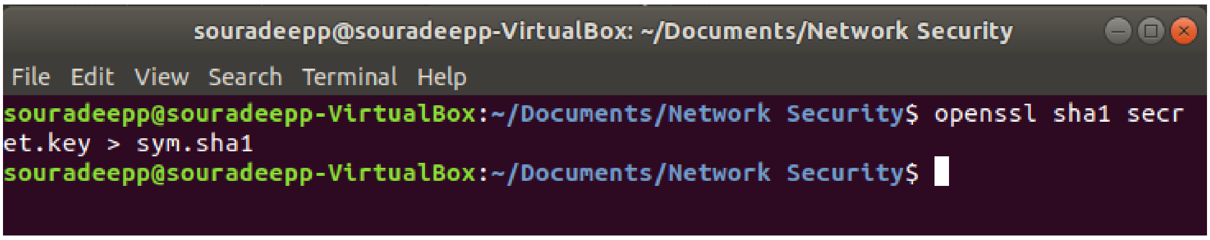
Ans:


souradeepp@souradeepp-VirtualBox: ~/Documents/Network Security
File Edit View Search Terminal Help

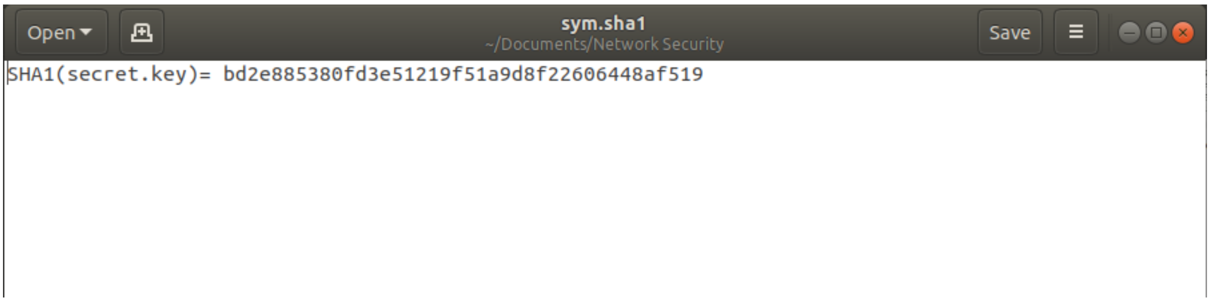
```
souradeepp@souradeepp-VirtualBox:~/Documents/Network Security$ openssl rsautl -e
ncrypt -inkey pubB.key -pubin -in sym.key -out secret.key
souradeepp@souradeepp-VirtualBox:~/Documents/Network Security$
```

f) Generate the hash value of symmetric key using SHA1 (sym.sha1)

Ans: We use the command→ openssl sha1 secret.key > sym.sha1 to save the hash key in sym.sha1


souradeepp@souradeepp-VirtualBox: ~/Documents/Network Security
File Edit View Search Terminal Help

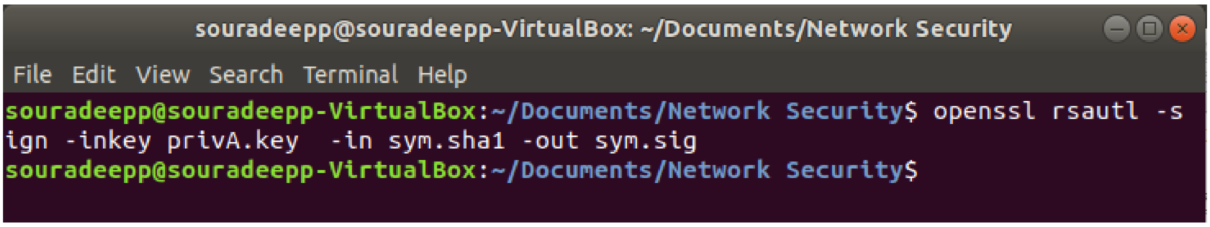
```
souradeepp@souradeepp-VirtualBox:~/Documents/Network Security$ openssl sha1 secr
et.key > sym.sha1
souradeepp@souradeepp-VirtualBox:~/Documents/Network Security$ 
```



```
SHA1(secret.key)= bd2e885380fd3e51219f51a9d8f22606448af519
```

g) Sign sym.sha1, generate a file sym.sig

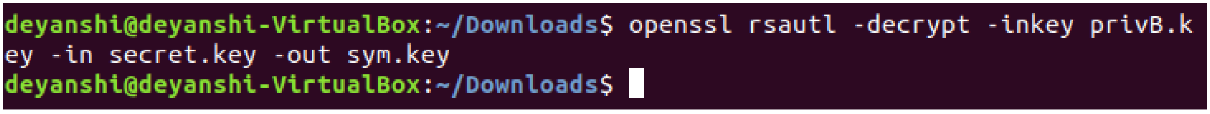
Ans:


souradeepp@souradeepp-VirtualBox: ~/Documents/Network Security
File Edit View Search Terminal Help

```
souradeepp@souradeepp-VirtualBox:~/Documents/Network Security$ openssl rsautl -s
ign -inkey privA.key  -in sym.sha1 -out sym.sig
souradeepp@souradeepp-VirtualBox:~/Documents/Network Security$
```

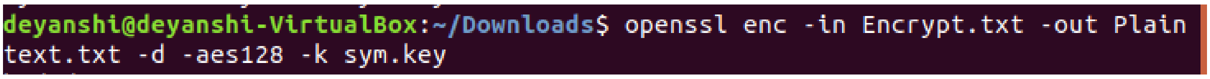
h) Send the necessary files to your colleague that allows decrypting your message, and verify your signature (you have to use the same options for decrypting as encrypting)

Ans: My colleague decrypts the secret key using her private key.



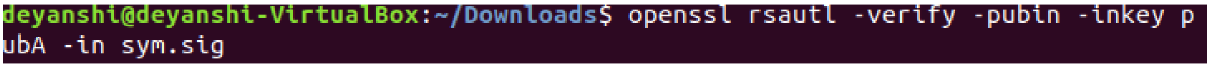
```
deyanshi@deyanshi-VirtualBox:~/Downloads$ openssl rsautl -decrypt -inkey privB.k
ey -in secret.key -out sym.key
deyanshi@deyanshi-VirtualBox:~/Downloads$ 
```

Now my colleague uses the above symmetric key to decrypt the encrypted text.



```
deyanshi@deyanshi-VirtualBox:~/Downloads$ openssl enc -in Encrypt.txt -out Plain
text.txt -d -aes128 -k sym.key
```

The signature of the sender is also being verified by the following command:



```
deyanshi@deyanshi-VirtualBox:~/Downloads$ openssl rsautl -verify -pubin -inkey p
ubA -in sym.sig
```

Using this process of encryption and decryption we can make sure that neither the Cipher text nor the symmetric key used to encrypt the original text file is being altered by anyone or being spied over by anyone while transferring it between 2 clients. It prevents vulnerabilities like man in the middle attack, etc. Use of signature can help the receiver to be sure of the fact that the file hasn’t been altered by anyone while completing the process of transfer.