Experiment-2

2.1 Aim: Basic Symmetric and Asymmetric Encryption: Demonstrate the basic principles of symmetric and asymmetric encryption using common tools.

2.2 Course Outcome:

Apply foundational security principles and cryptographic solutions to protect systems and data.

2.3 Lab Objective: To understand and demonstrate the process of encrypting and decrypting data using symmetric (e.g., AES) and asymmetric (e.g., RSA) cryptographic algorithms.

2.4 Requirements:

- OS: Windows/Linux/macOS
- Tools: OpenSSL or Python (PyCryptodome / cryptography library)
- Sample files (.txt, .pdf, etc.)

2.5 Theory:

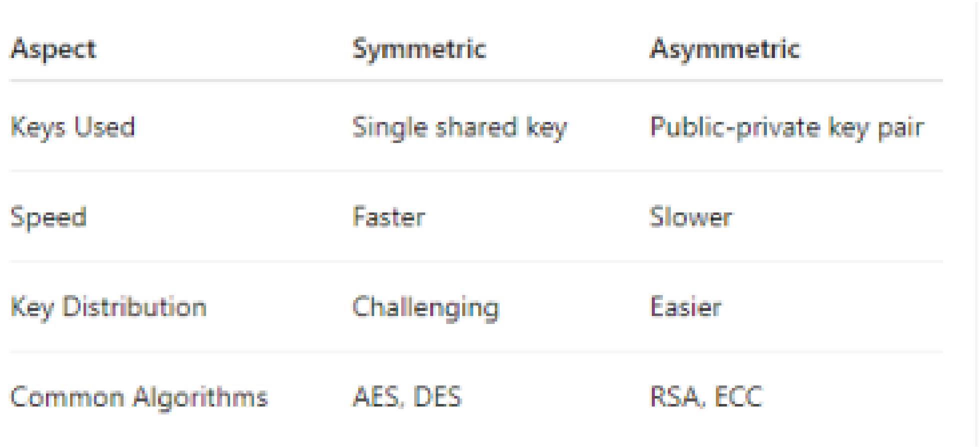
Encryption is the process of converting plaintext into ciphertext to prevent unauthorized access. Decryption reverses this process.

- **Symmetric Encryption** uses the same key for encryption and decryption (e.g., AES). It is fast and suitable for bulk data encryption, but secure key sharing is a challenge.
- **Asymmetric Encryption** uses a public key for encryption and a private key for decryption (e.g., RSA). It enables secure key exchange and digital signatures but is computationally slower.

Applications:

- Secure data transmission
- Digital signatures and certificates
- Email encryption (e.g., PGP)
- VPNs and secure web (SSL/TLS)

Key Differences:

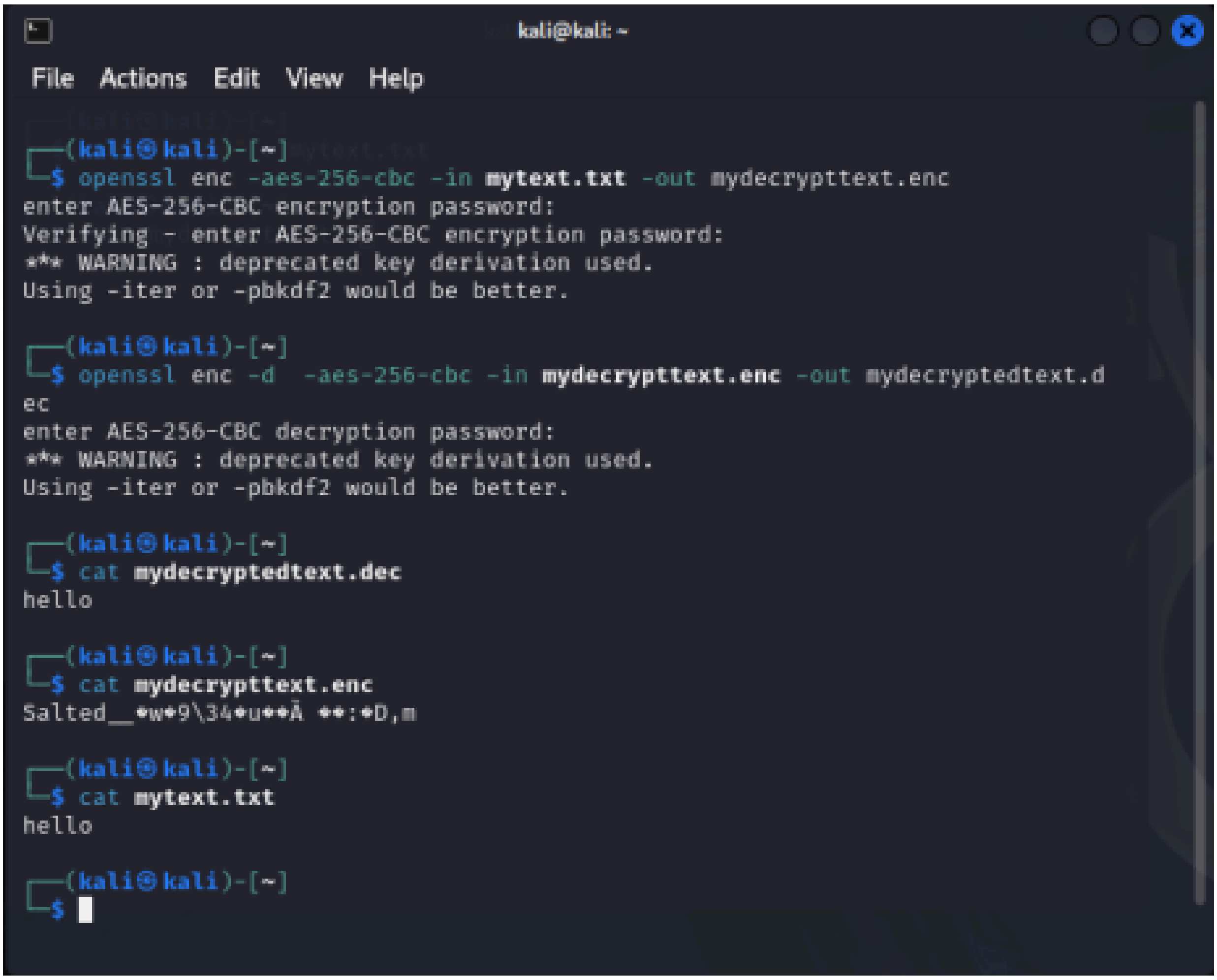


Aspect	Symmetric	Asymmetric
Keys Used	Single shared key	Public-private key pair
Speed	Faster	Slower
Key Distribution	Challenging	Easier
Common Algorithms	AES, DES	RSA, ECC

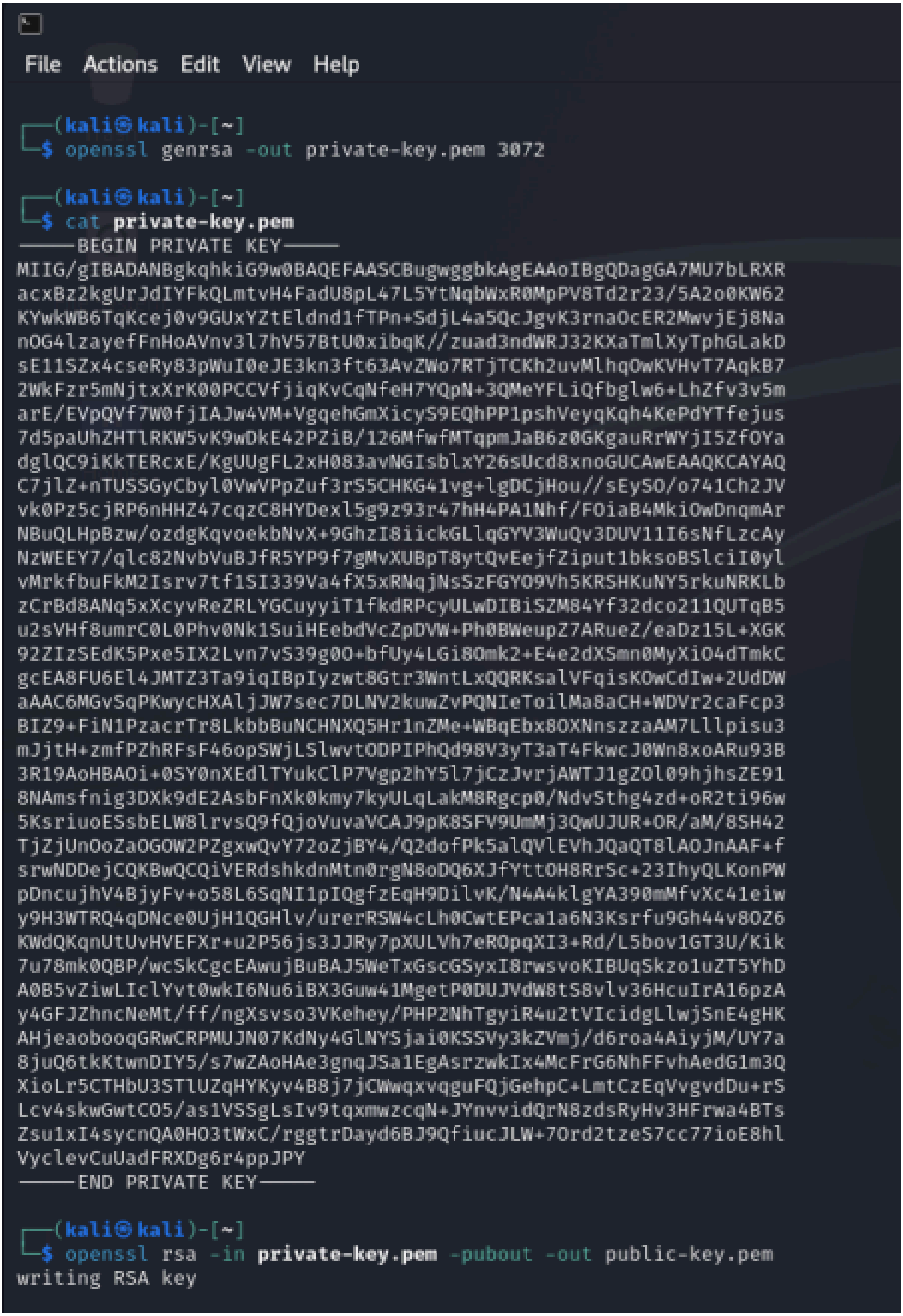
Tasks:

1. Encrypt and decrypt a message using AES with a shared key.
2. Generate RSA keys using OpenSSL.
3. Encrypt a message with the public key and decrypt with the private key.
4. Observe and compare encryption/decryption outputs.

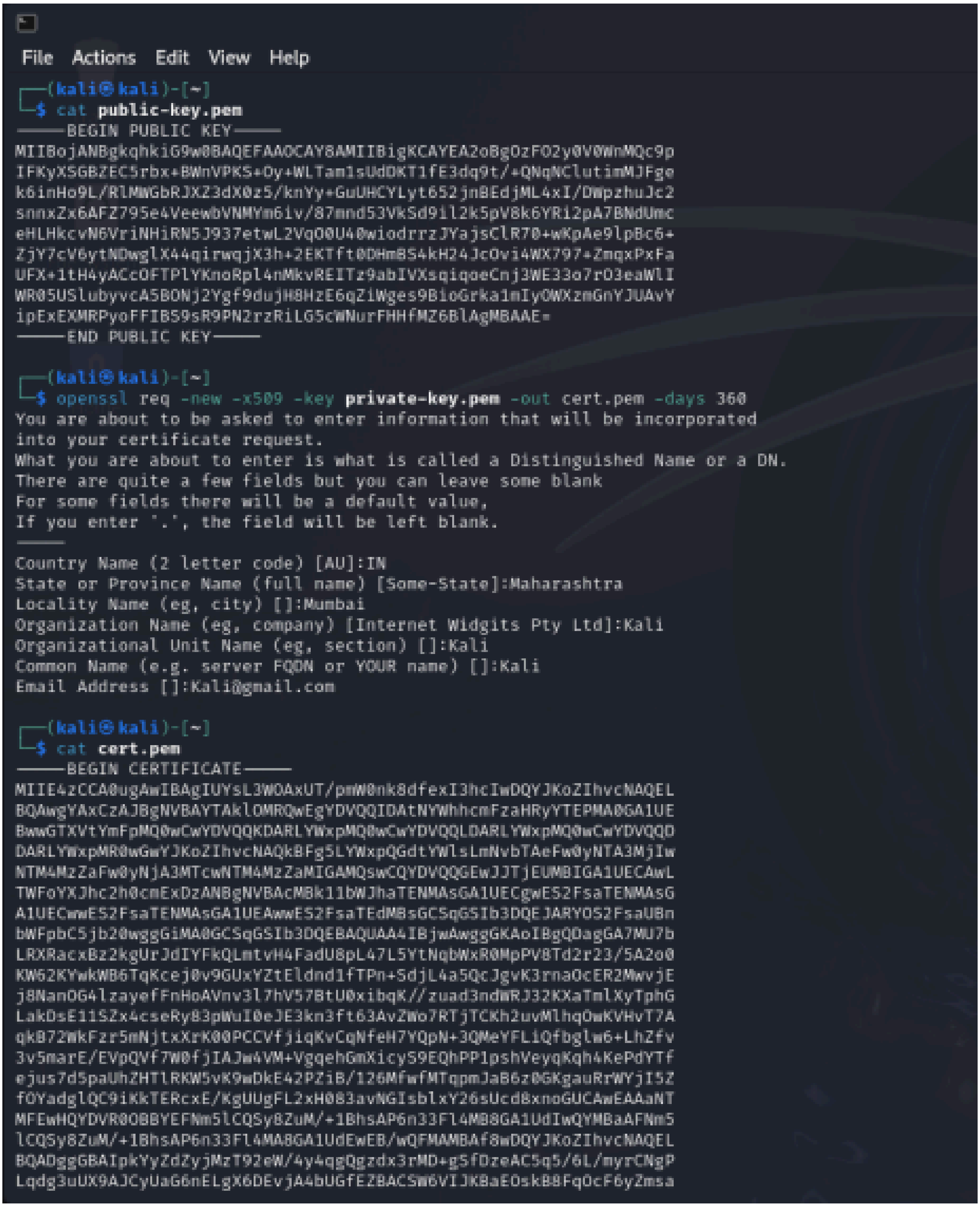
2.6 Output Screenshots:



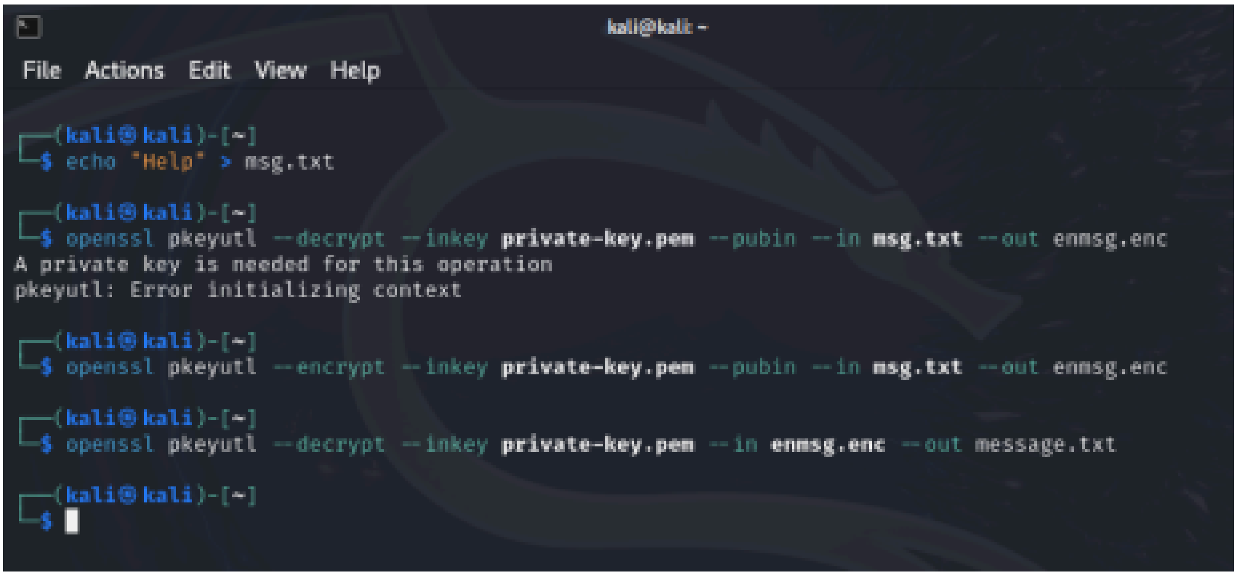
```
┌──(kali㉿kali)-[~]
└─$ openssl enc -aes-256-cbc -in mytext.txt -out mydecrypttext.enc
enter AES-256-CBC encryption password:
Verifying - enter AES-256-CBC encryption password:
*** WARNING : deprecated key derivation used.
Using -iter or -pbkdf2 would be better.

┌──(kali㉿kali)-[~]
└─$ openssl enc -d  -aes-256-cbc -in mydecrypttext.enc -out mydecryptedtext.d
ec
enter AES-256-CBC decryption password:
*** WARNING : deprecated key derivation used.
Using -iter or -pbkdf2 would be better.

┌──(kali㉿kali)-[~]
└─$ cat mydecryptedtext.dec
hello

┌──(kali㉿kali)-[~]
└─$ cat mydecrypttext.enc
Salted__*w*9\34*u**Ã **:*D,m

┌──(kali㉿kali)-[~]
└─$ cat mytext.txt
hello

┌──(kali㉿kali)-[~]
└─$ 
```



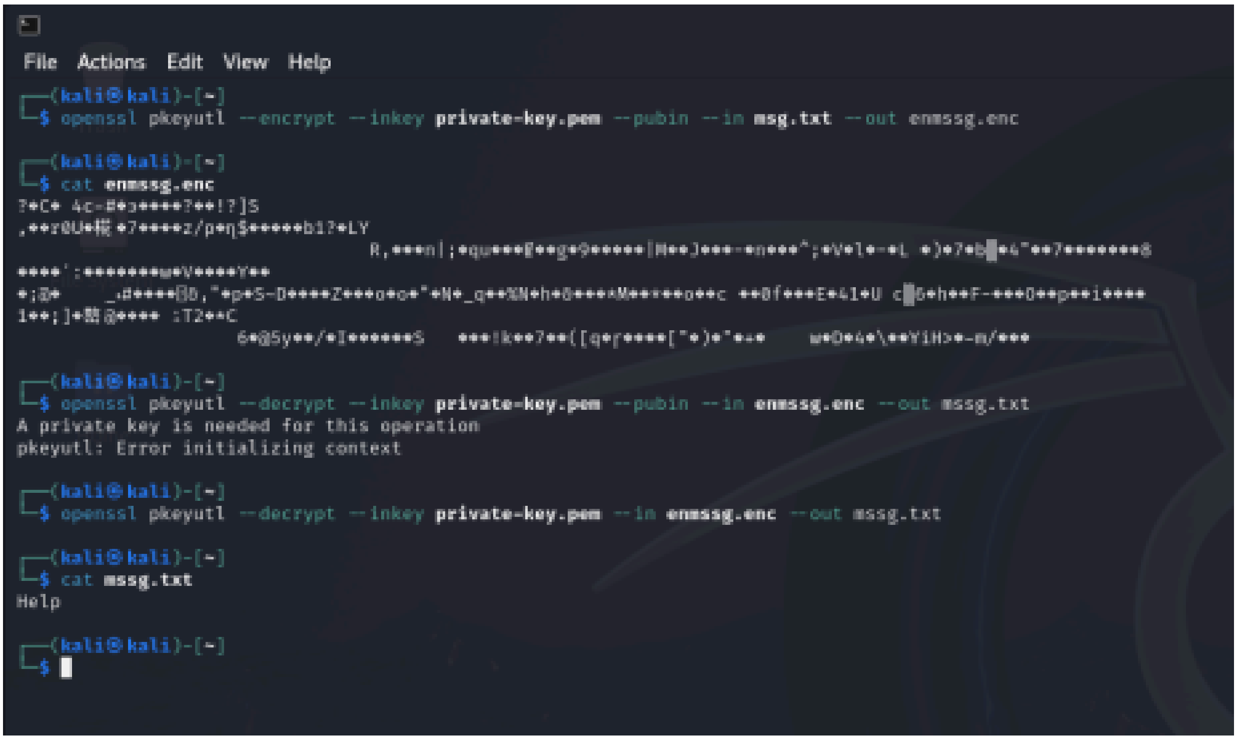
```
┌──(kali㉿kali)-[~]
└─$ openssl genrsa -out private-key.pem 3072

┌──(kali㉿kali)-[~]
└─$ cat private-key.pem
-----BEGIN PRIVATE KEY-----
MIIG/gIBADANBgkqhkiG9w0BAQEFAASCBugwggbkAgEAAoIBgQDagGA7MU7bLRXR
acxBz2kgUrJdIYFkQLmtvH4FadU8pL47L5YtNqbWxR0MpPV8Td2r23/5A2o0KW62
KYwkWB6TqKcej0v9GUxYZtEldnd1fTPn+SdjL4a5QcJgvK3rnaOcER2MwvjEj8Na
nOG4lzayefFnHoAVnv3l7hV57BtU0xibqK//zuad3ndWRJ32KXaTmlXyTphGLakD
sE11SZx4cseRy83pWuI0eJE3kn3ft63AvZWo7RTjTCKh2uvMlhqOwKVHvT7AqkB7
2WkFzr5mNjtxXrK00PCCVfjiqKvCqNfeH7YQpN+3QMeYFLiQfbglw6+LhZfv3v5m
arE/EVpQVf7W0fjIAJw4VM+VgqehGmXicyS9EQhPP1pshVeyqKqh4KePdYTfejus
7d5paUhZHTlRKW5vK9wDkE42PZiB/126MfwfMTqpmJaB6z0GKgauRrWYjI5ZfOYa
dglQC9iKkTERcxE/KgUUgFL2xH083avNGIsblxY26sUcd8xnoGUCAwEAAQKCAYAQ
C7jlZ+nTUSSGyCbyl0VwVPpZuf3rS5CHKG41vg+lgDCjHou//sEySO/o741Ch2JV
vk0Pz5cjRP6nHHZ47cqzC8HYDexl5g9z93r47hH4PA1Nhf/FOiaB4MkiOwDnqmAr
NBuQLHpBzw/ozdgKqvoekbNvX+9GhzI8iickGLlqGYV3WuQv3DUV11I6sNfLzcAy
NzWEEY7/qlc82NvbVuBJfR5YP9f7gMvXUBpT8ytQvEejfZiput1bksoBSlciI0yl
vMrkfbuFkM2Isrv7tf1SI339Va4fX5xRNqjNsSzFGYO9Vh5KRSHKuNY5rkuNRKLb
zCrBd8ANq5xXcyvReZRLYGCuyyiT1fkdRPcyULwDIBiSZM84Yf32dco211QUTqB5
u2sVHf8umrC0L0Phv0Nk1SuiHEebdVcZpDVW+Ph0BWeupZ7ARueZ/eaDz15L+XGK
92ZIzSEdK5Pxe5IX2Lvn7vS39g0O+bfUy4LGi8Omk2+E4e2dXSmn0MyXiO4dTmkC
gcEA8FU6El4JMTZ3Ta9iqIBpIyzwt8Gtr3WntLxQQRKsalVFqisKOwCdIw+2UdDW
aAAC6MGvSqPKwycHXAljJW7sec7DLNV2kuwZvPQNIeToilMa8aCH+WDVr2caFcp3
BIZ9+FiN1PzacrTr8LkbbBuNCHNXQ5Hr1nZMe+WBqEbx8OXNnszzaAM7Lllpisu3
mJjtH+zmfPZhRFsF46opSWjLSlwvtODPIPhQd98V3yT3aT4FkwcJ0Wn8xoARu93B
3R19AoHBAOi+0SY0nXEdlTYukClP7Vgp2hY5l7jCzJvrjAWTJ1gZOl09hjhsZE91
8NAmsfnig3DXk9dE2AsbFnXk0kmy7kyULqLakM8Rgcp0/NdvSthg4zd+oR2ti96w
5KsriuoESsbELW8lrvsQ9fQjoVuvaVCAJ9pK8SFV9UmMj3QwUJUR+OR/aM/8SH42
TjZjUnOoZaOGOW2PZgxwQvY72oZjBY4/Q2dofPk5alQVlEVhJQaQT8lAOJnAAF+f
srwNDDejCQKBwQCQiVERdshkdnMtn0rgN8oDQ6XJfYttOH8RrSc+23IhyQLKonPW
pDncujhV4BjyFv+o58L6SqNI1pIQgfzEqH9DilvK/N4A4klgYA390mMfvXc41eiw
y9H3WTRQ4qDNce0UjH1QGHlv/urerRSW4cLh0CwtEPca1a6N3Ksrfu9Gh44v8OZ6
KWdQKqnUtUvHVEFXr+u2P56js3JJRy7pXULVh7eROpqXI3+Rd/L5bov1GT3U/Kik
7u78mk0QBP/wcSkCgcEAwujBuBAJ5WeTxGscGSyxI8rwsvoKIBUqSkzo1uZT5YhD
A0B5vZiwLIclYvt0wkI6Nu6iBX3Guw41MgetP0DUJVdW8tS8vlv36HcuIrA16pzA
y4GFJZhncNeMt/ff/ngXsvso3VKehey/PHP2NhTgyiR4u2tVIcidgLlwjSnE4gHK
AHjeaobooqGRwCRPMUJN07KdNy4GlNYSjai0KSSVy3kZVmj/d6roa4AiyjM/UY7a
8juQ6tkKtwnDIY5/s7wZAoHAe3gnqJSa1EgAsrzwkIx4McFrG6NhFFvhAedG1m3Q
XioLr5CTHbU3STlUZqHYKyv4B8j7jCWwqxvqguFQjGehpC+LmtCzEqVvgvdDu+rS
Lcv4skwGwtCO5/as1VSSgLsIv9tqxmwzcqN+JYnvvidQrN8zdsRyHv3HFrwa4BTs
Zsu1xI4sycnQA0HO3tWxC/rggtrDayd6BJ9QfiucJLW+7Ord2tzeS7cc77ioE8hl
VyclevCuUadFRXDg6r4ppJPY
-----END PRIVATE KEY-----

┌──(kali㉿kali)-[~]
└─$ openssl rsa -in private-key.pem -pubout -out public-key.pem
writing RSA key
```



```
┌──(kali㉿kali)-[~]
└─$ cat public-key.pem
-----BEGIN PUBLIC KEY-----
MIIBojANBgkqhkiG9w0BAQEFAAOCAY8AMIIBigKCAYEA2oBgOzFO2y0V0WnMQc9p
IFKyXSGBZEC5rbx+BWnVPKS+Oy+WLTam1sUdDKT1fE3dq9t/+QNqNClutimMJFge
k6inHo9L/RlMWGbRJXZ3dX0z5/knYy+GuUHCYLyt652jnBEdjML4xI/DWpzhuJc2
snnxZx6AFZ795e4VeewbVNMYm6iv/87mnd53VkSd9il2k5pV8k6YRi2pA7BNdUmc
eHLHkcvN6VriNHiRN5J937etwL2VqO0U40wiodrrzJYajsClR70+wKpAe9lpBc6+
ZjY7cV6ytNDwglX44qirwqjX3h+2EKTft0DHmBS4kH24JcOvi4WX797+ZmqxPxFa
UFX+1tH4yACcOFTPlYKnoRpl4nMkvREITz9abIVXsqiqoeCnj3WE33o7rO3eaWlI
WR05USlubyvcA5BONj2Ygf9dujH8HzE6qZiWges9BioGrka1mIyOWXzmGnYJUAvY
ipExEXMRPyoFFIBS9sR9PN2rzRiLG5cWNurFHHfMZ6BlAgMBAAE=
-----END PUBLIC KEY-----

┌──(kali㉿kali)-[~]
└─$ openssl req -new -x509 -key private-key.pem -out cert.pem -days 360
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]:Maharashtra
Locality Name (eg, city) []:Mumbai
Organization Name (eg, company) [Internet Widgits Pty Ltd]:Kali
Organizational Unit Name (eg, section) []:Kali
Common Name (e.g. server FQDN or YOUR name) []:Kali
Email Address []:Kali@gmail.com

┌──(kali㉿kali)-[~]
└─$ cat cert.pem
-----BEGIN CERTIFICATE-----
MIIE4zCCA0ugAwIBAgIUYsL3WOAxUT/pmW0nk8dfexI3hcIwDQYJKoZIhvcNAQEL
BQAwgYAxCzAJBgNVBAYTAklOMRQwEgYDVQQIDAtNYWhhcmFzaHRyYTEPMA0GA1UE
BwwGTXVtYmFpMQ0wCwYDVQQKDARLYWxpMQ0wCwYDVQQLDARLYWxpMQ0wCwYDVQQD
DARLYWxpMR0wGwYJKoZIhvcNAQkBFg5LYWxpQGdtYWlsLmNvbTAeFw0yNTA3MjIw
NTM4MzZaFw0yNjA3MTcwNTM4MzZaMIGAMQswCQYDVQQGEwJJTjEUMBIGA1UECAwL
TWFoYXJhc2h0cmExDzANBgNVBAcMBk11bWJhaTENMAsGA1UECgwES2FsaTENMAsG
A1UECwwES2FsaTENMAsGA1UEAwwES2FsaTEdMBsGCSqGSIb3DQEJARYOS2FsaUBn
bWFpbC5jb20wggGiMA0GCSqGSIb3DQEBAQUAA4IBjwAwggGKAoIBgQDagGA7MU7b
LRXRacxBz2kgUrJdIYFkQLmtvH4FadU8pL47L5YtNqbWxR0MpPV8Td2r23/5A2o0
KW62KYwkWB6TqKcej0v9GUxYZtEldnd1fTPn+SdjL4a5QcJgvK3rnaOcER2MwvjE
j8NanOG4lzayefFnHoAVnv3l7hV57BtU0xibqK//zuad3ndWRJ32KXaTmlXyTphG
LakDsE11SZx4cseRy83pWuI0eJE3kn3ft63AvZWo7RTjTCKh2uvMlhqOwKVHvT7A
qkB72WkFzr5mNjtxXrK00PCCVfjiqKvCqNfeH7YQpN+3QMeYFLiQfbglw6+LhZfv
3v5marE/EVpQVf7W0fjIAJw4VM+VgqehGmXicyS9EQhPP1pshVeyqKqh4KePdYTf
ejus7d5paUhZHTlRKW5vK9wDkE42PZiB/126MfwfMTqpmJaB6z0GKgauRrWYjI5Z
fOYadglQC9iKkTERcxE/KgUUgFL2xH083avNGIsblxY26sUcd8xnoGUCAwEAAaNT
MFEwHQYDVR0OBBYEFNm5lCQSy8ZuM/+1BhsAP6n33Fl4MB8GA1UdIwQYMBaAFNm5
lCQSy8ZuM/+1BhsAP6n33Fl4MA8GA1UdEwEB/wQFMAMBAf8wDQYJKoZIhvcNAQEL
BQADggGBAIpkYyZdZyjMzT92eW/4y4qgQgzdx3rMD+g5fDzeAC5q5/6L/myrCNgP
Lqdg3uUX9AJCyUaG6nELgX6DEvjA4bUGfEZBACSW6VIJKBaEOskB8FqOcF6yZmsa
```



```
┌──(kali㉿kali)-[~]
└─$ echo "Help" > msg.txt

┌──(kali㉿kali)-[~]
└─$ openssl pkeyutl --decrypt --inkey private-key.pem --pubin --in msg.txt --out enmsg.enc
A private key is needed for this operation
pkeyutl: Error initializing context

┌──(kali㉿kali)-[~]
└─$ openssl pkeyutl --encrypt --inkey private-key.pem --pubin --in msg.txt --out enmsg.enc

┌──(kali㉿kali)-[~]
└─$ openssl pkeyutl --decrypt --inkey private-key.pem --in enmsg.enc --out message.txt

┌──(kali㉿kali)-[~]
└─$ █
```



```
┌──(kali㉿kali)-[~]
└─$ openssl pkeyutl --encrypt --inkey private-key.pem --pubin --in msg.txt --out enmssg.enc

┌──(kali㉿kali)-[~]
└─$ cat enmssg.enc
?*C* 4c-#*ɜ****?**!?]S
,**r@U*桜 *7****z/p*η$*****b1?*LY
                              R,***n|;*qu***@**g*9*****|M**J***-*n***^;*V*l*-*L *)*7*b█*4"**7*******8
****';*******w*V****Y**
*;@*    _.d****⑪b,"*p*S-D****Z***o*o*"*N*_q**%N*h*8****M*****o**c **0f***E*41*U c█6*h**F-***0**p**i****
1**;]*慰@**** :T2**C
                   6*@5y**/*I******S   ***!k**7**([q*ɼ****["*)*"*-*    w*D*4*\**YiH>*-m/***

┌──(kali㉿kali)-[~]
└─$ openssl pkeyutl --decrypt --inkey private-key.pem --pubin --in enmssg.enc --out mssg.txt
A private key is needed for this operation
pkeyutl: Error initializing context

┌──(kali㉿kali)-[~]
└─$ openssl pkeyutl --decrypt --inkey private-key.pem --in enmssg.enc --out mssg.txt

┌──(kali㉿kali)-[~]
└─$ cat mssg.txt
Help

┌──(kali㉿kali)-[~]
└─$ █
```

2.7 Conclusion:

In this experiment, we applied AES & RSA encryption & decryption techniques. By applying this, we understood the differences between Symmetric & Asymmetric decryption techniques.