## Experiment-2

## Cryptanalysis of RSA

**Date:** 31/7/25

### AIM

Implementation of Cryptanalysis using RSA.

### PROCEDURE

**Step-1:** Install VMWare and host Kali Linux.

**Step-2:** Login to Kali Linux and open Terminal and run commands.

**Step-3:** Use Hexadecimal to decimal convertor.

**Step-4:** Use factordb.com to find the factors for the decimal value.

**Step-5:** Write an exploit in python and get the plain text.

### SOURCECODE

```
$mkdir rsa
$ cd rsa
$ ls
$cat enc.txt
$ cat Pubkey.Pem
->To generate Public Key
$openssl rsa -Pubin -inform PEM -text -noout <PubKey.Pem
```

->Copy the hexadecimal Code into a notepad as n value. As it is a hexadecimal we can convert it into decimal for gaining the Plain text.

->Hexadecimal to decimal Convertor.

->click on Convert and Convert the hexadecimal to decimal.

->Now Copy the decimal value and Paste in the notepad as n value.

->we need to factorize n.

->So go to website factordb.com click Search, Paste decimal value of n. and click on factorize. we get the value.

->Create a exploit.py

->To install Pycrypto

pip install pycryptodome

->Copy the Code in the exploit.py file and Paste it

n=1881988129206079638697239461650439807
1635633794173827007633564229888599152

e=65537.

P=398075086424064937397125505508649119 90
6436234252670840685189575946388957261

q=4727721461074353025302536223671973048 22
4632914695302971146459852171130520711.

```
phi_n = (P-1)*(q-1)
d=inverse (e,Phi_n)
Key=RSA.Construct ((n,e,d,P,q))
fn = "Private.Pem"
with open (fn,"wb")as f:
    f.write(Key.exPortKey()
        )
```

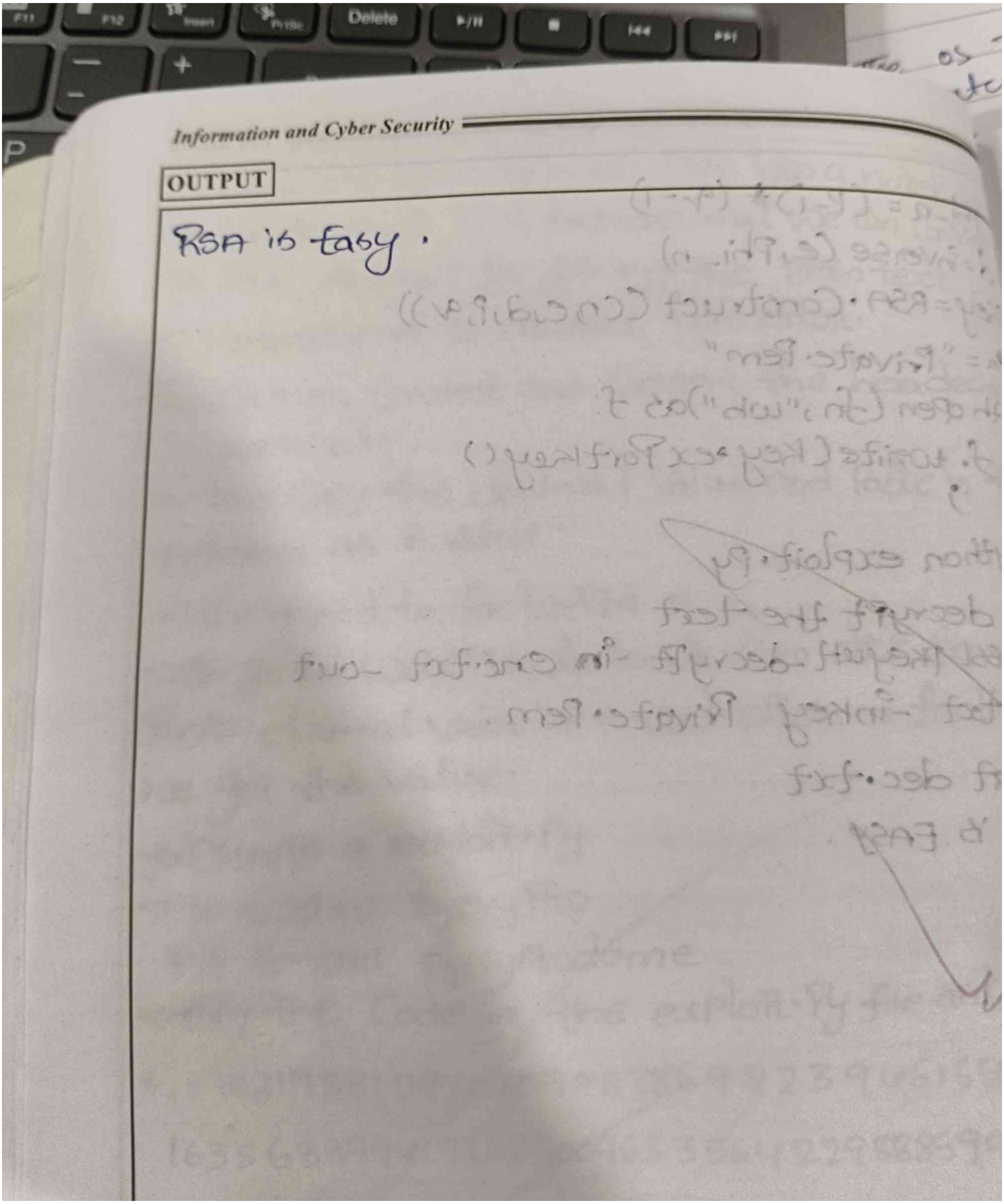
-> Python exploit.Py

-> To decrypt the text

```
openssl pkeyutl -decrypt -in enc.txt -out
dec.txt -inkey Private.Pem.
```

-> $cat dec.txt

RSA is EASY.



OUTPUT

RSA is Easy .