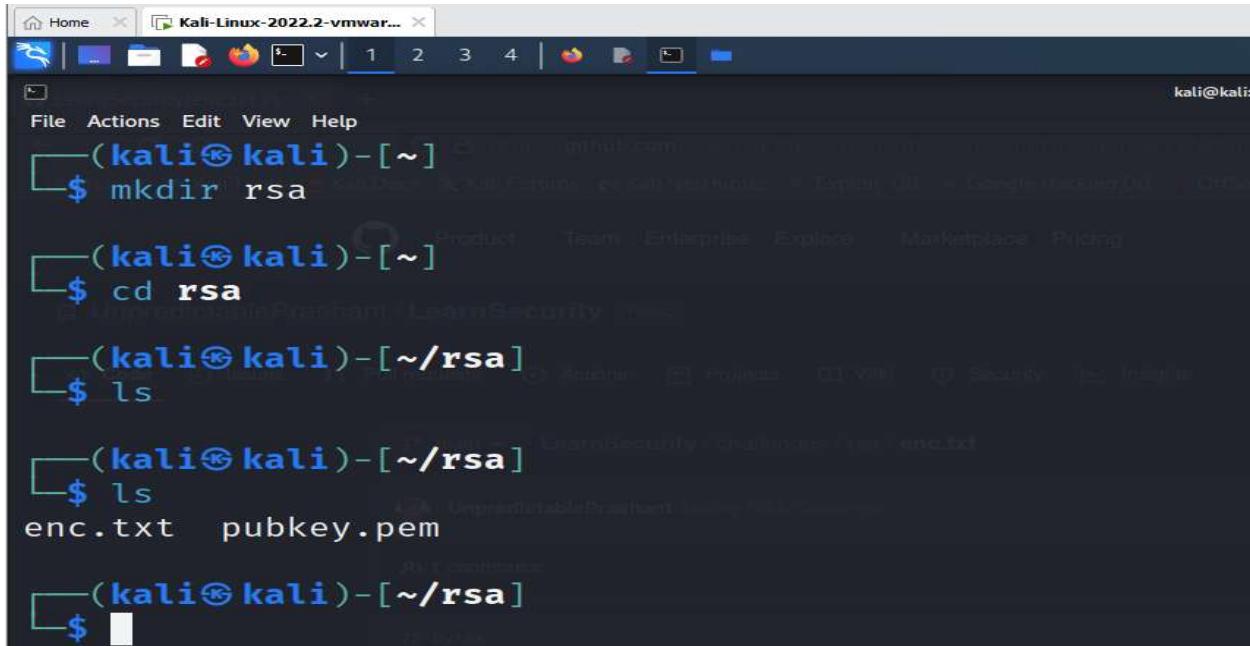
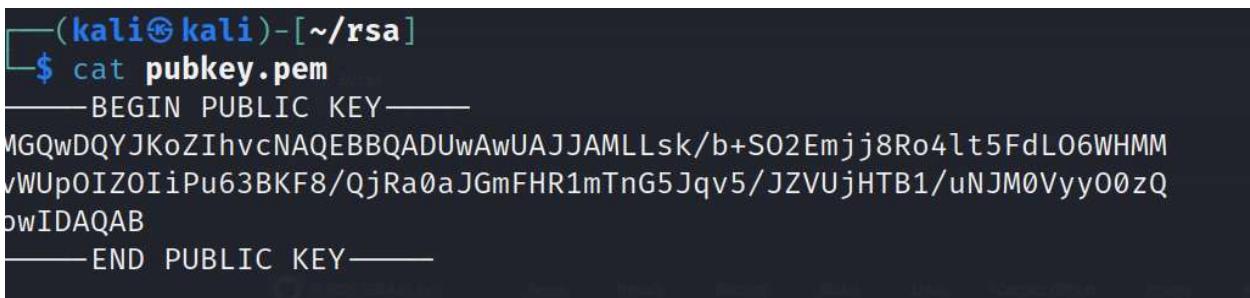


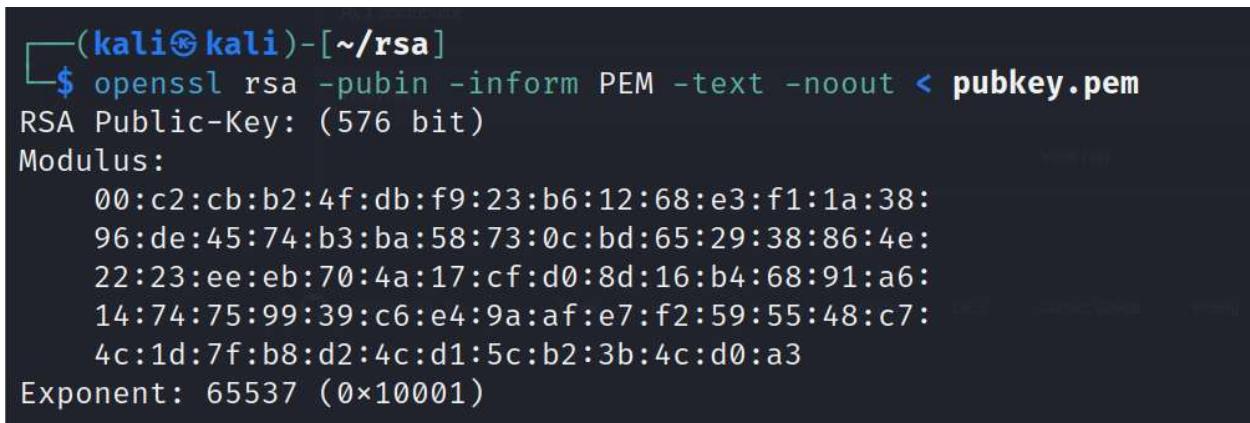
Experiment 2: Implementation of Cryptanalysis using RSA.



```
(kali㉿kali)-[ ~ ]
$ mkdir rsa
(kali㉿kali)-[ ~ ]
$ cd rsa
(kali㉿kali)-[~/rsa]
$ ls
enc.txt  pubkey.pem
(kali㉿kali)-[~/rsa]
$
```



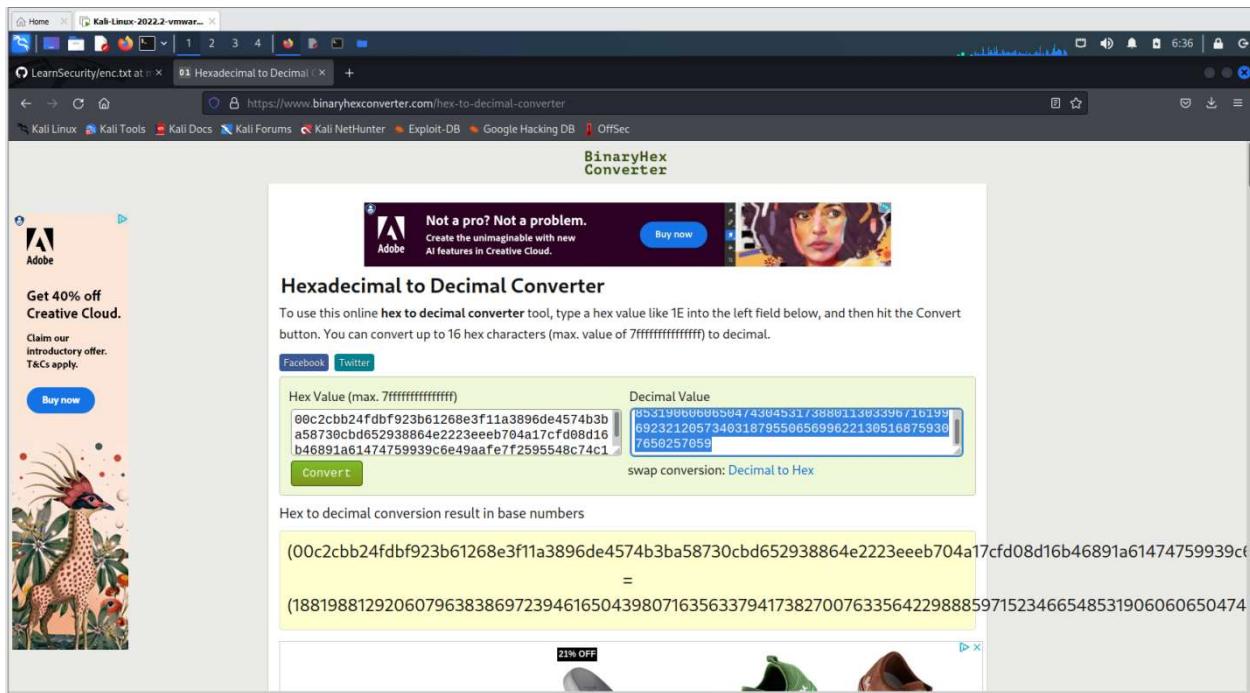
```
(kali㉿kali)-[~/rsa]
$ cat pubkey.pem
-----BEGIN PUBLIC KEY-----
MGQwDQYJKoZIhvcNAQEBBQADUwAwUAJJAMLLsk/b+S02Emjj8Ro4lt5FdL06WHMM
vWUpOIZOIiPu63BKF8/QjRa0aJGmFHR1mTnG5Jqv5/JZVUjHTB1/uNJM0Vyy00zQ
owIDAQAB
-----END PUBLIC KEY-----
```



```
(kali㉿kali)-[~/rsa]
$ openssl rsa -pubin -inform PEM -text -noout < pubkey.pem
RSA Public-Key: (576 bit)
Modulus:
00:c2:cb:b2:4f:db:f9:23:b6:12:68:e3:f1:1a:38:
96:de:45:74:b3:ba:58:73:0c:bd:65:29:38:86:4e:
22:23:ee:eb:70:4a:17:cf:d0:8d:16:b4:68:91:a6:
14:74:75:99:39:c6:e4:9a:af:e7:f2:59:55:48:c7:
4c:1d:7f:b8:d2:4c:d1:5c:b2:3b:4c:d0:a3
Exponent: 65537 (0x10001)
```

Copy the hexadecimal decimal code into a notepad as n value. As it is a hexadecimal we can convert it into decimal for gaining the plaintext.

Hexadecimal to decimal convertor



Paste the decimal code in the **notepad** as n value

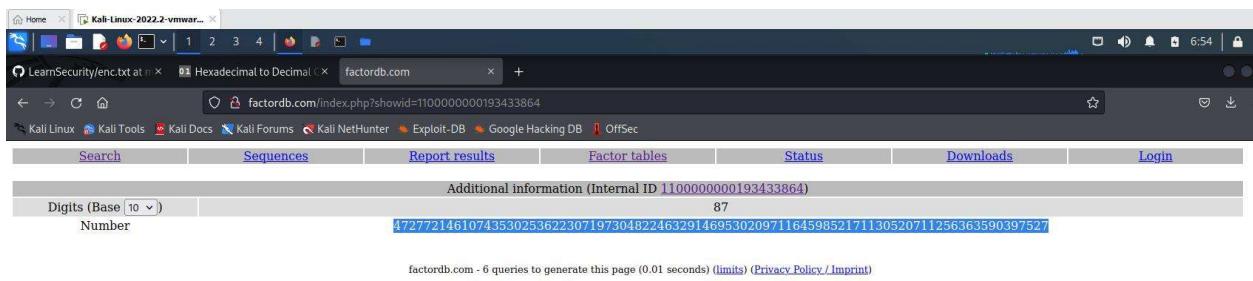
```
n=
00:c2:cb:b2:4f:db:f9:23:b6:12:68:e3:f1:1a:38:96:de:45:74:b3:ba:58:73:0c:bd:65:29:38:86:4e:22:23:ee:eb:70:4a:17:cf:d0:8d:16:b4:68:91:a6:14:74:75:99:39:c6:e4:9a:af:e7:f2:59:55:48:c7:4c:1d:7f:b8:d2:4c:d1:5c:b2:3b:c:d0:a3

n=
1881988129206079638386972394616504398071635633794173827007633564229888597152346654853190606504743045317388011303396716199692321205734031879550656996221305168759307650257059

e=65537
```

Need to factorize n

So go to website **factordb.com** click search, paste decimal value of n



Create a exploit.py

```
(kali㉿kali)-[~/rsa]
$ touch exploit.py
```

To install pycrypto

```
(kali㉿kali)-[~/rsa]
$ pip install pycrypto
Defaulting to user installation because normal site-packages is not writeable
Collecting pycrypto
  Downloading pycrypto-2.6.1.tar.gz (446 kB)
    446.2/446.2 KB 6.3 MB/s eta 0:00:00
  Preparing metadata (setup.py) ... done
  Building wheels for collected packages: pycrypto
    Building wheel for pycrypto (setup.py) ... done
      Created wheel for pycrypto: filename=pycrypto-2.6.1-cp310-cp310-linux_x86_64.whl size=525978 sha256=3b7c400979f80da91a88d5da8d1f62a06583ac503db06fd8bc0a99f9fff08ba0
      Stored in directory: /home/kali/.cache/pip/wheels/e8/4b/5b/b10a6fc885057b6ff9fb5691d7e700d0a9408f80b7e6f12e0
  Successfully built pycrypto
  Installing collected packages: pycrypto
  Successfully installed pycrypto-2.6.1
```