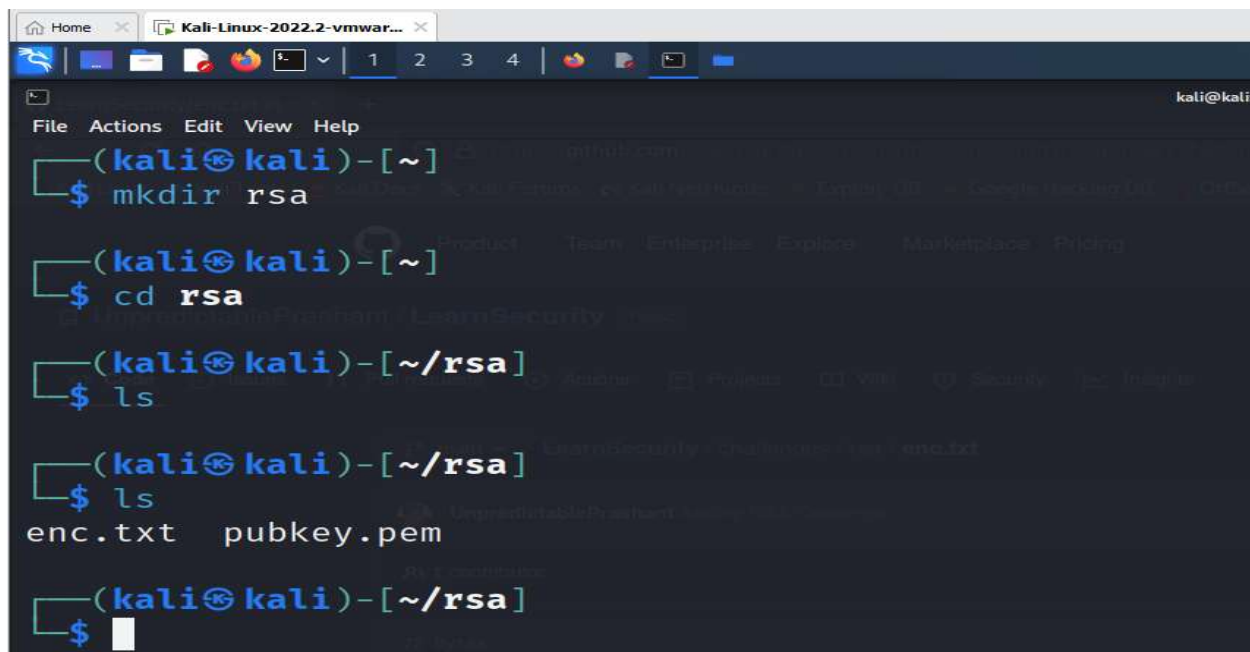


Experiment 2: Implementation of Cryptanalysis using RSA.

```
(kali㉿kali)-[~]
$ mkdir rsa

(kali㉿kali)-[~]
$ cd rsa

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

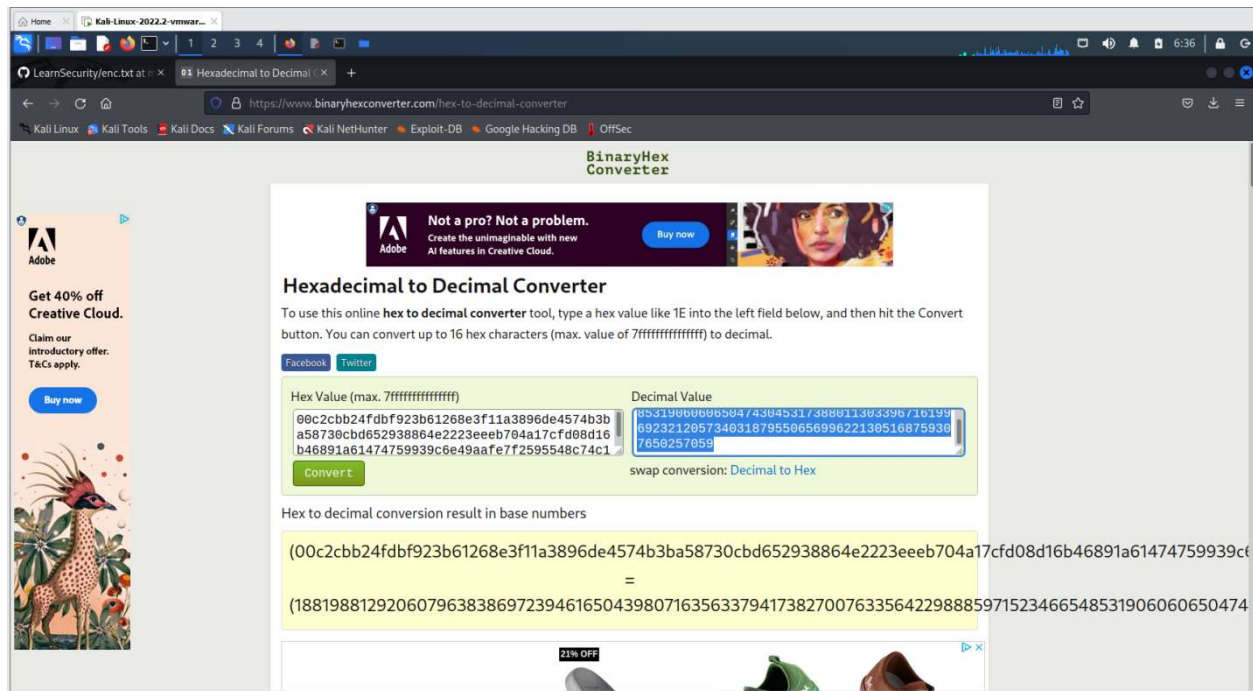
(kali㉿kali)-[~/rsa]
$
```

```
(kali㉿kali)-[~/rsa]
$ cat pubkey.pem
-----BEGIN PUBLIC KEY-----
MGQwDQYJKoZIhvcNAQEBBQADUwAwUAAJAMLLSk/b+SO2Emjj8Ro4lt5FdLO6WHMM
vWUpOIZOIiPu63BKF8/QjRa0aJGmFHR1mTnG5Jqv5/JZVUjHTB1/uNJM0Vyy00zQ
bwIDAQAB
-----END PUBLIC KEY-----
```

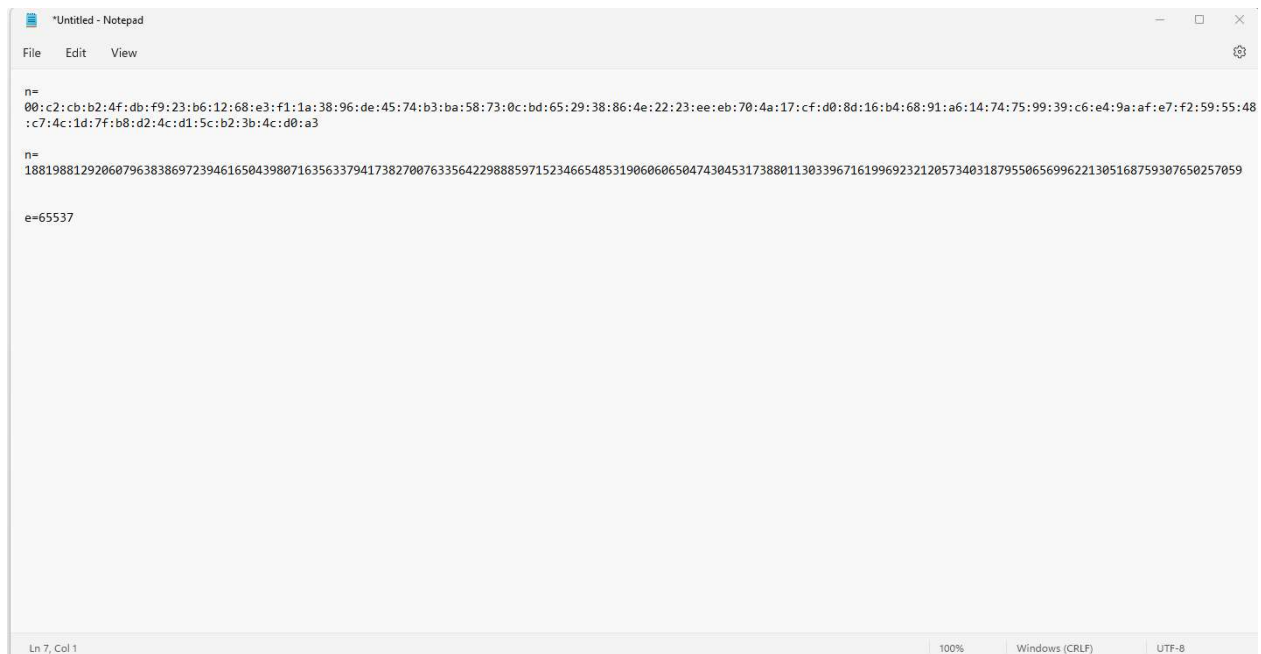
```
(kali㉿kali)-[~/rsa]
$ openssl rsa -pubin -inform PEM -text -noout < pubkey.pem
RSA Public-Key: (576 bit)
Modulus:
  00:c2:cb:b2:4f:db:f9:23:b6:12:68:e3:f1:1a:38:
  96:de:45:74:b3:ba:58:73:0c:bd:65:29:38:86:4e:
  22:23:ee:eb:70:4a:17:cf:d0:8d:16:b4:68:91:a6:
  14:74:75:99:39:c6:e4:9a:af:e7:f2:59:55:48:c7: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

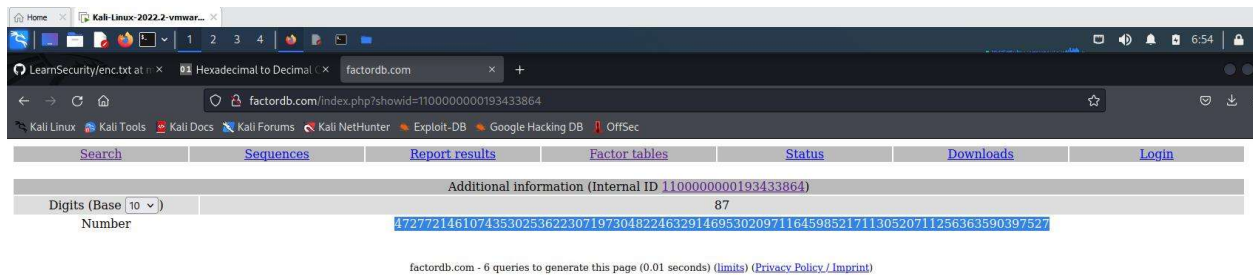


Paste the decimal code in the **notepad** as n value



Need to factorize n

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



Create a exploit.py



To install pycrypto

