Name:-Yerram Setty Gowri Anvesh
discord_id:-anvesh_potterhead
Branch: S2-CYS

WRITEUP-WEEK-2

p 3

Task 3 - Crypto Hack

ENCODING

ASCII:

[99, 114, 121, 112, 116, 111, 123, 65, 83, 67, 73, 73, 95, 112, 114, 49, 110, 116, 52, 98, 108, 51, 125]

the above string is given to me and i need to convert them to thier respective ascii values for that i used chr() in python to convert i written a small python code as shown below it given me password

---

```
arr=[99, 114, 121, 112, 116, 111, 123, 65, 83, 67, 73, 73, 95, 112, 114, 49, 110, 116, 52, 98, 108, 51, 125]
tmp=""
for i in range (0,len(arr)):
        tmp=tmp+chr(arr[i])
print(tmp)
```

The flag i found crypto{ASCII_pr1nt4bl3}

HEX:

63727970746f7b596f755f77696c6c5f62655f776f726b696e675f776974685f6865785f737472696e67735f615f6c6f747d

the above thing is given to me and i need to convert them to bytes to get by the ascii text so i used bytes.fromhex() function to get back the string.

```
h="63727970746f7b596f755f77696c6c5f62655f776f726b696e675f776974685f6865785f737472696e67735f615f6c6f747d"
print(bytes.fromhex(h))
```

The flag i found crypto{You_will_be_working_with_hex_strings_a_lot}

Name:-Yerram Setty Gowri Anvesh
discord_id:-anvesh_potterhead
Branch: S2-CYS

BASE64:

72bca9b68fc16ac7beeb8f849dca1d8a783e8acf9679bf9269f7bf
the above thing is given to me and i need to convert them to bytes from hex and encode them using base64 module using `base64.b64encode()` function
Now we will get the ascii text.so i created the following python code
---
```
import base64
bs="72bca9b68fc16ac7beeb8f849dca1d8a783e8acf9679bf9269f7bf"
he=bytes.fromhex(bs)
hex2=base64.b64encode(he)
print(hex2)
```

The flag i found **crypto/Base+64+Encoding+is+Web+Safe/**

Bytes and Big Integers:

11515195063862318899931685488813747395775516287289682636499965282714637259206269
`from Crypto.Util.number import *`
This time it we need to convert long to bytes so i used
from Crypto.Util.number import *
so i used long_to_bytes() to change it to ascii

```
from Crypto.Util.number import *
x=11515195063862318899931685488813747395775516287289682636499965282714637259206269
y=long_to_bytes(x)
print(y)
```

The flag i found **crypto{3nc0d1n6_4ll_7h3_w4y_d0wn}**

FINAL CHALLENGE:

This time they given to python codes and make a automation code by using them both which can decode upto 100 codes so i used both of them by copying one side to another side and also of error rectification some

Name:-Yerram Setty Gowri Anvesh
discord_id:-anvesh_potterhead
Branch: S2-CYS

google things i finally built a python code shown below which can be able to decode 100 encoded things but this at finally given me flag

----

```
from pwn import *
import json
from Crypto.Util.number import bytes_to_long, long_to_bytes
import base64
import codecs
import random
from binascii import unhexlify


r = remote('socket.cryptohack.org', 13377, level = 'debug')

def json_recv():
    line = r.recvline()
    return json.loads(line.decode())

def json_send(hsh):
    request = json.dumps(hsh).encode()
    r.sendline(request)

def list_to_string(s):
    output = ""
    return(output.join(s))

for i in range(0,101):
    received = json_recv()
    if "flag" in received:
        print("\n[*] FLAG: {}".format(received["flag"]))
        break

    print("\n[-] Cycle: {}".format(i))
    print("[-] Received type: {}".format(received["type"]))
    print("[-] Received encoded value: {}".format(received["encoded"]))

    word = received["encoded"]
    encoding = received["type"]

    if encoding == "base64":
        decoded = base64.b64decode(word).decode('utf8').replace("""", "")
    elif encoding == "hex":
        decoded = (unhexlify(word)).decode('utf8').replace("""", "")
    elif encoding == "rot13":
        decoded = codecs.decode(word, 'rot_13')
    elif encoding == "bigint":
        decoded = unhexlify(word.replace("0x", "")).decode('utf8').replace("""", "")
    elif encoding == "utf-8":
        decoded = list_to_string([chr(b) for b in word])

    print("[-] Decoded: {}".format(decoded))
    print("[-] Decoded Type: {}".format(type(decoded)))

    to_send = {
        "decoded": decoded
    }

    json_send(to_send)
```

The flag i found **crypto{3nc0d3_d3c0d3_3nc0d3}**

Name:-Yerram Setty Gowri Anvesh
discord_id:-anvesh_potterhead
Branch: S2-CYS

XOR

XOR STARTER:

Given the string ‘label’ where we need to xor each character and and convert back to strings to get the flag so i created a small python code as shown below which do xor as directed

---

```
str='label'
tmp=""
for i in str:
    tmp2=chr(ord(i)^13)
    tmp=tmp+tmp2
print(tmp)
```

The flag i found crypto{aloha}

XOR PROPERTIES:

Given KEY1 = a6c8b6733c9b22de7bc0253266a3867df55acde8635e19c73313----------->1
KEY2 ^ KEY1 = 37dcb292030faa90d07eec17e3b1c6d8daf94c35d4c9191a5e1e---------->2
KEY2 ^ KEY3 = c1545756687e7573db23aa1c3452a098b71a7fbf0fddddde5fc1---------->3
FLAG^KEY1 ^ KEY3 ^ KEY2 = 04ee9855208a2cd59091d04767ae47963170d1660df7f56f5faf->4

So if we xor 4 and 3 we get
FLAG^KEY1 ^ KEY3 ^ KEY2 ^ KEY2 ^ KEY3 = FLAG^KEY1
then FLAG^KEY1 ^ KEY1= FLAG
But first we need to convert them hexa to binary

```
from pwn import xor
a= 'a6c8b6733c9b22de7bc0253266a3867df55acde8635e19c73313'
ab= '37dcb292030faa90d07eec17e3b1c6d8daf94c35d4c9191a5e1e'
bc= 'c1545756687e7573db23aa1c3452a098b71a7fbf0fddddde5fc1'
fabc = '04ee9855208a2cd59091d04767ae47963170d1660df7f56f5faf'
a=bytes.fromhex(a)
ab=bytes.fromhex(ab)
bc=bytes.fromhex(bc)
fabc=bytes.fromhex(fabc)
print(xor(xor(fabc,bc),a))
```

The flag i found crypto{x0r_i5_ass0c1at1v3}

Name:-Yerram Setty Gowri Anvesh
discord_id:-anvesh_potterhead
Branch: S2-CYS

FAVAOURITE BYTE:

Given 73626960647f6b206821204f21254f7d694f7624662065622127234f726927756d
a hexadecimal code and it was xored with a byte which means 8 bits so i xored with all posibilities of bits then i got the answer

---

```
a=bytes.fromhex('73626960647f6b206821204f21254f7d694f76246620656
22127234f726927756d')
flag=""
for i in range (256):
	result=[chr(n^i) for n in a]
	flag="".join(result)
	if flag.startswith("crypto"):
		print(flag)
		break
```

The flag i found crypto{0x10_15_my_f4v0ur173_by7e}

FAVAOURITE BYTE:

Given 73626960647f6b206821204f21254f7d694f7624662065622127234f726927756d
a hexadecimal code and it was xored with a byte which means 8 bits so i xored with all posibilities of bits then i got the answer

---

```
a=bytes.fromhex('73626960647f6b206821204f21254f7d694f76246620656
22127234f726927756d')
flag=""
for i in range (256):
	result=[chr(n^i) for n in a]
	flag="".join(result)
	if flag.startswith("crypto"):
		print(flag)
		break
```

The flag i found crypto{0x10_15_my_f4v0ur173_by7e}

Name:-Yerram Setty Gowri Anvesh
discord_id:-anvesh_potterhead
Branch: S2-CYS

YOU EITHER KNOW,XOR YOU DON'T KNOW:

Given
0e0b213f26041e480b26217f27342e175d0e070a3c5b103e2526217f27342e175d0e077e263451150104
a hexadecimal code and it was xored by a secret key and we need to find it to decrypt
the idea is
secret key ^ message=crypto{"....
so ,
message ^ crypto{".... = secret key part
so i written a python code

```
---------------------------------------------
from pwn import xor
a=bytes.fromhex('0e0b213f26041e480b26217f27342e175d0e070a3c5b103e2526217f27342e175d0e077e263451150104')
result=xor(a[:7],"crypto{")
print(result)
---------------------------------------------
```

then i got myXORke lets guess that it is myXORkey
and use 'myXORkey' as key and decode it

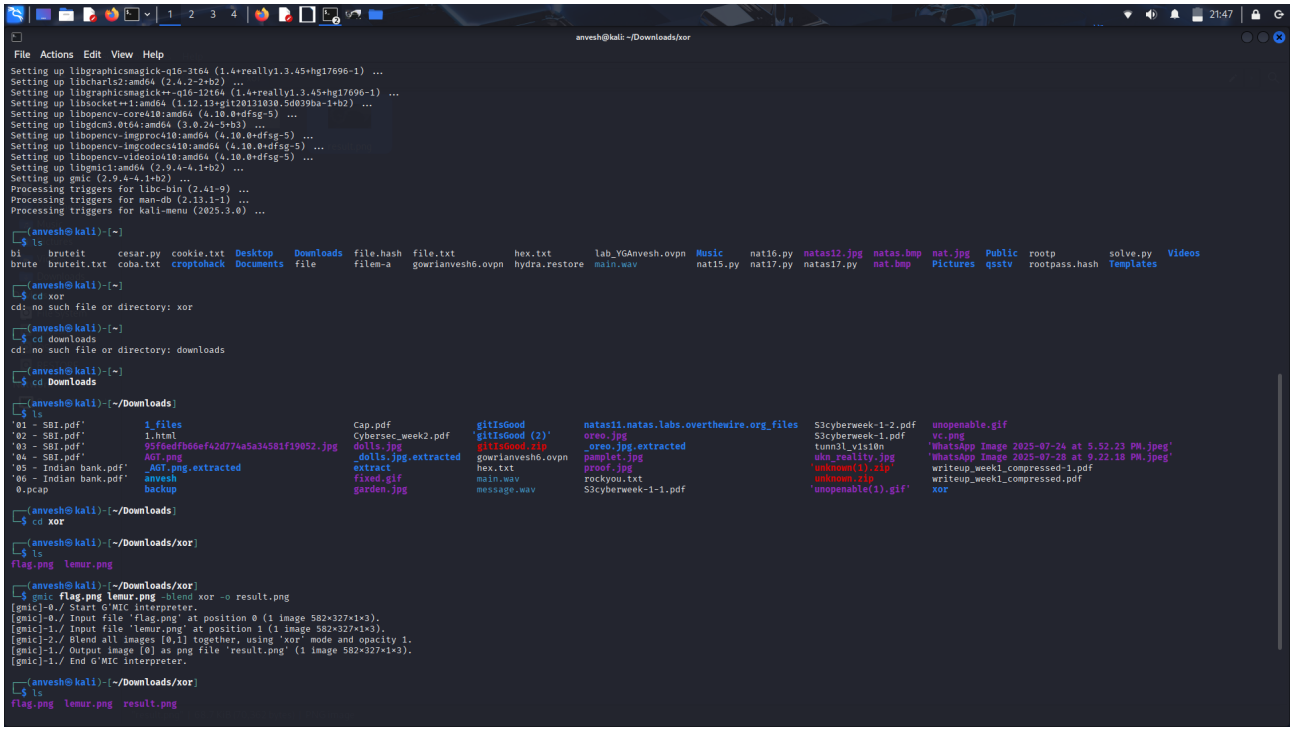
```
---------------------------------------------------
from pwn import xor
a=bytes.fromhex('0e0b213f26041e480b26217f27342e175d0e070a3c5b103e2526217f27342e175d0e077e263451150104')
key='myXORkey'
result=xor(a,key)
print(result)
---------------------------------------------------
```

Then i found flag crypto{1f_y0u_Kn0w_En0uGH_y0u_Kn0w_1t_4ll}

Lemur XOR:

Name:-Yerram Setty Gowri Anvesh
discord_id:-anvesh_potterhead
Branch: S2-CYS

Given 2 png images so i downloaded it. I used a tool called gmic tool which is used to xor 2 images and gives me a new output image so i used the command
gmic flag.png lemur.png -blend xor -o result.png
this will xor the 2 images and give me the output as result.png
---



---

when i did it suddenly i got my friend's photo

Name:-Yerram Setty Gowri Anvesh
discord_id:-anvesh_potterhead
Branch: S2-CYS

The flag i found crypto crypto{x0Rly_n0t!}

WRITEUP-CRYPTO HACK

MATHEMATICS :

1. GCD :

I know gcd well so i created python recursion program which uses euclid's Algorithm to do it to code as follows

```
def gcd(a,b):
        if (a%b==0) :
                return b
        else :
                return gcd(b,a%b)

a=int(input("Enter larger number : "))
b=int(input("Enter smaller number : "))
print(gcd(a,b))
```

Now i got the gcd directly as 1512

2. Extended GCD :

The extended gcd is a bit hard but it took more time to write the proram for it

```
def extengcd(a,b):
        if (b==0) :
                return (a,1,0)
        else :
                g,x1,y1=extengcd(b,a%b)
                x=y1
                y=x1-(a//b)*y1
                return (g,x,y)
```

Name:-Yerram Setty Gowri Anvesh
discord_id:-anvesh_potterhead
Branch: S2-CYS

```
a=int(input("Enter larger number : "))
b=int(input("Enter smaller number : "))
print(extengcd(a,b))
```

Now i got the x and y values as (-8404, 10245)

The smallest one is -8404

3. Modular Arthematic :

Given that,

11≡xmod6

8146798528947≡ymod17

We can easily type 11%6 and 8146798528947 % 17 in python idle then we will get the answer directly

the shortest number is 4

4. Modular Arthematic 2 :

Given that,

the prime p=65537. Calculate 273246787654^(65536) mod65537.

In fermat's little thereom there is a thing like if p is a prime number then any number power p-i mod p is always 1 i.e..,

(SOME NUMBER)^(p-1) mod p =1

so, we can say direct it as 1 or we can also check it in python also

So, verified the answer is 1

Name:-Yerram Setty Gowri Anvesh
discord_id:-anvesh_potterhead
Branch: S2-CYS

5. Modular Inverting :

Given to find inverse of element now i extended the gcd code and gave some restriction for that to find the inverse in python itself

---

```
def gcd(a,b):
        if (a%b==0) :
                return b
        else :
                return gcd(b,a%b)

a=int(input("Enter the a number : "))
b=int(input("Enter the b number : "))

for i in range(1,b):
        if gcd(i,b)==1 :
                if ((i*a)%b==1) :
                        break
print(i)
```

Now i got the answer directly as 9

Name:-Yerram Setty Gowri Anvesh
discord_id:-anvesh_potterhead
Branch: S2-CYS

WRITEUP-CRYPTO HACK

DATA FORMATS :

1. Privacy Enhanced mail stortly pem

It is used for sending keys ,certificats and soon..,

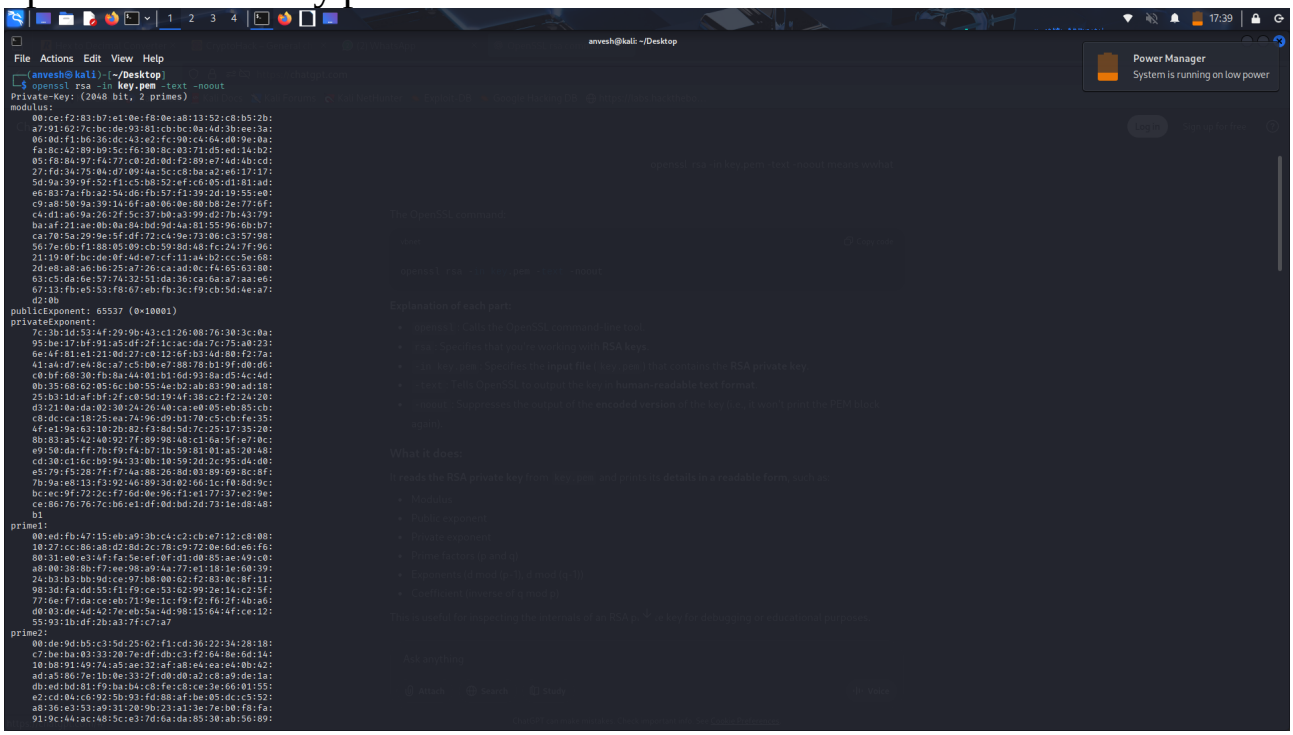
in this challenge they given us a pem file i named it as key.pem and saved it in the desktop

Now i opend the terminal and used the command

>openssl rsa -in key.pem -text -noout

so now i got the public exponent ,private exponent and so on as below..,

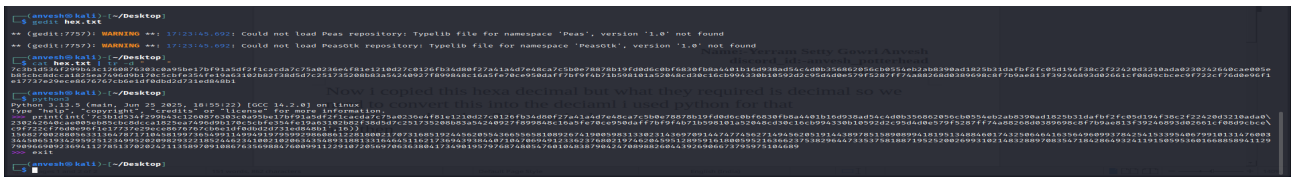
openssl rsa -in key.pem -text -noout



Here at private exponent there is our key but in hexa decimal from with “:” in between so. First we need to remove the “:” for that i used the command

Name:-Yerram Setty Gowri Anvesh
discord_id:-anvesh_potterhead
Branch: S2-CYS

Now i copied this hexa decimal but what they required is decimal so we need to convert this into the deciaml i used python for that
first i opened python3 in terminal
and then
print(int(“THAT HEXA DECIMAL VALUE”,16))

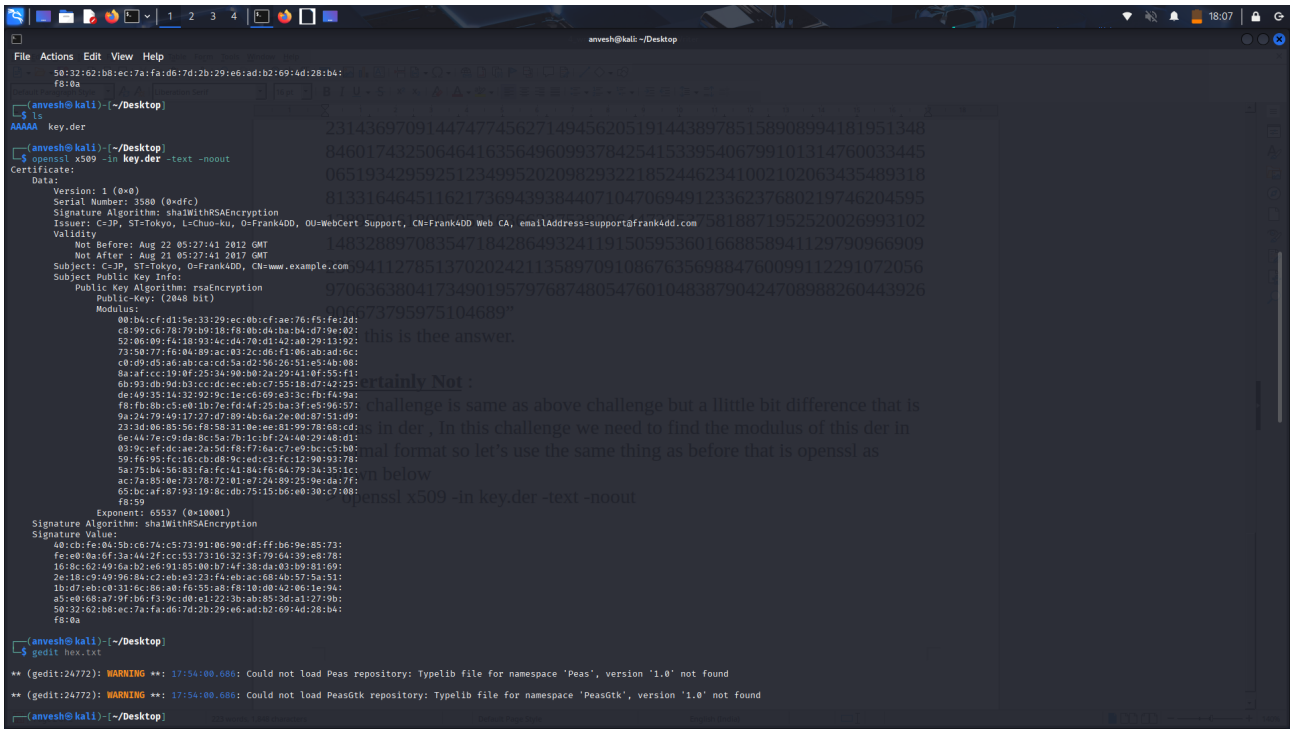


Now i got the decimal value as
“15682700288056331364787171045819973654991149949197959929860
86122818002170731685192445620554366556581089267419005983133 0
23143697091447477456271494562051914438978515890899418195134 8
84601743250646416356496099378425415339540679910131476003344 5
06519342959251234995202098293221852446234100210206343548931 8
81331646451162173694393844071047069491233623768021974620459 5
12895916180059521636623753829644733537581887195252002699310 2
14832889708354718428649324119150595360166885894112979096690 9
23694112785137020242113589709108676356988476009911229107205 6
97063638041734901957976874805476010483879042470898826044392 6
906673795975104689”
and this is thee answer.

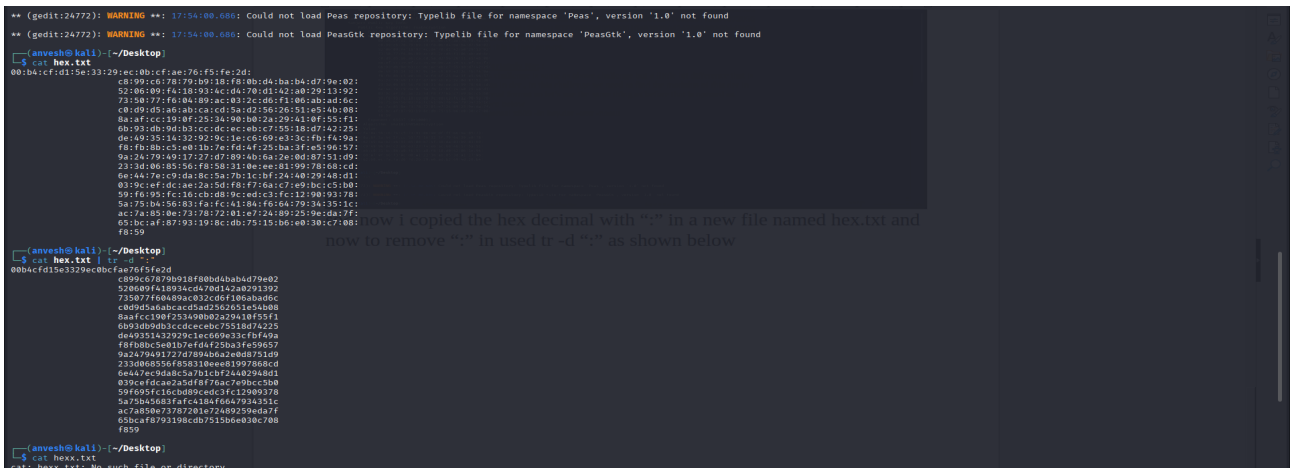
<u>2. Certainly Not</u> :

This challenge is same as above challenge but a llittle bit difference that is it was in der , In this challenge we need to find the modulus of this der in decimal format so let’s use the same thing as before that is openssl as shown below
> openssl x509 -in key.der -text -noout

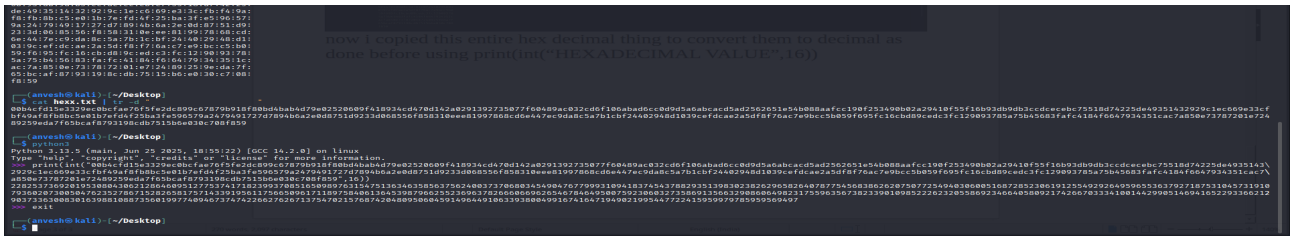
Name:-Yerram Setty Gowri Anvesh
discord_id:-anvesh_potterhead
Branch: S2-CYS



so< now i copied the hex decimal with “:” in a new file named hex.txt and now to remove “:” in used tr -d “:” as shown below



now i copied this entire hex decimal thing to convert them to decimal as done before using print(int(“HEXADECIMAL VALUE”,16))



Name:-Yerram Setty Gowri Anvesh
discord_id:-anvesh_potterhead
Branch: S2-CYS

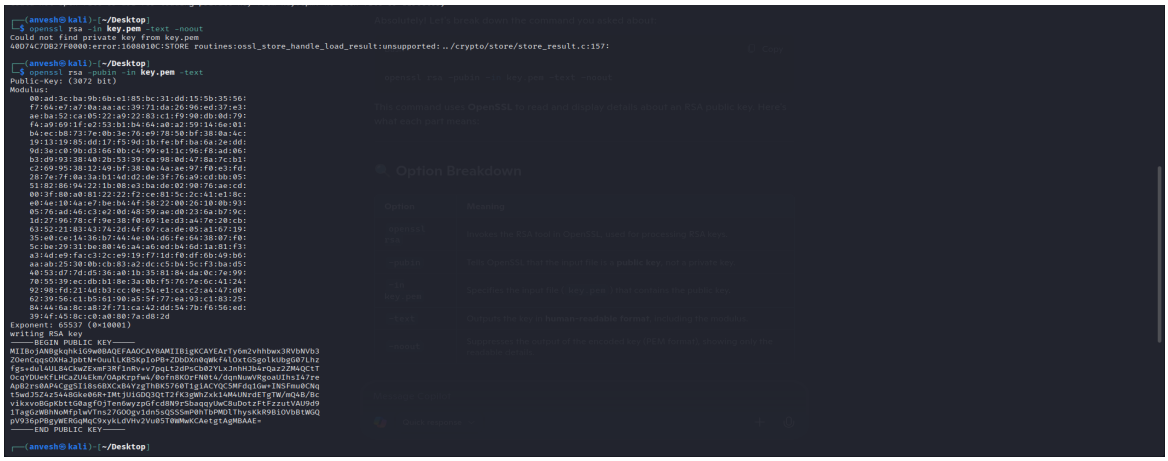
Now i got the decimal value of the modulus as given below and it is correct answer
“22825373692019530804306212864609512775374171823993708516509
89763154751363463585637562400373706803454904767799931094183 7
45437882935139830238262965826407877545683862620750772549403 0
60051687285230619125549292649596553637927187531045731910793 6
02073005047623527867152826581757143391956117566509617118975 8
40613645398796625523696378266606696265467846495007592306032 7
35869135663290860649823175596356738233901098522262320558692 3
46640580921742667033341001442990514694165229336621290373363 0
08301639881088735601997740946737474226627626713754702157687 4
20480950604591496449106339380049916741647194902199544772241 5
9599797859595694 97”

<u>3. Ssh keys</u> :
In this challenge it has ssh public key which is stored in pem FORMAT. So, first we need to change it to pem format for extracting modulus in it. They also given hint to use ssh-keygen to crack it so i am giving the command
>ssh-keygen -f bruce.pub -e -m PEM >key.pem

Name:-Yerram Setty Gowri Anvesh
discord_id:-anvesh_potterhead
Branch: S2-CYS

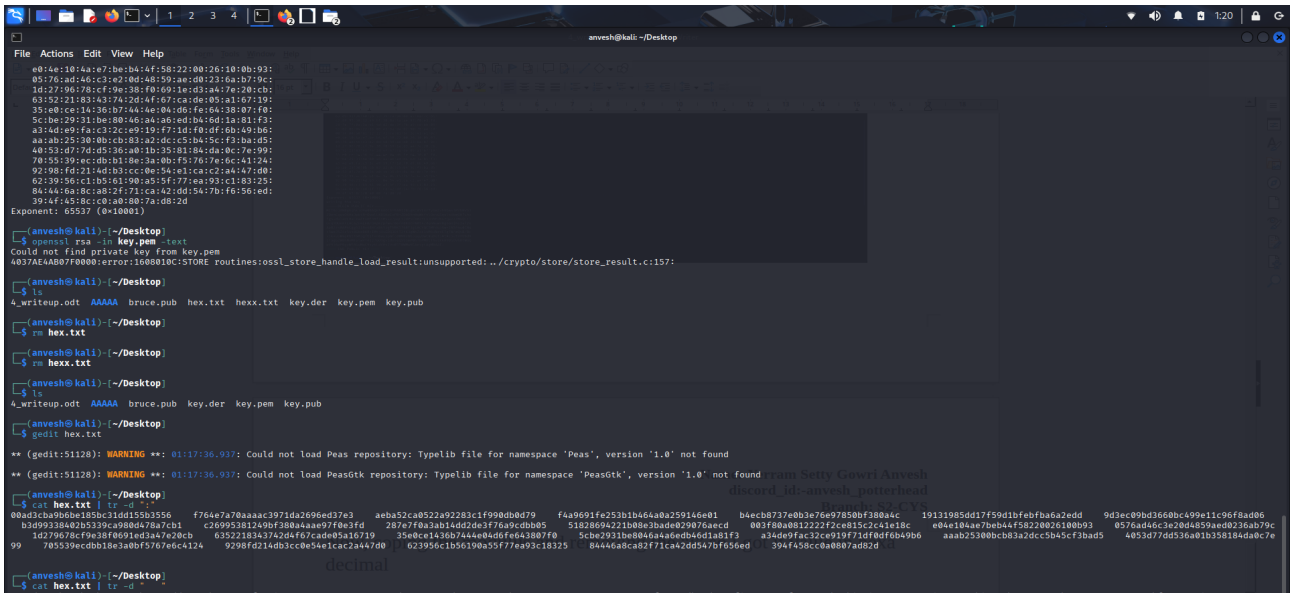
Here -f is for specifing input public file, -e to export the key and -m PEM to set output file to pem

Now i got the key in pem file so, i need to extract the the modulus in pem so i used the command as before
>openssl rsa -pubin -in key.pem -text
here new “one -pubin” is to specify that it is public key no private key

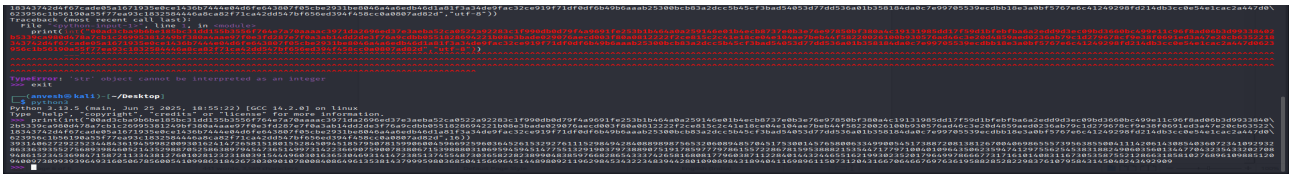


Now, coping the modulus and removing the “:” so i got it value in hexa decimal

Name:-Yerram Setty Gowri Anvesh
discord_id:-anvesh_potterhead
Branch: S2-CYS



Now i got hexadecimal value so i am changing it to decimal value



now i got the decimal value flag
{“39314062729225234484361945998200930162414726581518015528450945185795078159906004596692596036452615329276111529849428408898987565320608948570451753001457658006334990054517388720813812670040698655573956385500411142061430854036072341092932863363935527568939846052143529887052586389794547365149973142236690759007838067153988803106959459451477551329190379738890751917859777978615572286781595388821535447177971004010964350623594741297556254538318824906035601344770432354332027089486152345369847158721133438127601028123231803915444960301636530469314147238513745548730365822823899048385976682865433374265816808177960387112284014432446551621993023520179649978666773171610140831167305358755212866318581027689610988512094009738993939649316050678560054109986318426730309010780084086496135381437999598036850415669645144898092119629845343223483944280109089843189404116989611507312043166706466769763619588285282298376107958431450482434929 09”}