

Proggres LKSN

Malas Pakai gitbook

- [picoCTF](#)
 - [Small Trouble](#)

picoCTF

isinya Crypto doang paling

Small Trouble

Jadi pada chall ini saya mendapatkan 2 attachment

out.txt

n =

```
3344578841910085289721654626262326010845768385227099605558651942081071769793901612508903464039
4296298220690757379654561790697268556429594770027332609276366603251400451939116550640417072245
6559456201660383169415900725662379422172594874316761131126845640036313886686720129726464656561
3548756102494275232075974607911027233443230903715559237552333202783046092774829941983452928495
8948222124250319549904704481592140012436203455174677782600936332645028773127855707707164778918
5104446013969558462273397308379096814269694311980025430266686865648596281167886636442534225514
3542696783776859775321608098576115248892823803330812848566835108023
```

e =

```
1535998946214289952950464225137364655759843718627075274326171999259119238259829945221197856072
6117753508116263642285062560451680747388409497697266748585386489935152626147478188859036194239
5742041774234952714330855780112941058820698988164791716206032077619752319021649837329965078835
6335527880440970881136773456287176391092672985253350317427626933666072099540953179908825812310
3754104938339929721874058227870747658885444687697298475049309721898432468772529864447226120895
1967037496074581672911547261836640699407756586820543947953849758019339133552317763059808992278
7316621165116310355083445633057272514380678453790856930594089043193
```

c =

```
5086880055138641874208402870465642516072182984439060897000932412022198520556281889403734721105
4092217856647404083319057380487124162172358890291271224191448228324258347112077960474004635186
8016509523053434635827665292160043436280116928584863998076246578510569159714741098713097686136
172590134837304417457291638991618062016772592994639092216869901820044613233885837946777740009
9418388782261941911497961896493679487996646915306630597704608478763039887735028467457498653411
0904429641439674643946402617659930041442155326967046914630042645322340556563330008814781111337
571189435901241462737418162532467035047557360943639034638792119126
```

dan

```
from Crypto.Util.number import getPrime, inverse, bytes_to_long
import random

# Generate two large primes (1048 bits each)
```

```

p = getPrime(1048)
q = getPrime(1048)
n = p * q
phi = (p - 1) * (q - 1)

# compute d
d = getPrime(256)

# Compute the public exponent
e = inverse(d, phi)

# Encrypt a flag
flag = b'picoCTF{...}'
m = bytes_to_long(flag)
c = pow(m, e, n)

# Output for the challenge
with open("message.txt", "w") as f:
    f.write(f"n = {n}\n")
    f.write(f"e = {e}\n")
    f.write(f"c = {c}\n")

```

dan dari kode python di atas terutama di `encryption.py`

```

p = getPrime(1048)
q = getPrime(1048)

```

tapi

```

d = getPrime(256)

```

jadi saya bisa simpulkan bahwa d nya itu kecil jadi saya bisa simpulkan juga ini mungkin bisa dilakukan *weiner* attack

maka dari itu saya membuat decrypt seperti ini

```

# pip install owiener
from Crypto.Util.number import long_to_bytes
from owiener import attack

n =
3344578841910085289721654626262326010845768385227099605558651942081071769793901612508903464039
4296298220690757379654561790697268556429594770027332609276366603251400451939116550640417072245

```

```
6559456201660383169415900725662379422172594874316761131126845640036313886686720129726464656561
3548756102494275232075974607911027233443230903715559237552333202783046092774829941983452928495
8948222124250319549904704481592140012436203455174677782600936332645028773127855707707164778918
5104446013969558462273397308379096814269694311980025430266686865648596281167886636442534225514
3542696783776859775321608098576115248892823803330812848566835108023
```

```
e =
```

```
1535998946214289952950464225137364655759843718627075274326171999259119238259829945221197856072
6117753508116263642285062560451680747388409497697266748585386489935152626147478188859036194239
5742041774234952714330855780112941058820698988164791716206032077619752319021649837329965078835
6335527880440970881136773456287176391092672985253350317427626933666072099540953179908825812310
3754104938339929721874058227870747658885444687697298475049309721898432468772529864447226120895
1967037496074581672911547261836640699407756586820543947953849758019339133552317763059808992278
7316621165116310355083445633057272514380678453790856930594089043193
```

```
c =
```

```
5086880055138641874208402870465642516072182984439060897000932412022198520556281889403734721105
4092217856647404083319057380487124162172358890291271224191448228324258347112077960474004635186
8016509523053434635827665292160043436280116928584863998076246578510569159714741098713097686136
1725901348373044174572916389916180620167725929946390922168699018200446132338858379467777740009
9418388782261941911497961896493679487996646915306630597704608478763039887735028467457498653411
0904429641439674643946402617659930041442155326967046914630042645322340556563330008814781111337
571189435901241462737418162532467035047557360943639034638792119126
```

```
d = attack(e,n)
```

```
print(d)
```

```
print(long_to_bytes(pow(c,d,n)))
```