BUUCTF 每日打卡 2021-8-5

原创

Σ2333! 于 2021-08-05 21:16:57 发布 89 收藏 1

分类专栏： crypto 文章标签： 密码学

本文链接：https://blog.csdn.net/weixin_52446095/article/details/119422735

引言

无

[b01lers2020]safety_in_numbers

题目给了两个很大的文件：

flag.enc	3/13/2020 3:12 AM	ENC 文件	1,208 KB
pubkey.pem	3/13/2020 3:12 AM	PEM 文件	1,654 KB

加密代码如下：

```
import sys
import Crypto.PublicKey.RSA as RSA


def enc(msg, pubkey):
  (n,e) = pubkey
  m = int.from_bytes(msg, byteorder = 'little')
  c = pow(m, e, n)
  ctxt = (c).to_bytes(c.bit_length() // 8 + 1, byteorder = 'little')
  return ctxt


with open("pubkey.pem", "r") as f:
  ciph = RSA.importKey(f.read())    # chill out, Crypto.RSA takes its sweet time... (minutes)

pubkey = (ciph.n, ciph.e)


with open("flag.txt", "rb") as f:
  flag = f.read()

sys.stdout.buffer.write(enc(flag, pubkey))
```

`# chill out, Crypto.RSA takes its sweet time... (minutes)`

啊这

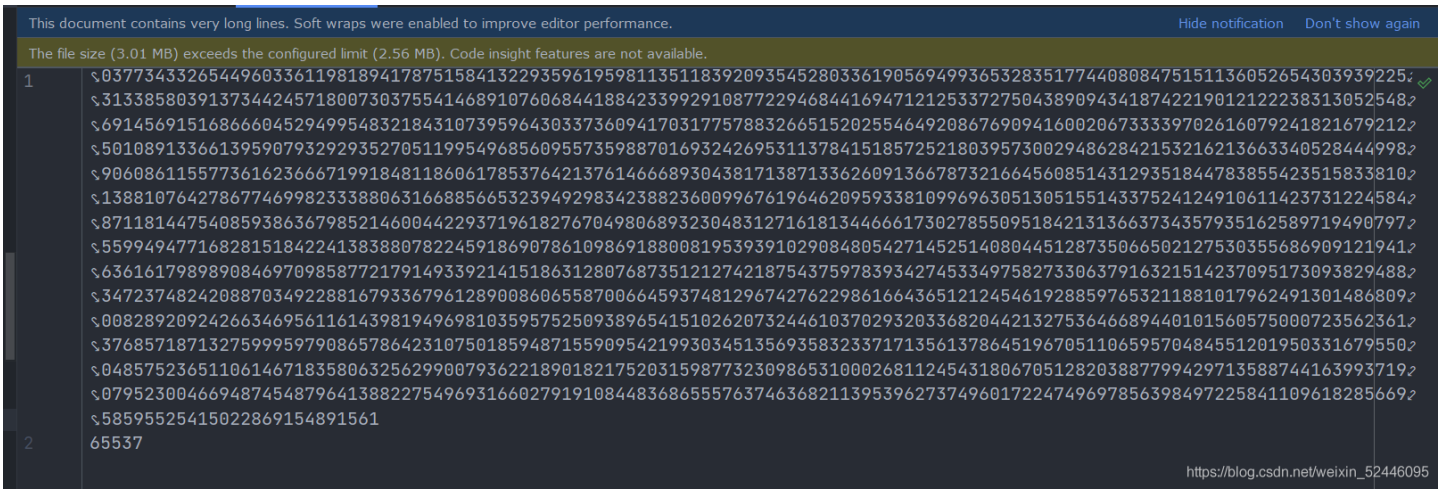
获取公钥代码如下：

```
from Crypto.PublicKey import RSA

with open("pubkey.pem", "r") as f:
    ciph = RSA.importKey(f.read())    # chill out, Crypto.RSA takes its sweet time... (minutes)

e = ciph.e
n = ciph.n
with open('publickey.txt', 'w') as f:
    f.write(str(n))
    f.write('\n')
    f.write(str(e))
```

结果为：



发现n是上面一大串，而e=65537

然后关于怎么处理这个ctxt

其实只要知道`from_bytes`和`to_bytes`互为“逆运算”就行了，具体可以参照官方文档

代码如下：

```
with open("flag.enc", "rb") as f:
    ctxt = f.read()
    print(ctxt)
c = int.from_bytes(ctxt, byteorder='little')

with open('cipher.txt', 'w') as f:
    f.write(str(c))
```

publickey.txt	8/1/2021 8:54 AM	文本文档	2,940 KB
cipher.txt	8/1/2021 9:02 AM	文本文档	2,909 KB

两个文件都非常大

然后就没什么别的信息了，出题人总不能让我做不出来吧

猜测由于n很大，e相对n很小，那么就有可能出现 $c = m^e$ 的情况

```python
from Crypto.Util.number import *
import gmpy2

with open("flag.enc", "rb") as f:
    ctxt = f.read()

c = int.from_bytes(ctxt, byteorder='little')
e = 65537
m = gmpy2.iroot(c, e)[0]
print(long_to_bytes(m)[::-1])
```

结果为：

```
b'pctf{!fUtuR3_pR00f}'
```

[AFCTF2018]MagicNum

题目就给了一个txt文件，里面一串浮点数：

```
1  720659105101771380000000000000000.000000
2  71863209670811371000000.000000
3  184896826254127600000000000000000.000000
4  72723257588050687000000.000000
5  46746591674697662000000000.000000
6  190616988374992920000000000000000000000.000000
```

想起之前写的[ACTF新生赛2020]crypto-des也是一样的情况
解密代码如下：

```python
from Crypto.Util.number import *
import struct

s = [720659105101771380000000000000000.000000, 71863209670811371000000.000000, 184896826254127600000000000000000.000000
, 72723257588050687000000.000000, 46746591674697662000000000.000000, 190616988374992920000000000000000000000.000000,]
a = ''
b = ''
for i in s:
    a += struct.pack('<f', i).hex()       # 小端
print(a)

for j in s:
    b += struct.pack('>f', j).hex()       # 大端
print(b)

print(long_to_bytes(int(a, 16)))
print(long_to_bytes(int(b, 16)))
```

结果为：

```
61666374667b7365635f69735f6576657279776865726 57d
7463666165737b6673695f63657665 5f687779727d657265
b'afctf{sec_is_everywhere}'
b'tcfaes{fsi_ceve_hwyr}ere'
```

[XNUCA2018]Warmup

加密代码如下：

```
from Crypto.Util.number import bytes_to_long, getPrime
from random import randint
from gmpy2 import powmod
import sys

p = getPrime(1024)
q = getPrime(1024)
N = p*q
Phi = (p-1)*(q-1)

with open("flag", 'r') as fr:
 flag = bytes_to_long(fr.read().strip())

def get_enc_key(BitLen, Phi):
    e = getPrime(BitLen)
    if Phi % e == 0:
        return get_enc_key(BitLen, Phi)
    else:
        return e

def sprint(message):
 print(message)
 sys.stdout.flush()

def communicate():
 sprint("This is a message distribute system. Please tell me your name: ")
 user = raw_input()
 bakcdoor(user)
 e = get_enc_key(randint(13, 13 + (len(user) % 4)), Phi)
 ct = powmod(flag, e, N)
 sprint("Hi %s, your N is: %d\nAnd your exponent is: %d\nLast but not least, your secret is: %d" % (user, N, e, ct))
 sprint("You will know the secret after I give you P,Q.\nSee you next time!")

if __name__ == "__main__":
 communicate()
```

明显需要交互嘛

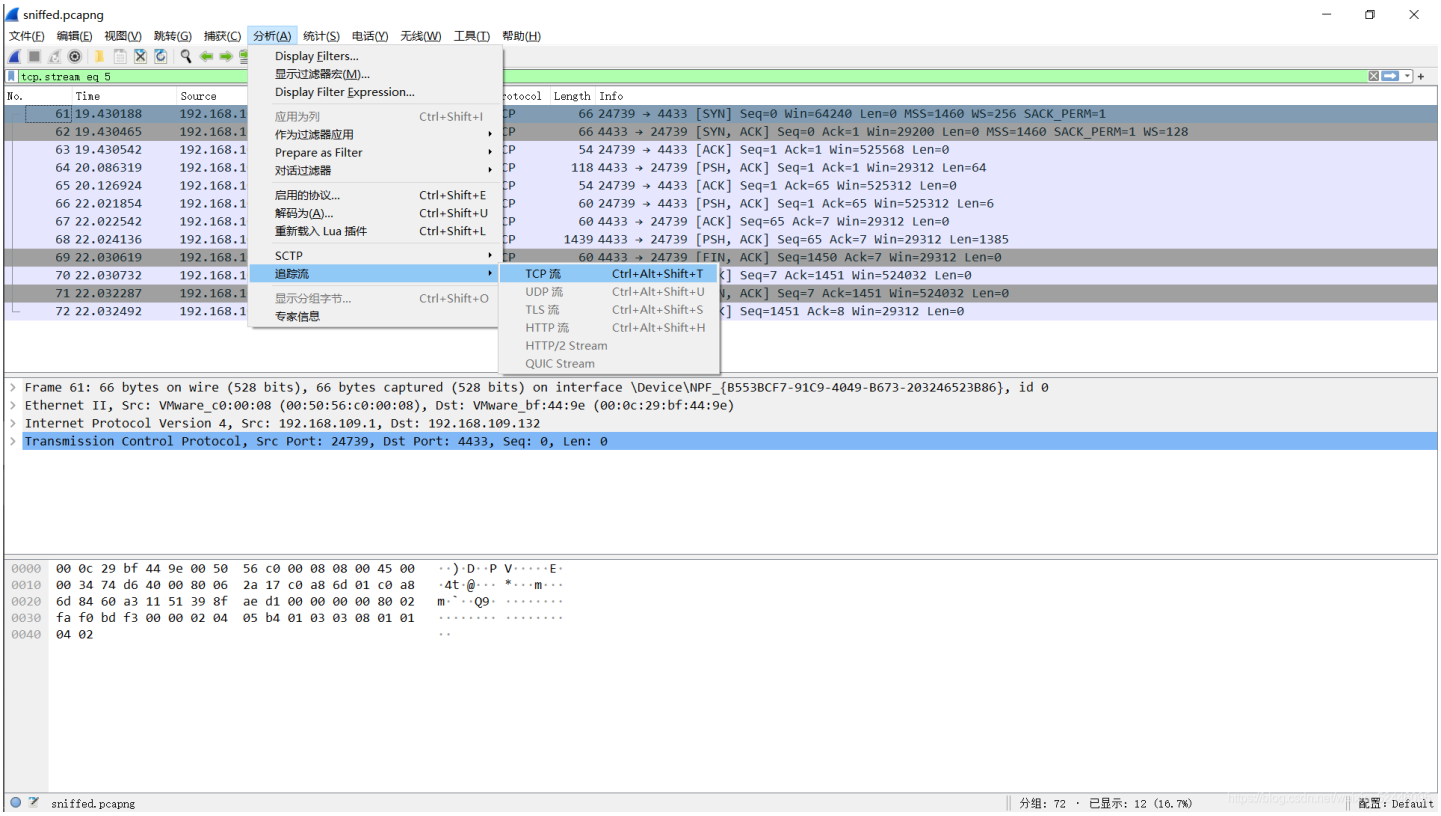
但是没给输出结果

题目给了一个后缀是.pcapng的文件，图片？

不懂，找wp，考的是**流量包文件提取**，没见过

使用的工具叫wireshark，建议使用镜像下载

下载下来之后导入文件，选择分析中的追踪TCP流



得到六段文件

分别为：

```
This is a message distribute system. Please tell me your name:
Alice
Hi Alice, your N is: 25118186052801903419891574512806521370646053661385577314262283167479853375867074736882903917202574957661470179148882538361560784362740207649620536746860883395110443930778132343642295247749797041449601967434690280754279589691669366595486824752597992245067619256368446164574344449914827664991591873150416287647528776014468498025993455819767004213726389160036077170973994848480739499052481386539293425983093644799960322581437734560001018025823047877932105216362961838959964371333287407071080250979421489210165485908404019927393053325809061787560294489911475978342741920115134298253806238766543518220987363050115050813263
And your exponent is: 7669
Last but not least, your secret is: 22917655888781915689291442748409371798632133107968171254672911561608350738343707972881819762532175014157796940212073777351362314385074785400758102594348355578275080626269137543136225022579321107199602856290254696227966436244618441350564667872879196269074433751811632437228139470723203848006803856868237706401868436321225656126491701750534688966280578771996021459620472731406728379628286405214996461164892486734170662556518782043881759918394674517409304629842710180023814702447187081112856416034885511215626693534876901484105593275741829434329109239483368867518384522955176807332437540578688867077569728548513876841471
You will know the secret after I give you P,Q.
See you next time!
```

This is a message distribute system. Please tell me your name:
Bob
Hi Bob, your N is: 164694360768918191074306645865707900583653325326744387891466759973145954911872444593839214248350320670618852755547355571457125214982532961639103903063301358553029221572729369078980450062608832743338342294181521556942955707822079995650527653302282423629689332987588114040313220691813628552437058387996456850663321729694017432117509045092262919466625787519917159961033039766477308748452830208150003218926782207248024502488722346640366672640223845883713732493906420535391944232826942489407365286967138959352521379172608563211143707438038666017612115522289034258503654573608768989405832213945827235576053090722328558221215222890342585036545736087689894058322139458272355760530907223285582212152228903425850365457360876898940583221394582723557605309072232855822121
And your exponent is: 6581
Last but not least, your secret is: 450506375791223703063562874722127299457269535919458822713774518403815699368496769295038237941667004835269719203484743764100511839677845157325207996032942373085731290390547315382167172822171119604186467161255311748196721934665095358966173812500438550677027095085030501842813370257000748993382080528237478644704310107536815952462716031754699498307427174443883075870367254902179439600599665756389364762385805334080250827596622473115606649413078152428269206937403484852321141878634892066010264550624525326635092869186811703780231120742985452789310162935089906479360605384576887525108707967657110639573585606897303472110 1
You will know the secret after I give you P,Q.
See you next time!

This is a message distribute system. Please tell me your name:
Carol
Hi Carol, your N is: 251188740533285467530242639895634157275020480750259918335695012056322423371130779015323323747753954193483487010481894080926320798148323637320109261779120825629640166708909362810508644961557216722810933440822819636383719777583612021319706094905122452657195388796959447217444923576974388650169525315562003223908885055529794211314191427242582712300594224203363638797872010724945583512669679203578588734581217485829856403756049867417275010584949515335323411255067345412163052710461437057547999107290454355645385029621450486528208795908959932258691894299463291683858729643571337802908644546383640092525484943234380222313491
And your exponent is: 7603
Last but not least, your secret is: 190487375769870450632265902501272322464758090974325044283649080566040252813470911068638187701798869460368280333698114362586838366406864821862958879546033336747901265310248251962752474309178742300199376461541286865659593825499279747215959077200526833263478839172883870118986106885859675490632939990076621795372085411145286459068678342839115308270094963505648180509269925783548453753851365189222786659679147070356759261661959590841308786664463444923989321380980066906968111673139885613193142859360599262199645505605668929321462267657569397588147999080597438865028821066270854042961990275293282510355212246280038329138541
You will know the secret after I give you P,Q.
See you next time!

This is a message distribute system. Please tell me your name:
Dave
Hi Dave, your N is: 251181860528019034198915745128065213706460536613855773142622831674798533758670747368829039172025749576614701791488825383615607843627402076496205367468608833951104439307781323436422952477497904144960196743469028075427958969166936659548682475259799224506761925636844616457434444991482766499159187315041628764752877601446849802599345581976700421372638916003607717097399484848073949905248138653929342598309364479996032258143773456000101802582304787793210521636296183895996437133328740707108025097942148921016548590840401992739305332580906178756029448991147597834274192011513429825380623876654351822098736305011505081326 3
And your exponent is: 6947
Last but not least, your secret is: 204946658791166661599610161259490700975304137703918938582155472290711160255818227297983137968232048616249129090309754507421228027758791944523206436777103601102136612339391735413484991167530787732410383487128851327445794103645347703479864718210642261950434505525954367575299833078690637683033540333961090354725596512719631511333130051264104693322700810140141602680925681322148060466201210154284647905283212878827903172788075064249932904178037240556781690438416455919187942261523858018135718388211124993949266832877161450947622978506281958679666037079803056280522470449757044684413165003007500490121614189342014014056 8
You will know the secret after I give you P,Q.
See you next time!

```
This is a message distribute system. Please tell me your name:
Eve
Hi Eve, your N is: 228909212964893914687235632074824393687150485289548577276966119972138494539254076394783110648490020928413321870299228295037325948194053345578990181938365738275383677328763152611077863758830327023363699498133833598229454473487386398984883492499307946851476806023695745832722331866386390067229325144924124734996712406727866093926231086687406114091924103530887929268637591365742346827124376581675444203885034621919666642974860168643005871003390170328690185506937881568239528345869151807698420013797262718154070427364148173199300703631236719547722006186989750992851755232734934546550688150921640267905755525998148975990192851755232734934546550688150921640267905755525998148975990193
And your exponent is: 32869
Last but not least, your secret is: 104429179887667733964909919406673178080473279713179251371024890440305285578979926725079375546974828074816870870323491445512624716823070716589618785323829718280911093542576214913440134506047608700601427365514783016841438247508332855952474738211084233253841798831939885172868662634484906039665729756380619537522624995939052242153503129555892633760138861434616268771004415137450961298183793353822868220933589338809661805166288216468282144704200859457062083016562967012457040536995250775306552253534660263255936199970219610400460336702738377146515008724929698637479736106559433660747445846522708447845910486700223729040941
You will know the secret after I give you P,Q.
See you next time!
```

```
This is a message distribute system. Please tell me your name:
Frank
Hi Frank, your N is: 136107346697571052625644985659030166288848974656421886269777126004694289434548593532885619533320711128381928953538393067286980728613174754833645994287384082034208594635457430335074539999027686709637601170022267388342128268669727907596188575921836394300061299618049693444580997392758017445558529084773991063709032748470081681914062120264962016834379887897503113571270308741972561080879690604291168936492570078632518573842207938981878637841430994300270043830262817313675124745852214236276264548945086174096009749248194589071769600873897765510212867490781385204141781316824092881755696038405177429666540202970532801204213
And your exponent is: 10369
Last but not least, your secret is: 338230230737795357907632634565480424320738100416872971593313504623031636549506308515885211507225139575284223841381475563865888650857636729319870056097265003381655374810743643787055050913356678153093440043937297044556267703050582739481148800234028265995678045070593516597241200279290432036592464223968778632301959998956082387007036826439290490046693942095006926116019667542427239110629330500882759564195704755475923049022289141527406786806241793809546426372343971278513127134648233599072200913066293287533269250758307985763118372706166149682768349327629911555785267589749222331760647201324907861960876452039787203524
You will know the secret after I give you P,Q.
See you next time!
```

然后发现，第一段和第四段的N是相同的，采用共模攻击
解密代码如下：

```
from Crypto.Util.number import *
import gmpy2

n = 25118186052801903419891574512806521370646053661385577314262283167479853375867074736882903917202574957661470179148882538361560784362740207649620536746860883395110443930778132343642295247749797041449601967434690280754279589691669366595486824752597992245067619256368446164574344449914827664991591873150416287647528776014468498025993455819767004213726389160036077170973994848480739499052481386539293425983093644799960322581437734560001018025823047877932105216362961838959964371333287407071080250979421489210165485908404019927393053325809061787560294489911475978342741920115134298253806238766543518220987363050115050813263
e1 = 7669
e2 = 6947

c1 = 22917655888781915689291442748409371798632133107968171254672911561608350738343707972881819762532175014157796940212073777351362314385074785400758102594348355578275080626269137543136225022579321107199602856290254696227966436244618441350564667872879196269074433751811632437228139470723203848006803856868237706401868436321225656126491701750534688966280578771996021459620472731406728379628286405214996461164892486734170662556518782043881759918394674517409304629842710180023814702447187081112856416034885511215626693534876901484105593275741829434329109239483368867518384522955176807332437540578688867077569728548513876841471

c2 = 20494665879116666159961016125949070097530413770391893858215547229071116025581822729798313796823204861624912909030975450742122802775879194445232064367771036011021366123393917354134849911675307877324103834871288513274457941036453477034798647182106422619504345055259543675752998330786906376830335403339610903547255965127196315113331300512641046933227008101401416026809256813221480604662012101542846479052832128788279031727880750642499329041780372405567816904384164559191879422615238580181357183882111249939492668328771614509476229785062819586796660370798030562805224704497570446844131650030075004901216141893420140140568
# s & t
gcd, s, t = gmpy2.gcdext(e1, e2)
if s < 0:
    s = -s
    c1 = inverse(c1, n)
if t < 0:
    t = -t
    c2 = inverse(c2, n)
plain = pow(c1, s, n) * pow(c2, t, n) % n
print(long_to_bytes(plain))
```

结果为：

```
b'FLAG{g00d_Luck_&_Hav3_Fun}'
```

结语

希望继续坚持