LikiPrime

描述

Wow! RSA!

题目地址

https://prime.liki.link/

解题过程

1. 将链接下载的文件用记事本打开得到

```
n =
153618988782356965746670001051090097207178065847609350922062429604075492363635014172136963463709996079741042478564794588337724125369803657401617173692685478765679305816624609468565620307223307834219959554473785941197585503297598493935350183441391030421436212390114699556482059349039040455648468221599981748796957744194503997239701482701410030029029270027679842540999722887462434810843816437197319583607025618186635697305976249665612688247376108935160320686131200898556905800476205891960799074774585437833002823934954617463060964154432740843629562672391868230893490903989197488149388729384780970652671562316484872033294124226157117118861646340597233621672361185214584972483051157645107627319152918821554940117132954626032214397632184774556745846625241379917308917768268491889756503541651063788340149876955927468369980022328266783399199187997812468274596170826874259554306418155184168780157285144772871929341939578335329966872345542802638170681068054408484756688305051801720496747569798562869071986482671609263053289868530528888316780870298679461806090
```

```
e = 65537
```

```
c =
792718762802605532278394090155065193789395366006553460971400171192445696309560301366708547014614487498196057423346639744344997714999735747157543169502541552642112792742458525353399996126506677910325962345120811170908229213934705931214913766542646238181632917822948468027536865745000304670135598501400970091543941746682644684887732928481080294944043312220743013694438057609568108174019779859755943716370251171244889298697822928557767241086599188963468602462907190279377862069254854823427667865319564830546270362357936930995648160622304304090308218055972055123551570008066123419069309457140667955750241304974532530174758870783992052291092301886400900398847537125874296993238159030838154303553904314963487162292769564595304424933188905808169978388496596498691985207576811918548650672995848168884854773013104035018041144626339468611954678135054273704911280014060173488332502407300015607842759235048437997661556158686088265640319895236141159912535842267682895490879754222561141896923398550290031634289690316181189406182630830259427320913113280227041600
```

2. 在http://factordb.com/这个网站将n分解得到
   p=2^2203-1
   q=2^1279-1

```
import binascii

import sys

sys.setrecursionlimit(1000000)

def ByteToHex(bins):

return ''.join(["%02X" % x for x in bins]).strip()

def n2s(num):

t = hex(num)[2:-1] # python

if len(t) % 2 == 1:

t = '0' + t

\#print(t)

return(binascii.a2b_hex(t).decode('latin1'))

def egcd(a, b):

if a == 0:

return (b, 0, 1)

else:

g, y, x = egcd(b % a, a)

return (g, x - (b // a) * y, y)

def modinv(a, m):

g, x, y = egcd(a, m)

if g != 1:

print('modular inverse does not exist')

return 'null'

else:

return x % m
```

```
c =
792718762802605532278394090155065193789395366006553460971400171192445696309560301366708547014614487498196057423346639744344997714999735747157543169502541552642112792742458525353399996126506677910325962345120811170908229213934705931214913766542646238181632917822948468027536865745000304670135598501400970091543941746682644684887732928481080294944043312220743013694438057609568108174019779859755943716370251171244889298697822928557767241086599188963468602462907190279377862069254854823427667865319564830546270362357936930995648160622304304090308218055972055123551570008066123419069309457140667955750241304974532530174758870783992052291092301886400900398847537125874296993238159030838154303553904314963487162292769564595304424933188905808169978388496596498691985207576811918548650672995848168884854773013104035018041144626339468611954678135054273704911280014060173488332502407300015607842759235048437997661556158686088265640319895236141159912535842267682895490879754222561141896923398550290031634289690316181189406182630830259427320913113280227041600 6

p=2**2203-1
q=2**1279-1

e = 65537

n = p * q

d = modinv(e, (p - 1) * (q - 1))

m = pow(c, d, n)

\#print 'm \n', m

print (m)

print("十进制:\n%s"%m)

m_hex = hex(m)[2:]print("十六进制:\n%s"%(m_hex,))

\#print("ascII:\n%s"%((binascii.b2a_hex(hex(m)[2:])).decode('hex'),))

print("ascii:\n%s"%(binascii.a2b_hex(m_hex).decode("utf8"),))
```

输出结果为

```
570893384134068466208821377109160724312908349446672517317197670470917011893446249830488673439525850 85
十进制:
570893384134068466208821377109160724312908349446672517317197670470917011893446249830488673439525850 85
十六进制:
6867616d657b4d657273336e6e657e5072214d655e7265346c31795f73302b354f2d6c6937746c65217d
ascii:
hgame{Mers3nne~Pr!Me^re4l1y_s0+5O-li7tle!}
```