Crypto--RSA因数分解

原创

yumengzth 于 2019-07-11 17:59:22 发布 3530 收藏 5

分类专栏： ctf crypto 文章标签： RSA crypto ctf

本文链接：https://blog.csdn.net/yumengzth/article/details/95500279

ctf 同时被 2 个专栏收录

1 篇文章 0 订阅

订阅专栏

crypto

1 篇文章 0 订阅

订阅专栏

0x00

这是i春秋上的一道简单的RSA因数分解题。

题目链接：https://www.ichunqiu.com/battalion?q=4623

下载后打开rsa.txt，看到提供的参数

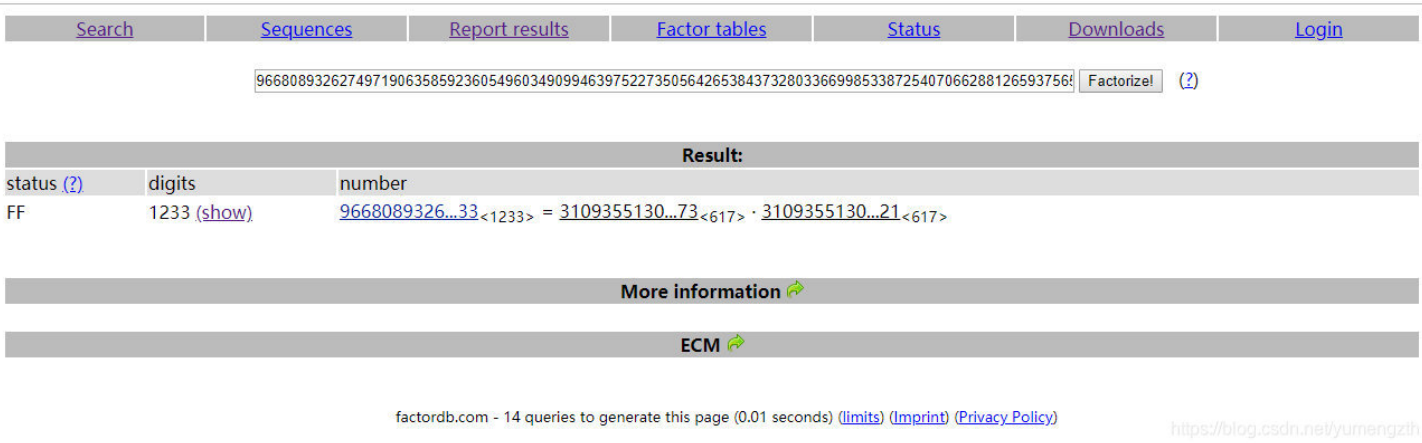
```
n（两个大素数p、q的乘积）
e（公钥）
c（密文）
```

0x01

对n进行因数分解

如果n比较小，那么可以通过工具进行直接n分解，从而得到私钥。如果n的大小小于256bit，那么我们通过本地工具即可爆破成功。例如采用windows平台的RSATool2v17，可以在几分钟内完成256bit的n的分解。

如果n在768bit或者更高，可以尝试使用一些在线的n分解网站，这些网站会存储一些已经分解成功的n，比如：**http://factordb.com** 通过在此类网站上查询n，如果可以分解或者之前分解成功过，那么可以直接得到p和q。



q =
3109355130292288099988302080366553661627214702287742874531483086751935101324891424488010109436581599805011541530843961006700139164376274980650005150267949853671653233491784289493988946869396093730966325659249796545878080119206283512342980854475734097108975670778836003822789405498941374798016753689377992355122774401780930185598458240894362246194248623911382284169677595864501475308194644140602272961699230282993020507668939980205079239221924230430230318076991507619960330144745307022538024878444458717587446601559546292026245318907293584609320115374632235270795633933755350928537598242221421667449640962592899787722 1

p =
3109355130292288099988302080366553661627214702287742874531483086751935101324891424488010109436581599805011541530843961006700139164376274980650005150267949853671653233491784289493988946869396093730966325659249796545878080119206283512342980854475734097108975670778836003822789405498941374798016753689377992355122774401780930185598458240894362246194248623911382284169677595864501475308194644140602272961699230282993020507668939980205079239221924230430230318076991507619960330144745307022538024878444458717587446601559546292026245318907293584609320115374632235270795633933755350928537598242221421667449640962592879745047 3

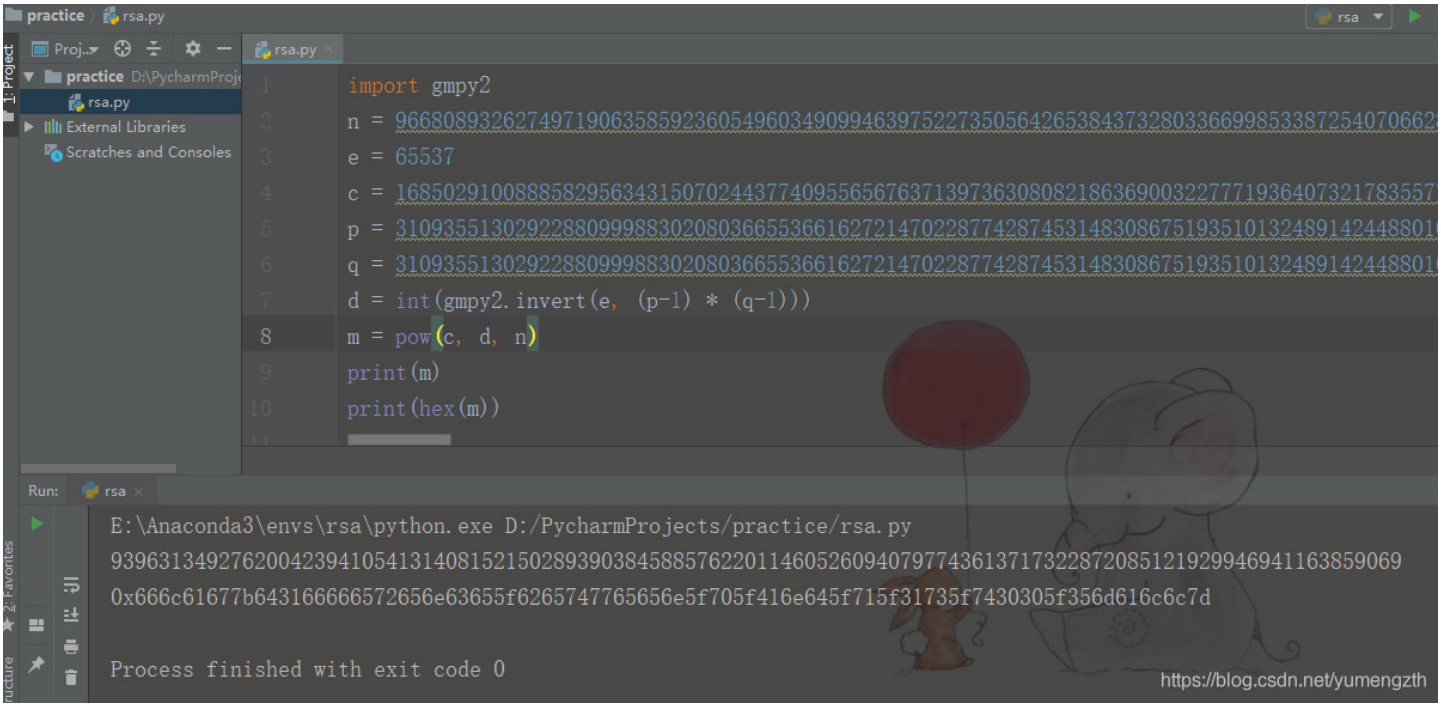
0x02

到现在RSA相关参数均已具备，编写代码，求出明文信息
（在此之前需要安装gmpy2模块，可参考此链接进行安装：https://blog.csdn.net/dongyanwen6036/article/details/77176731）

```
import gmpy2
n = 96680893262749719063585923605496034909946397522735056426538437328033669985338725407066288126593756516300075860615430875794403057183717504851457447306140156633083633464717665528261926859256017272652664307449953412987821740904604553365689705011743849635723157599918552767507100280395180063522002901593200746511781873994890375020083085611566869100770683695224484271941945294625927525177329833816238993051883827270490888701647400705139719458839603911121670886621461477962756695933517067605502585093263105364157656616569412142054608104328580678323929679979565519112196637759017578061894491053281698814305675705405267996853890146089357120490439497571408105545524052389565330531551774572933411454975669533417114287608047710507040954477798160215276215461073854016379616429522281024330905150309086667463444035922619253072463547705157651517986446117491197566716259728676907938066078264795294480859631047697393915618747207695293572824906113748188758910397359108287298864195827028516965080379239555636330405629007780145398082209758357430968293569726020486275692386555639768669685423956454140718570994010780653677316026376448344385942572695314296414821620996843758704461761351805877928716785334936453371645867606673421687756618151460769388237553300e = 65537
c = 16850291008885829563431507024437740955656763713973630808218636900322777193640732178355779562427916216230520043644690397638594867789766546629085276987756216748714238530802734163981640105508182049700201890889620286034239102908258162198730553309738665218384965706595206243398838764099038362326440552514400350028653126267431590053700184504322536314835976677103389968011107618167279707741058474750958193204554080177773854887274759789996536695082750552943248377982115815292889994783719639155566616548644187818328800875356110899571596192047292784487756985594050514884353099887811372283042780792667932424114118223890356768204241014534555188944215889515787579899090371510578268208388646166130706358344769616882868712695614795588649338380551355760417902905098167875505494560786635319579365410840393924272386165191915236992390400296687399481182639108031814626041697849937718254068440979035725749081620313849936963449089755322776356355398124689167761344639013447783214317524899216164169801119596879210520184797608232278662339024247022674068582221814026318202422622869215938055766159163307209194507733419198786026244838512359945964722856213736917806907280449804946313623385633781738597799014557104223179533299552398817489543281987283217002969084800e = 65537
p = 31093551302922880999883020803665536616272147022877428745314830867519351013248914244880101094365815998050115415308439610066700139164376274980650005150267949853671653233491784289493988946869396093730966325659249796545878080119206283512342980854475734097108975670778836003822789405498941374798016753689377992355122774401780930185598458240894362246194248623911382284169677595864501475308194644140602272961699230282993020507668939980205079239221924230430230318076991507619960330144745307022538024878444458717587446601559546292026245318907293584609320115374632235270795633933755350928537598242214216674496409625928797450473q = 31093551302922880999883020803665536616272147022877428745314830867519351013248914244880101094365815998050115415308439610066700139164376274980650005150267949853671653233491784289493988946869396093730966325659249796545878080119206283512342980854475734097108975670778836003822789405498941374798016753689377992355122774401780930185598458240894362246194248623911382284169677595864501475308194644140602272961699230282993020507668939980205079239221924230430230318076991507619960330144745307022538024878444458717587446601559546292026245318907293584609320115374632235270795633933755350928537598242214216674496409625928997877221d = int(gmpy2.invert(e, (p-1) * (q-1))) #计算私钥
m = pow(c, d, n) #解密
print(m)
print(hex(m))
```

运行结果十六进制输出：

0x666c61677b643166666572656e63655f6265747765656e5f705f416e645f715f31735f7430305f356d616c6c7d



0x03

将十六进制转化为字符串得到flag：

flag{d1fference_between_p_And_q_1s_t00_5mall}

工具地址：**https://tool.lu/hexstr/**

在线工具

搜索其实很简单 正则 解密 运行代码 搜索

所有 开发类 站长类 极客类 HR 其它 码农文库 奇淫巧技 软件推荐 网址导航 Wiki

```
flag{d1fference_between_p_And_q_1s_t00_5mall}
```

字符串(Str) 十六进制(Hex)