BUUCTF_Crypto_Dangerous RSA

原创

qq_58370970 于 2021-11-17 20:16:03 发布 49 收藏
文章标签： 经验分享

题目：给了一个文件

用txt文本打开

```
#n:  0x52d483c27cd806550fbe0e37a61af2e7cf5e0efb723dfc81174c918a2762777
#e:  0x3
#c:0x10652cdfaa6b63f6d7bd1109da08181e500e5643f5b240a9024bfa84d5f2cac9
so,how to get the message?
```


从字面上就可以知道这是一个危险的加密，由于e=3，攻击者可以很容易的解开

当e=3时：

情况一，当m的e次方小于n时，m^emodn=c,这个时候m^e=c，直接对c开三次方得到m

情况二，当m的e次方大于n时，m^e=k*n+c,由于e比较小，可以直接爆破将k求出来，在开e次方解出m（求出当k满足k*n+c能够被开e次方根时）

方法一：

直接开方：

```
import gmpy2
import libnum
n=0x52d483c27cd806550fbe0e37a61af2e7cf5e0efb723dfc81174c918a27627779b21fa3c851e9e94188eaee3d5cd6f752406a43f
e=0x3
c=0x10652cdfaa6b63f6d7bd1109da08181e500e5643f5b240a9024bfa84d5f2cac9310562978347bb232d63e7289283871efab83d8
n=int(n)
c=int(c)
m=gmpy2.iroot(int(c),3)
m2=13040000448281971381981734052456302315991930504782460047879974048879771035557949448672899135 7
print(libnum.n2s(m2))
```

（由于gmpy2.iroot()的返回值是这个

(mpz(10134909992911077921771534663618052362414162888170786873119317244632144897941084389 7
True)

所以我走了两边程序）

得到flag

方法二：

爆破求k

```
import gmpy2
import libnum
c=38898214388891356643295289982643539244185842201247441811555489667740931290436968953273121356589485238349 2
n=60467951213861703784306340033585227791775930272068075780181934332216917731778963921171768651935270496270 8
k=0
def dec(c,N):
    k=0
    while 1:
        (x,y)=gmpy2.iroot(c+k*N,3)
        if y:
            print(gmpy2.iroot(c+k*N,3))
            break
        k=k+1
    print(k)
dec(c,n)
m=10134909992911077921771534663618052362414162888170786873119317244632144897941084389753290115633419670869 8
print(libnum.n2s(m))
```

（同上）

得到flag