CTF Crypto---RSA dp泄露

原创

3tefanie丶zhou 于 2022-01-13 11:14:52 发布 17 收藏

分类专栏： CTF 文章标签： 动态规划 算法 leetcode 安全

本文链接：https://blog.csdn.net/luochen2436/article/details/122468232

文章目录

题目

已知n,c,e,dp

```
e = 65537
n = 24825400785152624117772152669890180298583276617622160961225887737162058006043310153832803030521991869764361981420093067961210988553380133534844502375167047843707305554472428068473329805159916766030364518314616149748535863368149212966880240206579778990555048954764511878726660192942972413316776846530966590611 3
dp = 90507449805234690464302513287951833069192517457305400462187725331868267505542197094355201669552856036483444630319693920705664292714809329037444021050365 7
c = 14042367097625269680753367358620940057566428210068411978420352712452118899640382659743688376604187906749428095741020195893573736038080184545382929399743341418883872575179626170262202858721156035336284719106030657851051138096516213347269871306359262102895916707278148256267368309059052121421807116028766518075 1
```

题目解析

数学解析

已知公钥n,c、密文c以及dp

其中dp = d mod (p-1)

已知

```
c = m^e mod n
m = c^d mod n
φ(n)=(p-1)*(q-1)
d*e ≡ 1 mod φ(n)
dp = d mod (p-1)
```

由上述式子可以得到

```
dp*e ≡ d*e mod (p-1)
```

进而分解为

```
d*e = k*(p-1)+dp*e
```

又因为`d*e ≡ 1 mod φ(n)`
所以得到`k*(p-1)+dp*e ≡ 1 mod φ(n)`
化简

```
--->k*(p-1)+dp*e ≡ 1 mod φ(n)
--->k*(p-1)+dp*e ≡ 1 mod (p-1)*(q-1)
--->k1*(p-1)+dp*e = 1 + k2*(p-1)*(q-1)
--->dp*e = k2*(p-1)*(q-1)-k1*(p-1)+1
--->dp*e = [k2*(q-1)-k1)]*(p-1)+1
```

因为`dp = d mod (p-1)`
即,dp为d%(p-1)；所以`dp<p-1`
那么，`e>k2*(q-1)-k1`
令`i = k2*(q-1)-k1`
则`i`的范围为(1,e)
上述式子最终化简为
`dp*e = i*(p-1)+1`
在(1,e)范围内存在一个p可以被n整除并且满足上式

解密脚本

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

e = 65537
n = 24825400785152624117772152669890180298583276617622160961225887737162058006043310153832803030521991869764361981420093067961210988553380133534844502375167047843707305554472428068473329805159916766030364518314616149748535863368149212966880240206579778990555048954764511878726660192942972413316776846530966590611 3
dp = 90507449805234690464302513287951833069192517457305400462187725331868267505542197094355201669552856036483444630319693920705664292714809329037444021050365 7
c = 14042367097625269680753367358620940057566428210068411978420352712452118899640382659743688376604187906749428095741020195893573736038080184545382929399743341418883872575179626170262202858721156035336284719106030657851051138096516213347269871306359262102895916707278148256267368309059052121421807116028766518075 1

for i in range(1,e+1):
    if (dp*e-1)%i == 0:
        if n%(((dp*e-1)//i)+1) ==0:
            p = ((dp*e-1)//i)+1
            q = n//p
            phi = (p-1)*(q-1)
            d = gmpy2.invert(e,phi)
            m = pow(c,d,n)
            print(long_to_bytes(m))
```

【很多时候自顾自的生闷气，就跟会变味的酒一样，自己又喝不掉，一打开酒坛子，谁都不愿意喝。那股子酒气，就是一个人不太好的情绪，积攒多了，看上去谁都闻不着，其实谁都知道，但是只能假装闻不着，不知道。日子久了，看上去好像谁都在照顾对方，其实谁都委屈哩，很累人的。】