网鼎杯CRYPTO-shenyue2题解

原创

一梦不醒 于 2018-11-02 23:38:37 发布 439 收藏

此题为RSA加密算法的变形，题目给出了p、d之间的关系使得RSA算法可以被攻破，解题用到了费马小定理

RSA相关

费马小定理

其内容为： 假如p是质数，且gcd(a,p)=1，那么 a^(p-1)≡1（mod p），例如：假如a是整数，p是质数，则a,p显然互质(即两者只有一个公约数1)，那么我们可以得到费马小定理的一个特例，即当p为质数时候， a^(p-1)≡1(mod p)。

分析题目

RSA相关公式

`N=p*q` p、q位质数

`phi_N=(p-1)(q-1)` phi_N为欧拉函数值

`c=m^e mod N` e为公钥，c为密文

`ed=1 mod phi_N` d为私钥

`m=c^d mod N` m为明文

题目已知项

N(两质数乘积) r k k=(p-r)*d* *c(密文)* *e(公钥)*
可用费马小定理来求得质数p,从而得到私钥：

*`m^(p-1)≡1(mod p)`几乎所有的整数m都满足此公式，由此可以得知A=m^(p-1)-1为p的倍数，利用公约数gcd(A,N),可以计算A和N的公约数得到p，因为N=pq,*所以A N互质。

推导过程

(图中phi_N应为N)

U6GqMYW.jpg

题目内容：

```
from gmpy2 import *
import sys
import time
import struct
from Crypto.Util import number
from common_math import xgcd, modular_mul_inverse

FLAG = "**********************************"
flag = int('0x'+FLAG.encode('hex'), 16)

e = 65537
p = number.getPrime(2048)
q = number.getPrime(2048)
r = 663111019425944540514080507309 # number.getPrime(100)
phi = (p-1)*(q-1)
d = modular_mul_inverse(e, phi)
k = (p-r)*d

enc = powmod(flag, e, p*q)
print "n", p*q
print "e", e
print "k", k
print "enc", enc

#n 764789710135699120066739558828098633577013306253421553430847195908034244362783426399681889172711929793560
#e 65537
#k 113762308794647571382907112999849087784642890051733086081895454354635257772682659777291289942283980918340
#enc 519467713751094904598159022987103691511259274774209441519584888564069062035542644790087060987328959901
```

求A、N公约数及求私钥和明文

```
import libnum
import gmpy2
enc=519467713751094904598159022987103691511259274774209441519584888564069062035542644790087060987328959901700
n=764789710135699120066739558828098633577013306253421553430847195908034244362783426399681889172711929793563
k=113762308794647571382907112999849087784642890051733086081895454354635257772682659777291289942283980918340

e=65537
r=663111019425944540514080507309
aa=pow(2,e*k+r-1,n)-1
p=libnum.gcd(aa,n)
q=n/p
phi_n=(p-1)*(q-1)
d=gmpy2.invert(e,phi_n)
m=pow(enc,d,n)
print libnum.n2s(m)
```

运行结果

另一篇writeup：
https://xz.aliyun.com/t/2687
赏
你的支持是我最大的动力！


支付宝


微信