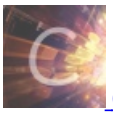
Crypto-RSA加密

原创

Qwzf 于 2019-08-06 23:16:10 发布

文章标签： CTF

本文链接：https://blog.csdn.net/qq_43625917/article/details/98314507


Crypto 同时被 2 个专栏收录

5 篇文章 0 订阅

订阅专栏


RSA

1 篇文章 0 订阅

订阅专栏

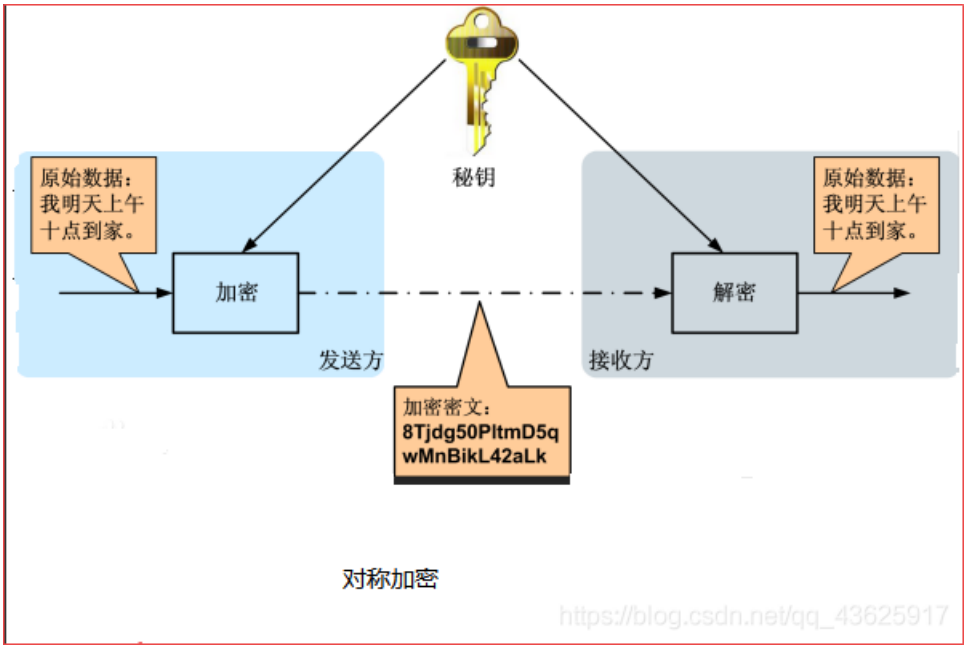
前言

最近学习了RSA加密原理，并且做了些有关RSA的Crypto题。收获很大，总结了一下

一、对称加密和非对称加密

对称加密算法

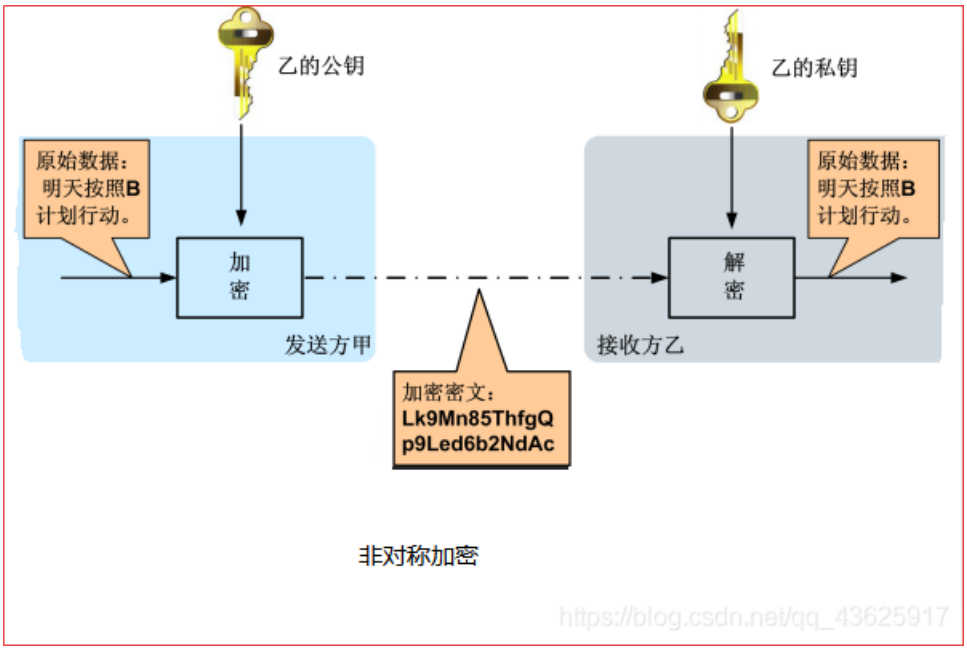
```
（1）甲方选择某一种加密规则，对信息进行加密；
（2）乙方使用同一种规则，对信息进行解密。
```



最大弱点：甲方必须把加密规则告诉乙方，否则无法解密。保存和传递密钥，就成了最头疼的问题。

非对称加密算法

```
（1）乙方生成两把密钥（公钥和私钥）。公钥是公开的，任何人都可以获得，私钥则是保密的。
（2）甲方获取乙方的公钥，然后用它对信息加密。
（3）乙方得到加密后的信息，用私钥解密。
```



公钥加密的信息只有私钥解得开，那么只要私钥不泄漏，通信就是安全的

二、RSA基本介绍

介绍

- RSA加密算法是一种非对称加密算法。在公开密钥加密和电子商业中RSA被广泛使用。
- 对极大整数做因数分解的难度决定了RSA算法的可靠性。换言之，对一极大整数做因数分解愈困难，RSA算法愈可靠。现在只有短的RSA钥匙才可能被强力方式解破。到目前为止，世界上还没有任何可靠的攻击RSA算法的方式。只要其钥匙的长度足够长，用RSA加密的信息实际上是不能被解破的。

RSA签名验签

使用私钥将明文进行签名生成密文串与明文一起传输。对方收到数据后使用公钥和密文串进行验签。如果验签通过就说明就说明第一数据没有被修改过；第二这些数据一定是持有私钥的人发送的，因为私钥只有自己持有，起到防抵赖的作用。

三、RSA数学知识

1、互质关系

如果两个正整数，除了1之外没有其他公因子，我们称这两个数是互质关系。不是质数也可以构成互质关系。
关于互质关系，有以下结论：

- 任意两个质数构成互质关系，比如13和61.
- 一个数是质数，另一个数只要不是前者的倍数，两者就构成互质关系，比如3和10.
- 如果两个数中，较大的那个数是质数，则两者构成互质关系，比如97和57.
- 1和任意一个自然数都是互质关系。
- p是大于1的整数，则p和p-1构成互质关系，比如57和56.
- p是大于1的奇数，则p和p-2构成互质关系，比如17和15.

2、欧拉函数

任意给定正整数n,计算在小于等于n的正整数之中，有多少个与n构成互质关系。计算这个值的方法叫做欧拉函数。以φ(n)表示。在1到8之中，与8形成互质关系的是1、3、5、7，所以 φ(n) = 4。

如果n=1，则 φ(1) = 1 。因为1与任何数（包括自身）都构成互质关系。

如果n是质数，则 φ(n)=n-1 。因为质数与小于它的每一个数，都构成互质关系。比如5与1、2、3、4都构成互质关系。

如果n是质数的某一个次方，即 n = p^k (p为质数，k为大于等于1的整数)，则

$$\phi(p^k) = p^k - p^{k-1}$$

比如 φ(8) = φ(2^3) =2^3 - 2^2 = 8 -4 = 4。
这是因为只有当一个数不包含质数p，才可能与n互质。而包含质数p的数一共有p^(k-1) 个，即1×p、2×p、3×p、…、p^(k-1)×p，把它们去除，剩下的就是与n互质的数。
上面的式子还可以写成下面的形式：

$$\phi(p^k) = p^k - p^{k-1} = p^k(1-\frac{1}{p})$$

可以看出，上面的第二种情况是 k=1 时的特例。

如果n可以分解成两个互质的整数之积，
n = p1 × p2
则
φ(n) = φ(p1p2) = φ(p1)φ(p2)
即积的欧拉函数等于各个因子的欧拉函数之积。比如，φ(56)=φ(8×7)=φ(8)×φ(7)=4×6=24。

因为任意一个大于1的正整数，都可以写成一系列质数的积。

$$n = p_1^{k1}p_2^{k2}...p_r^{kr}$$

根据第4条的结论，得到

$$\phi(n) = \phi(p_1^{k1})\phi(p_2^{k2})...\phi(p_r^{kr})$$

再根据第3条的结论，得到

$$\phi(n) = p_1^{k1}p_2^{k2}...p_r^{kr}(1-\frac{1}{p_1})(1-\frac{1}{p_2})...(1-\frac{1}{p_r})$$

也就等于

$$\phi(n) = n(1-\frac{1}{p_1})(1-\frac{1}{p_2})...(1-\frac{1}{p_r})$$

这就是欧拉函数的通用计算公式。比如，1323的欧拉函数，计算过程如下：
φ(1323)=φ(3^2 * 7^2)=1323(1-1/3)(1-1/7)=756

3、欧拉定理

如果两个正整数a和n互质，则n的欧拉函数 φ(n) 可以让下面的等式成立：

$$a^{\phi(n)} \equiv 1 (mod\ n)$$

也就是说，a的φ(n)次方被n除的余数为1。或者说，a的φ(n)次方减去1，可以被n整除。比如，3和7互质，而7的欧拉函数φ(7)等于6，所以3的6次方（729）减去1，可以被7整除（728/7=104）。

如果正整数a与质数p互质，应为φ§=p-1，所以欧拉函数可写成：

$$a^{p-1} \equiv 1 (mod\ p)$$

这是著名的费马小定理。它是欧拉定理的特例。欧拉定理是RSA算法的核心。

4、模反元素

如果两个正整数a和n互质，那么一定可以找到整数b，使得 ab-1 被n整除。

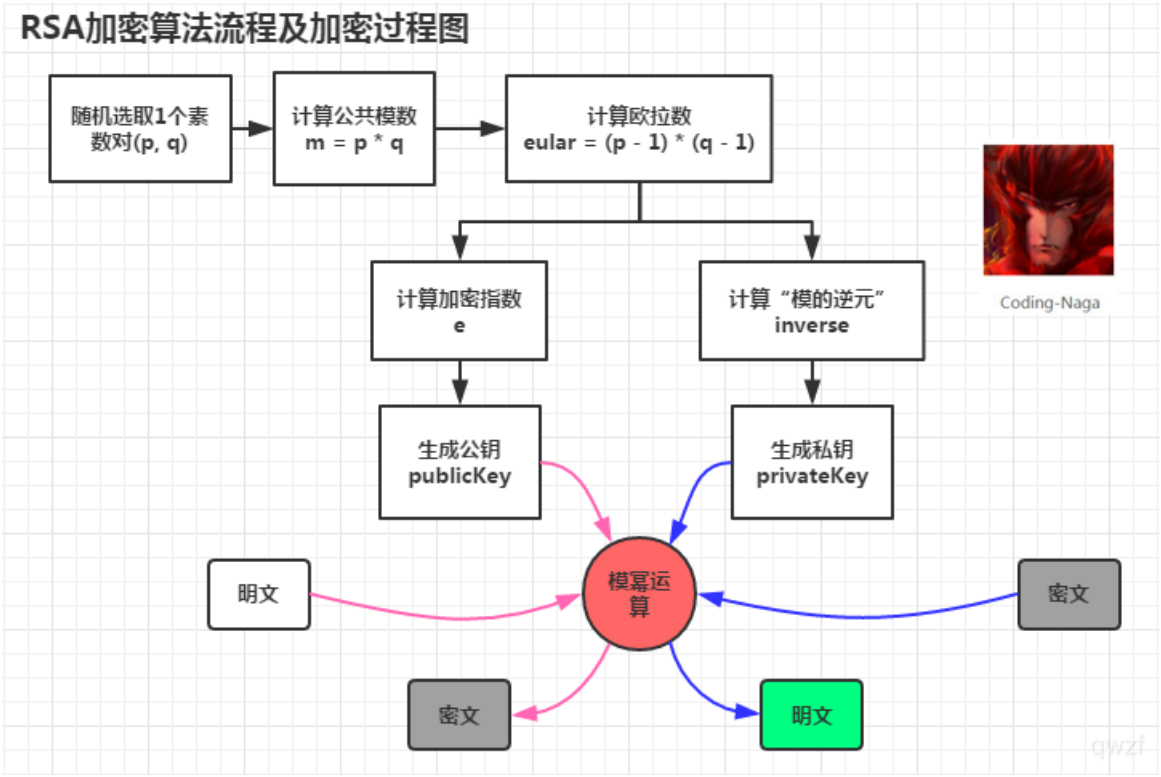
$$ab \equiv 1 (mod\ n)$$

比如：3和11互质，那么3的模反元素是4，应为3*4-1 可以被11整除。4加减11的整数倍数都是3的模反元素。
欧拉定理可以用来证明模反元素必然存在：

$$a^{\phi(n)} = a \times a^{\phi(n)-1} \equiv 1 (mod\ n)$$

a的φ(n)-1次方，就是a的模反元素

四、RSA算法



1、公钥和私钥的生成

RSA算法之一种非对称加密算法。具体的加密工程如下：
使用A和他的小伙伴B来举例子。
假设AI想通过一个不可靠的媒体接受B的一条私人消息，他可以用下面的方式产生一个公钥和私钥。

```
1. 随意选择两个大的质数p和q，p不等于q，计算N = pq.
2. 根据欧拉函数，求得r=φ(N)=φ(p)φ(q)=(p-1)(q-1)。
3. 选择一个小于r的整数e,是e与r互质。并求得e关于r的模反元素，命名为d。(求d令ed≡1(mod r))。(模反元素存在，当且仅当e与r互质)
4. 将p和q的记录销毁。
```

其中(N，e)是公钥，(N，d)是私钥。

例子：

1. AI随机选两个不相等的质数61和53，并计算两数的积N=61*53=3233，N的长度就是密钥长度。3233的二进制是110010100001，一共12位，所以这个密钥就是12位。实际应用中，RSA密钥一般是1024位，总要的场合是2048位。
2. 计算N的欧拉函数。 φ(N)=(p-1)(q-1)=60*52=3120.
3. A 在1到3120上随机选择了一个随机数e=17。
4. 计算e对φ(N)的模反元素d，ed ≡ 1 (mod φ(N))等价于ed-1=kφ(N)。
   找到模反元素d，实质上就是对这个二元一次方程求解：17x+3120y=1。
   用扩展欧几里得算法求解。可以算出一组解(x,y)=(2753,-15)，即d=2753。

其中N=3233,e=17,d=2753。所以公钥就是(N,e)=(3233,17)，私钥(N,d)=(3233,2753)。实际应用中公钥和私钥都是采用ASN.1格式表达的。

2、可靠性

密钥生成步骤，一共出现六个数字：p、q、N、φ(N)、e、d
一旦d泄露，就等于私钥泄露。

```
ed ≡ 1(mod ϕ(N))。只有知道e和ϕ(N)，才能算出d
ϕ(N)=(p-1)(q-1)。只有知道p和q,才能算出ϕ(N)
N=pq,只有将n分解才能算出p和q
```

只有将n质因数分解，才能算出d。也就意味着私钥破译。但大整数的质因数分解是非常困难的。

3、加密和解密

加密

加密要用到公钥(N,e)。
假设B要向A发送加密信息m，B就要用A的公钥(N,e)对m进行加密。
但m必须是整数(字符串可以取ascii值或unicode值)，且m必须小于n。
加密就是计算下式的c。

```
m^e ≡ c (mod n)
```

假设m=65,A的公钥(3233,17),所以等式如下：

```
65^17≡2790（mod 3233）
```

所以c等于2790，B就把2790发给A。

解密

A收到B发来的c(也就是2790)后，就用自己的私钥(3233,2753)进行解密。

```
c^d ≡ m (mod n)
```

也就是c的d次方除以n的余数就是m。
2790^2753 ≡ 65 (mod 3233)
因此得到原文65。

证明

证明为什么用私钥就能解密。就是要证明这个式子：

```
c^d ≡ m (mod n)
```

因为加密规则是：

```
m^e ≡ c (mod n)
```

于是，c可以写成：

```
c = m^e - kn
```

将c代入要我们要证明的那个解密规则：

```
(m^e - kn)^d ≡ m (mod n)
```

等同于求证：

```
m^ed ≡ m (mod n)
因为:ed ≡ 1 (mod ϕ(n))
所以:ed = hϕ(n)+1
将ed代入:
m^(hϕ(n)+1) ≡ m (mod n)
```

接下来，分成两种情况证明上面这个式子。

1. 当m与n互质

```
根据欧拉定理，此时
m^ϕ(n) ≡ 1 (mod n)
得到:(m^ϕ(n))^h × m ≡ m (mod n)
由此原始得到证明。
```

2. 当m与n不是互质时

此时，由于n等于质数p和q的乘积，所以m必然等于kp或kq。
以 m = kp为例，考虑到这时k与q必然互质，则根据欧拉定理，下面的式子成立：

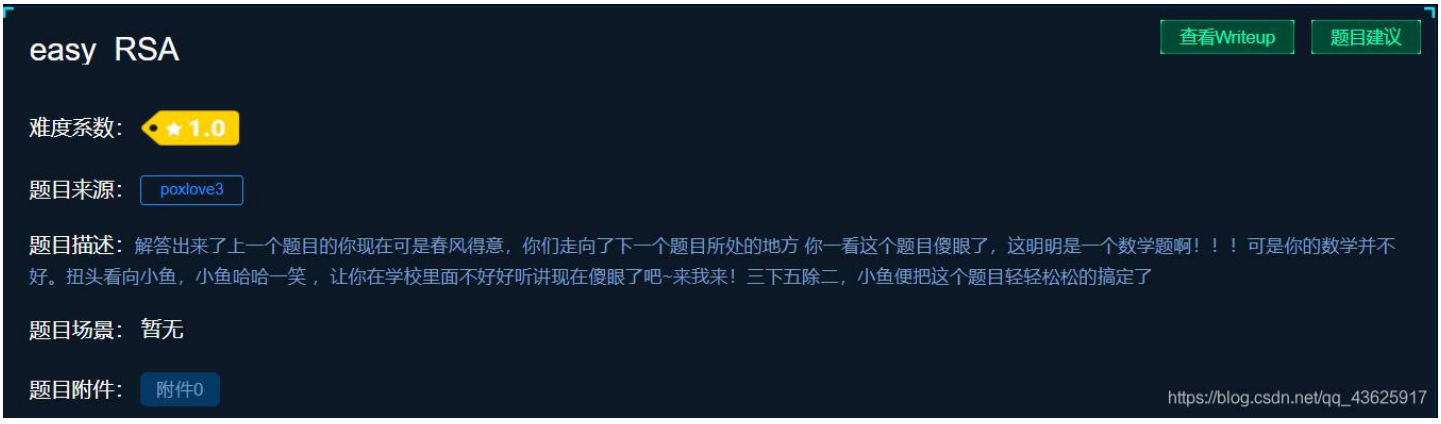
```
(kp)^q-1 ≡ 1 (mod q)
进一步得到：
[(kp)^(q-1)]^(h(p-1))× kp ≡ kp (mod q)
即：(kp)^ed ≡ kp (mod q)
改写成：(kp)^ed = tq + kp
上式t必然能被p整除，即t=t'p
(kp)^ed = t'pq + kp
因为m=kp,n=pq,所以：
m^ed ≡ m (mod n)
```

证明完毕。

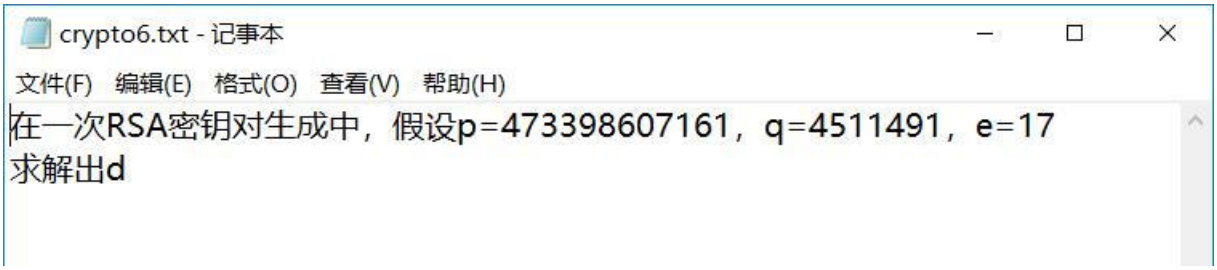
参考博客：
RSA算法原理(一)
RSA算法原理(二)

五、RSA实战

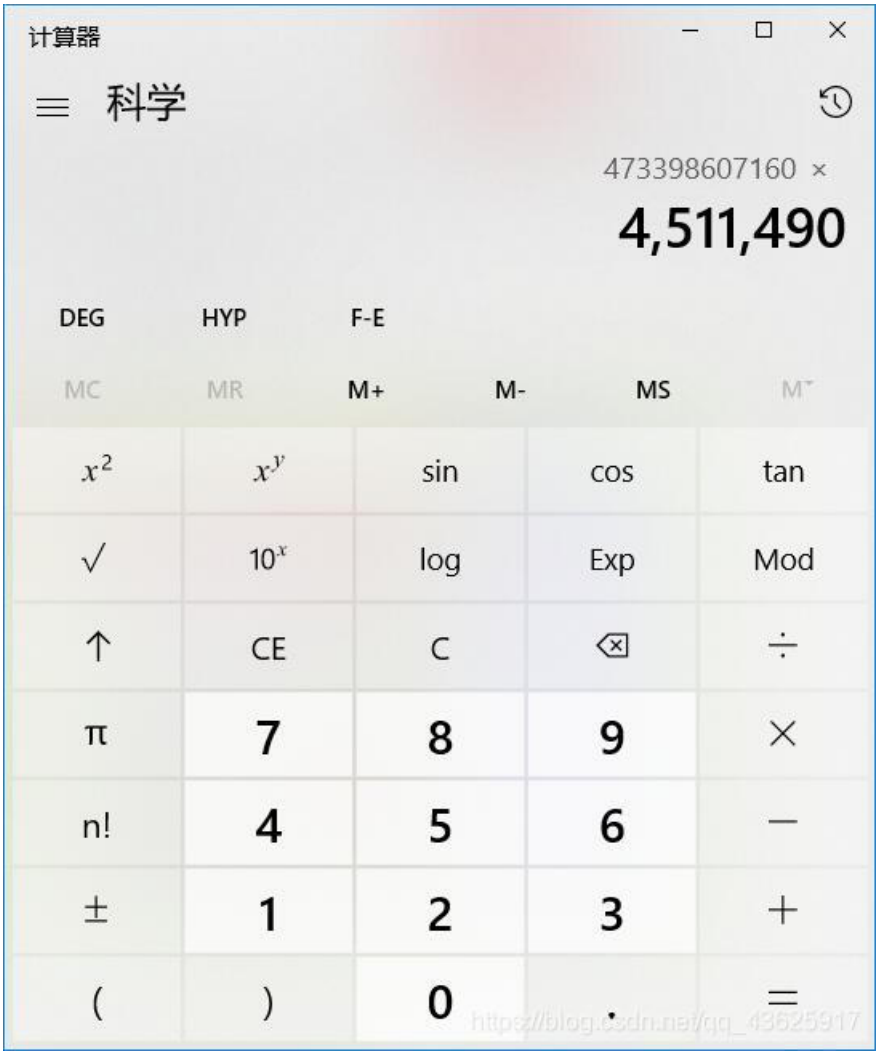
Crypto1：easy_RSA



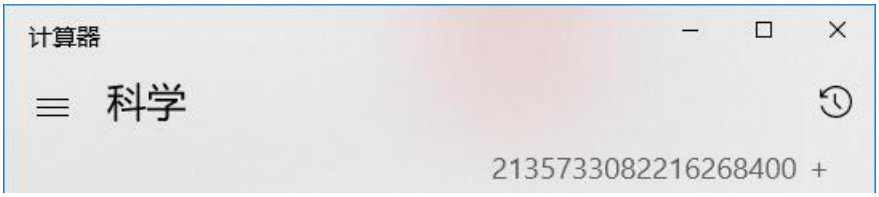
题目提示是RSA，下载题目查看

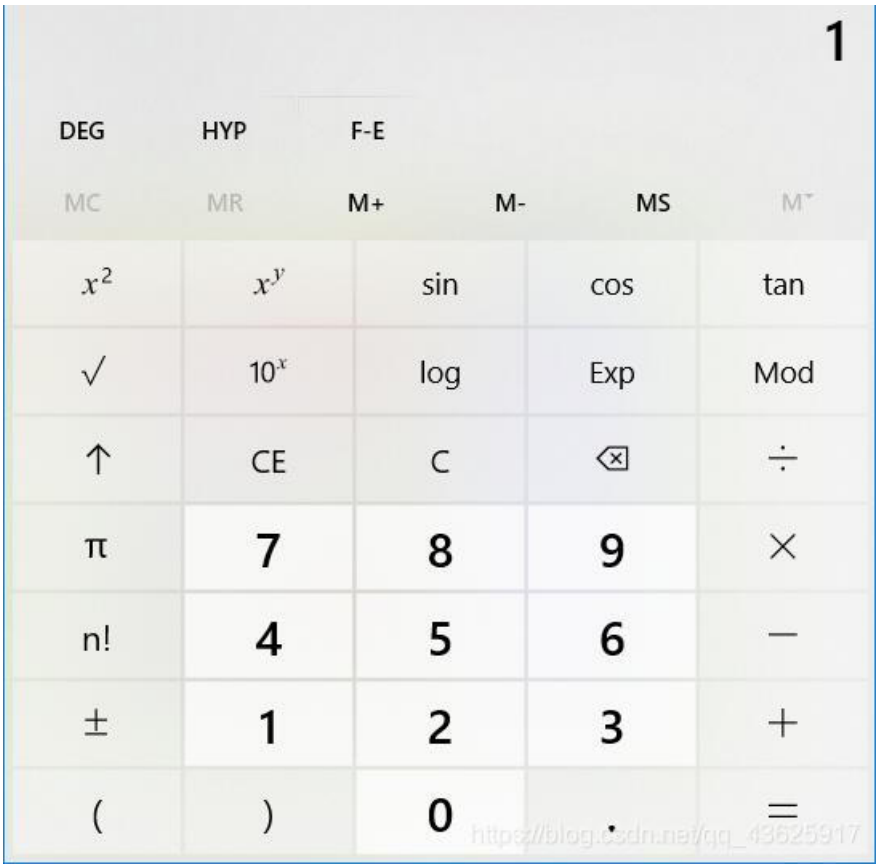


由题目可知，只要计算出私钥d即可
φ(N)=φ§φ(q)=(p-1)(q-1)
ed ≡ 1 (mod φ(N))
所以ed=φ(N)+1，即17d=(p-1)(q-1)+1=473398607160*4511490+1
先计算欧拉函数φ(N)

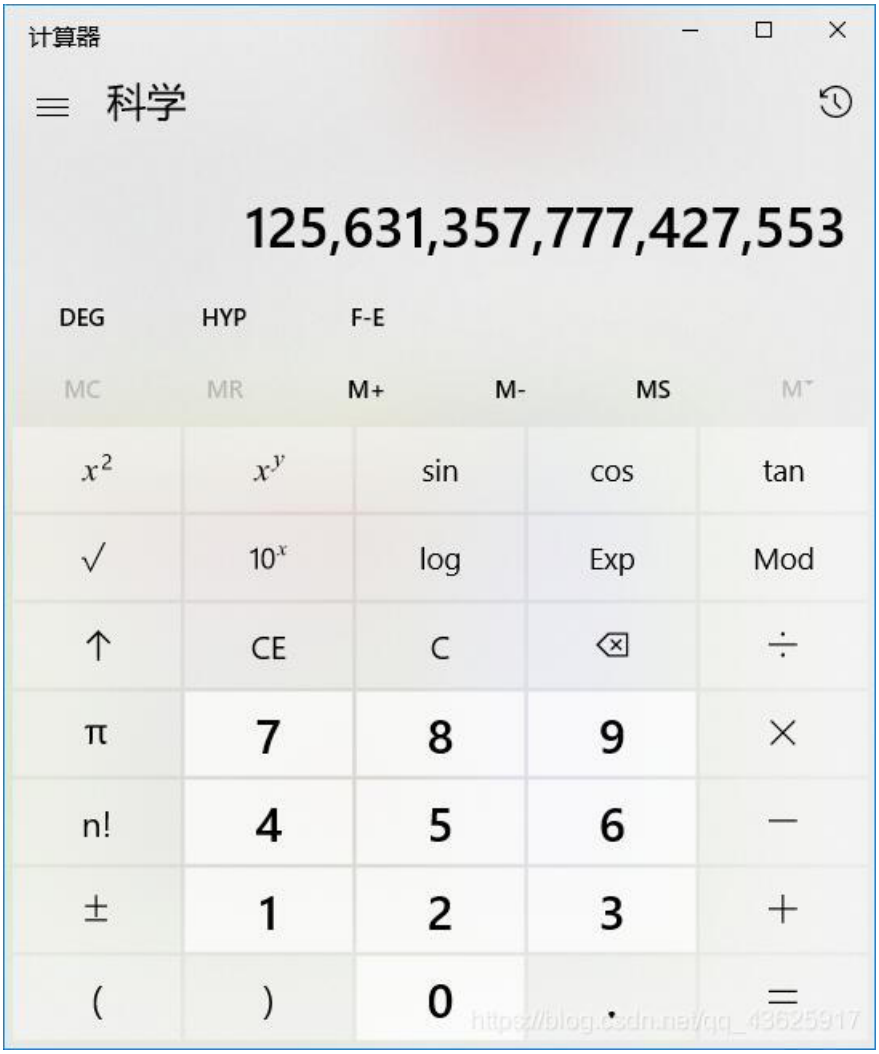


再加1





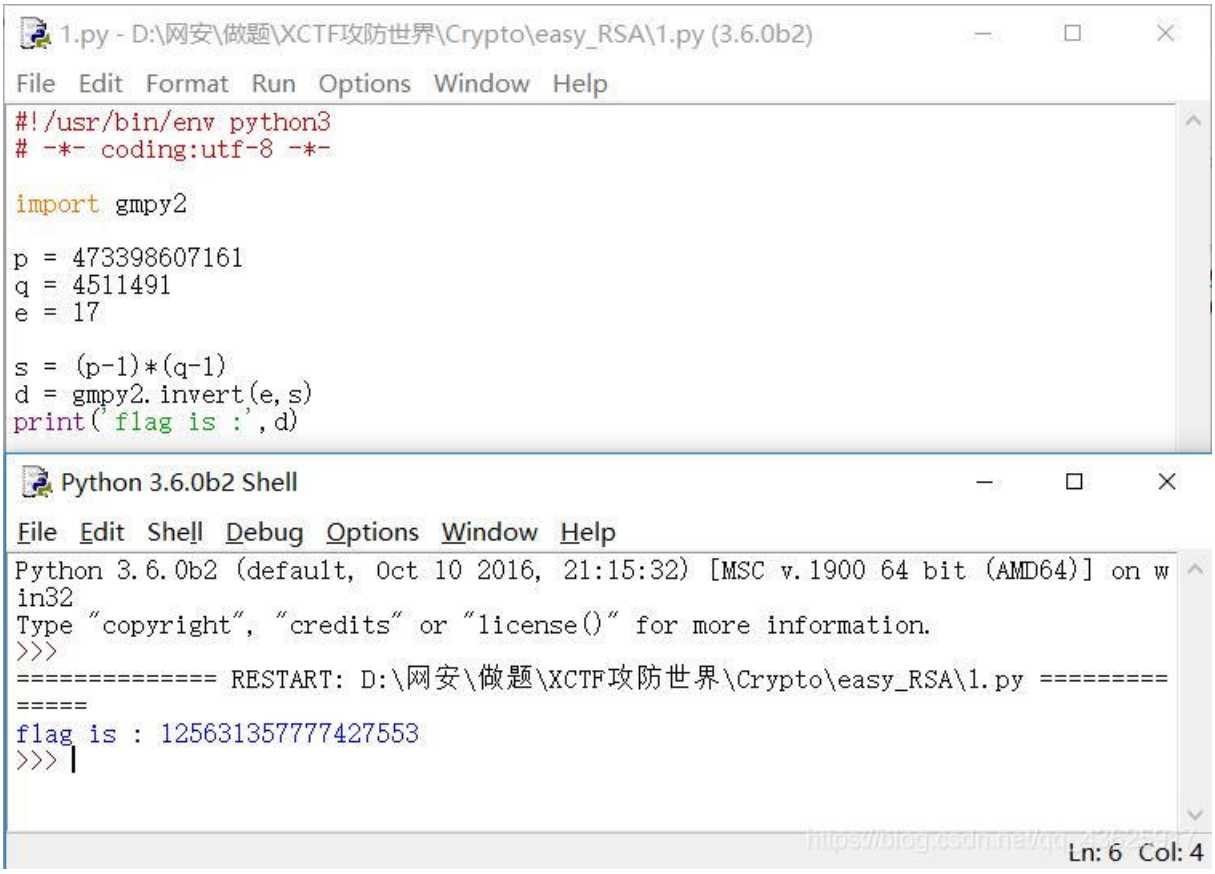
然后除以17即是私钥d，也即是flag内容，加上flag{}提交



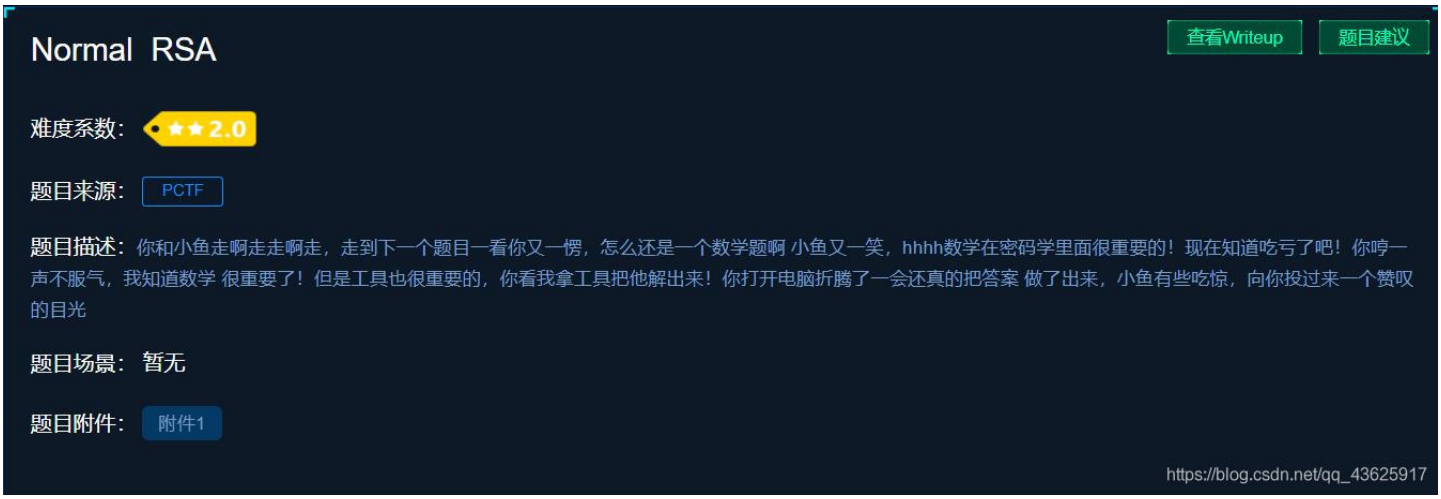
百度发现一个脚本，不过要安装gmpy2库

```
#!/usr/bin/env python3
# -*- coding:utf-8 -*-
import gmpy2

p = 473398607161
q = 4511491
e = 17
s = (p-1)*(q-1)
d = gmpy2.invert(e,s)
print('flag is :',d)
```



Crypto2：Normal_RSA



下载题目，得到flag.enc和pubkey.pem。根据题目提示肯定是需要用到工具。RSA工具及使用

这道题目主要需要用到RSAtools和OpenSSL

1、用OpenSSL得到N

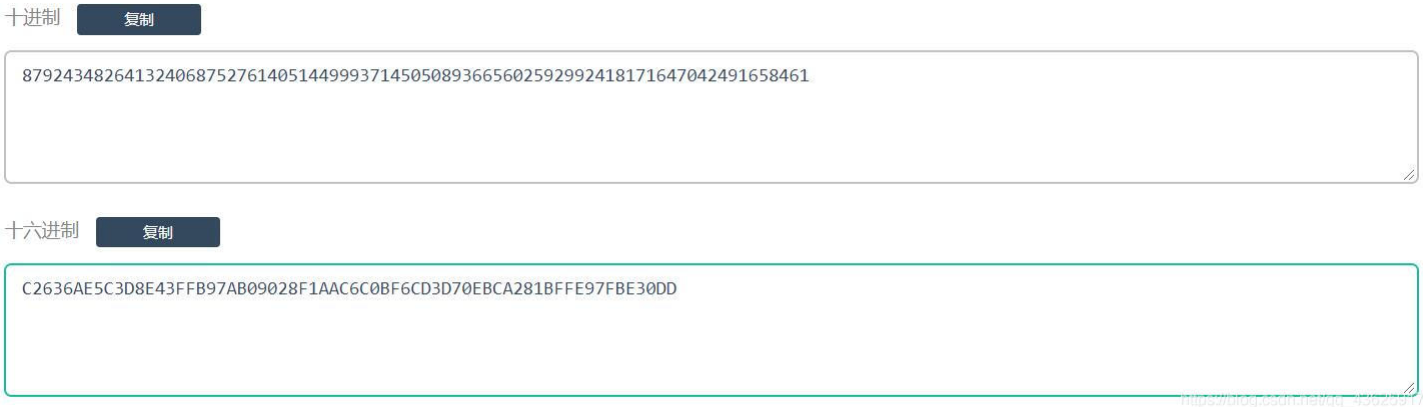
命令：

```
openssl rsa -pubin -text -modulus -in public.pem
```

N=C2636AE5C3D8E43FFB97AB09028F1AAC6C0BF6CD3D70EBCA281BFFE97FBE30DD

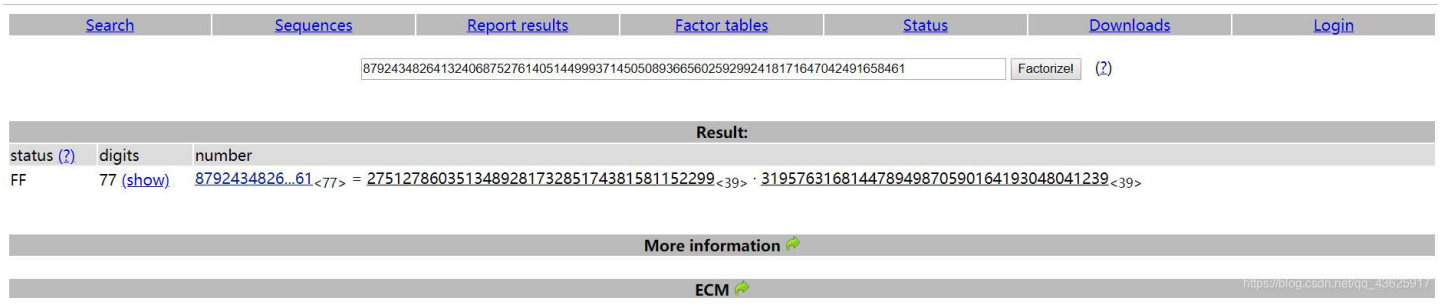
Modulus 是N的值， Exponent是e的值。

16进制转10进制



2、分解N的值，得到p、q

在线大数分解

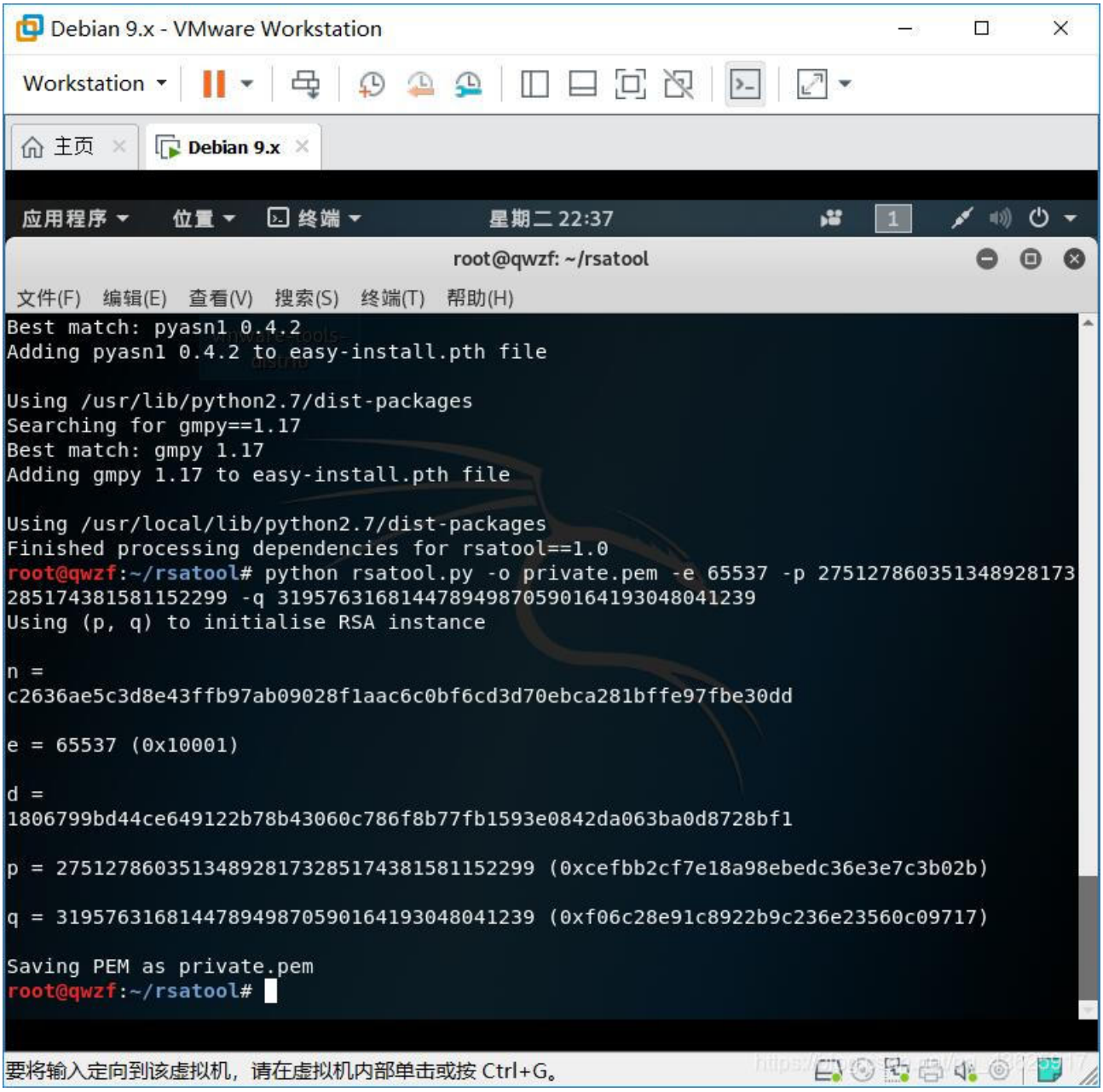


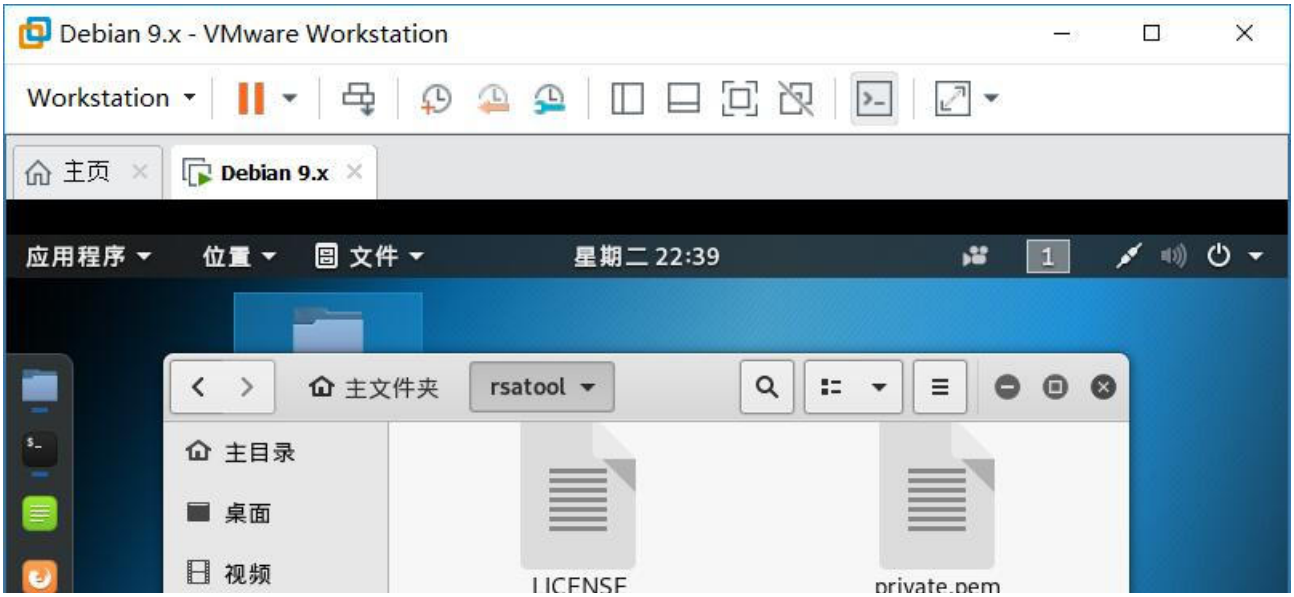
即p=275127860351348928173285174381581152299、q=31957631681447894987059016419304804123 9

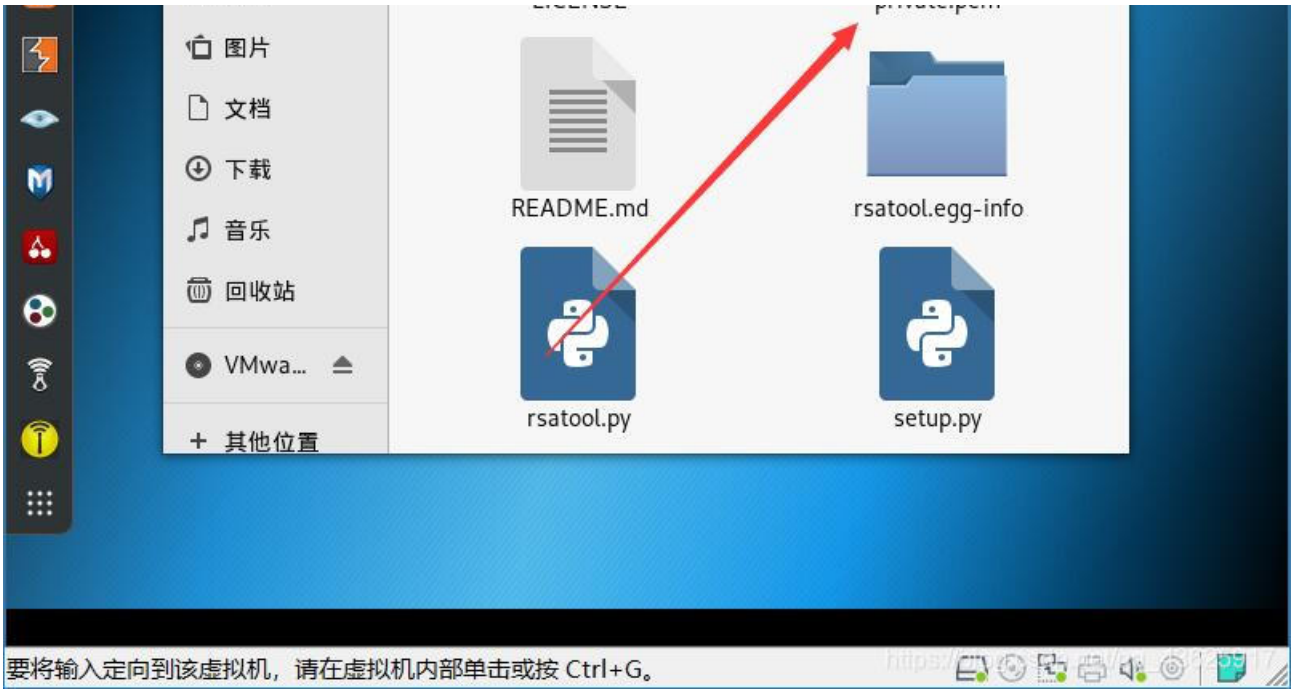
3、用RSAtools生成私钥文件private.pem

命令：

```
python rsatool.py -o private.pem -e 65537 -p 275127860351348928173285174381581152299 -q 319576316814478949870590164193048041239
```



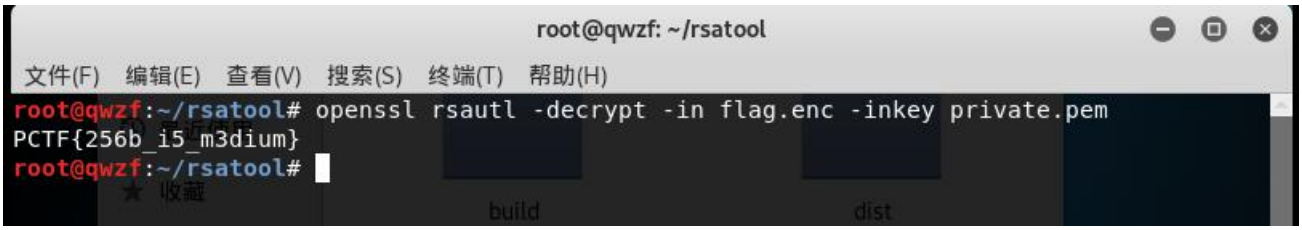




4、用生成的private.pem和OpenSSL对flag.enc文件进行解密

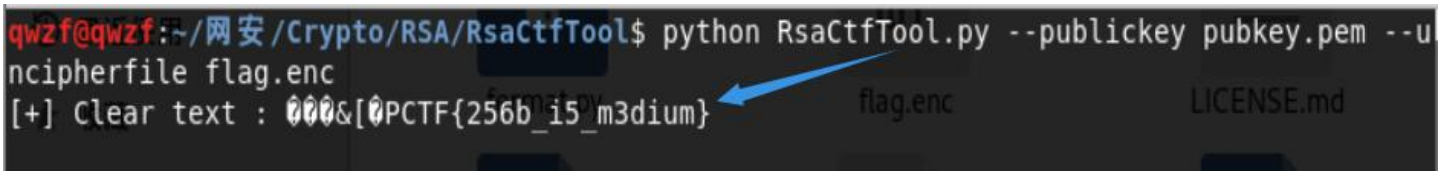
命令：

```
openssl rsautl -decrypt -in flag.enc -inkey private.pem
```



得到flag

当然也有个强大的工具RsaCtfTool



感悟

学习了RSA加密算法之后，对RSA加密解密有了认识。同时为了能顺利使用rsatool，特意又搭了Kali虚拟机。

果然Kali真的是强大的一批。小白进阶ing