蓝鲸安全CTF打卡题——第一期密码学

转载

weixin_34162629 于 2018-09-21 14:35:00 发布 748 收藏 1
文章标签： 密码学 操作系统 5g
原文链接：https://yq.aliyun.com/articles/649034

前言

渣渣一枚，萌新一个，会划水，会喊六六

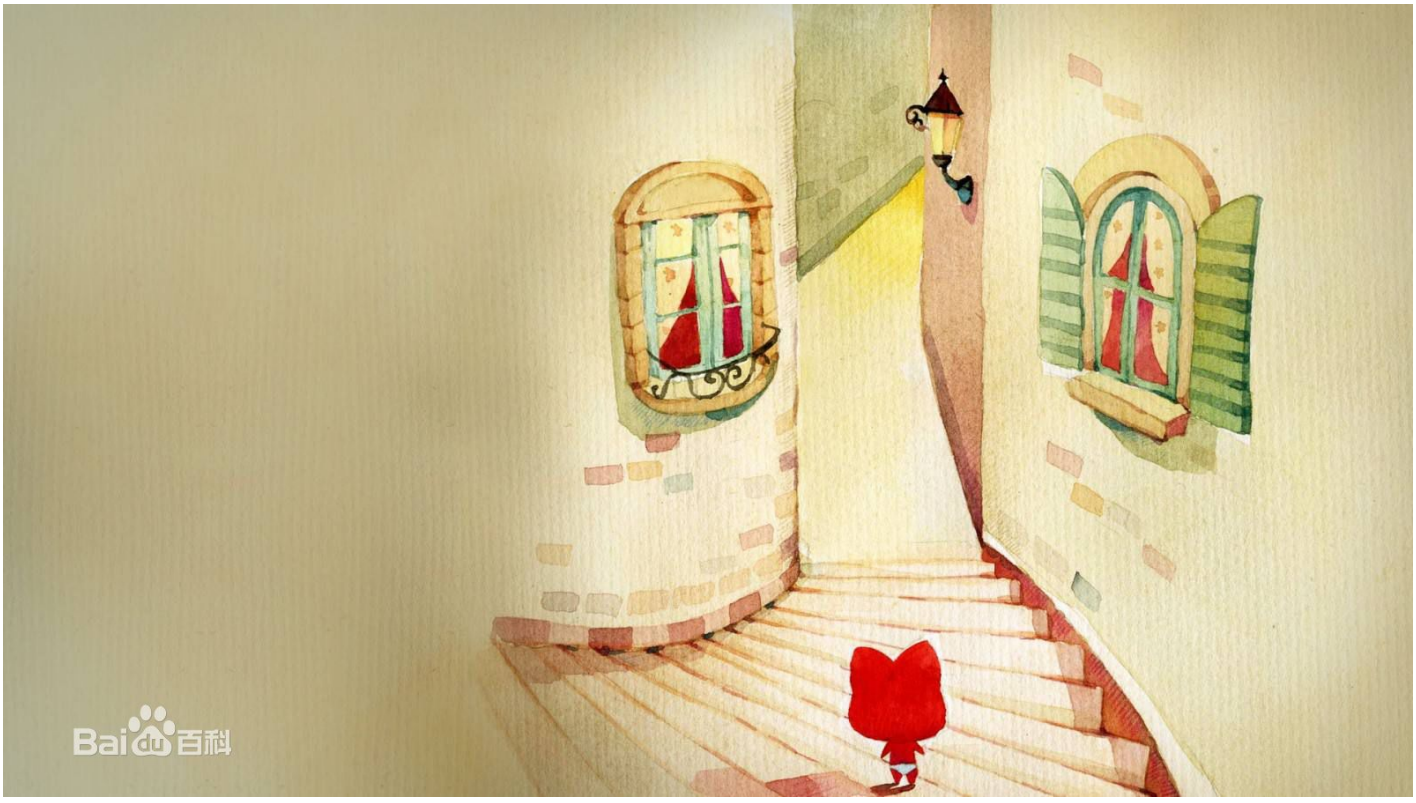
本文首发于先知社区：https://xz.aliyun.com/t/2778

再发于i春秋平台：https://bbs.ichunqiu.com/thread-46119-1-1.html

个人博客：https://www.cnblogs.com/lxz-1263030049/

再过几天就是中秋节了，我打算尽自己最大的能力把蓝鲸安全平台上面的打卡题目的`writeup`整理出来。

有什么错误的地方 希望各位大佬指正(谢谢Orz)



一：检查符号

知识点

摩斯密码、替换密码

解题思路

这道题很容易就可以看出是摩斯密码 摩斯密码就是由'.'和'-'组成的密码 先丢在notepad++里转换下

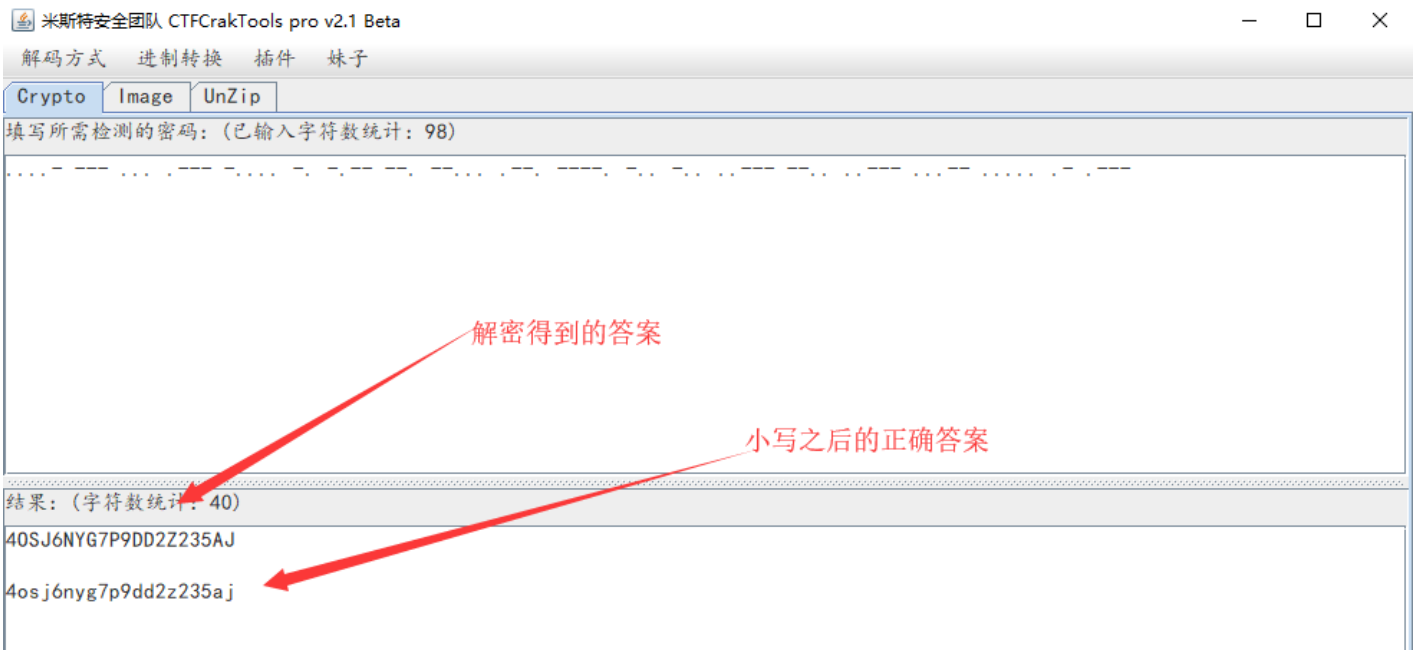
把。换成 空格

把o转换成.

把0转换成-

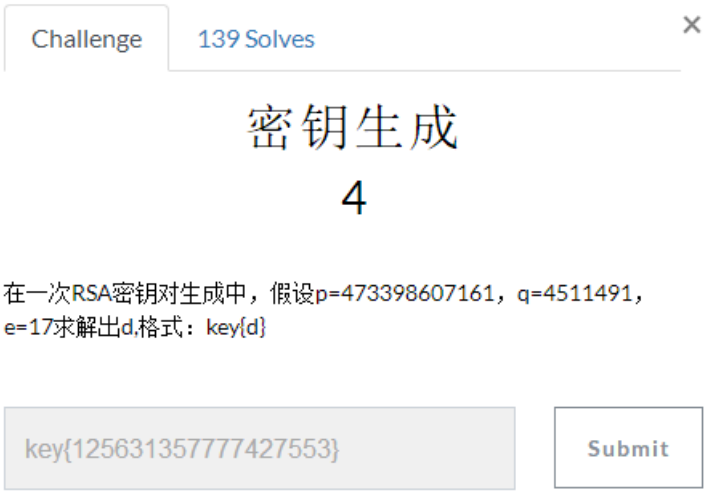
就会得到：....- --- ... .--- -.... -. -.-- --. --... .--. ----. -.. -.. ..--- --.. ..--- ...-- ..... .- .---

放在解密工具里面就会得到：



最后得到答案：**key{4osj6nyg7p9dd2z235aj}**

二： 密钥生成

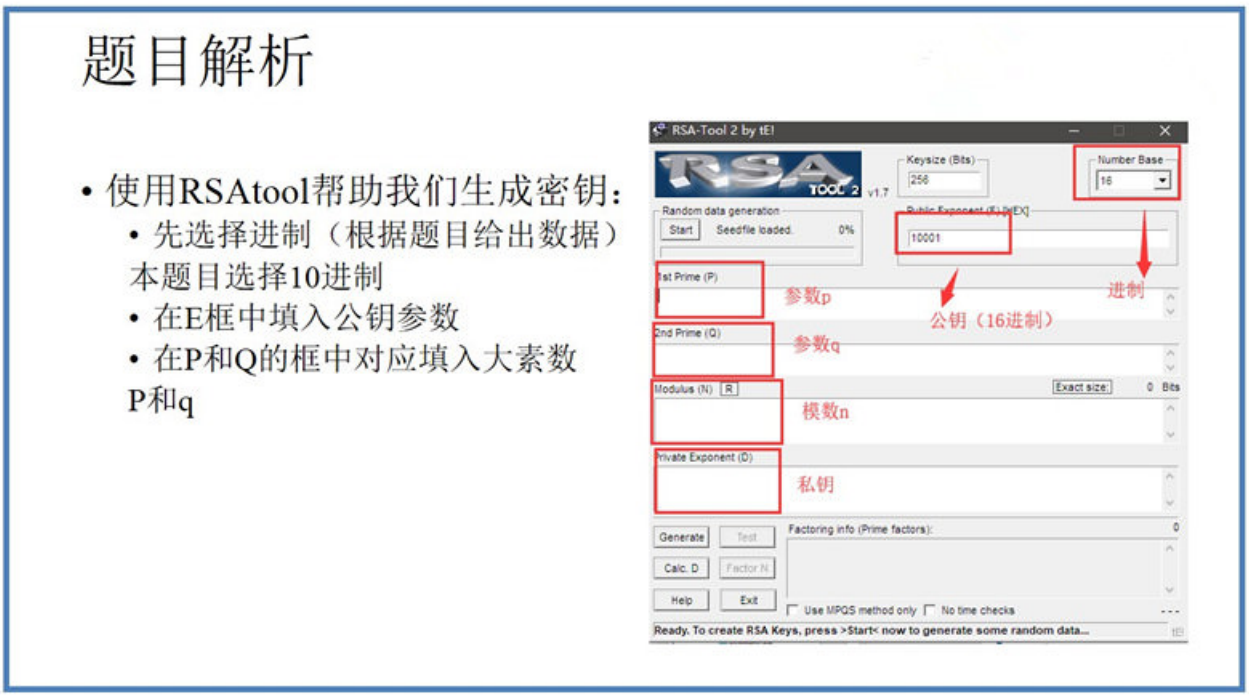


知识点

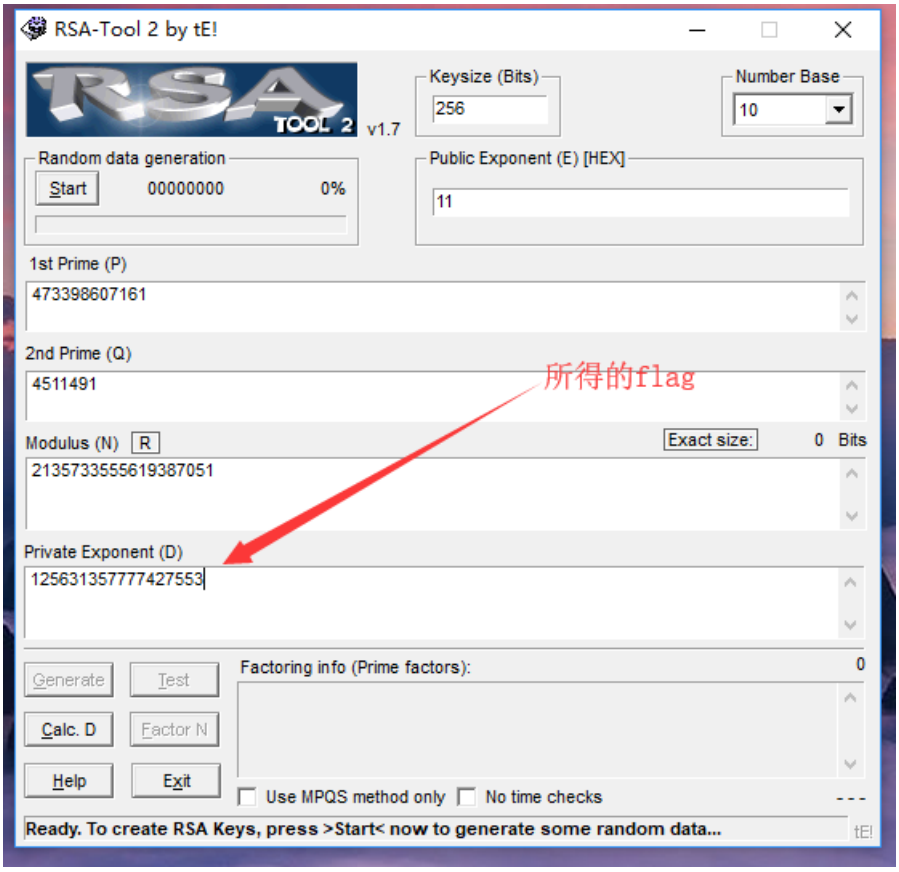
RSA密钥生成 RSA-Tool工具的使用

解题思路

首先放一张关于RSA-Tool工具使用的方法图；



我们只需要根据上面的解释以及下面一些关于RSA算法的资料就可以得到：



即最后答案：**key{125631357777427553}**

三： **RSA解密**

知识点

zip伪加密、RSA解密，openssl用法

解题思路

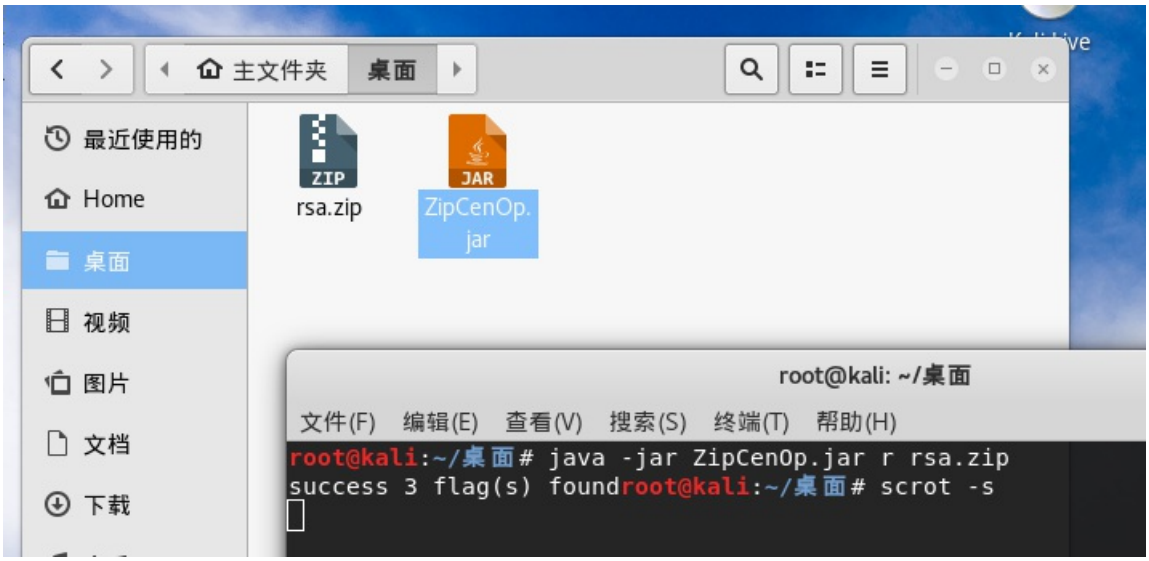
下载下来题目，告诉我们需要解压密码

这里就要涉及到伪加密的知识了

解开伪加密有多种方法，包括用7z，在linux下直接打开，更改伪加密位置处的奇数位为0（偶数）等方法，我选择使用ZipCenOp.jar这个工具来解密

```
# 在window下
$ java -jar ZipCenOp.jar r rsa.zip
```

使用linux



两种都可以的(我个人更偏向于使用linux),打开经过解密之后的伪加密文件：

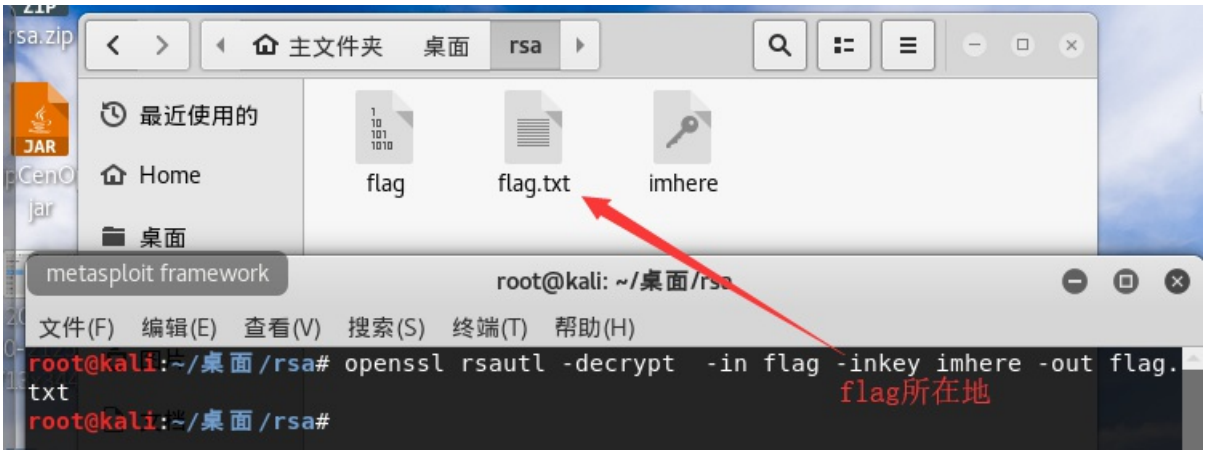
..			文件夹		
flag	128	133	文件	2015/7/26 19	C7CBF558
imhere	887	689	文件	2015/7/13 13	05E6B015

用notepad++打开imhere文件打开看到

```
-----BEGIN RSA PRIVATE KEY-----
MIICXQIBAAKBgQCw44GKtDqBlD2hTQVm9oMyp7w3C8i4tCE0zsWTWtV0gVaofyF9
idBeZR3AX/crKnlX1QC6YD/pUJJRPzoKY+bk0YFT64mca7oW2fP719LFiQReirGM
fs4n9mvIYeBx1TtHfFwWBDeIHcjP33eR1hue69Dq5tZYRl2e3SrUJXvRFwIDAQAB
AoGAMUQcF1KdHOv5wkweXg/4eIpJHJe2nuLkgL26P5FD9D/1r9ZAsKNKmo/VGnhf
8fDRfQoBOueFxWjAZ8qRUsWCT+/0ZDs0xCKrQ7YuxO2p9HV1sMQF74D2TVcoFZ4d
P5sjTvs0MutaoTdU0YDNO/ssqk3We2e11tr6ii3HmHtquwkCQQDezreUOIjWV30n
ndoGwYf9LsXoEZVMSI6vw/SqiqOvagN3mufApNfj+JrZ6LvV0hHbYfaVkEUvqMyq
BKAQapNFAkEAyz2RlugQ20fVzUkzDCSF8ByWjK4GgAqQ/qioXJ9tSPcsgV1yUem4
WM7rTBDWaohHT3N+vhAcsszQ2VJZy6vKqwJBAL2liH7CLD79Uwswgg70FfM8J7oj
lUfMDp+vFIdA4JiDjRX2JUNFTHm/9tZ6Eb+rQgXQ+ZlOpoUtkZ85tqCihl0CQCQI
R16MyChIRRR/LMizVPer6dkJJWff97LebfL15OcxwzcwPQtet2svTDIRLiJ3BMWG
QWsq6hudCk3tNrRQQb8CQQCTcs0uWBe6klDKWLCPEYxuTqB9xksQTmlqvdwfdCZF
BWaxHtc/ByfAisj9cfq2CY/fEoeGqLagZ5tG5G81V9VZ
-----END RSA PRIVATE KEY-----
```

看到是RSA私钥文件，说明我们要用这个私钥去解密我们的flag文件 这里就需要用到openssl文件了 kali里自带了openssl工具

使用命令：openssl rsautl -decrypt -in flag -inkey imhere -out flag.txt



打开flag.txt文件就会得到答案：**key{c42bcf773d54cf03}**

四： 公平交易

知识点

playfair加密 pycipher库使用

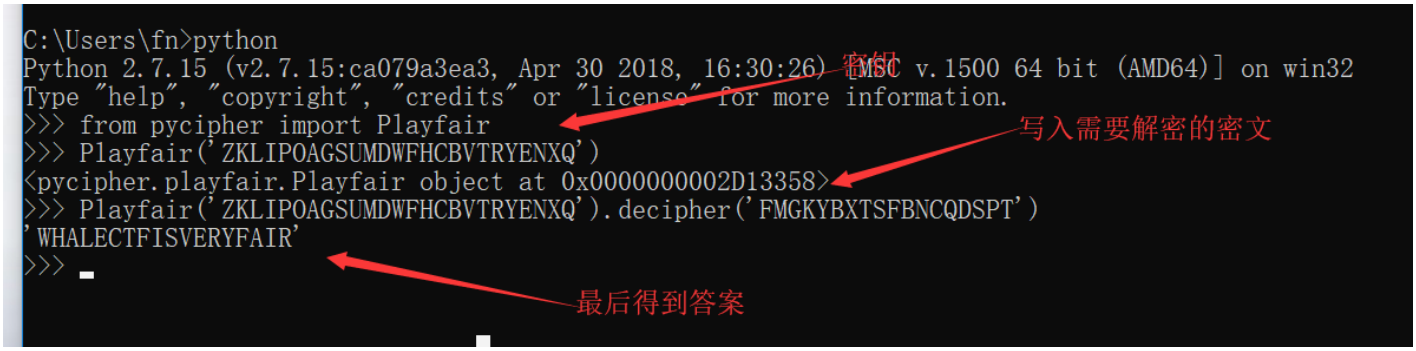
解题思路

第一种方法：

使用pycipher库，就可以得到答案

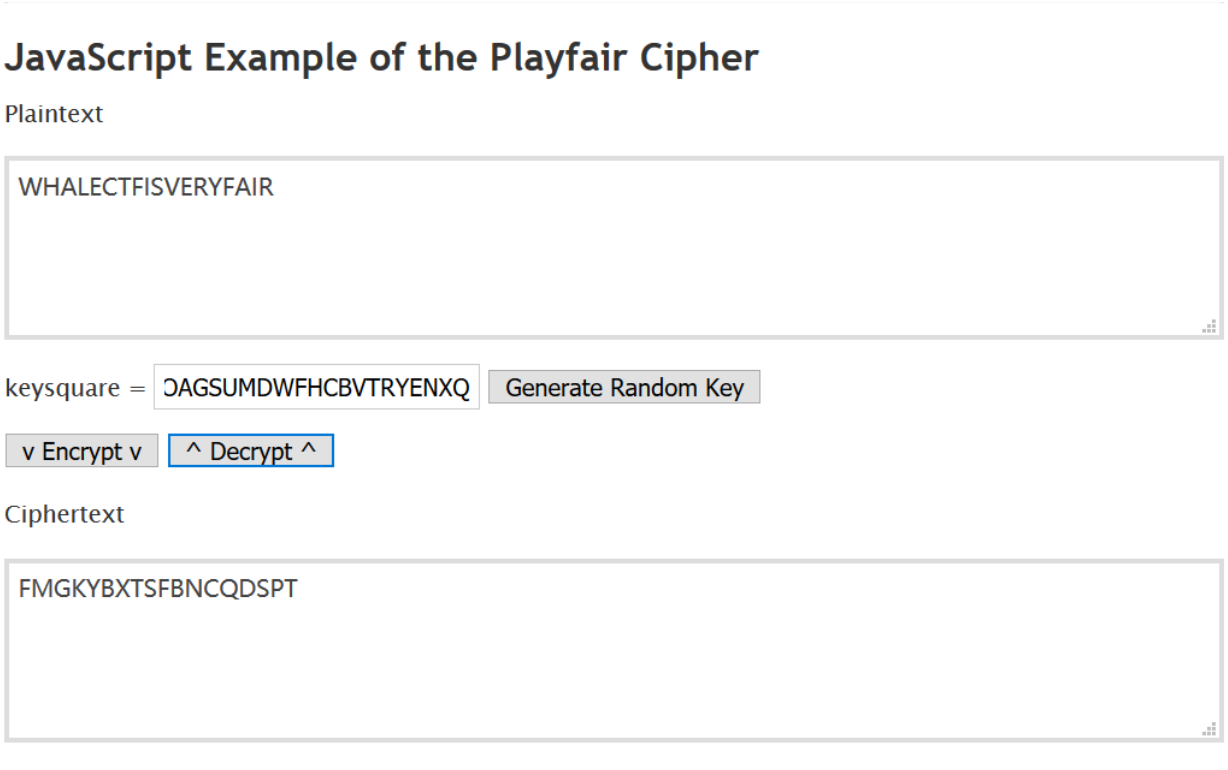
由于pycipher库是python中的第三方库，所以使用的时候需要安装即：pip install pycipher

使用pycipher就可以得到答案：



第二种方法：

使用在线解密工具：http://www.practicalcryptography.com/ciphers/classical-era/playfair/



最后得到答案：**key{WHALECTFISVERYFAIR}**

五：填空题

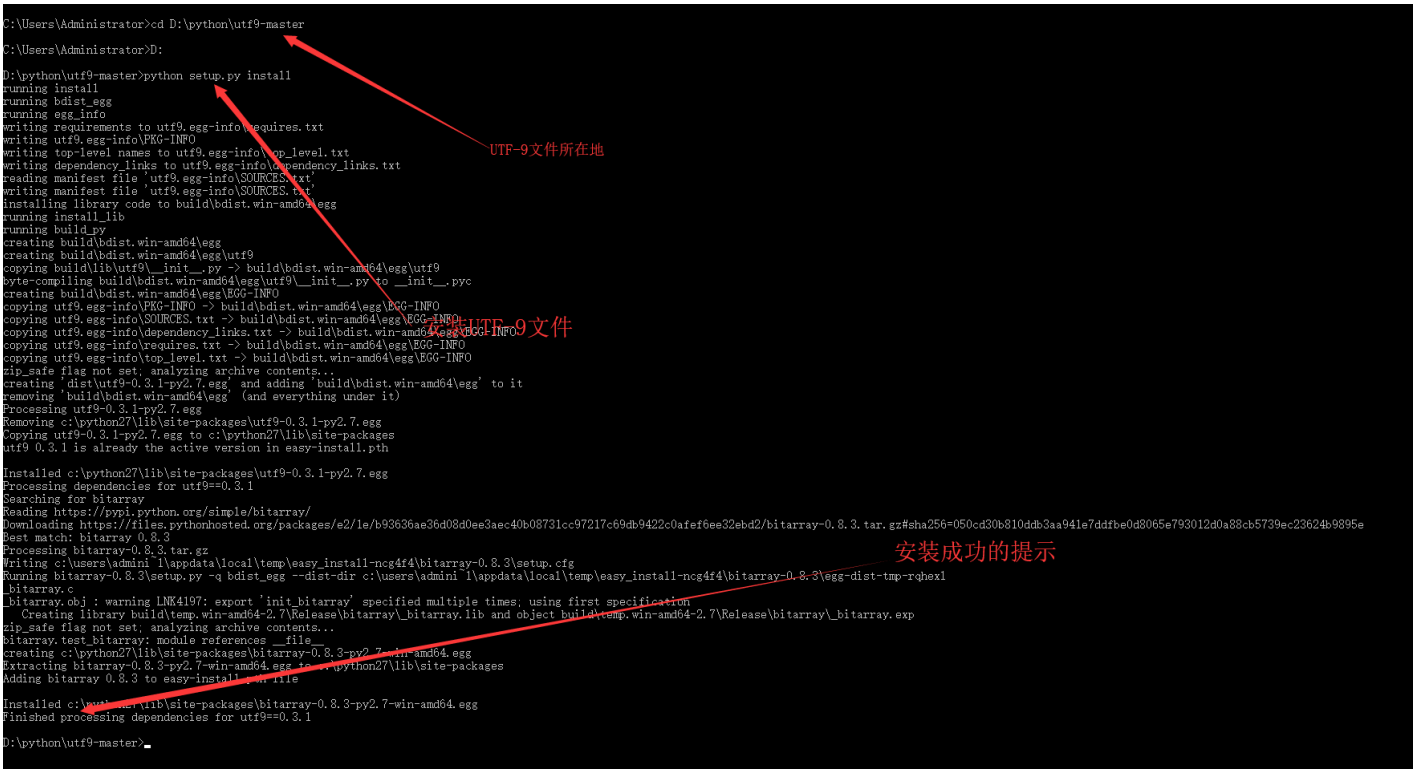
知识点

utf-9编码，替换密码，进制ascii码转换

解题思路

下载得到一个叫做flag_is_here_rfc4042的文件 看到rfc4042，知道了应该是utf-9编码了文件
用python2来解，我们需要先安装VCForPython27.msi

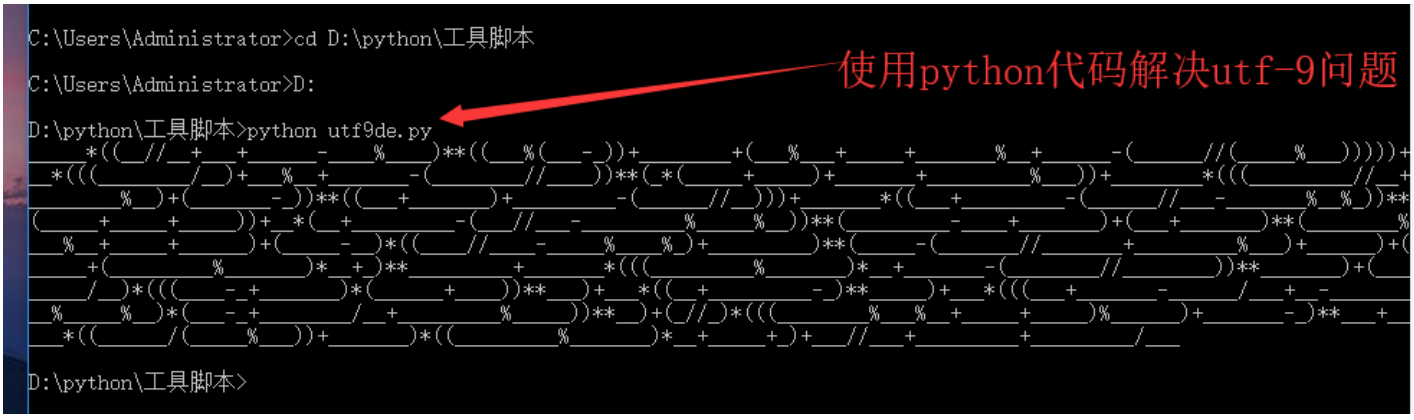
接下来就是需要安装UTF-9文件



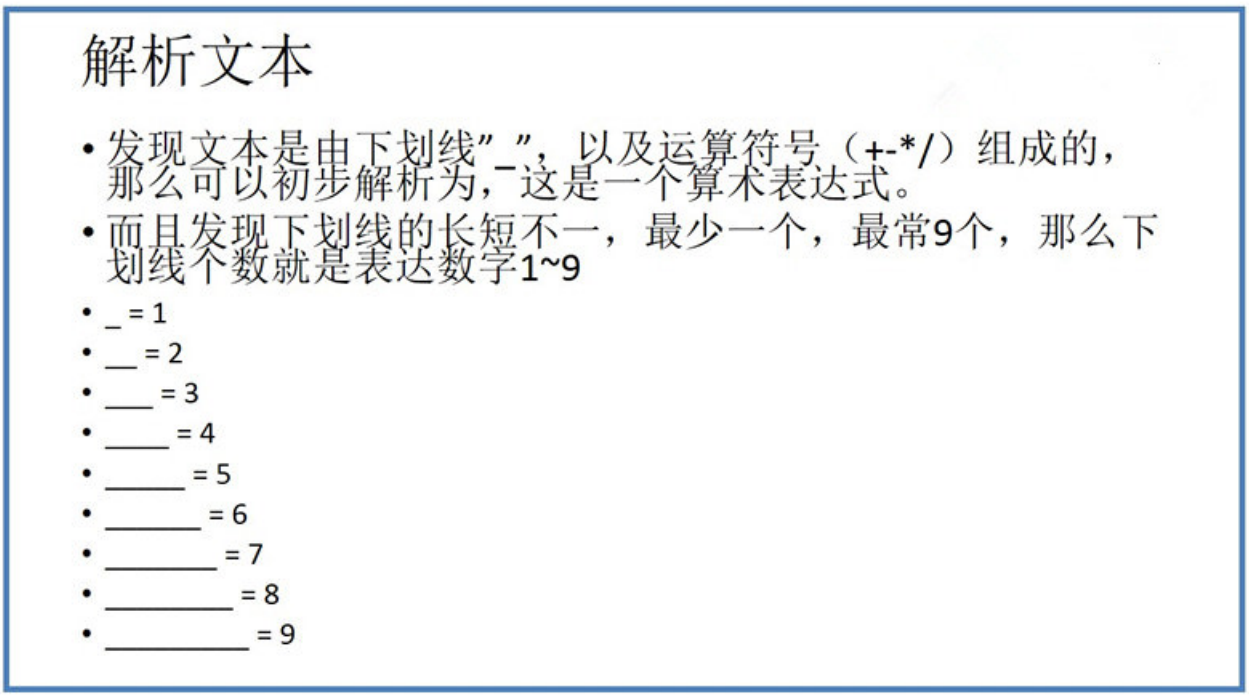
关于UTF-9中的问题，我们只需要写一段python代码就可以解决了：

```
import utf9
f1 = open('flag_is_here_rfc4042','r')
f2 = open('flag.txt','w')
str1 = f1.read()
print utf9.utf9decode(str1)
f2.write(utf9.utf9decode(str1))
```

我们采用的是直接读取flag_is_here_rfc4042文件的方法是为了避免复制粘贴时格式出现问题,下面就是具体的操作方法：



我们先来分析一下关于解密出来的内容：

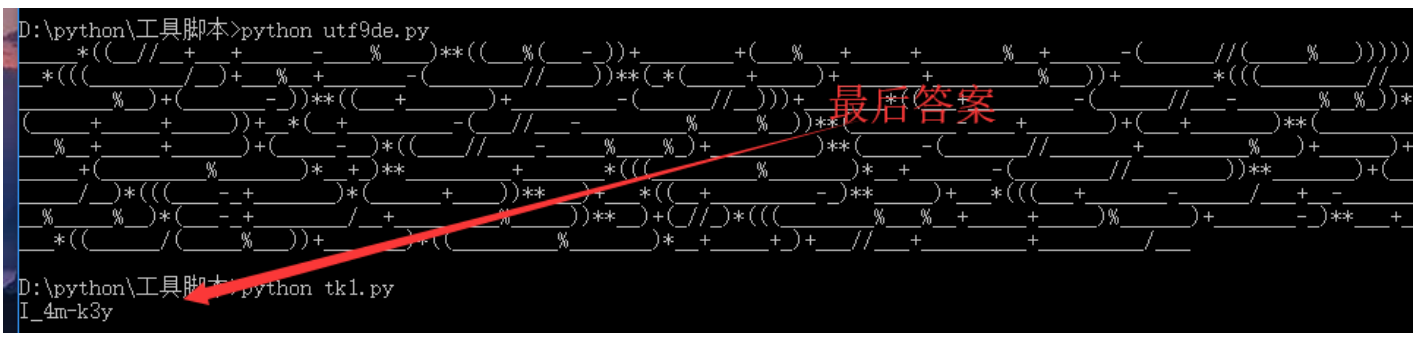


我们由以上的分析可以写出脚本：

```
import binascii
_ = 1
__ = 2
___ = 3
____ = 4
_____ = 5
______ = 6
_______ = 7
________ = 8
_________ = 9

a = _____*((__//__+___+______-____%____)**((___%(___-_))+________+(___%___+_____+_______%__+______-(______/
a = hex(a)[2:][:-1]
a = binascii.a2b_hex(a)
print a
```

运行之后就会得到：



最后得到答案：**key{I_4m-k3y}**

六：RSA破解

知识点

RSA模数分解，RSA解密 openssl使用方法

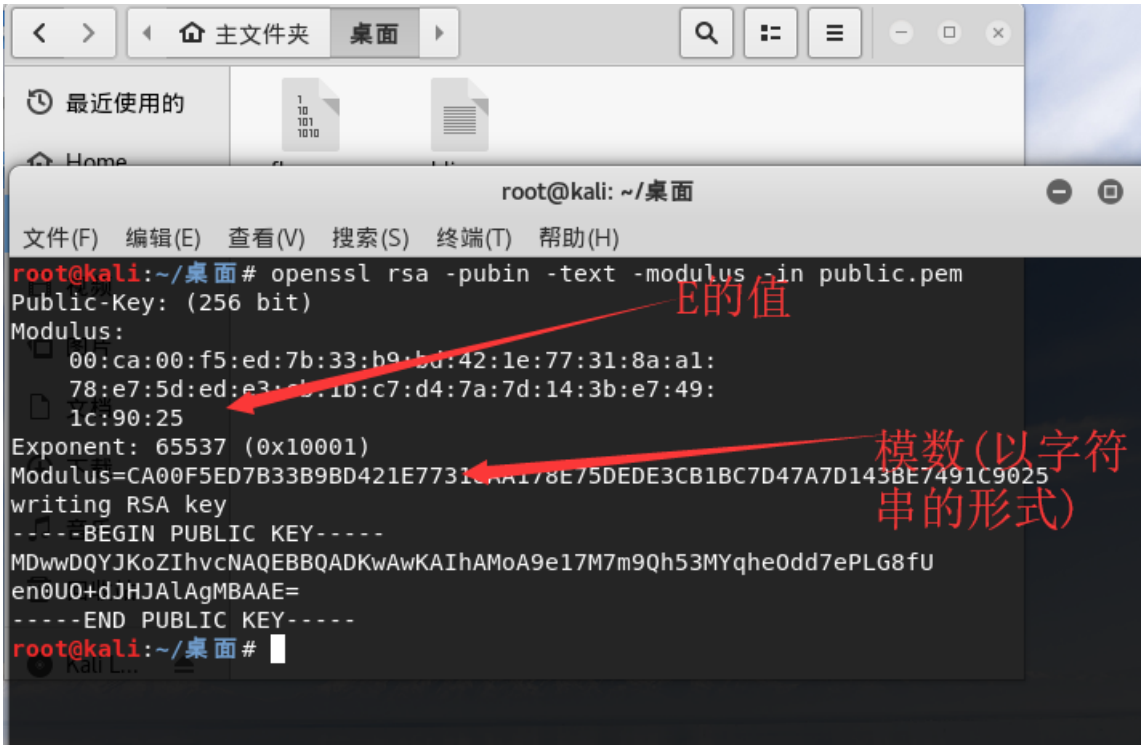
解题思路

下载并打开压缩包文件就会发现：

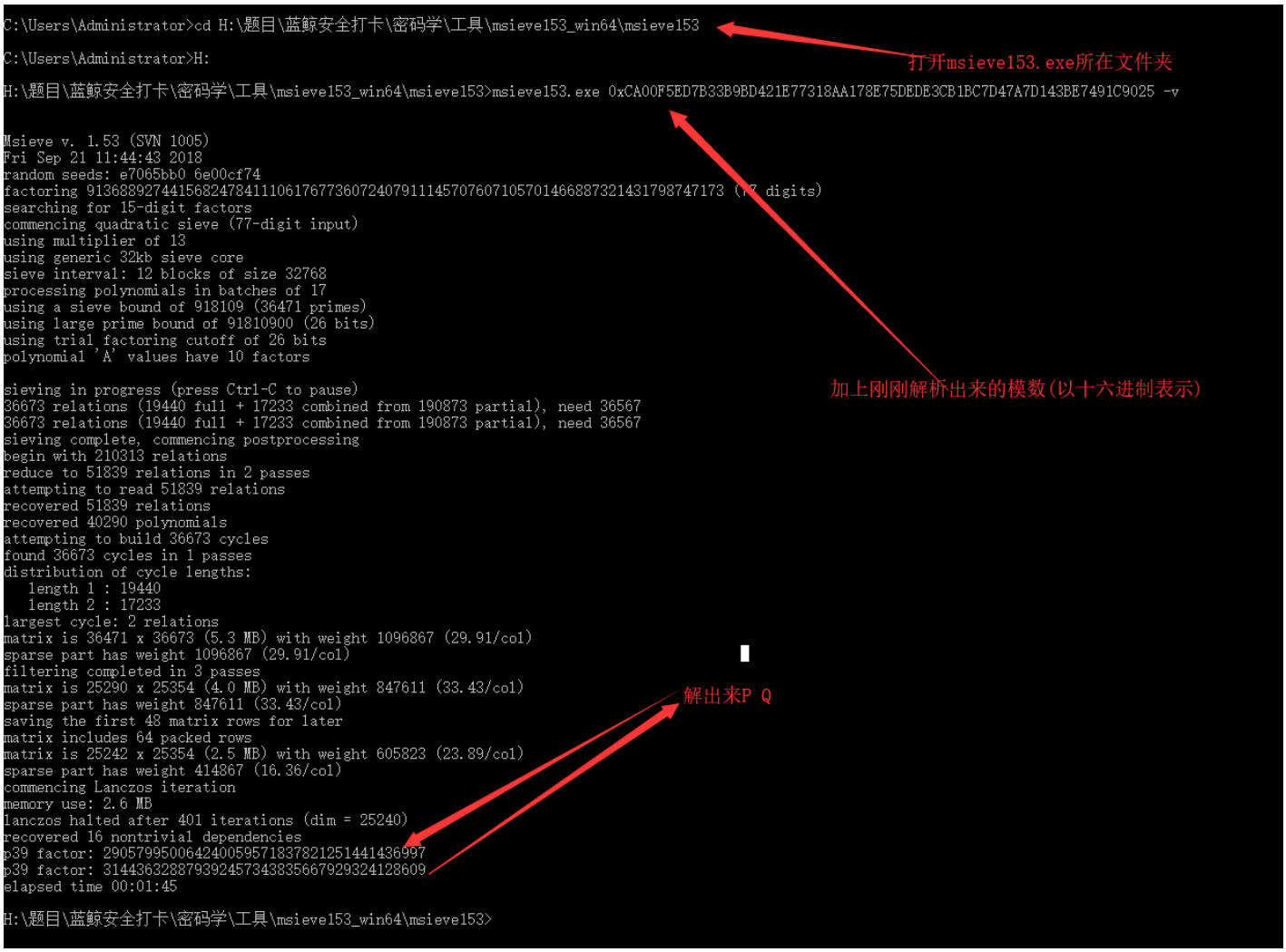
这是一个加密的flag文件和公钥文件 我们先通过openssl来分析一下公钥是否可以被攻击

使用linux，其中的命令是：

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



我们接着使用msieve就可以了



就会得到相应的P Q

我们需要使用脚本生成使用文件

```
import math

import sys

from Crypto.PublicKey import RSA
keypair = RSA.generate(1024)

keypair.p = 290579950064240059571837821251441436997

keypair.q = 31443632887939245734383566792932412860 9

keypair.e = 65537

keypair.n = keypair.p * keypair.q

Qn = long((keypair.p-1) * (keypair.q-1))

i = 1

while (True):

x = (Qn * i ) + 1

if (x % keypair.e == 0):

keypair.d = x / keypair.e

break

i += 1

private = open('private.pem','w')

private.write(keypair.exportKey())

private.close()
```

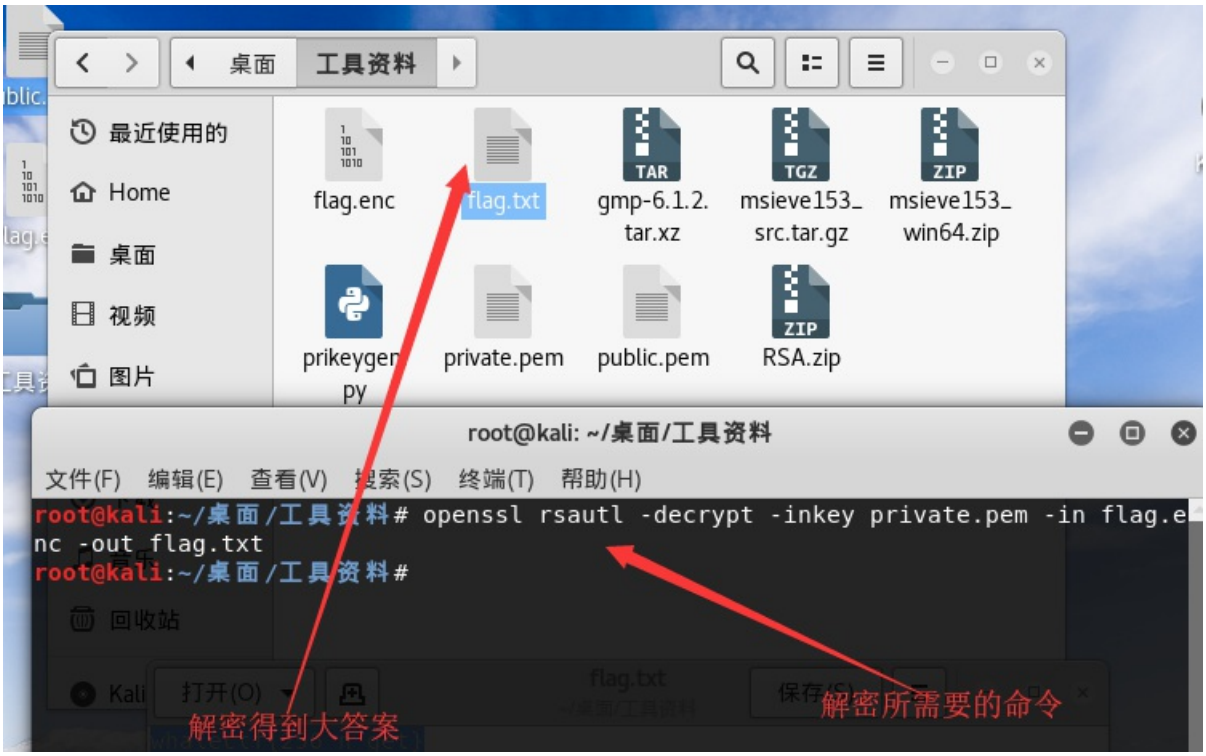
使用linux运行脚本很简单 进入文件直接使用命令：

```
python prikeygen.py
```

就会生成相应的私钥

```
-----BEGIN RSA PRIVATE KEY-----
MIGpAgEAAiEAygD17Xszub1CHncxiqF4513t48sbx9R6fRQ750kckCUCAwEAAQIg
XbBsX6TQrMj2raKiu6WAqRtv86ps6lbgXsftak7iqgECEQDam6mnJeZJM1o5QlZY
XKlFAhEA7I478Iv1HnDUJ/xGsCkJYQIQFvqv7bMNLvqn7Ebt3qH25QIQFwZlKS3G
Rxc+X0H782ubIQIQL2kzJ1i8luHD5eQlbYjXgg==
-----END RSA PRIVATE KEY-----
```

接下来就是需要使用openssl命令了



就会得到答案：**whalectf{256_n_get}**

参考资料：

RSA算法原理（一）： http://www.ruanyifeng.com/blog/2013/06/rsa_algorithm_part_one.html

RSA算法原理（二）： http://www.ruanyifeng.com/blog/2013/07/rsa_algorithm_part_two.html

CTF中那些脑洞大开的编码和加密： https://www.tuicool.com/articles/2E3lNnm

UTF-9: https://github.com/enricobacis/utf9

CTF中RSA的常见攻击方法： https://www.anquanke.com/post/id/84632

您可以考虑给博主来个小小的打赏以资鼓励，您的肯定将是我最大的动力。

作者：落花四月
出处：https://www.cnblogs.com/lxz-1263030049/
关于作者：潜心于网络安全学习。如有问题或建议，请多多赐教！