NWU-moectf_crypto

原创

LittleKeKe_rong 于 2019-04-11 18:21:42 发布 424 收藏

分类专栏： writeup（平台_内容）

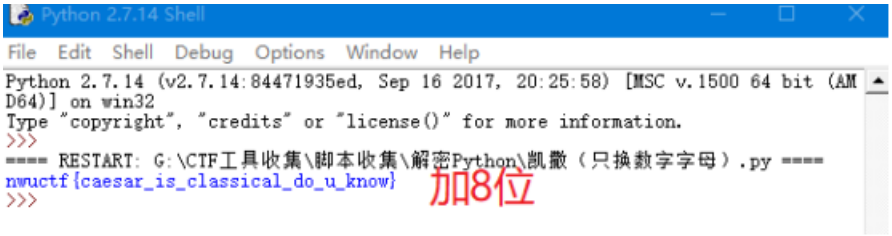
本文链接：https://blog.csdn.net/weixin_44713659/article/details/89217089

rsa还是做不出啊。。。

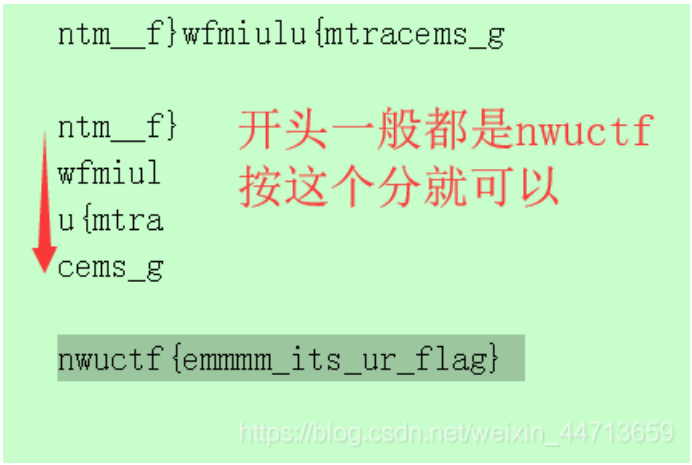
Caesar's code

fomulx{uswksj_ak_udskkausd_vg_m_cfgo}

猜测前面为nwuctf，对比相差8



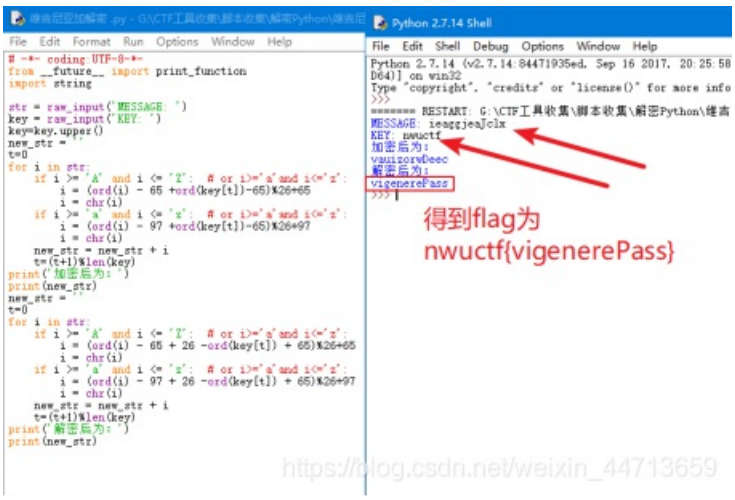
栅栏密码



nwuctf{emmmm_its_ur_flag}

维吉尼亚密码

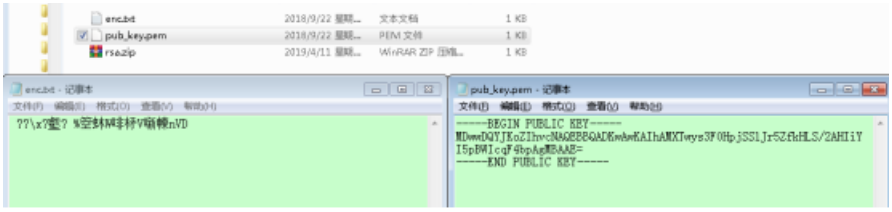
密文（注意有一个大写字母）：ieaggjeaJclx
hint: nwuctf



维吉尼亚加解密规则：
设密钥K=k1k2…kd,明文与密文表中均包含n个字母
明文M=m1m2… 密文C=c1c2…
加密：Ci=(mi+ki)mod n
解密：Mi=(Ci-ki+n)%n
附上Python：

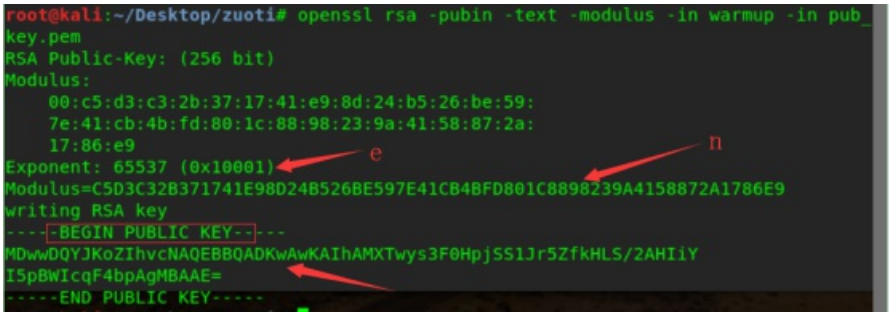
```
# -*- coding:UTF-8-*-
from __future__ import print_function
import string

str = raw_input('MESSAGE: ')
key = raw_input('KEY: ')
key=key.upper()
new_str = ''
t=0
for i in str:
    if i >= 'A' and i <= 'Z':  # or i>='a'and i<='z':
        i = (ord(i) - 65 +ord(key[t])-65)%26+65
        i = chr(i)
    if i >= 'a' and i <= 'z':  # or i>='a'and i<='z':
        i = (ord(i) - 97 +ord(key[t])-65)%26+97
        i = chr(i)
    new_str = new_str + i
    t=(t+1)%len(key)
print('加密后为: ')
print(new_str)
new_str = ''
t=0
for i in str:
    if i >= 'A' and i <= 'Z':  # or i>='a'and i<='z':
        i = (ord(i) - 65 + 26 -ord(key[t]) + 65)%26+65
        i = chr(i)
    if i >= 'a' and i <= 'z':  # or i>='a'and i<='z':
        i = (ord(i) - 97 + 26 -ord(key[t]) + 65)%26+97
        i = chr(i)
    new_str = new_str + i
    t=(t+1)%len(key)
print('解密后为: ')
print(new_str)
```

Open the door of Crypto



参考大神的writeup：http://cdusec.happyhacking.top/?post=27
OpenSSL使用：https://www.cnblogs.com/aLittleBitCool/archive/2011/09/22/2185418.html
OpenSSL下载地址：https://github.com/openssl/openssl
先用OpenSSL解密得到公钥

```
openssl rsa -pubin -text -modulus -in warmup -in pub_key.pem
```



注意n要base64一下，然后用yafu分解，得到：

p = 305657283092588037926335272811666485179

q = 292745463160071549856213815233114677163

然后用Python跑出私钥private.pem

```
# coding=utf-8
import math
import sys
from Crypto.PublicKey import RSA

keypair = RSA.generate(1024)

keypair.p = 305657283092588037926335272811666485179
keypair.q = 292745463160071549856213815233114677163
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()
```

最后用OpenSSL解密密文enc.txt，得到flag.txt即可

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