

NWU-moectf_crypto

原创

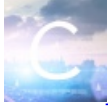
[LittleKeKe_rong](#) 于 2019-04-11 18:21:42 发布 424 收藏

分类专栏: [writeup \(平台_内容\)](#)

版权声明: 本文为博主原创文章, 遵循 [CC 4.0 BY-SA](#) 版权协议, 转载请附上原文出处链接和本声明。

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

版权



[writeup \(平台_内容\)](#) 专栏收录该内容

5 篇文章 0 订阅

订阅专栏

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

```
Python 2.7.14 Shell
File Edit Shell Debug Options Window Help
Python 2.7.14 (v2.7.14:84471935ed, Sep 16 2017, 20:25:58) [MSC v.1500 64 bit (AMD64)] on win32
Type "copyright", "credits" or "license()" for more information.
>>>
==== RESTART: G:\CTF工具收集\脚本收集\解密Python\凯撒(只换数字字母).py ====
nwuctf{caesar_is_classical_do_u_know} 加8位
>>>
```

栅栏密码

```
ntm__f}wfmiulu {mtracems_g

ntm__f} 开头一般都是nwuctf
wfmiul 按这个分就可以
u {mtra
cems_g

nwuctf{emmmm_its_ur_flag}
```

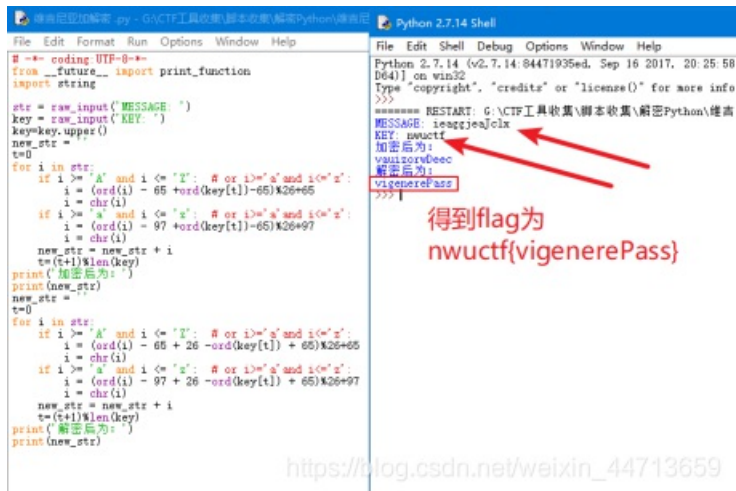
https://blog.csdn.net/weixin_44713659

nwuctf{emmmm_its_ur_flag}

维吉尼亚密码

密文 (注意有一个大写字母) : feaggjeaJclx

hint: `nwuctf`



```
# -*- 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)
```

Python 2.7.14 (v2.7.14:84471935ed, Sep 16 2017, 20:25:58 D64) on win32
Type "copyright", "credits" or "license()" for more info
>>>
***** RESTART: C:\CTF工具收集\脚本收集\解密Python\维吉
MESSAGE: feaggjeaJclx
KEY: nwuctf
加密后为:
vwuztornBeec
解密后为:
nwuctf{vigenerePass}
>>>

得到flag为
nwuctf{vigenerePass}

https://blog.csdn.net/weixin_44713659

维吉尼亚加解密规则:

设密钥 $K=k_1k_2\dots k_d$,明文与密文表中均包含 n 个字母

明文 $M=m_1m_2\dots$ 密文 $C=c_1c_2\dots$

加密: $C_i=(m_i+k_i)\bmod n$

解密: $M_i=(C_i-k_i+n)\%n$

附上Python:

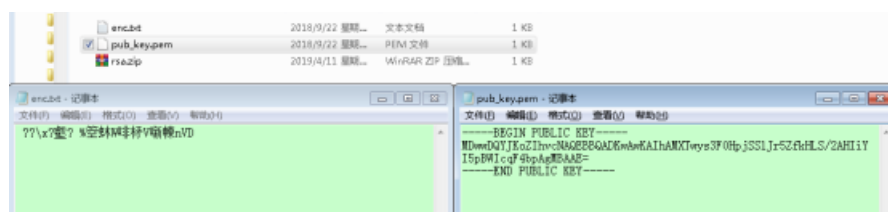
```

# -*- 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
```

```
root@kali:~/Desktop/zuoti# openssl rsa -pubin -text -modulus -in warmup -in pub_
key.pem
RSA Public-Key: (256 bit)
Modulus:
  00:c5:d3:c3:2b:37:17:41:e9:8d:24:b5:26:be:59:
  7e:41:cb:4b:fd:80:1c:88:98:23:9a:41:58:87:2a:
  17:86:e9
Exponent: 65537 (0x10001)
Modulus=C5D3C32B371741E98D24B526BE597E41CB48FD801C8898239A4158872A1786E9
writing RSA key
-----BEGIN PUBLIC KEY-----
MDwwDQYJKoZIhvcNAQEBBQADKwAwKAIhAMXTwys3F0HpjSS1Jr5ZfkHLS/2AHIiY
I5pBWIcqF4bpAgMBAAE=
-----END PUBLIC KEY-----
```

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
```