

WEEK 1

{Re}

[Pro 的 Python 教室(二)]

先反编译看到源码。

```
#!/usr/bin/env python
# encoding: utf-8
# 如果觉得不错，可以推荐给你的朋友! http://tool.lu/pyc
print "Welcome to Processor's Python Classroom Part 2!\n"
print "Now let's start the origin of Python!\n"
print 'Plz Input Your Flag:\n'
enc = raw_input()
len = len(enc)
enc1 = []
enc2 = ''
aaa = 'io0avquaDb}x2ha4[~ifqZaujQ#'
for i in range(len):
    if i % 2 == 0:
        enc1.append(chr(ord(enc[i]) + 1))
        continue
    enc1.append(chr(ord(enc[i]) + 2))

s1 = []
for x in range(3):
    for i in range(len):
        if (i + x) % 3 == 0:
            s1.append(enc1[i])
            continue
```

```

print~("Welcome to Processor's Python Classroom Part 2!\n")
print~("Now let's start the origin of Python!\n")
print~('Plz Input Your Flag:\n')
enc = input()
len = len(enc)
enc1 = []
enc2 = ''
aaa = 'io0avquaDb}x2ha4[~ifqZaujQ#'
for i in range(len):
    if i % 2 == 0:
        enc1.append(chr(ord(enc[i]) + 1))
        continue
    enc1.append(chr(ord(enc[i]) + 2))

s1 = []
for x in range(3):
    for i in range(len):
        if (i + x) % 3 == 0:
            s1.append(enc1[i])
            continue

enc2 = enc2.join(s1)
if enc2 in aaa:
    print~("You 're Right!")
else:
    print~("You're Wrong!")
    exit(0)

```

过程大概就是先输入一个字符串，然后偶数位每个字符加 1，奇数位每个字符加 2。之后再重新排序，得到的可能是 aaa 那个字符串或者它的子串。关键是前五个字母 hgame 是确定的，还有{}，然后可以发现应该就是 aaa。然后就是算回去，我是手算的。

```

x=0
0 3 6 9 12 15 18 21 24
i o O a v q u a D
x=1
2 5 8 11 14 17 20 23 26
b } x 2 h a 4 [ ~
x=2
1 4 7 10 13 16 19 22 25
i f q Z a u j Q #

```

```

a b c d e
f g h i j
k l m n o
p q r s t
u v w x y
z

```

iiibof}OqxaZ2vahquauj4aQ[D#~

hgame{Now_Y0u_got_th3_PYC!}

{Misc}

[\[Are You Familiar with DNS Records?\]](#)

根据 hint，找到 TXT。然后查百度发现 nslookup 命令。

```

C:\Users\>nslookup -qt=TXT project-all.club
服务器: UnKnown
Address: fe80::1

非权威应答:
project-all.club      text =
    "v=spf1 include:spf.mail.qq.com ~all"
project-all.club      text =
    "flag=hgame{seems_like_you_are_familiar_with_dns}"

```

{Crypto}

[\[Vigener~\]](#)

直接在线解密

维吉尼亚密码在线解密

请输入要加密的明文

The Vigenere ciphe is a method of encrypting alphabetic text by using a series of interwoven Caesar ciphers, based on the letters of a keyword. It is a form of polyalphabetic substitution. The cipher is easy to understand and implement, but it resisted all attempts to break it for three centuries, which earned it the description le chiffre indechiffable. Many people have tried to implement encryption schemes that are essentially Vigenere ciphers. In eighteen sixty three, Friedrich Kasiski was the first to publish a general method of deciphering Vigenere ciphers. The Vigenere cipher was originally described by Giovan Battista Bellaso in his one thousand five hundred and fifty-one book La cifra del. Sig. Giovan Battista Bellaso, but the scheme was later misattributed to Blaise de Vigenere in the nineth century and so acquired its present name. flag is gfyuytukxariyydfjlpwxsdbzwvqt

请输入要解密的密文

Zbi Namyrwjk wmhzk cw s eknlgv uz ifuxstlata edhnufwlow xwpz vc mkohk s kklmwk uz mflklagnkh Gswyuv uavbijk, huwww uh xzw ryxlwxm sx s qycogxx. Ml ay u jgjs ij hgrsedhnufwlow wmtynmlmzcsf. Lny gahnvy ak kuwq lu orvwxmxsfj urv asjpwekhx, tmz cx jwycwlwj upd szniehzm xg txyec az zsj lnliw ukhxmjoyw, ozowl wsxhiv az nlw vkmgjavnmgf ry gzalzw abxiuzozjjshfi. Ests twgvfi zsby xjakk xg asjpwekhx wfilchloir kunyqwk zbel sxy ikkkhxasrfc Namyrwjk wmhzklw. Af kckzlkyl kadnc lzxyi, Xjoyhjaib Oskomoa ogm xzw lcvkl zi tmtrcwz s myrwjgf qwl nih gx jygahnyvafm Pmywtyvw uojlwjy. Nlw Noaifwxy gahnvy osy ivayohedde xikuxcfwv hs Kagbur Tsznmklg Viddgms af ncw gfk nlgmyurv xopi zmtxvww gh h xalnc-gfk vsgc Ru gaxxu hwd. Yck. Yaupef Tgnxakzu Fwdruwg, tan xzw ywlwek qek dgnij eomellxcfmklx xg Trumkw jy Zaykhijw oh xzw tcrwl n wifalc sfj ms suwomjwj cxx hxywwfz heew. Ifey ay ajqmenycpglmqqjzndhrqwpvhtaniz

加密

无密钥解密

密钥: guess

密钥长度(选填)

有密钥解密

密钥