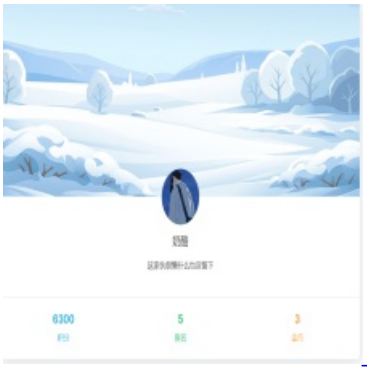
BugKu-CTF(解密篇Crypto)---道友不来算一算凶吉？

原创

Nailaoyyds 已于 2022-04-07 13:46:21 修改 2222 收藏
分类专栏： CTF 文章标签： 蓝桥杯 安全
于 2022-04-02 10:29:54 首次发布



目录

题目

半仙我夜观天象，掐指一算，卜出卦象如下，不知道的有无道友可解此卦。

密文:升益艮归妹井萃旅离旅困未济屯未济中孚未济升困噬嗑鼎震巽噬嗑解节井萃离未济蒙归妹大畜无妄解兑临睽升睽未济无妄遁涣归妹

嗯？为什么还有a和b呢？
a=5
b=7

```
# -- coding:UTF-8 --
from secret import flag

def encrpyt5():
    enc=''
    for i in flag:
        enc+=chr((a*(ord(i)-97)+b)%26+97)
    return(enc)

def encrypt4():
    temp=''
    offset=5
    for i in range(len(enc)):
        temp+=chr(ord(enc[i])-offset-i)
    return(temp)
```

题解

编码方式

易经有64卦 采用编码 000000 -> 1111111

二进制转字符串

bsae64 解密

加密脚本4逆回

加密脚本5逆回

总结

此题的代码如下

```
import base64
s = '升益艮归妹井萃旅离旅困未济屯未济中孚未济升困噬嗑鼎震巽噬嗑解节井萃离未济蒙归妹大畜无妄解兑临睽升睽未济无妄遁涣归妹'
dic = {'坤': '000000', '剥': '000001', '比': '000010', '观': '000011', '豫': '000100', '晋': '000101', '萃':
       '复': '100000', '颐': '100001', '屯': '100010', '益': '100011', '震': '100100', '噬嗑': '100101', '随'
l = []
k = 0  # 两个字符的标志位
for i in range(len(s)):
    if k == 1:
        k = 0
        continue
    try:
        l.append(dic[s[i]])
    except:
        l.append(dic[s[i]+s[i+1]])
        k = 1

ss = ''.join(l)

# print(ss)

enc = ''
for i in range(0, len(ss), 8):
    enc += chr(eval('0b'+ss[i:i+8]))

# print(enc)

s = base64.b64decode(enc).decode()

# print(s)


def encrypt4(enc):
    temp = ''
    offset = 5
    for i in range(len(enc)):
        temp += chr(ord(enc[i])-offset-i)
    return(temp)


def decrypt4(enc):
    temp = ''
    offset = 5
    for i in range(len(enc)):
        temp += chr(ord(enc[i])+offset+i)
    return(temp)
```

```
a, b = 5, 7


def encrpyt5(flag):
    enc = ''
    for i in flag:
        enc += chr((a*(ord(i)-97)+b) % 26+97)
    return(enc)


def decrypt5(flag):
    enc = ''
    for i in flag:
        for k in range(20):
            if (ord(i) - 97 - b+26*k) % a == 0:
                enc += chr((ord(i) - 97 - b + 26 * k) // a + 97)
                break
    return(enc)


print(decrypt5(decrypt4(s)))
```

解出flag

```
import base64
s = '升益艮归妹井萃旅离旅困未济屯未济中孚未济升困噬嗑鼎震巽噬嗑解节井萃离未济蒙归妹大畜
dic = {'坤': '000000', '剥': '000001', '比': '000010', '观': '000011', '豫': '000100',
       '复': '100000', '颐': '100001', '屯': '100010', '益': '100011', '震': '100100',
l = []
k = 0  # 两个字符的标志位
for i in range(len(s)):
    if k == 1:
        k = 0
        continue
    try:
        l.append(dic[s[i]])
    except:
        l.append(dic[s[i]+s[i+1]])
        k = 1

ss = ''.join(l)

# print(ss)

enc = ''
for i in range(0, len(ss), 8):
    enc += chr(eval('0b'+ss[i:i+8]))

# print(enc)
```

shaodayouxiduoduyijing


```
flag{shaodayouxiduoduyijing}
```