

BugKu-CTF(解密篇Crypto)---道友不来算一算凶吉？

原创

[Nailooyds](#) 已于 2022-04-07 13:46:21 修改 2222 收藏

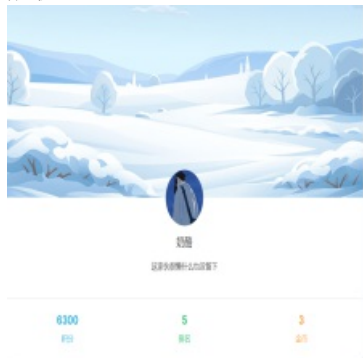
分类专栏: [CTF](#) 文章标签: [蓝桥杯](#) [安全](#)

于 2022-04-02 10:29:54 首次发布

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_53095382/article/details/123914165

版权



[CTF 专栏收录该内容](#)

19 篇文章 0 订阅

订阅专栏

目录

题目

题解

编码方式

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

解出flag

题目

道友不来算一算凶吉?

Crypto

未解决

分数: 20 金币: 2

题目作者: 浮梦

一血: volcano

一血奖励: 3金币

解决: 98

提示:

描述: flag{}

其他: [↓ 下载](#)

请输入flag

提交

CSDN @Nailaoyyds

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 encrypt5():
    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': '000110', '复': '100000', '颐': '100001', '屯': '100010', '益': '100011', '震': '100100', '噬嗑': '100101', '随': '100110'}
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 encrypt5(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

```

1 import base64
2 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
3 dic = {'坤': '000000', '剥': '000001', '比': '000010', '观': '000011', '豫': '000100',
4       '复': '100000', '颐': '100001', '屯': '100010', '益': '100011', '震': '100100',
5 l = []
6 k = 0 # 两个字符的标志位
7 for i in range(len(s)):
8     if k == 1:
9         k = 0
10        continue
11    try:
12        l.append(dic[s[i]])
13    except:
14        l.append(dic[s[i]+s[i+1]])
15        k = 1
16
17 ss = ''.join(l)
18
19 # print(ss)
20
21 enc = ''
22 for i in range(0, len(ss), 8):
23     enc += chr(eval('0b'+ss[i:i+8]))
24
25 # print(enc)
26
27

```

shaodayouxiduoduyijing

CSDN @Nailaoyyds

flag{shaodayouxiduoduyijing}