第四届Xman个人排位赛之commom_encrypt解题思路

原创

KogRow 于 2019-12-26 09:17:24 发布 235 收藏 1
分类专栏： Crypto 文章标签： CTF Crypto

题目：

```
def encrypt(data,groupnums):
    a=[]
    b=[]
    section=int(len(data)/groupnums)
    for i in range(0,len(data),section):
        a.append(data[i:i+section])
    print(a)
    for i in range(section):
        for j in range(groupnums):
            print(a[j])
            b.append(a[j][i])
    cipher=(''.join(chr(ord(b[i])^i)for i in range(len(b))))
    print(cipher)
    return cipher
```

我个人在做题之前并没有了解过什么是栅栏加密，直接看着代码逆出来的。

对于栅栏的猜测我是看密文的长度。比如给的是24位密文，推测是4×6或者2×12，稍微试一下得到正确的flag也就出来了。

给出还原密文的代码：

```
def fuck():
    miwen = "---------此处填写要还原的密文-------"
    mid = ""
    for i in range(len(miwen)):
        mid+=chr(ord(miwen[i])^i)
    b=[]
    for i in range(0,len(mid)):
        b.append(mid[i])
    section = 14
    groupnums=2
    a=[]
    mid3=[]
    for i in range(0,len(b),groupnums):
        mid2 = b[i:i+groupnums]
        mid3.append(mid2)
    print(mid3)
    data = ""
    for i in range(groupnums):
        for j in range(section):
            data+=(mid3[j][i])
    print(data)
    #设section=4,groupnums=7
    #len(data=12)
```