CTFshow crypto wp

原创

是真的白 于 2022-01-11 16:08:56 发布 178 收藏
文章标签： 密码学
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/m0_62506844/article/details/122433816
版权

今天开始我的ctf crypto生涯了，之后会陆续从各大平台找一些密码的题目来做，先从萌新杯入手！

说明一下，懒得调整字体啥的~~

签到题：

佬说了，Ao(mg就是flag用base85编码之后的表示形式，在这里可以从网站上直接base85解码，也可用python中的base64库解码，但解码的时候遇到一个有趣的问题

```
import base64
a="Ao(mgHX^E)AN2PSBOu3qI0o"
a=base64.b85decode(a)
print(a)
#b' \xf9,96"\xaa\x96\x1f\xf4\xf7\x10# \xc7~8\x06'
```

可以看到用base85解码得到的不是flag，这是怎么回事？

我又试了一下flag用这个base85编码之后得到的是 b'W^7?+',也不是Ao(mg哇，百思不得其解的我找到大佬问了一下，得知base85有好多编码表？？

在python的base64库里还有一种方式，是**a85.encode（）！**

我特意上网搜了一下a85和b85的区别--*它们的区别在于用于编码的字符映射等细节*

大体意思是，在a85encode中，映射ascii顺序中的所有字符，bsae85里用的字符集顺序和种类都不同吧，网上大多推荐使用a85encode，那我们就用a85再写一次！

```
import base64
a="Ao(mgHX^E)AN2PSBOu3qI0o"
a=base64.a85decode(a)
print(a)
```

得到flag

抱我：

给的是一个py文件，打开如下：

```
import random
cstring = 'abcdefghijklmnopqrstuvwxyz{}_0123456789'
key = 'flag{********}'
length = 300

def encode():
    res = ''
    for i in range(1, length):
        c = random.randint(0, 36)
        res += cstring[c]
        for n in range(10):
            c = random.randint(0, len(key) - 1)
            res += key[c]
    return res

#qdfl33{6{6gs3afa6{3}agf{}aagdf}6fl36d{dfl{6ay6gafddfg}{j3f}}6la{3}bfdf3}gla}65}lg6g6dflf0{dfgd3fdfgc{g6a}a
```

可以看到在encode函数里，有299个大循环，每个大循环里包含一个10次的小循环；每个大循环中，首先给c赋值一个0-36的随机数，然后将c作为cstring的下表输出里面的内容。cstring里的内容和flag没有什么关系，添加到秘文里就是混淆视听的。

真正的内容都在小循环里，res中每次添加的都是key里的某个字符，首先把输出的字符中小循环开始前的一次无关字符删掉，然后用set函数将重复字符删掉（删掉重复字符可能对产生的明文有影响，但我想不出还能怎么做）

```
ss="qdfl33{6{6gs3afa6{3}agf{}aagdf}6fl36d{dfl{6ay6gafddfg}{j3f}}6la{3}bfdf3}gla}65}lg6g6dflf0{dfgd3fdfgc{g6
s=""
for i in range(0,len(ss),11):
    s+=ss[i+1:i+11]
print(set(s))
#{'3', 'f', '6', 'a', 'l', '{', 'd', 'g', '}'}
```

可以看到结果出来之后除了flag{}之外就只有36d了。

妈呀，完了：

hint：图文无关，与妈呀有关

给了一串0和1，先把他转成16进制试一下，解出来的字符串看不懂。

再解成10进制试一下，得到一组整数，推测可能是ascii值，再转成字符：

```
s="01000100 01010011 01111001 00110011 01001010 01111001 01001011 01110110 01010000 01000011 01010000 01101
s=s.split()
#print(s)
n=[]
for i in s:
    n.append(int(i,2))
print(n)
#[68, 83, 121, 51, 74, 121, 75, 118, 80, 67, 80, 109, 72, 52, 87, 67, 122, 43, 84, 104, 87, 105, 50, 70, 10
a=""
for i in n:
    a+=chr(i)
print(a)
#DSy3JyKvPCPmH4WCz+ThWi2FgKo9eSPU4e5g+jZU3FrWNvLM55kEf1hEmNru+NE3
```

以为是base64编码，用base64解一下，解出来的东西我依然看不懂

有大佬说是AES加密，并且群主在群里给了密钥20121221，看来这是挺早的题了嘿嘿

http://tool.chacuo.net/cryptaes 这里aes解密，ecb模式，**编码用utf-8，得到flag**

flag{第13个伯克盾将会结束}