BUUCTF_Crypto题目：[BJDCTF2020]这是base

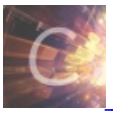
原创

好想变强啊 已于 2022-03-18 15:02:46 修改 1187 收藏 1

分类专栏： BUUCTF刷题记录 文章标签： python 网络安全

于 2022-03-18 14:56:07 首次发布

本文链接：https://blog.csdn.net/qq_38798840/article/details/123570461



BUUCTF刷题Crypto篇

文章目录

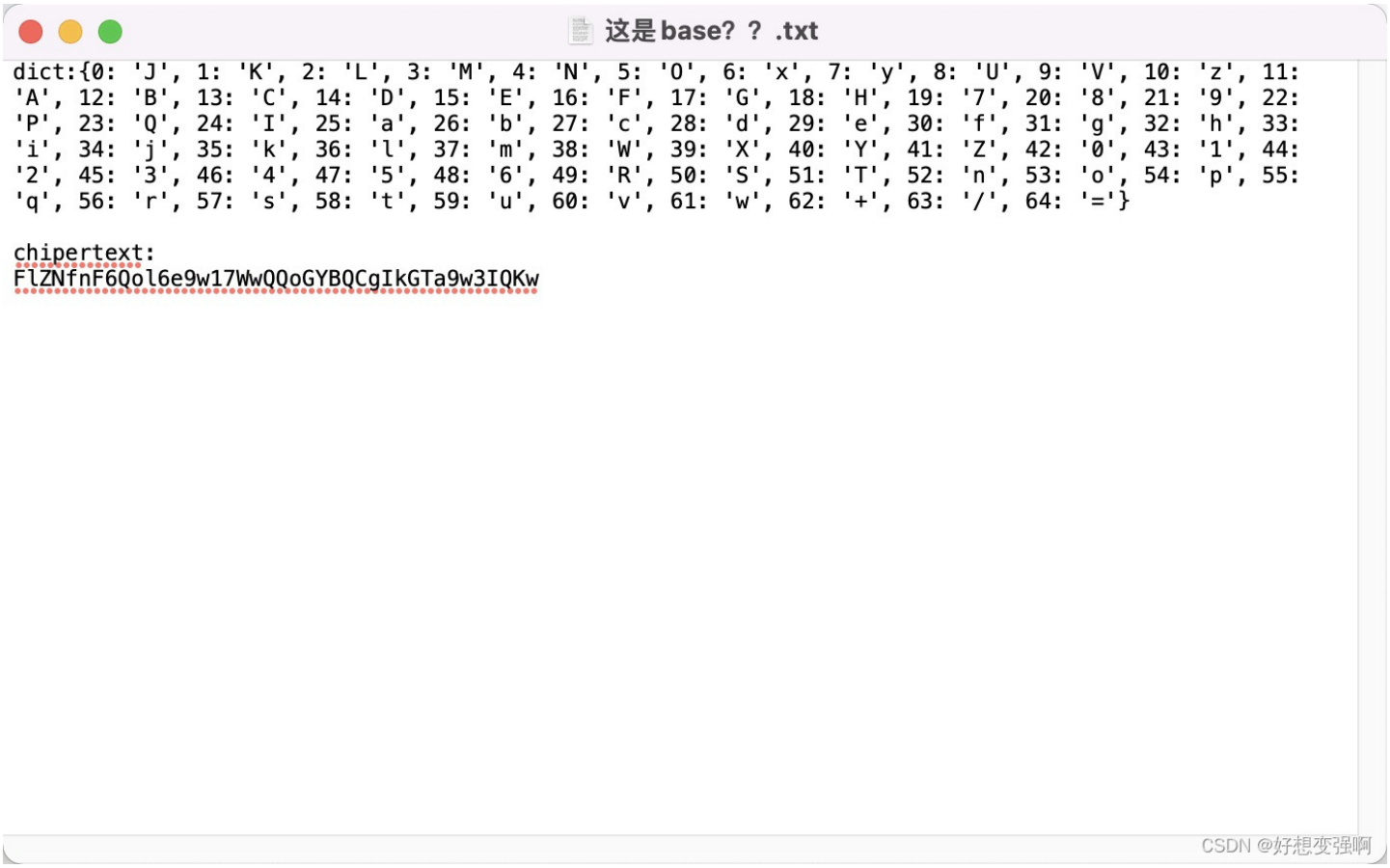
前言

本篇内容记录的是一道涉及到“换表”的题目，题目中给出的密文是经过“被替换了的”base64编码表得出的，而解题的大体思路就是先把密文恢复成用标准的base64编码表编码（之前搜索base64的时候看到一种说法是应该称base64是一种编码方式，而非加密算法，所以我这里用“编码”）的结果，再调用Python中已有的base64.b64decode()函数恢复出明文即可。

一、原题

BUUCTF网站Crypto类别第2页的题目：[BJDCTF2020]这是base？？

打开题目文件，给出是密文和得到这串密文所用的编码对应表（字典类型的变量dict），根据dict中键和值的范围，可以推断出这是字符顺序被替换的base64编码表。



二、解题步骤

1.换表

就是要找到密文c中的每个字符在dict中对应的位置（下标），再找到这些位置在标准base64编码表中对应的字符。

因为base64的编码过程（原理）是不变的，只是最后一步根据数字找对应的字符时，字符的顺序变了，所以我们只要找到这些数字在标准base64编码表中对应的字符，就转换回了我们熟悉的base64编码结果，也就可以进一步借助Python已有的base64库来恢复出明文了。

2.调用函数恢复明文

调用Python的base64库函数b64decode()即可得到明文，记得要import base64

代码如下：

```
import base64

dict={0: 'J', 1: 'K', 2: 'L', 3: 'M', 4: 'N', 5: 'O', 6: 'x', 7: 'y', 8: 'U', 9: 'V', 10: 'z', 11: 'A', 12: 'B',
 13: 'C', 14: 'D', 15: 'E', 16: 'F', 17: 'G', 18: 'H', 19: '7', 20: '8', 21: '9', 22: 'P', 23: 'Q', 24: 'I', 25:
 'a', 26: 'b', 27: 'c', 28: 'd', 29: 'e', 30: 'f', 31: 'g', 32: 'h', 33: 'i', 34: 'j', 35: 'k', 36: 'l', 37: 'm'
, 38: 'W', 39: 'X', 40: 'Y', 41: 'Z', 42: '0', 43: '1', 44: '2', 45: '3', 46: '4', 47: '5', 48: '6', 49: 'R', 50
: 'S', 51: 'T', 52: 'n', 53: 'o', 54: 'p', 55: 'q', 56: 'r', 57: 's', 58: 't', 59: 'u', 60: 'v', 61: 'w', 62: '+
', 63: '/', 64: '='}

a = 'ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz0123456789+/='     #标准表

c='FlZNfnF6Qol6e9w17WwQQoGYBQCgIkGTa9w3IQKw'

ds=''  #把dict转换成字符串方便处理
for i in range(65):
    ds+=dict[i]

l=[]
for i in range(len(c)):
    l.append(ds.index(c[i]))  #无论换不换表，base64变换本身产生的6位二进制数对应的十进制数是不变的，这里就是找到密文c的每
个字符在dict表中键值

#print(l)  #l中存的是索引值（下标数字）

m1=''
for ll in l:
    m1+=a[ll]  #找到l中所存的每个数字在标准的base64加密表中所对应的字符
print(m1)  #m1是标准base64表编码结果

m2=base64.b64decode(m1)  #直接调用函数恢复出明文
print(m2)
```

m2的输出结果就是我们想要找的flag了！贴一张运行结果：
（这里上一行输出的是标准base64编码的结果）

```
QkpEe0QwX1kwdV9rTm9XX1RoMXNfYjRzZV9tYXB9
b'BJD{D0_Y0u_kNoW_Th1s_b4se_map}'
```

flag{D0_Y0u_kNoW_Th1s_b4se_map}

总结

以上就是对于这道题的全部记录了，关于base64的编码方式可以去百度一下哈哈。