CTF-bugku-crypto-[小山丘的秘密]-希尔密码

原创

沧海一粟日尽其用 已于 2022-03-08 11:33:17 修改 4218 收藏

文章标签： 算法 安全 python

于 2022-02-27 17:30:05 首次发布

本文链接：https://blog.csdn.net/m0_43405474/article/details/123166837

bugku-crypto-[小山丘的秘密]-希尔密码

1.解题背景

希尔密码的直观数学原理- Wikipedia

step1:字母表

```
  首先根据A=1的提示构造出字母表
['z','a','b','c','d','e','f','g','h',
'i','j','k','l','m','n','o','p','q',
'r','s','t','u','v','w','x','y']
```

step2:密文

```
 密文:plgtgbqhm
```

step3:密钥

```
根据棋盘获得3*3的密钥
[[1,2,3],
[0,1,4],
[5,6,0]]
```

2.解题脚本

```
import numpy as np
table=['z','a','b','c','d','e','f','g','h',
       'i','j','k','l','m','n','o','p','q',
       'r','s','t','u','v','w','x','y']
key_inv=np.matrix(np.array([[1,2,3],[0,1,4],[5,6,0]])).I%26
result=key_inv*np.array([[16,20,17],
                [12,7,8],
                [7,2,13]])%26
str=''
resulttable=[]
for i in range(result.shape[0]):
    for j in range(result.shape[1]):
        resulttable.append(round(result.T[i,j]))
for i in range(9):
    str+=table[resulttable[i]]
print("bugku{"+str+'}')
#bugku{whatahill}
```

3.flag

bugku{whatahill}