NSSCTF刷题wp——单表替换密码

原创

DerJaeger 于 2022-04-12 19:25:41 发布 1586 收藏

分类专栏： NSSCTF 文章标签： 网络安全

本文链接：https://blog.csdn.net/YougerXen/article/details/124083829

NSSCTF 专栏收录该内容

3 篇文章 0 订阅

订阅专栏

NSSCTF Crypto 模块

单表替换密码

[HGAME 2022 week1]Matryoshka ID:1855

打开Matryoshka.txt,发现是一堆点，看标签可能是Braille盲文，仔细比对后发现重点不是将盲文翻译成英语，而是后面得标签莫斯密码，可以发现□非常像平时解莫斯密码的分隔符，□和□就很可能对应着摩斯密码里面的长,短码

在线摩斯密码工具

结果前面完全不对，后面部分对，考虑到在莫斯密码里面，长短和短长是完全不一样的，反转一手

```
[illegible]
```

再解

```
46,66,42,75,66,45,46,6E,6D,4C,73,36,44,33,73,69,59,74,4C,36,58,32,70,34,69,4E,30,63,64,53,6C,79,6B,6D,39,72,51,4E,39,6F,4D,53,31,6A,6B,73,39,72,4B,32,52,36,6B,4C,38,68,6F,72,30,3D
```

去掉逗号(附上代码)

```
str='46,66,42,75,66,45,46,6E,6D,4C,73,36,44,33,73,69,59,74,4C,36,58,32,70,34,69,4E,30,63,64,53,6C,79,6B,6D,39,72,51,4E,39,6F,4D,53,31,6A,6B,73,39,72,4B,32,52,36,6B,4C,38,68,6F,72,30,3D'
for i in str:
    str =str.replace(',','')
print(str)
```

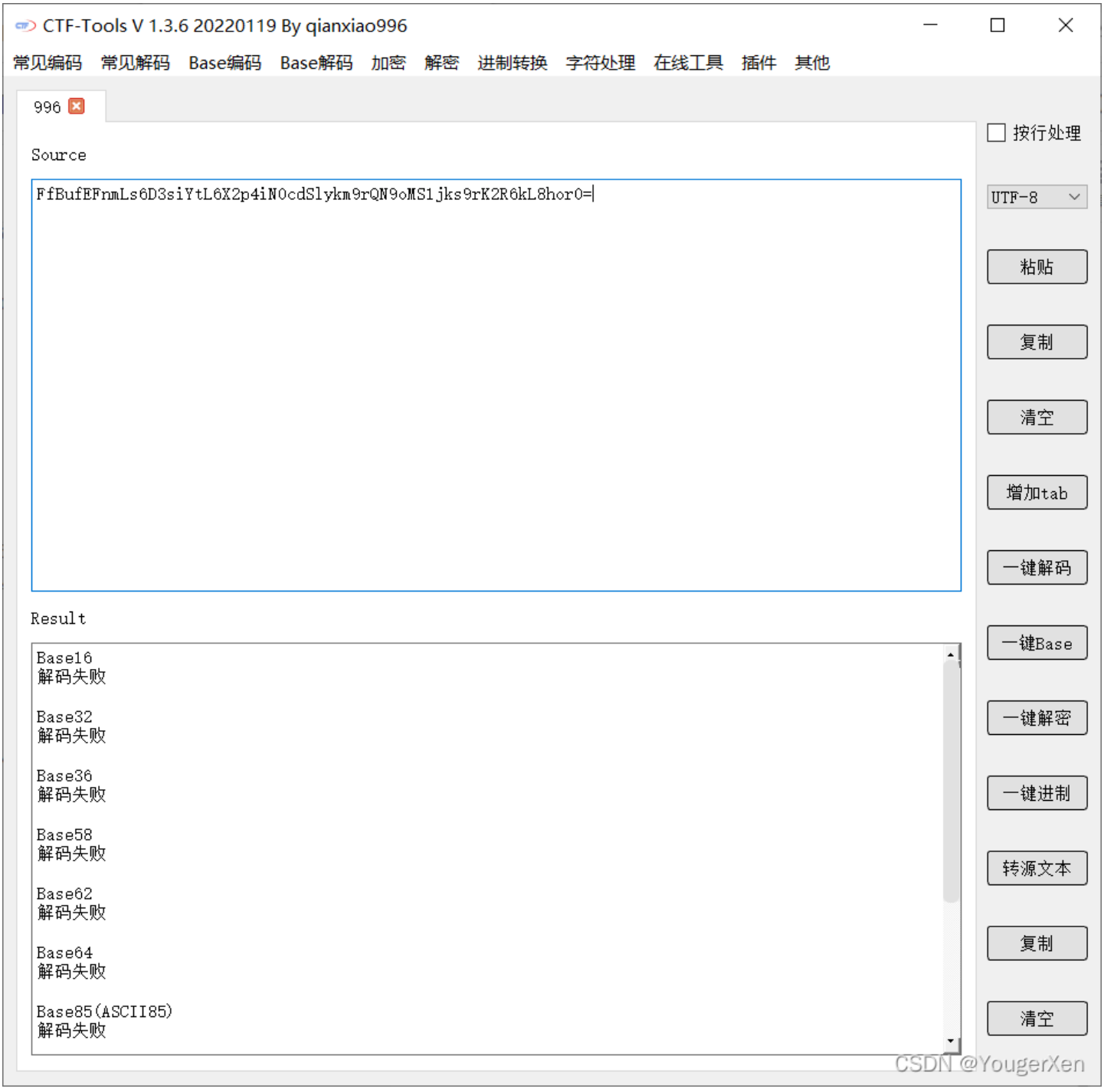
得

```
466642756645466E6D4C73364433736959744C3658327034694E306364536C796B6D3972514E396F4D53316A6B7339724B3252366B4C38686F72303D
```

观察到字母大小不超过F，考虑是否为16进制，hex转str

```
FfBufEFnmLs6D3siYtL6X2p4iN0cdSlykm9rQN9oMS1jks9rK2R6kL8hor0=
```

再用base解码失败



再回看txt`Caesar：21; Vigenère:hgame`

因为凯撒密码会位移字符，base终止符=会被移动，所以尝试维吉尼亚密码，再base

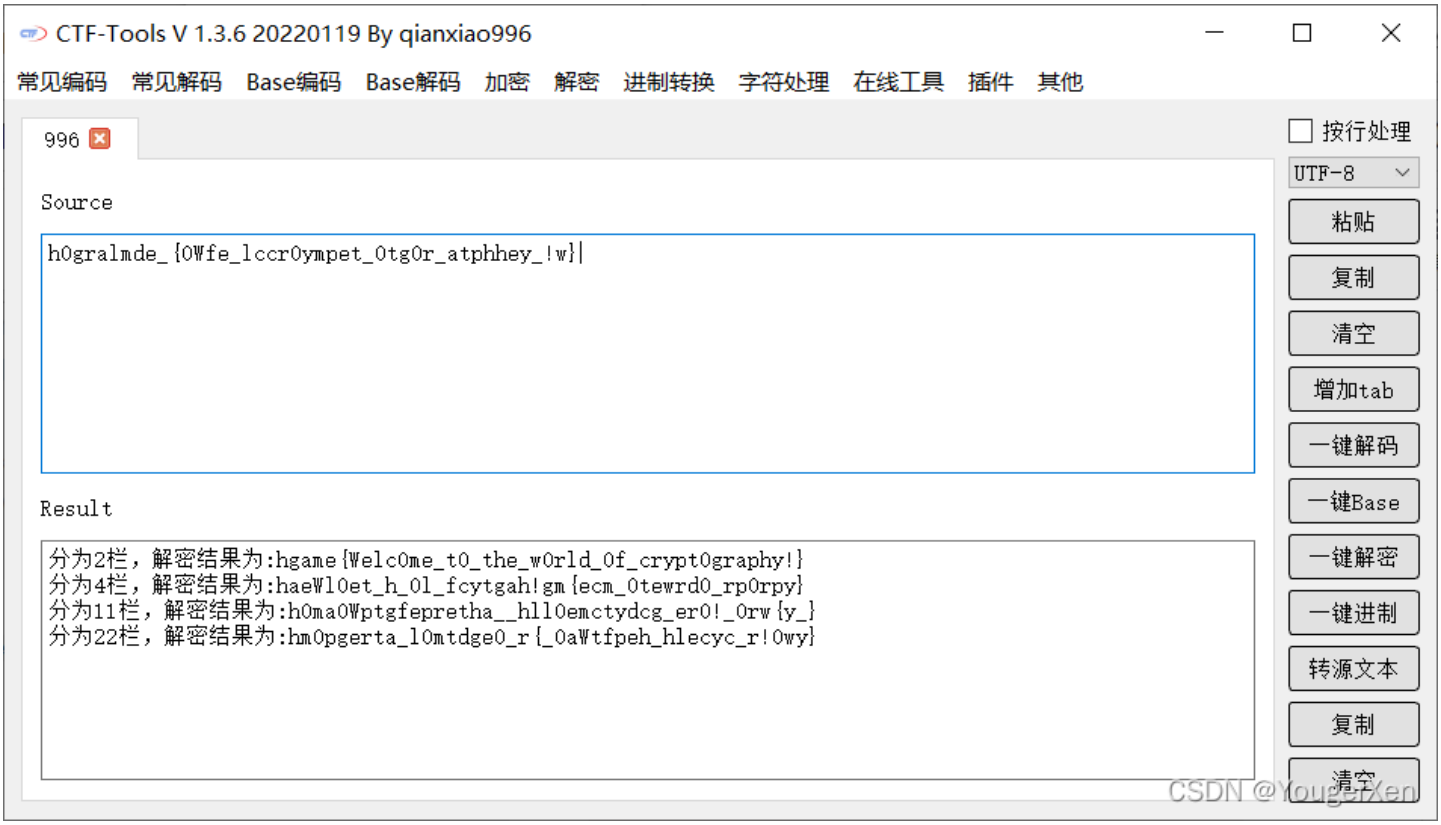
发现是base64

`c0bmvghyz_{0Raz_gxxm0thkzo_0ob0m_vokcczt_!r}`

再凯撒21位

`h0gralmde_{0Wfe_lccr0ympet_0tg0r_atphhey_!w}`

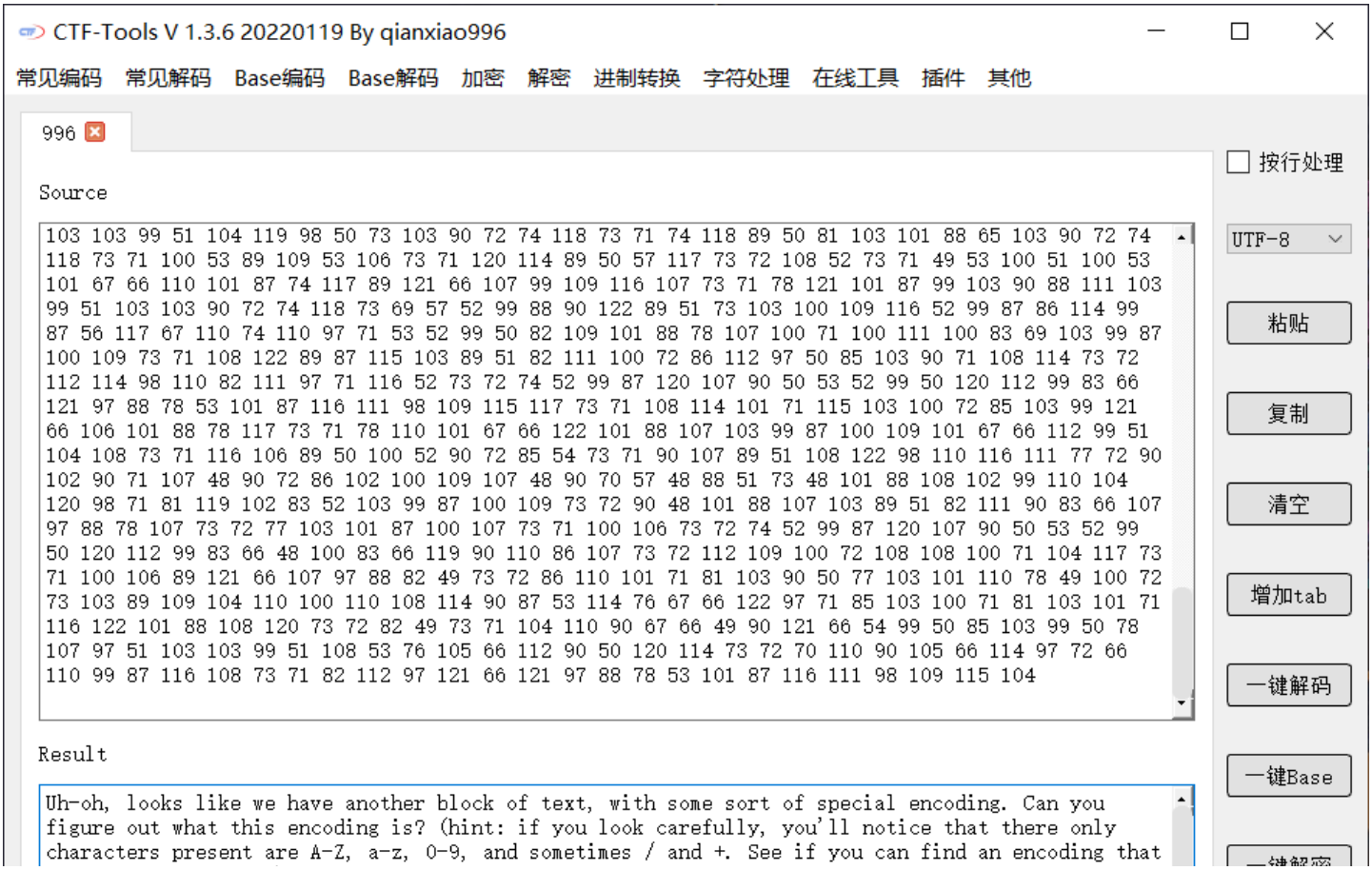
发现不对，再看标签栅栏，再解



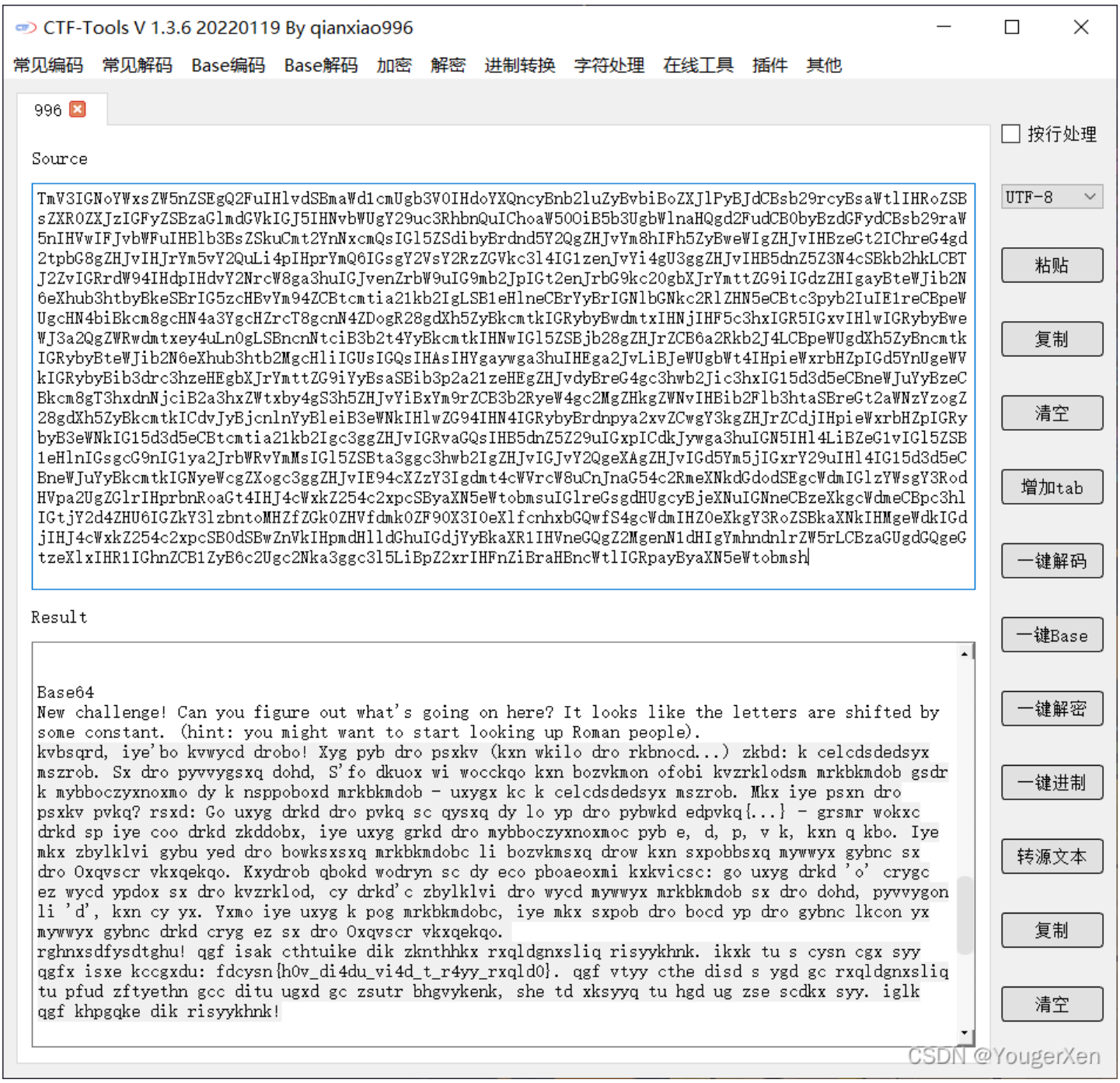
`hgame{Welc0me_t0_the_w0rld_0f_crypt0graphy!}`

[UTCTF 2020]basics ID:201

打开txt全是01并且每隔8个字符就被分割，直接二进制转ASCII码(ps:我先转成了10进制)



读文本大概意思是说恭喜你过关，成功下一关，并且给出下一关的提示:那种code是A-Z,a-z,0-9,有时加上/和+，，这不就是base64嘛，直接解



再读下一天的提示什么Roman people,我们凯撒大帝老罗马人了，再凯撒解码(我的这里用的位移密码，所以偏移量是凯撒的26-n,意思是一样的)

再看提示： 提示：我们知道标志将采用 utflag{...} 格式 - 这意味着如果您看到该模式，您就会知道 u、t、f、la 和 g 的对应关系是什么。直接quip quip

```
congratulations! you have finished the beginner cryptography challenge. here is a flag for all your hard efforts: utflag{n0w_th4ts_wh4t_i_c4ll_crypt0}. you will find that a lot of cryptography is just building off this sort of basic knowledge, and it really is not so bad after all. hope you enjoyed the challenge!
```

什么恭喜你，什么什么巴拉巴拉的,直接跳过得flag `utflag{n0w_th4ts_wh4t_i_c4ll_crypt0}`

ps:最后一句话：你会发现很多密码学只是建立在这种基础知识的基础上，毕竟它真的没有那么糟糕。 希望你喜欢挑战！

[AFCTF 2018]Single ID:936

打开txt读函数

```
#include <bits/stdc++.h>
using namespace std;
int main()
{
 freopen("Plain.txt","r",stdin);
 freopen("Cipher.txt","w",stdout);
 map<char, char> f;
 int arr[26];
 for(int i=0;i<26;++i){
  arr[i]=i;
 }
 random_shuffle(arr,arr+26);
 for(int i=0;i<26;++i){
  f['a'+i]='a'+arr[i];
  f['A'+i]='A'+arr[i];
 }
 char ch;
 while((ch=getchar())!=EOF){
  if(f.count(ch)){
   putchar(f[ch]);
  }else{
   putchar(ch);
  }
 }
 return 0;
}
```

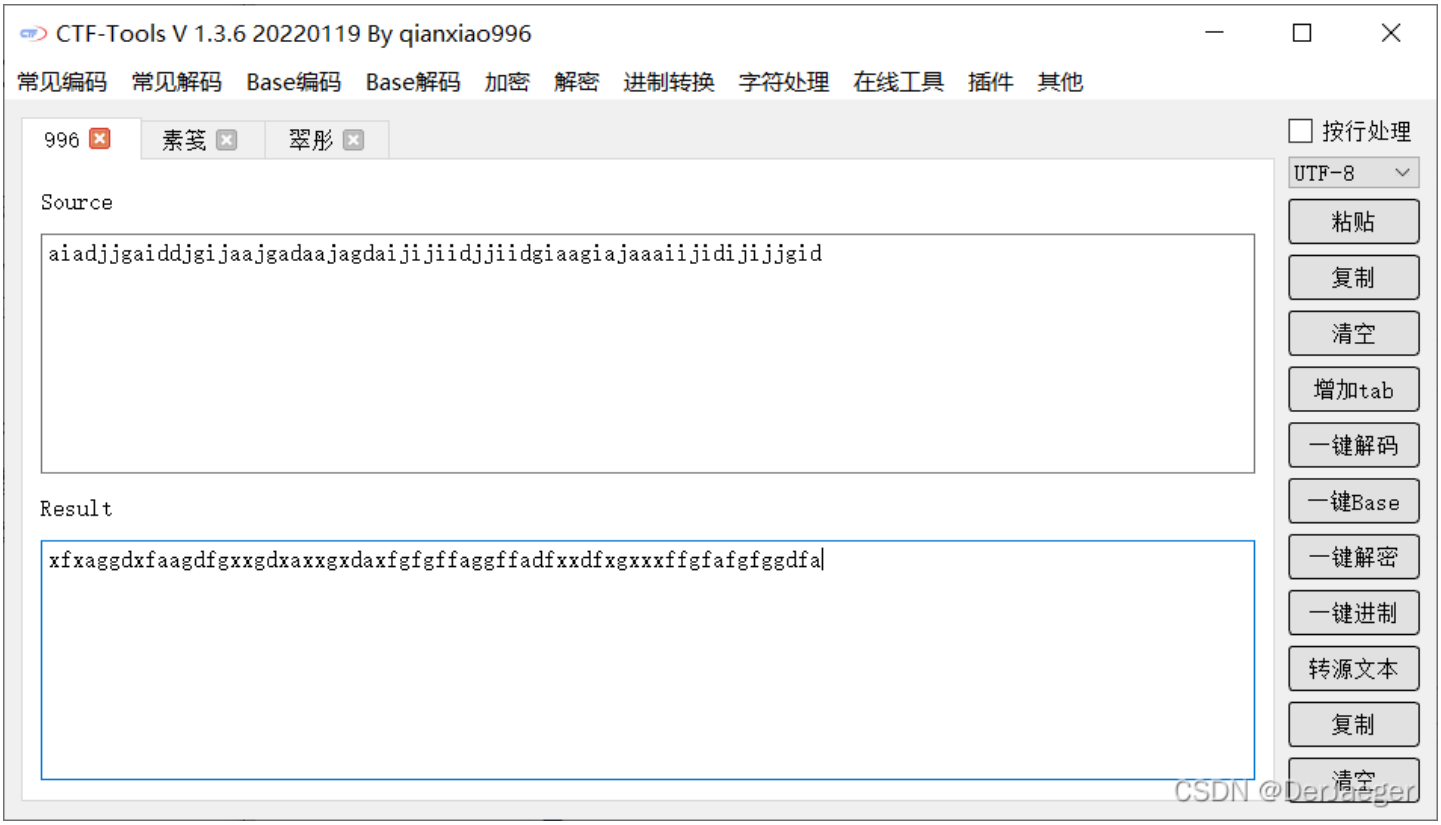
其中`random_shuffle(arr,arr+26);`预示着代码加密是随机的，只有通过词频分析

我的做的时候，quipqiup直接爆破出来，无心之举，结果直接出了□

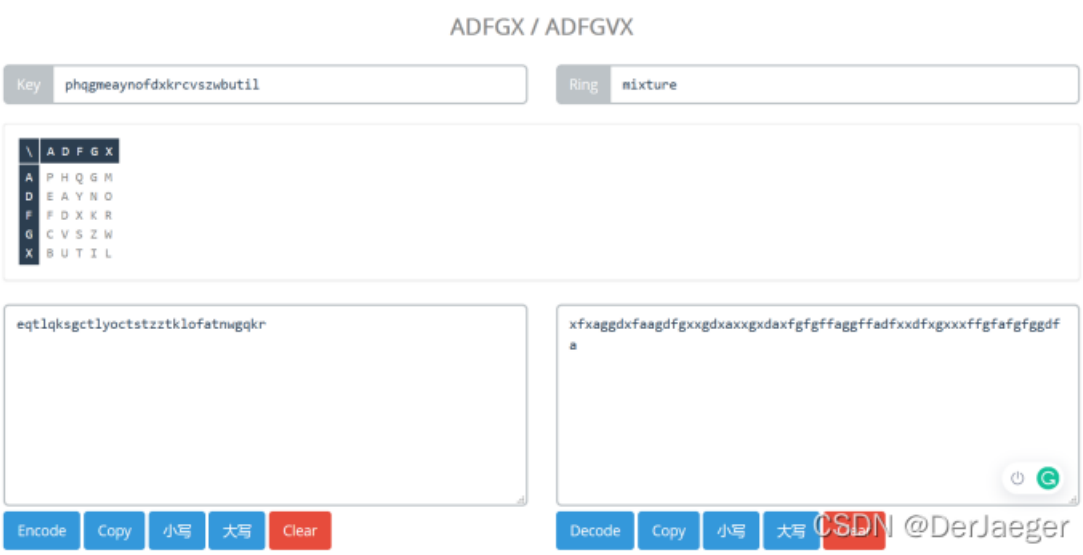
[广东省大学生攻防大赛 2021]classic ID:1251

这个题我自己的做的时候直接裂开，这个脑洞题有点离谱，需要熟悉各种密码，当时网上也没有wp，后来找到一位大佬(当时大赛的特等奖)给的wp，再次感谢！

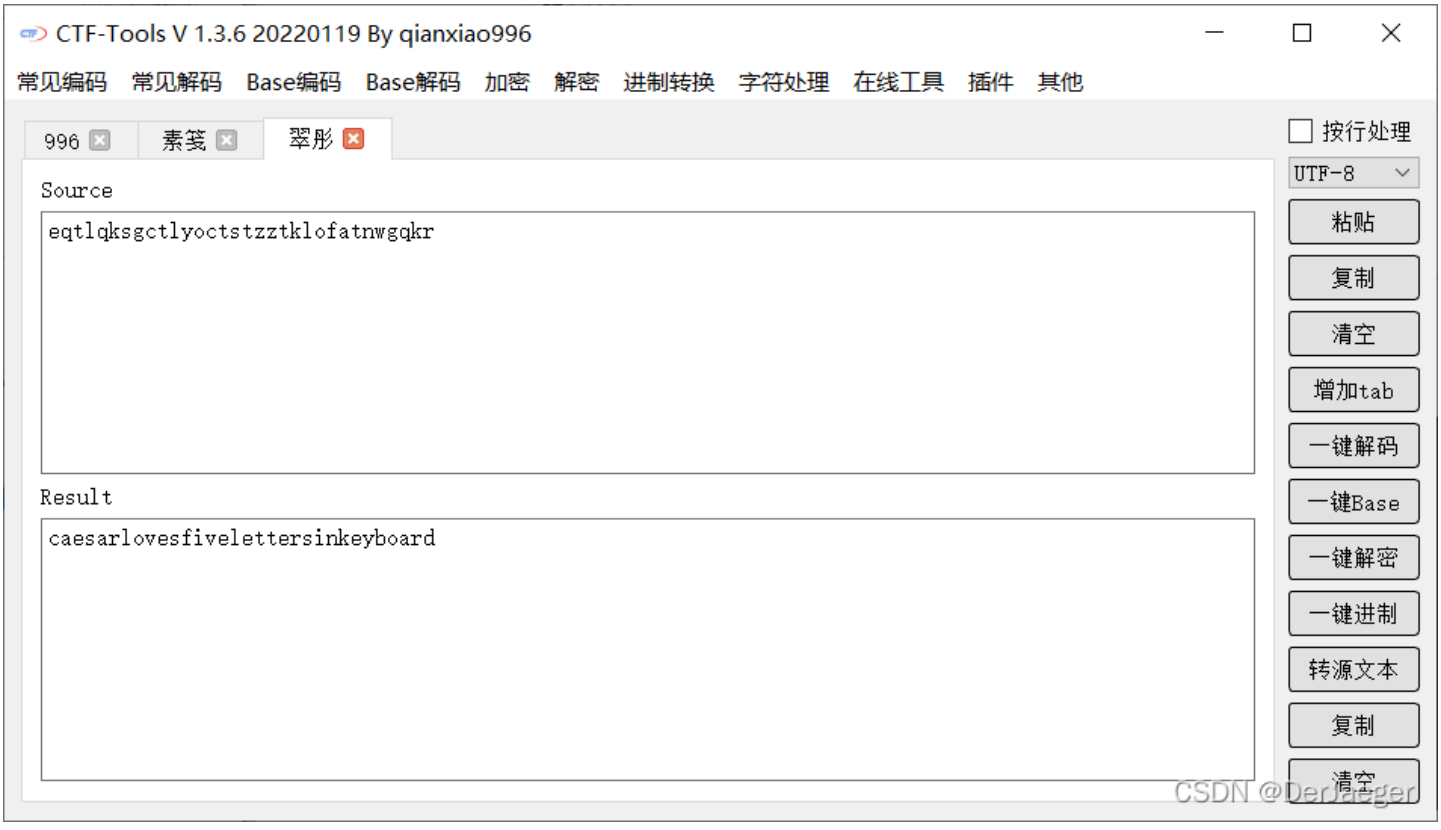
看到密文只有5个字母，考虑ADFGX密码。但是字母不对应，可能是移位或者替换了。
发现凯撒密码移动3位可以全转换为ADFGX


CTF-Tools V 1.3.6 20220119 By qianxiao996
常见编码 常见解码 Base编码 Base解码 加密 解密 进制转换 字符处理 在线工具 插件 其他
996
素笺
翠彤
按行处理
UTF-8
Source
aiadjjgaiddjgijaajgadaajagdaijijiidjjiidgiaagiajaaaiijidijijjgid
粘贴
复制
清空
增加tab
一键解码
一键Base
一键解密
一键进制
转源文本
Result
xfxaggdxfaagdfgxxgdxaxxgxdaxfgfgffaggffadfxxdfxgxxxffgfafgfggdfa
复制
清空
CSDN @DerDaeger

ADFGX密码，mixture



键盘密码解码



得flag `flag{caesarlovesfivelettersinkeyboard}`

[SWPUCTF 2021 新生赛]ez_caesar ID:430

```
import base64
def caesar(plaintext):
    str_list = list(plaintext)
    i = 0
    while i < len(plaintext):
        if not str_list[i].isalpha():
            str_list[i] = str_list[i]
        else:
            a = "A" if str_list[i].isupper() else "a"
            str_list[i] = chr((ord(str_list[i]) - ord(a) + 10) % 26 + ord(a) or 5)
        i = i + 1

    return ''.join(str_list)

flag = ""
str = caesar(flag)
print(str)
#str="U1hYSFlLe2R0em1mYWpwc3RiaGZqeGZ3fQ=="
```

首先import base64，解出str=SXXHYK{dtzmfajpstbhfjxfw}

然后预期解法看加密程序，不难看得出是位移5位的凯撒密码

非预期就直接爆破

得flag`NSSCTF{youhaveknowcaesar}`