BUUCTF Crypto

原创

smile*** 于 2020-04-04 21:19:56 发布 2123 收藏 7

分类专栏： CTF 文章标签： 密码学

本文链接：https://blog.csdn.net/qq_45784859/article/details/105316224

BUUCTF Crypto

Windows系统密码

题目

给了一个文件，名字为pass.hash,

```
Administrator:500:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
ctf:1002:06af9108f2e1fecf144e2e8adef09efd:a7fcb22a88038f35a8f39d503e7f0062:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
SUPPORT_388945a0:1001:aad3b435b51404eeaad3b435b51404ee:bef14eee40dffbc345eeb3f58e290d56:::
```

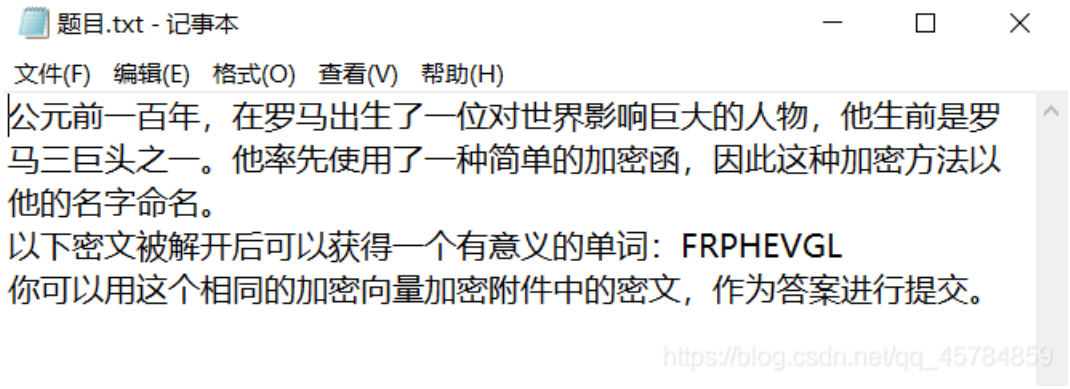
思路

很明显直接取ctf后面那32位的MD5就可以得到flag。

大帝的密码武器

题目

给了一个名叫zip的文件，更改后缀，看到压缩包里有两个文件



思路

很明显是凯撒加密，利用脚本跑一下

```
----
FRPHEVGL
GSQIFWHM
HTRJGXIN
IUSKHYJO
JVTLIZKP
KWUMJALQ
LXVNKBMR
MYWOLCNS
NZXPMDOT
OAYQNEPU
PBZROFQV
QCASPGRW
RDBTQHSX
SECURITY
TFDVSJUZ
UGEWTKVA
VHFXULWB
WIGYVMXC
XJHZWNYD
YKIAXOZE
ZLJBYPAF
AMKCZQBG
BNLDARCH
COMEBSDI
DPNFCTEJ
EQOGDUFK
```


可以看到第13个单词有意义，利用相同的加密方式加密密文就可以得到flag。代码如下

```
from __future__ import print_function
str = 'FRPHEVGL'       #凯撒密码字符串
for i in range(0,26):
    for item in str:
        num = ord(item)+int(i)
        if(num>90):          #到了Z以后往回取
            num-=26
            print (chr(num),end='')
        else:
            print (chr(num),end='')
    print ()
```

凯撒？替换？呵呵！

题目

MTHJ{CUBCGXGUGXWREXIPOYAOEYFIGXWRXCHTKHFCOHCFDUCGTXZOHIXOEOWMEHZO}

思路

利用普通的凯撒很明显解不出来，凯撒密码一般就是按字母顺序来位移实现的加密方法，进阶版的凯撒就不按照字母顺序的加密，要经过暴力破解出每一种可能的加密方式。用工具quipqiup

MTHJ应该就是flag，然后

这样就可以得到破解出来的明文

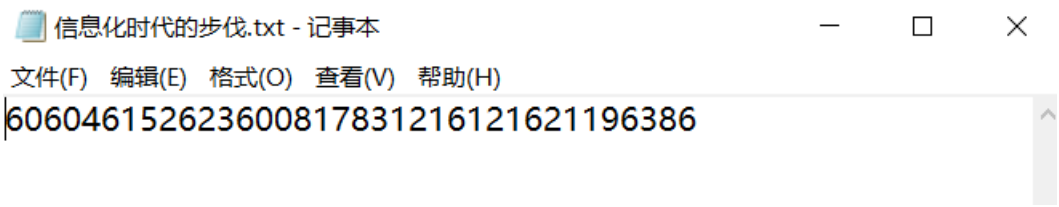
```
0    -1.686   FLAG{ SUBSTITUTION CIPHER DECRYPTION IS ALWAYS EASY JUST LIKE A PIECE OF CAKE}
1    -2.213   FLAG{ SUBSTITUTION RICKED HER DYCTION IS ALWAYS EASY JUST LIVE ACIERE OF RAVE}
2    -2.224   FLAG{ SUBSTITUTION RICHEMPER MYCTION IS ALWAYS EASY JUST LIKE A CIERE OF RAKE}
3    -2.603   FLAG{ SUBSTITUTI CO DIRZEMNED MYRTICO IS ALWAYS EASY JUST LIKE A RIE DE CFDA KE}
4    -2.608   FLAG{ SUBSTITUTINDRIC HEMPER MYCT IN D IS ALWAYS EASY JUST LIKE ACIER ENFRAKE}
5    -2.794   FLAG{ N OWN TITOTIUS CIPHER DECRYPTIUS IN ALBAYNE ANY MONT LIKE A PIECE UFC AKE}
6    -2.799   FLAG{S UPS TO TUTORINOCHEBKEN BY CTOR IOS ALWAYS EASY JUST LOVE A COENER FN AVE}
7    -2.834   FLAG{S ON STI TO TICH DIR ZEBUED BY R TICH IS ALWAYS EASY MOST LIKE A RIE DE CFDA KE}
8    -2.841   FLAG{ SUM SHI HUH IRONIC TED PENDY CHIRO IS ALWAYS EASY BUSH LIKE A CIENER F NAKE}
9    -2.885   FLAG{ TOP THE HOHEN CREW VIDBIRDS WHENCE TALK ASTI ATSUOTH LEMIA WEIR INFRA MI}
10   -2.908   FLAG{S UP SHEHU HE DONE TRICK IN CYT HE DOES ALWAYS IASY BUSH LEVIATE IN IDF NAVI}
11   -2.959   FLAG{S OVS TITO TINY BIPHER DEBR UP TINY IS AL CAUSE A SUMOST LIKE A PIEBEN F BAKE}
12   -3.008   FLAG{ SUN STOTUTORY DOCK EP WED PICTOR YOSAL HAISE AS I MUST LOVE A COEDER F DAVE}
```

读了之后发现第一个就是flag。

信息化时代的步伐

题目

也许中国可以早早进入信息化时代，但是被清政府拒绝了。附件中是数十年后一位伟人说的话的密文。请翻译出明文(答案为一串中文！)



思路

由于以前见过类似的题型，利用中文电报就可以得到flag。

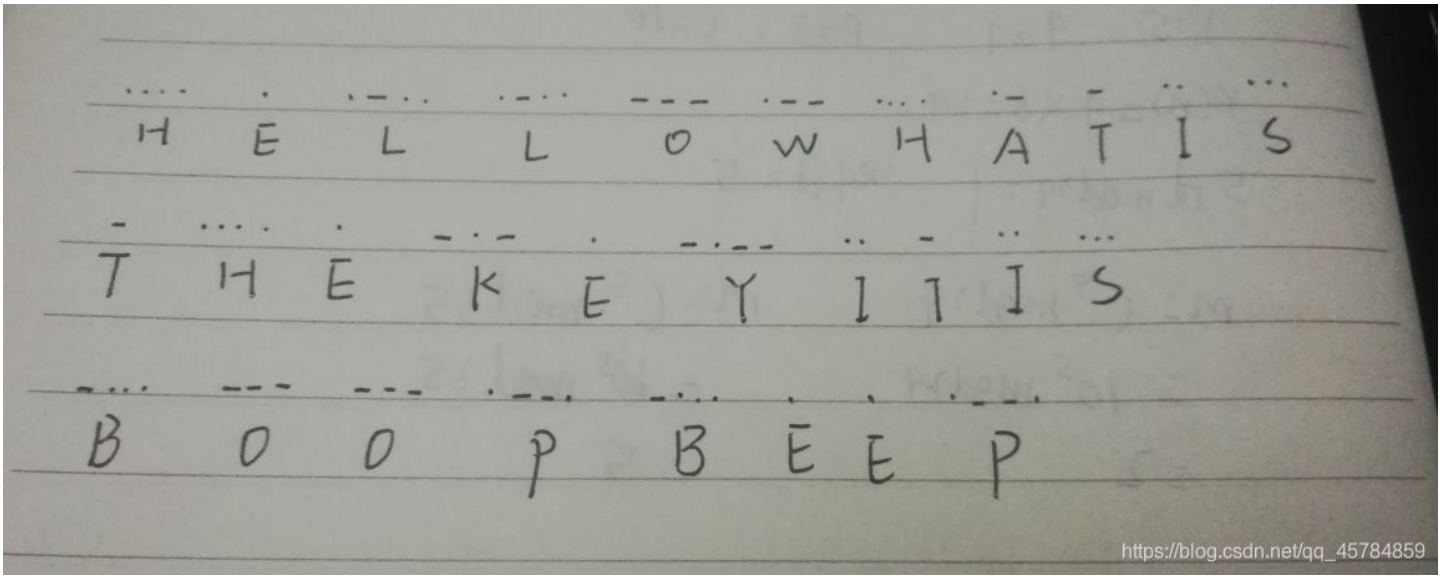
robomunication

题目

是一个mp3文件。

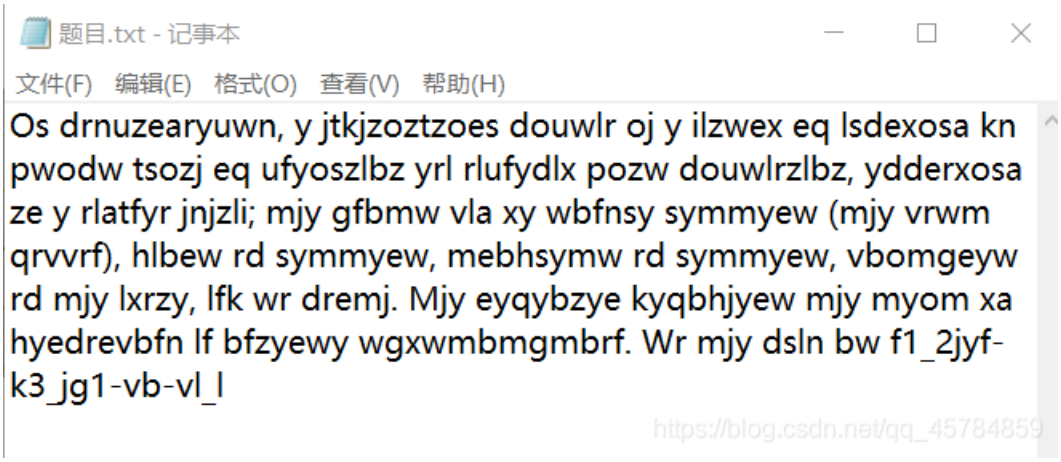
思路

很明显是摩斯电码，然后听声音，听到了之后对照表可得



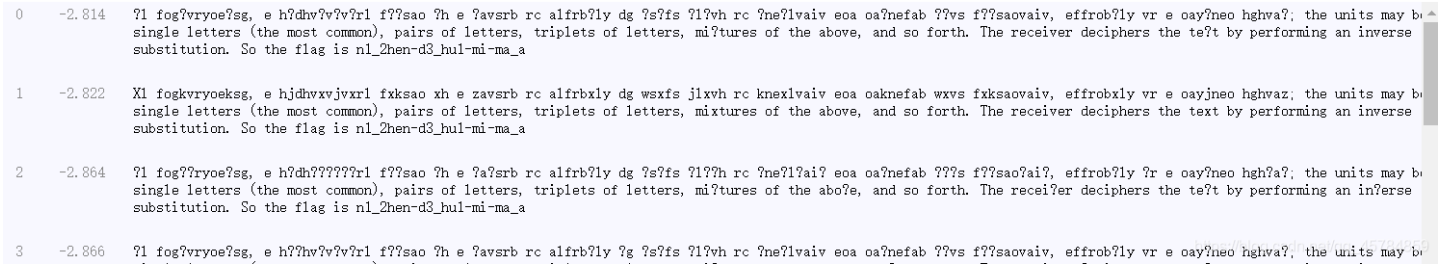
old-fashion

题目



思路

应该是词频分析，就用quipqiup试试，发现可以。



权限获得第一步

题目

你猜这是什么东西，记得破解后把其中的密码给我。答案为非常规形式。
然后给了一个文本

```
Administrator:500:806EDC27AA52E314AAD3B435B51404EE:F4AD50F57683D4260DFD48AA351A17A8:::
```

思路

直接对后32位进行MD5就可以得到flag。

世上无难事

题目

以下是某国现任总统外发的一段指令，经过一种奇异的加密方式，毫无规律，看来只能分析了。请将这段语句还原成通顺语句，并从中找到key作为答案提交，答案是32位，包含小写字母。

VIZZB IFIUOJBWO NVXAP OBC XZZ UKHVN IFIUOJBWO HB
XVIXW XAW VXFI X QIXN VBD KQ IFIUOJBWO WBKAH NBWXO
VBD XJBCN NKG QLKEIU DI XUI VIUI DKNV QNCWIANQ XN
DXPIMKIZW VKHV QEVBBZ KA XUZKAHNBA FKUHKAKX XAW DI
VXFI HBN QNCWIANQ NCAKAH KA MUBG XZZ XEUBQQ XGIUKEX
MUBG PKAWIUHXUNIA NVUBCHV 12NV HUXWI XAW DI XUI
SCQN QB HZXW NVXN XZZ EBCZW SBKA CQ NBWXO XAW DI
DXAN NB NVXAP DXPIMKIZW MBU JIKAH QCEV XA
BCNQNXAWKAH VBQN HKFI OBCUQIZFIQ X JKH UBCAW BM
XLLZXCQI XAW NVI PIO KQ
640I11012805M211J0XJ24MM02X1IW09

思路

直接词频分析

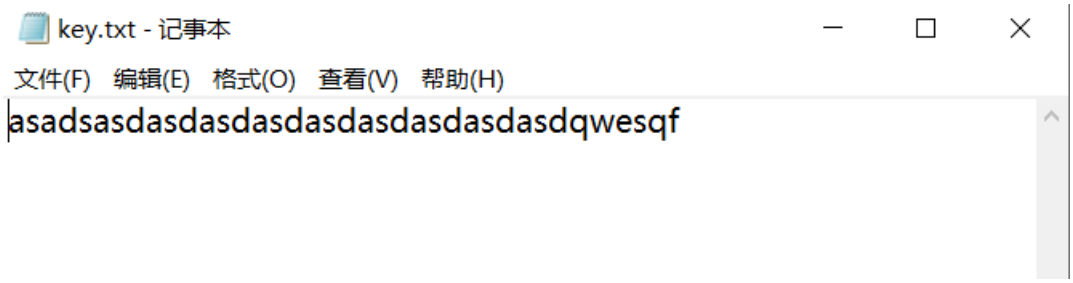
0	-1.288	HELLO EVERYBODY THANK YOU ALL RIGHT EVERYBODY GO AHEAD AND HAVE A SEAT HOW IS EVERYBODY DOING TODAY HOW ABOUT TIM SPICER WE ARE HERE WITH STUDENTS AT WAKEFIELD HIGH SCHOOL IN ARLINGTON VIRGINIA AND WE HAVE GOT STUDENTS TUNING IN FROM ALL ACROSS AMERICA FROM KINDERGARTEN THROUGH 12TH GRADE AND WE ARE JUST SO GLAD THAT ALL COULD JOIN US TODAY AND WE WANT TO THANK WAKEFIELD FOR BEING SUCH AN OUTSTANDING HOST GIVE YOURSELVES A BIG ROUND OF APPLAUSE AND THE KEY IS 640E11012805F211B0AB24FF02A1ED09
1	-3.037	HELLO EVERYBODY THANK YOU ALL RIGHT EVERYBODY GO AHEAD AND HAVE A SEAT HO? IS EVERYBODY DOING TODAY HO? ABOUT TI? SPICER ?E ARE HERE ?ITH STUDENTS AT ?AKEFIELD HIGH SCHOOL IN ARLINGTON VIRGINIA AND ?E HAVE GOT STUDENTS TUNING IN FRO? ALL ACROSS A?ERICA FRO? KINDERGARTEN THROUGH 12TH GRADE AND ?E ARE ?UST SO GLAD THAT ALL COULD ?OIN US TODAY AND ?E ?ANT TO THANK ?AKEFIELD FOR BEING SUCH AN OUTSTANDING HOST GIVE YOURSELVES A BIG ROUND OF APPLAUSE AND THE KEY IS 640E11012805F211B0AB24FF02A1ED09
2	-3.079	HELLO EVERYBODY THANK YOU ALL RIGHT EVERYBODY GO AHEAD AND HAVE A SEAT HO? IS EVERYBODY DOING TODAY HO? ABOUT TI? SPICER ?E ARE HERE ?ITH STUDENTS AT ?AKE?IELD HIGH SCHOOL IN ARLINGTON VIRGINIA AND ?E HAVE GOT STUDENTS TUNING IN ?RO? ALL ACROSS A?ERICA ?RO? KINDERGARTEN THROUGH 12TH GRADE AND ?E ARE ?UST SO GLAD THAT ALL COULD ?OIN US TODAY AND ?E ?ANT TO THANK ?AKE?IELD ?OR BEING SUCH AN OUTSTANDING HOST GIVE YOURSELVES A BIG ROUND O? APPLAUSE AND THE KEY IS 640E11012805?211B0AB24?F02A1ED09

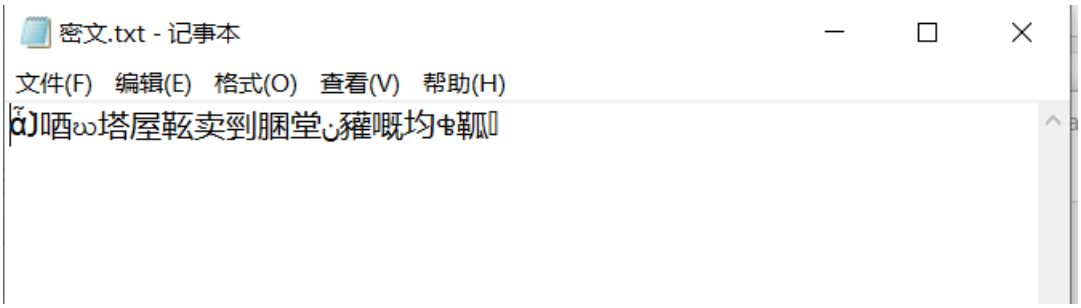
别忘记把大写改为小写。

异性相吸

题目

最近出现了一个奇葩观点，说性别都不一样，怎么能谈恋爱？为了证明这个观点错误，请大家证明异性是相吸的。里面有两个文本





思路

看到密文什么也没有发现，就看了一下两个文件的二进制，发现两个的二进制个数一样多，应该是异或，就用代码跑了一下

```
with open('密文.txt' )as a:
    a=a.read()
with open('key.txt' )as b:
    b=b.read()
d=''
for i in range(0,len(b)):
    c=chr(ord(a[i])^ord(b[i]))
    d+=c
print(d)
```

运行后就是flag。

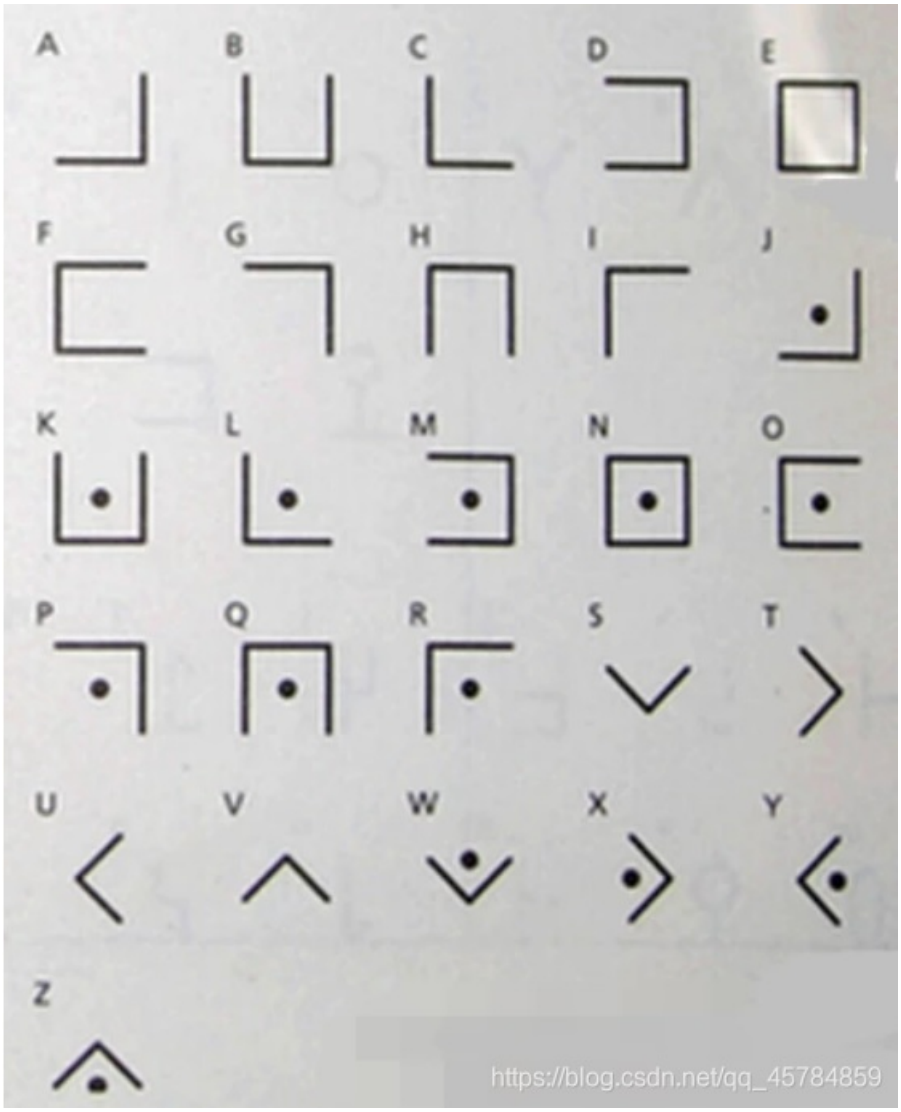
萌萌哒的八戒

题目

萌萌哒的八戒原来曾经是猪村的村长，从远古时期，猪村就有一种神秘的代码。请从附件中找出代码，看看萌萌哒的猪八戒到底想说啥

思路

很明显是猪圈密码，猪圈密码(Pigpen Cipher或称九宫格密码、朱高密码、共济会密码或共济会员密码)，是一种以格子为基础的简单替代式密码。更多参考

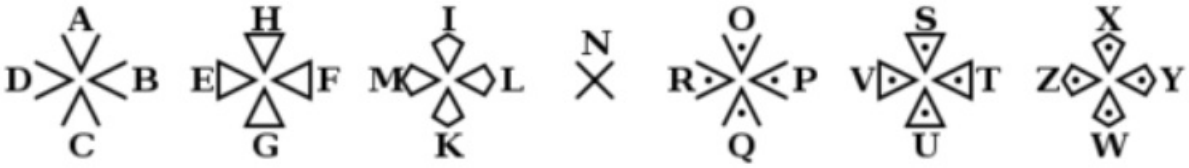


直接解密即可。

变种

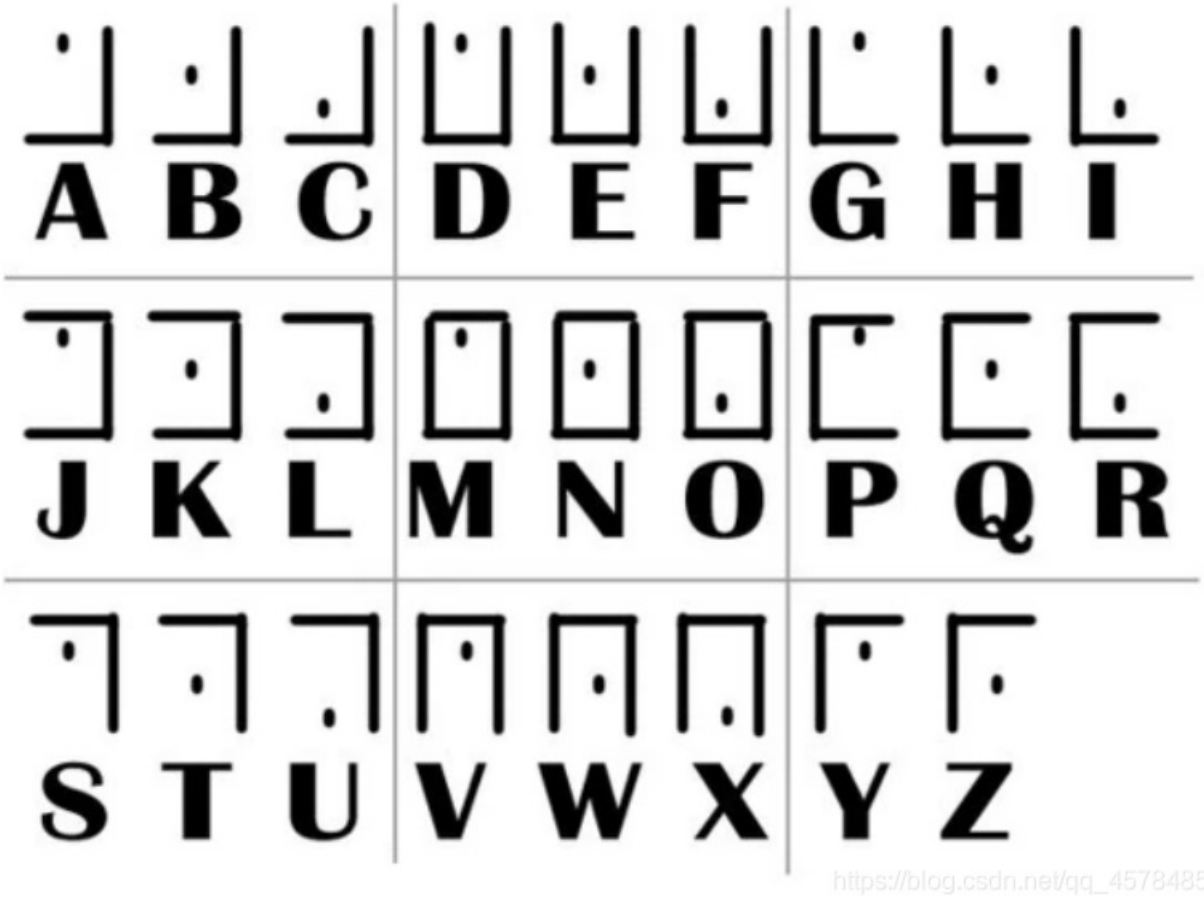
圣堂武士密码(Templar Cipher)是共济会的“猪圈密码”的一个变种，一直被共济会圣殿骑士用。

明文字母和对应密文：

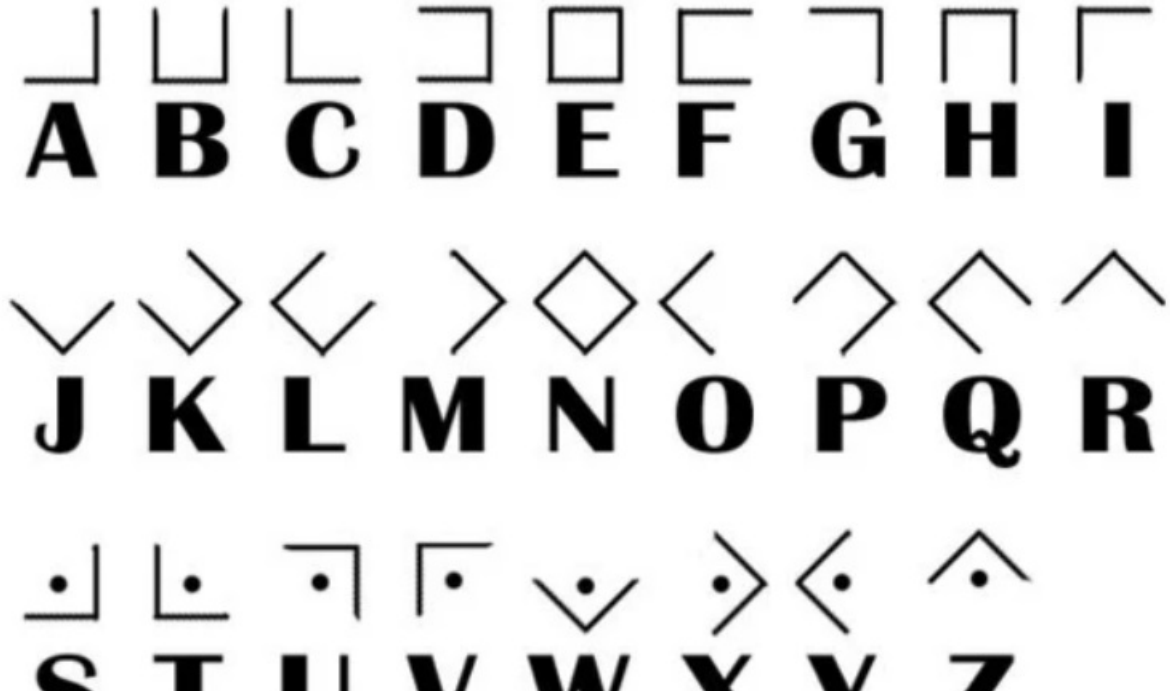


其他变种

明文字母和对应密文：



明文字母和对应密文：



明文字母和对应密文：