CRYPTO

原创

ngc2244 已于 2022-04-14 15:47:02 修改 144 收藏
分类专栏： CTF 文章标签： 安全
于 2022-04-14 13:03:53 首次发布

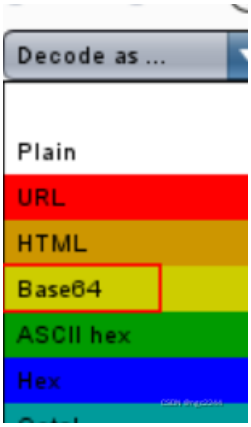
本文链接：https://blog.csdn.net/ngc2244/article/details/124168467

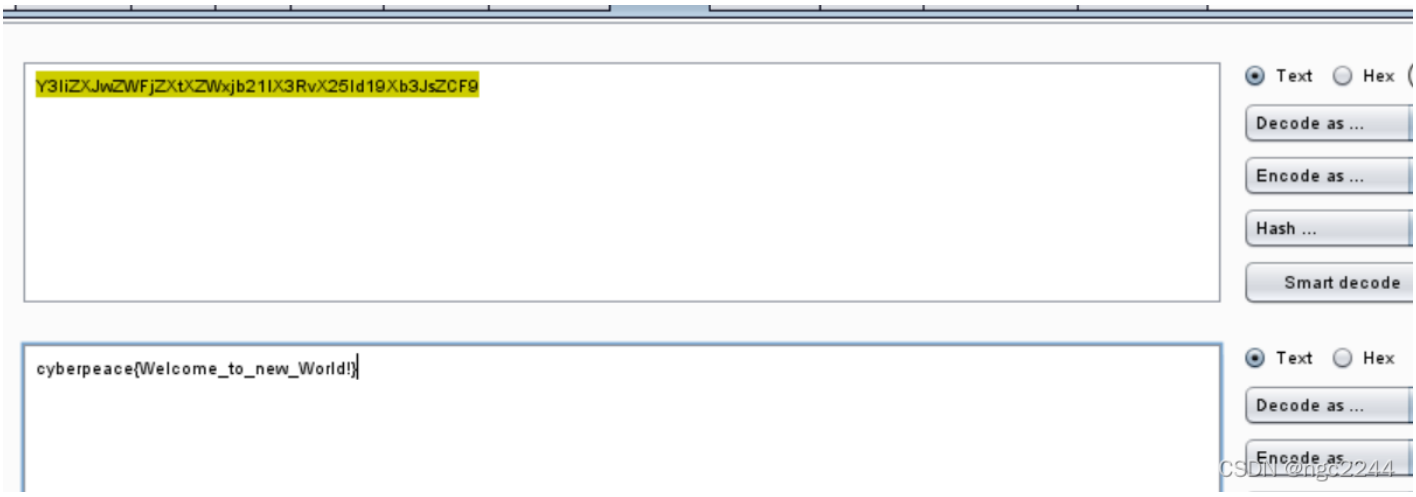

CTF 专栏收录该内容
4 篇文章 0 订阅
订阅专栏

1.base64

Y3liZXJwZWFjZXtXZWxjb21lX3RvX25ld19Xb3JsZCF9

解：





cyberpeace{Welcome_to_new_World!}

2.Caesar

凯撒密码

你成功的解出了来了灯谜，小鱼一脸的意想不到“没想到你懂得这么多啊！”你心里面有点小得意，“那可不是，论学习我没你成绩好轮别的我知道的可不比你少，走我们去看看下一个”你们继续走，看到前面也是热热闹闹的，同样的大红灯笼高高挂起，旁边呢好多人叽叽喳喳说个不停。你一看 大灯笼，上面还是一对字符，你正冥思苦想呢，小鱼神秘一笑，对你说道，我知道这个的答案是什么了

oknqdbqmoq

cyberpeace

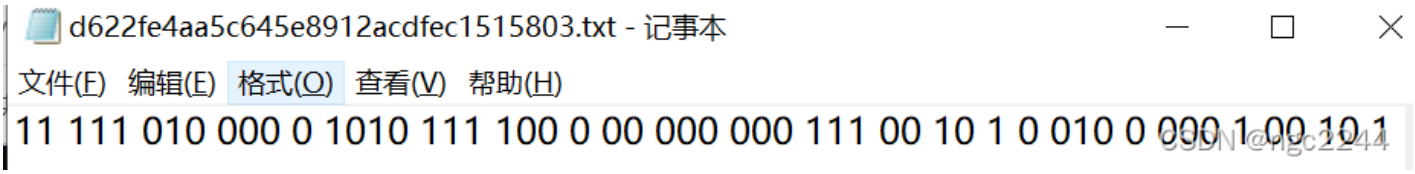
嗯。。。看样子移动了12位

凯撒密码在线加密解密 - 千千秀字 (qqxiuzi.cn)

cyberpeace{you_have_learned_caesar_encryption}

3.Morse

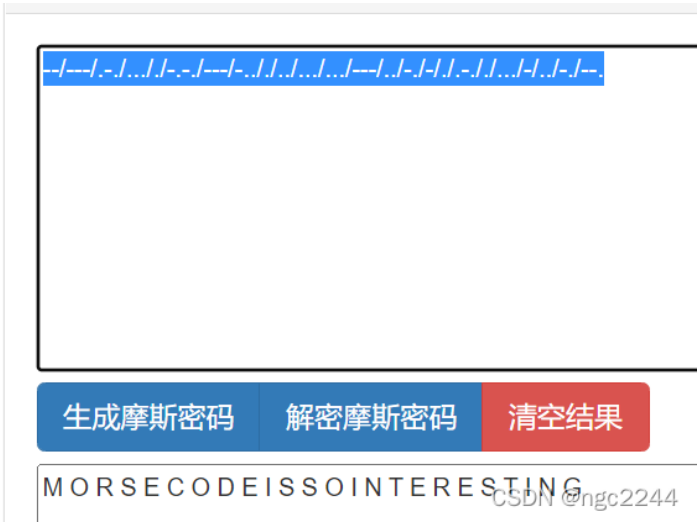
莫尔斯密码



工具： 在线摩斯密码加密,摩斯密码解密_懒人工具|www.ab173.com

> Morsecode：-- --- -·- ··· · / -·-· --- -·· · [3]
>
> 这里，“-”表示划，“.”表示点。这是上面消息的准确发报时间（“="表示信号有，”.“ 代表信号无，每个为一个点的长度

--/---/.-./..././-.-./---/-.././../.../.../---/../-./-/./.-././.../-/../-./--.



cyberpeace{morsecodeissointeresting}

4.幂数加密

云影密码（01248码）

这种加密方式仅使用01248这5种数字来进行，其中0用来唯一表示间隔，其他数字用加法和表示替换密文。再使用数字1~26表示字母A~Z。
如：18 = 1+8 = 9 = I，1248 = 1+2+4+8 = 15 = O

特点：密文中仅存在01248,加密对象仅有字母

例：CRYPTO001
88421 0122 048 02244 04 0142242 0248 0122
23 5 12 12 4 15 14 5
W E L L D O N E
可知falg为WELLDONE

答案：cyberpeace{WELLDONE}

答案：cyberpeace{WELLDONE}

5.Railfence

题目描述：被小鱼一连将了两军，你心里更加不服气了。两个人一起继续往前走， 一路上杂耍卖艺的很多，但是你俩毫无兴趣，直直的就冲着下一个谜题的地方去了。 到了一看，这个谜面看起来就已经有点像答案了样子了，旁边还画着一张画，是一副农家小院的 图画，上面画着一个农妇在栅栏里面喂5只小鸡，你嘿嘿一笑对着小鱼说这次可是我先找到答案了。

栅栏密码

就是把要加密的明文分成N个一组，然后把每组的第1个字连起来，形成一段无规律的话。 不过栅栏密码本身有一个潜规则，就是组成栅栏的字母一般不会太多。（一般不超过30个，也就是一、两句话）

原理：

①把将要传递的信息中的字母交替排成上下两行。

②再将下面一行字母排在上面一行的后边，从而形成一段密码。

③例如：

明文：THE LONGEST DAY MUST HAVE AN END

加密：

1、把将要传递的信息中的字母交替排成上下两行。

T E O G S D Y U T A E N N

H L N E T A M S H V A E D

2、 密文：

将下面一行字母排在上面一行的后边。

TEOGSDYUTAENN HLNETAMSHVAED

解密：

先将密文分为两行

T E O G S D Y U T A E N N

H L N E T A M S H V A E D

再按上下上下的顺序组合成一句话

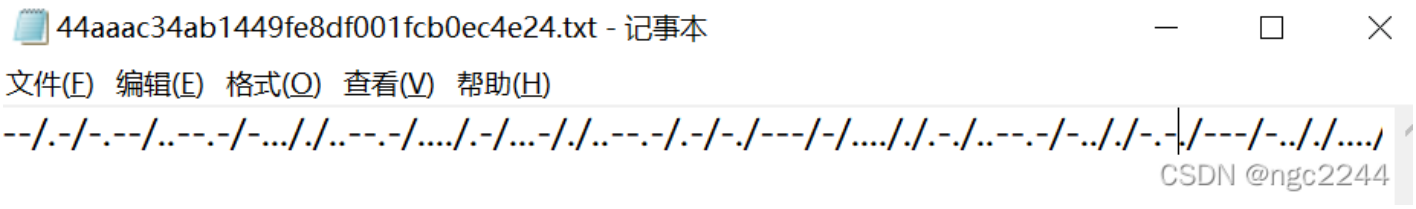
明文：THE LONGEST DAY MUST HAVE AN END

ccehgyaefnpeoobe{lcirg}epriec_ora_g

栅栏密码_栅栏密码在线加密解密【W型】-ME2在线工具 (metools.info)

6.不仅仅是Morse

题目描述：“这个题目和我们刚刚做的那个好像啊但是为什么按照刚刚的方法做出来答案却不对呢”，你奇怪的问了问小鱼，“可能是因为还有一些奇怪的加密方式在里面吧，我们在仔细观察观察”。两个人 安安静静的坐下来开始思考，很耐心的把自己可以想到的加密方式一种种的过了一遍，十多分钟后两个人 异口同声的说“我想到了！”。一种食物,格式为cyberpeace{小写的你解出的答案



在线摩斯密码加密,摩斯密码解密

```
--/.-/-.--/..--.-/-..././..--.-/..../.-/...-/./..--.-/.-/-./---/-/...././.-./..--.-/-.././-.-./--
-/-.././..../..../..../..../.-/.-/.-/.-/.-/-.../.-/.-/-.../-.../-.../.-/.-/-.../-.../.-/.-/.-/.-/.-/.-/.-/.-/-.../.-/.-/-.../.-/-.../.-/.-/.-/.-/.-/.-/.-/.-/-.../-.../.-/-.../.-/.-/.-/-.../-.../.-/.-/.-/-.../-.../.-/.-/-.../.-/.-/.-/.-/.-/-.../.-/-.../.-/.-/-.../.-/.-/.-/.-/-.../-.../.-/-.../.-/.-/.-/-.../.-/.-/.-/-.../.-/.-/-.../.-/-.../-.../.-/.-/-.../-.../-.../.-/-.../.-/.-/.-/-.../.-/-.../.-/-.../-.../.-/.-/.-/-.../-.../.-/-.../.-/.-/.-/-.../.-/.-/-.../.-/.-/-.../.-/.-/.-/.-/-.../-.../.-/-.../-.../.-/.-/-.../-.../.-/.-/-.../.-/.-/-.../.-/.-/.-/-.../.-/.-/-.../.-/.-/-.../.-/.-/-.../.-/-.../.-/.-/-.../-.../.-/-.../.-/.-/.-/.-/.-/-.../-.../.-/-.../.-/.-/-.../-.../.-
```

生成摩斯密码 | 解密摩斯密码 | 清空结果

```
MAY%udBE%udHAVE%udANOTHER%udDECODEHHHHAAAAABAABBBAABBAAAAAAAABAABABAAAAAAAABBABAAABBAAABB
AABAAAAABABAABAAAABBABAAABAAABAABABBAABBBABAAABABABBAAABBABAAABAABAABAAAABBABBAABBAABAABAA
ABAABAABAABABAABBABAAAAABBABAABBA
```

CSDN @ngc2244

AABBAA好规律，一查培根密码，不愧与食物有关啊

加密时，明文中的每个字母都会转换成一组五个英文字母。其转换依靠下表：

A/a	aaaaa	H/h	aabbb	O/o	abbba	V/v	babab
B/b	aaaab	I/i	abaaa	P/p	abbbb	W/w	babba
C/c	aaaba	J/j	abaab	Q/q	baaaa	X/x	babbb
D/d	aaabb	K/k	ababa	R/r	baaab	Y/y	bbaaa
E/e	aabaa	L/l	ababb	S/s	baaba	Z/z	bbaab
F/f	aabab	M/m	abbaa	T/t	baabb		
G/g	aabba	N/n	abbab	U/u	babaa		

加密者需使用两种不同字体，分别代表A和B。准备好一篇包含相同AB字数的假信息后，按照密文格式化假信息，即依密文中每个字母是A还是B分别套用两种字体。

解密时，将上述方法倒转。所有字体一转回A，字体二转回B，以后再按上表拼回字母。

CSDN @ngc2244

工具:在线工具|培根密码加解密 (bugku.com)

复制ABABA解密：

将空格去掉

aaaaabaabbbaabbaaaaaaaabaababaaaaaaaabbabaaabbaaabbaabaaaababaabaaaabbabaaabaaabaababbaabb

整理：

Bugku|培根密码加解密

ATTACKANDDEFENCEWORLDISINTERESTING
attackanddefenceworldisinteresting

CSDN @ngc2244

cyberpeace{attackanddefenceworldisinteresting}

7.混合编码

经过了前面那么多题目的历练，耐心细致在解题当中是 必不可少的品质，刚巧你们都有，你和小鱼越来越入迷。那么走向了下一个题目，这个题目好长 好长，你知道你们只要细心细致，答案总会被你们做出来的，你们开始慢慢的尝试，慢慢的猜想 ，功夫不负有心人，在你们耐心的一步步的解答下，答案跃然纸上，你俩默契一笑，相视击掌 走向了下面的挑战。格式为cyberpeace{小写的你解出的答案}

BASE64解密解出一长串数字

unicode编码

例如：原文本：You had me at hello

编码后

\u0059\u006f\u0075\u0020\u0068\u0061\u0064\u0020\u006d\u0065\u0020\u0061\u0074\u00
68\u0065\u006c\u006c\u006f

编码示例：

明文：hello

四种编码方式：

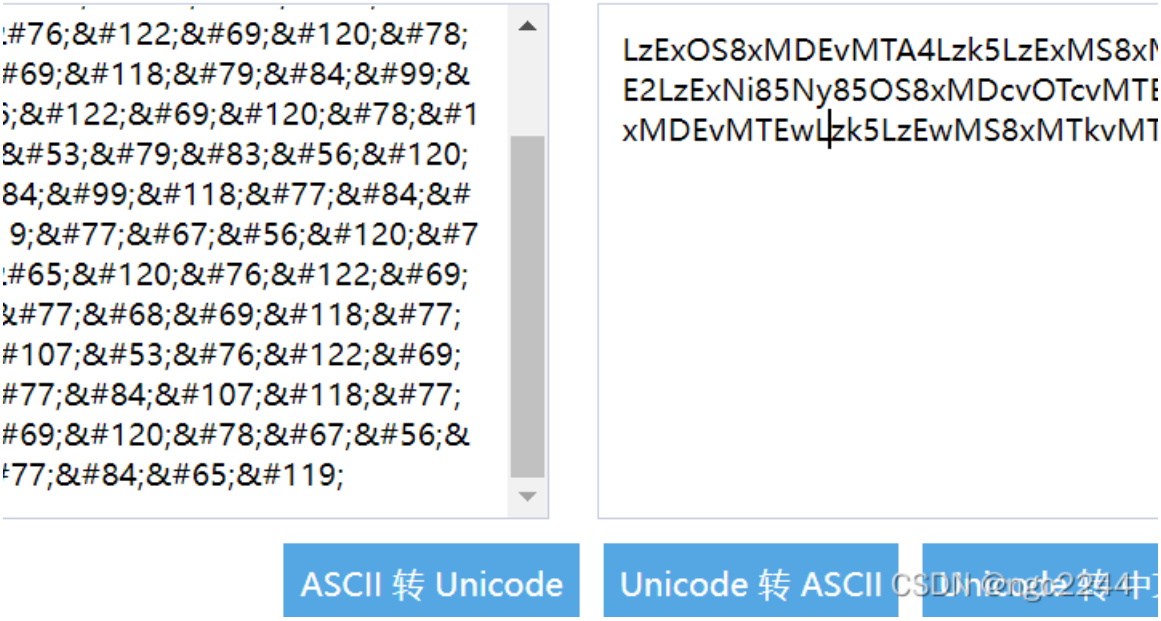
&#x [Hex]：hello

&# [Decimal]：hello

\U [Hex]：\U0068\U0065\U006C\U006C\U006F

\U+ [Hex]：\U+0068\U+0065\U+006C\U+006C\U+006F

工具：Unicode编码转换 - 站长工具 (chinaz.com)



再次BASE64

```
/119/101/108/99/111/109/101/116/111/97/116/116/97/99/107/97/110/100/100/101/102/101/110/99/101/119/111/114/
```

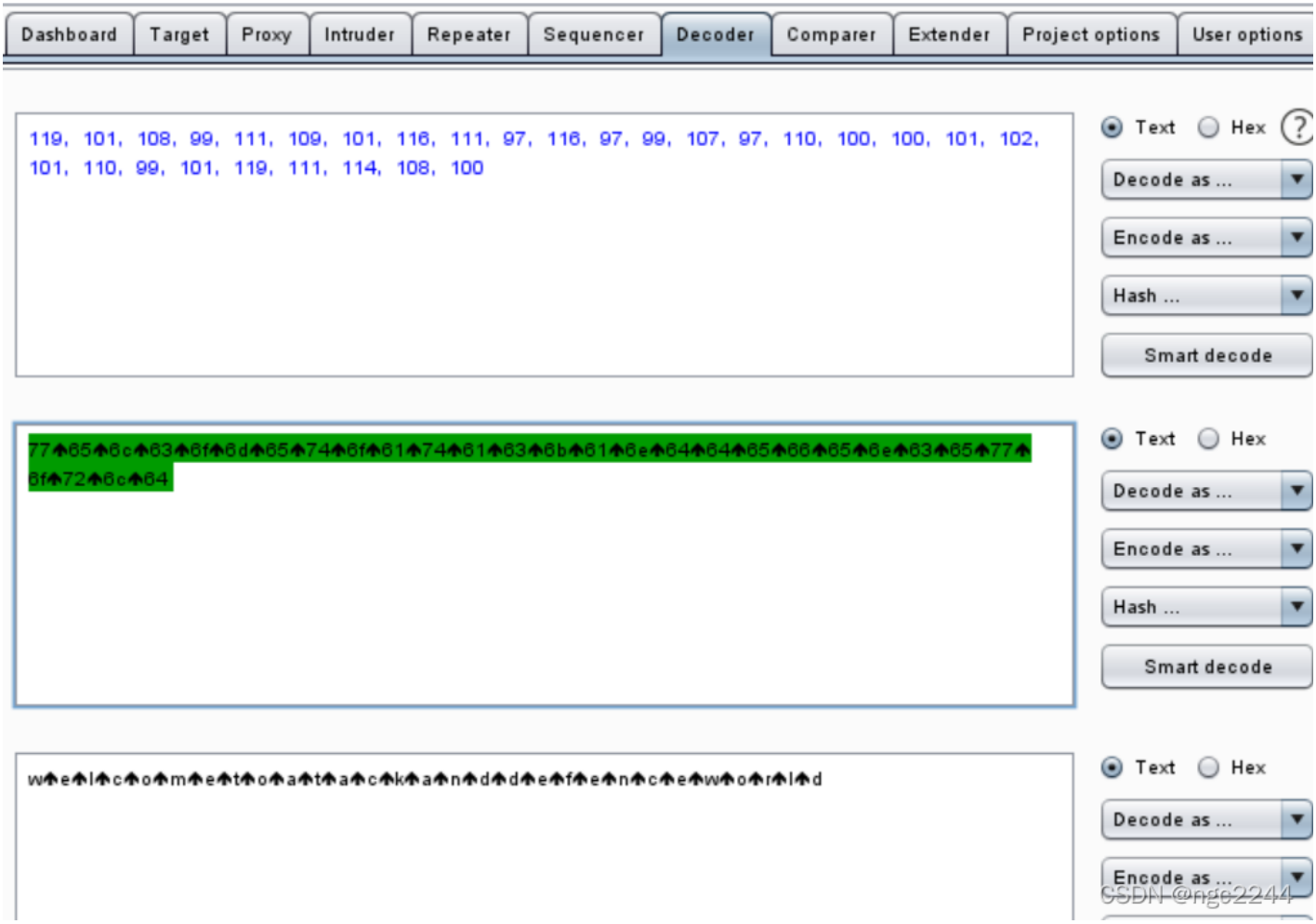
将/变成，

```
119，101，108，99，111，109，101，116，111，97，116，97，99，107，97，110，100，100，101，102，101，110，99，101，
```

弄到Burp中，将数字转换为ACSII

第一步encode as hex

第二步decode as ascii hex



整理：welcometoattackanddefenceworld

cyberpeace{welcometoattackanddefenceworld}

8.转轮机加密

你俩继续往前走，来到了前面的下一个关卡，这个铺面墙上写了好多奇奇怪怪的 英文字母，排列的的整整齐齐，店面前面还有一个大大的类似于土耳其旋转烤肉的架子，上面一圈圈的 也刻着很多英文字母，你是一个小历史迷，对于二战时候的历史刚好特别熟悉，一拍大腿：“嗨呀！我知道 是什么东西了！”。提示：托马斯·杰斐逊。 flag，是字符串，小写。

解：

攻防世界-新手-crypto-转轮机加密 - 知乎 (zhihu.com)

手工解密：

1: < ZWAXJGDLUBVIQHKYPNTCRMOSFE <
2: < KPBEL**NACZDTRXMJQOYHGVSFUWI** <
3: < BDMAIZVRNSJUWFHTEQGYXPLOCK <
4: < RPLNDVHGFCUKTEBSXQYIZMJWAO <
5: < IHFRLABEUOTSGJVDKCPMNZQWXY <
6: < AMKGHIWPNYCJBFZDRUSLOQXVET <
7: < GWTHSPYBXIZULVKMRAFDCEONJQ <
8: < NOZUTWDCVRJLXKISEFAPMYGHBQ <
9: < XPLTDSRFHENYVUBMCQWAOIKZGJ <
10: < UDNAJFBOWTGVRSCZQKELMXYIHP <
11： < MNBVCXZQWERTPOIUYALSKDJFHG <
12： < LVNCMXZPQOWEIURYTASBKJDFHG <
13： < JZQAWSXCDERFVBGTYHNUMKILOP <

密钥为：2,3,7,5,13,12,9,1,8,10,4,11,6
密文为：NFQKSEVOQOFNP

2行对应N，**N到第一位**

3行对应F，F到第一位

7行对应Q

得到下列等式

2: <**NACZDTRXMJQOYHGVSFUWI**KPBEL <
3: <FHTEQGYXPLOCKBDMAIZVRNSJUW <
7: <QGWTHSPYBXIZULVKMRAFDCEONJ<
5: <KCPMNZQWXYIHFRLABEUOTSGJVD<
13< SXCDERFVBGTYHNUMKILOPJZQAW <
12< EIURYTASBKJDFHGLVNCMXZPQOW <
9: < VUBMCQWAOIKZGJXPLTDSRFHENY <
1: <OSFEZWAXJGDLUBVIQHKYPNTCRM <
8: <QNOZUTWDCVRJLXKISEFAPMYGHB <
10:<OWTGVRSCZQKELMXYIHPUDNAJFB <
4: <FCUKTEBSXQYIZMJWAORPLNDVHG <
11< NBVCXZQWERTPOIUYALSKDJFHGM<
6: <PNYCJBFZDRUSLOQXVETAMKGHIW <

第一列的内容即为密文,按照列读找flag,找到了 fireinthehole

< NACZDTRXMJQOYHGVSFUWIKPBEL <
< FHTEQGYXPLOCKBDMAIZVRNSJUW <
< QGWTHSPYBXIZULVKMRAFDCEONJ <
< KCPMNZQWXYIHFRLABEUOTSGJVD <
< SXCDERFVBGTYHNUMKILOPJZQAW <
< EIURYTASBKJDFHGLVNCMXZPQOW <
< VUBMCQWAOIKZGJXPLTDSRFHENY <
< OSFEZWAXJGDLUBVIQHKYPNTCRM <
< QNOZUTWDCVRJLXKISEFAPMYGHB <
< OWTGVRSCZQKELMXYIHPUDNAJFB <
< FCUKTEBSXQYIZMJWAORPLNDVHG <
< NBVCXZQWERTPOIUYALSKDJFHGM <
< PNYCJBFZDRUSLOQXVETAMKGHIW <

9.

参考：https://blog.csdn.net/m0_59207381/article/details/119318350

五星：

(1条消息) CTF密码学——常见编解码及加解密总结_Ahuuua的博客-CSDN博客_元音密码

(1条消息) 常见古典密码_鹹魚不鹹的博客-CSDN博客_费纳姆密码

(1条消息) XCTF-攻防世界-密码学crypto-新手练习区-writeup_Ryannn-的博客-CSDN博客

大小写转换工具：在线英文字母大小写转换器工具-包含英文大写转小写-字母小写转大写_蛙蛙在线工具(iamwawa.cn)