

crypto密码总结

原创

 [tjy](#)  已于 2022-03-25 23:53:38 修改  258  收藏 2

文章标签: [web安全](#)

于 2022-03-24 00:07:36 首次发布

版权声明: 本文为博主原创文章, 遵循 [CC 4.0 BY-SA](#) 版权协议, 转载请附上原文出处链接和本声明。

本文链接: https://blog.csdn.net/weixin_63289925/article/details/123691439

版权

base64编码: 字母A-Z、a-z、数字0-9

base32编码: 大写字母(A-Z)和数字234567

base16编码: 数字0-9以及大写字母ABCDEF

base91编码:

例: @iH<,{bdR2H;i6*Tm,Wx2izpx2!

ASCII密码:

数字0~9对应的ASCII码(十进制)为“48”~“57”

大写字母A~Z对应的ASCII码(十进制)为“65”~“90”

小写字母a~z对应的ASCII码(十进制)为“97”~“122”

Morse Code

A	•—	M	—•—	Y	—•—•—	6	—••••
B	—•••	N	—••	Z	—••••	7	—•—•••
C	—••—•	O	—•—•—	Ä	•—••—	8	—•—•—••
D	—•••	P	•—•—••	Ö	—•—•—••	9	—•—•—•—••
E	•	Q	—•—••—	Ü	••—•—	.	•—••—•—•—
F	••—••	R	•—•••	Ch	—•—•—•—	,	—•—•••—•—
G	—•—••	S	••••	0	—•—•—•—•—	?	••—•—•••
H	•••••	T	—•—	1	•—•—•—•—	!	••—•—•••
I	•••	U	••—•—	2	••—•—•—•—	:	—•—•—•—•••
J	•—•—•—•—	V	••••—	3	••••—•—	"	•—••••—•—
K	—•••—	W	•—•—•—	4	•••••—	'	•—•—•—•—•—
L	•—••••	X	—••••—	5	••••••	=	—•••••—

CSDN @ tjtj

网站: <http://ctf.ssleye.com/morse.html>

栅栏密码: 大小写和字符

把要加密的明文分成N个一组, 然后把每组的第1个字符组合, 每组第2个字符组合...每组的第N(最后一个分组可能不足N个)个字符组合, 最后把他们全部连接起来就是密文。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)

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。

TEOGSDYUTAENN

HLNETAMSHVAED

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

TEOGSDYUTAENN

HLNETAMSHVAED

再按上下上下的顺序组合成一句话

明文: THE LONGEST DAY MUST HAVE AN END

栅栏密码变形: W型

ccehgyaefnpeoobe{lcirg}epriec_ora_g

CSDN @ t j y

例:

解密加密网站: 栅栏密码_栅栏密码在线加密解密【W型】-ME2在线工具

Input field containing the ciphertext: ccehgyaefnpeoobe{lcirg}epriec_ora_g

Control panel with '栏目数: 5', a dropdown arrow, and '加密>' and '解密>' buttons.

转换后: [copy icon]

Output field containing the plaintext: cyberpeace{railfence_cipher_gogogo}

CSDN @ t j y

Ook密码: Ook和三个标点(!?)

Ook.
Ook. Ook. Ook. Ook. Ook. Ook! Ook? Ook! Ook! Ook. Ook? Ook. Ook. Ook. Ook.

CSDN @ t j y

要么就是没有Ook只有标点

..... !?!! ?..... .??.! ?... !.....
!?. .. .!?! ?!!!! !!?.? !?! !!! .. .!?.

CSDN @ t j y

网站: <https://www.splitbrain.org/services/ook>

Brainfuck密码: +, -, [], <>组成

+++++ +++++ [->++ +++++ +++<] >++.+ +++++ .<+++ [->-- -<]>- -.+++ +++.<
+++++ [->+++ +<]>+ +++.< +++[- ->--<]>-- .---- .<+++ +++++ [->--

CSDN @ t j y

jsfuck密码: +,!,(),[]

(![]+[])[+[]]+(![]+[])[![]+[]+[]]+(!
[]+[])[+[]+[]]+(![]+[]+[])+([]+[]+[])

CSDN @ t j y

凯撒密码: 英文字母排序偏移

明文字母表: ABCDEFGHIJKLMNOPQRSTUVWXYZ

密文字母表: DEFGHIJKLMNOPQRSTUVWXYZABC

例: 攻防世界Caesar

oknqdbqmoq{kag_tmhq_xqmdzqp_oShqemd_qzodkbfuaz}

CSDN @ t j y

oknqdbqmoq(kag_tmhq_xqmdzqp_omqemd_qzodkbfuaz)

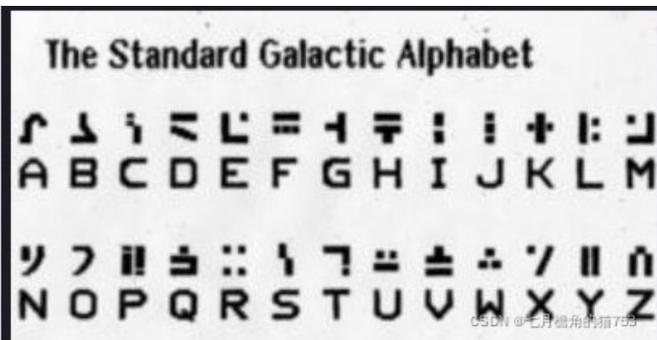
因为是凯撒密码，所以有位移的关系，因为说明了flag提交方式是cyberpeace{xxxxxxxx}把第一个字母o位移到字母c，位移量是12，解密即可

棋盘密码：一种查表加密法,小写字母(数字没两个一组,数字范围为1~5)

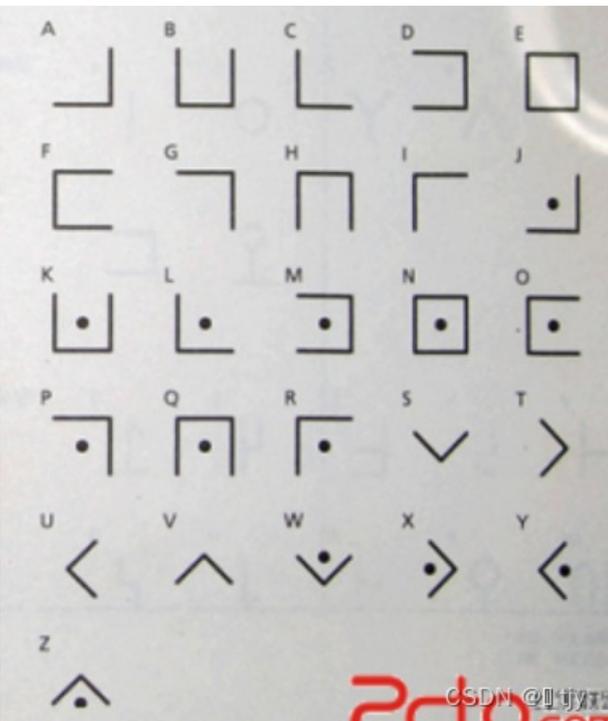
	1	2	3	4	5
1	a	b	c	d	e
2	f	g	h	i,j	k
3	l	m	n	o	p
4	q	r	s	t	u
5	v	w	x	y	

网站：<https://www.qqxiuzi.cn/bianma/qipanmima.php>

银河密码：



猪圈密码：



md5编码：一般为32位，由数字和小写字母组成（数字1~9，字母a~f）

18414996c5377f5f4419a40eba901789

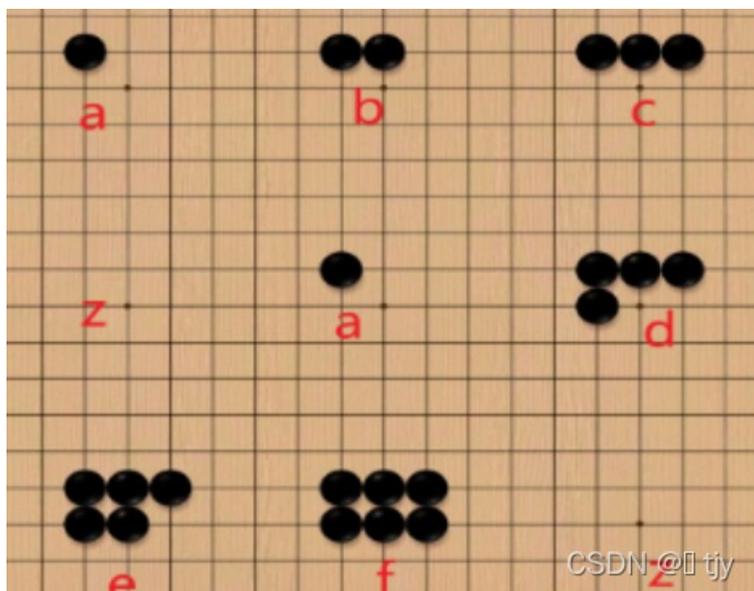
希尔密码：是运用基本矩阵论原理的替换密码，每个字母当作26进制数字：A=0, B=1, C=2... 一串字母当成n维向量，跟一个n×n的矩阵相乘，再将得出的结果MOD26。

■ Cipher Text = (Plain Text x Key) Mod 26

$$= \begin{bmatrix} 0 & 19 & 19 \\ 0 & 2 & 10 \\ 8 & 18 & 19 \\ 14 & 13 & 8 \\ 6 & 7 & 19 \end{bmatrix} \times \begin{bmatrix} 3 & 10 & 20 \\ 20 & 9 & 17 \\ 9 & 4 & 17 \end{bmatrix} \text{ Mod } 26$$

CSDN @ tjt

例题：bugku 小山丘的秘密



CSDN @ tjt

bugku{PLGTGBQHM}

其中A=1, flag全为小写

本来A=0, 所以现在Z=0, 字母表就变成zabcdefghijklmnopqrstuvwxy

密钥看图片一颗棋子代表数字1, 则表示a, 两颗棋子代表数字2, 表示b, 所以密钥为abczadefzs

字母表

zabcdefghijklmnopqrstuvwxy

plgtgbqhm

密钥

abczadefz

加密

解密

whatahill

CSDN @ t j y

希尔解密即可

希尔密码加密/解密 - 一个工具箱 - 好用的在线工具都在这里!

Unicode编码:每一字符都用一个5位字符编码表示,并用\分割

\u0066\u006c\u0061\u0067\u007b\u0069\
u005f\u0077\u0069\u006c\u006c\u0051\u006b

核心价值观编码:

自由友善爱国平等敬业平等和谐自由平等自由和谐法治诚信民主公正爱国公正平等平等友善敬业法治爱国公正敬业公正诚信自由平
等诚信平等公正诚信富强公正敬业公正民主平等诚信平等法治诚信富强公正爱国公正敬业法治友善法治

CSDN @ t j y

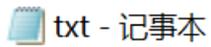
键盘解密:

例1: **qwerty**键盘

bhjm,6tghu7,wazxde,3wsdr4,xdfv,bhjm,ujko98,7yhji8,0ol

bhjm: 在键盘上将26个字母中的n包围了
 6tghu7: 在键盘上将26个字母中的y包围了
 wazxde: 在键盘上将26个字母中的s包围了
 3wsdr4: 在键盘上将26个字母中的e包围了
 xdfv: 在键盘上将26个字母中的c包围了
 bhjm: 在键盘上将26个字母中的n包围了
 ujko98: 在键盘上将26个字母中的i包围了
 7yhji8: 在键盘上将26个字母中的u包围了
 0ol: 在键盘上将26个字母中的p包围了

例2: 手机键盘



文件(F) 编辑(E) 格式(O) 查看(V) 帮助(H)

33 53 21 41 21 53 82 23 52 93 31 21 93

CSDN @七月橘角的猫753



33是指第三个按键里的第三个字母，既F。53则指第五个按键的第三个字母L

佛箴言密码:

佛曰：涅罰廬室呐礙侄穆俱南穆冥竟俱闍婆是哆殿俱至奢顛侄訶鉢亦故醯怯有依罰利梵等漫以訶梵喝咒鉢依鉢大奢礙奢得侄迦道。
 薩苦薩怯藐怯至得離孕夜若盡罰遠罰涅俱數除彌呐吉所諳沙咒所伽侄耶冥依奢夷夢知罰呼呐至諳究

CSDN @tjy

解密网站: [与佛论禅](#)

当铺密码: 中文和数字进行转化的密码，算法相当简单:当前汉字有多少笔画出头，就是转化成数字几（俺称笔画密码）

羊由大井夫大人王中工

词频密码:

```
Eg qnlyjtcnzydl z umaujejmjetg qeydsn eu z bsjdtx tw
sgqtxegc al kdeqd mgeju tw yrzegsoj zns nsyrzqsx kejd
qeydsnjsoj
Ew ltm fgtk jds kzl tw sgqtxegc m kerr csj jds wrzc
kdeqd eu qrzuueqzr-qeydsn_eu_gtj_usqmnejs_du @ t j y
```

加密网站: [quipqiup - cryptoquip and cryptogram solver](#)

urlencode编码: 将需要转码的字符转为**16进制**, 然后从右到左, 取4位(不足4位直接处理), 每2位做一位, 前面加上%, 编码成%ab格式。

空格**ASCII**码是32, 对应16进制是20, 那么urlencode编码结果是:%20,但在新标准中空格对应的是+。字母是不进行编码的

```
%68%61%63%6b%65%72%41%4a
```

sha1编码: 40 位 (由数字和小写字母组成)

```
7c2380341e0f03f81f873ab8d2ea5b88bc690703
```

博多密码: 是一种5位代表一个字节的编码。每一个字母都由五个单位的电流开或关信号组成, 它们的持续时间相等, 进而来传达信息

Letters	Figures	KEYS					Letters	Figures	KEYS					
		V	IV	I	II	III			V	IV	I	II	III	
A	1			⊙			P	+	⊙	⊙	⊙	⊙	⊙	
B	8		⊙			⊙	Q	/	⊙	⊙	⊙		⊙	
C	9		⊙	⊙		⊙	R	-	⊙	⊙			⊙	
D	0		⊙	⊙	⊙	⊙	S	7	⊙				⊙	
E	2				⊙		T	2	⊙		⊙		⊙	
F	3		⊙		⊙	⊙	U	4			⊙		⊙	
G	7		⊙		⊙		V	'	⊙		⊙	⊙	⊙	
H	1		⊙	⊙	⊙		W	?	⊙			⊙	⊙	
I	3				⊙	⊙	X	9	⊙			⊙		
J	6		⊙	⊙			Y	3						⊙
K	(⊙	⊙	⊙			Z	:	⊙		⊙	⊙		
L	=	⊙	⊙	⊙	⊙		-	.	⊙		⊙			
M)	⊙	⊙		⊙		*	*	⊙	⊙		(Erasure)		
N	£	⊙	⊙		⊙	⊙	Figure shift & space			⊙				
O	5			⊙	⊙	⊙	Letter shift & space		⊙					
/	1			⊙	⊙									

FIG. 22.

BAUDÔT SIGNALLING CODE OR ALPHABET (BRITISH).

https://blog.csdn.net/qq_34398519

网站: <https://www.boxentriq.com/code-breaking/ baudot-code>

培根密码: 加密时, 明文中的每个字母都会转换成一组五个英文字母。

第一种方式

A	aaaaa	H	aabbb	O	abbba	V	babab
B	aaaab	I	abaaa	P	abbbb	W	babba
C	aaaba	J	abaab	Q	baaaa	X	babbb
D	aaabb	K	ababa	R	baaab	Y	bbaaa
E	aabaa	L	ababb	S	baaba	Z	bbaab
F	aabab	M	abbaa	T	baabb		
G	aabba	N	abbab	U	babaa		

第二种方式

a	AAAAA	g	AABBA	n	ABBAA	t	BAABA
b	AAAAB	h	AABBB	o	ABBAB	u-v	BAABB
c	AAABA	i-j	ABAAA	p	ABBBA	w	BABAA
d	AAABB	k	ABAAB	q	ABBBB	x	BABAB
e	AABAA	l	ABABA	r	BAAAA	y	BABBA
f	AABAB	m	ABABB	s	BAAAB	z	BABBB

网站: [Baconian Cipher](#)

杰弗逊转轮加密:

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

密钥为: 2,3,7,5,13,12,9,1,8,10,4,11,6

密文为: NFQKSEVOQOFNP

CSDN @ tjtj

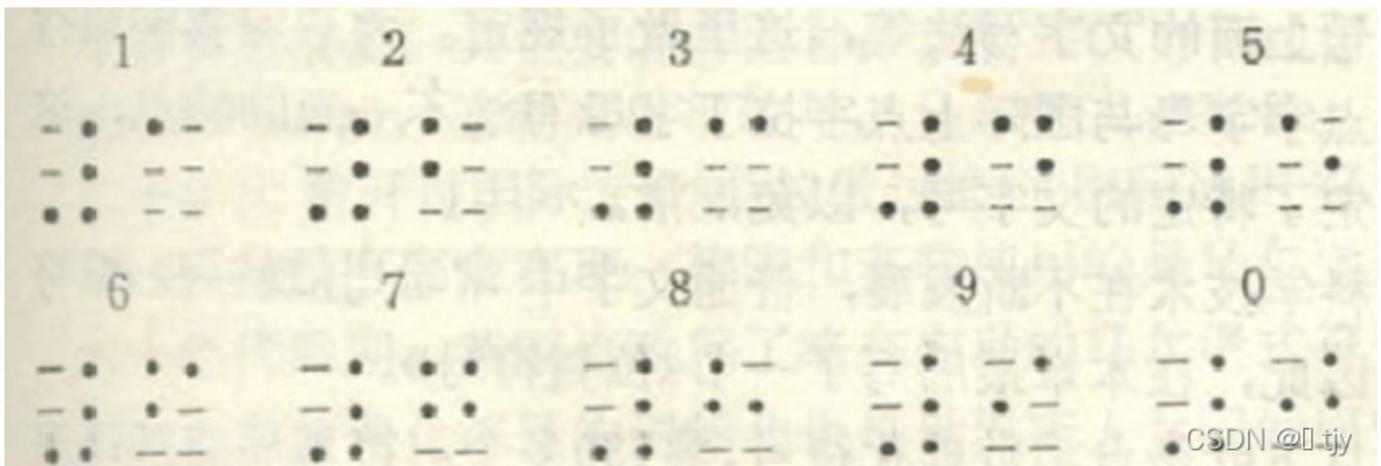
首先查看密钥第一个字符为2, 因此我们需要到加密表中去查找第2行的数据 2: <

KPBELNACZDTRXMJQOYHGVSFUWI < 这里我们再利用密文的第一个字符N进行旋转, N在这里的作用就是旋转过后的第一个字符即为N, 在这里的旋转为循环, 不为补0 因此我们可以来对加密表中的第一段密文进行解密: 原先: KPBELNACZDTRXMJQOYHGVSFUWI 旋转: NACZDTRXMJQOYHGVSFUWIKPBEL

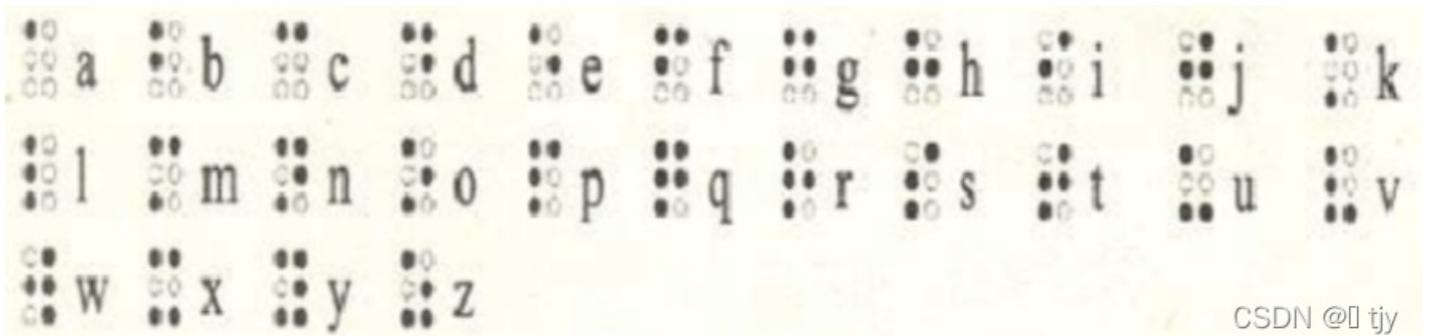
< NACZDTRXMJQOYHGVSFJWIKPBEL <
 < FHTEQGYXPLOCKBDMAIZVRNSJUW <
 < QGWITHSPYBXIZULVKMRAFDCEONJ <
 < KCPMNZQWXYIHFRLABEJOTSGJVD <
 < SXCDERFVBGTYHNUMKILOPJZQAW <
 < EIURYTASBKJDFHGLVNCMXZPQOW <
 < VUBMCQWAOIKZGJXPLTDSRFHENY <
 < OSFEZWAXJGDLUBVIQHKYPNTCRM <
 < QNOZUTWDCVRJLXKISEFAPMYGHB <
 < OWTGVRSCZQKELMXYIHPUDNAJFB <
 < FCUKTEBSXQYIZMJWAORPLNDVHG <
 < NBVCXZQWERTPOIUYALSKDJFHGM <
 < PNYCJBFZDRUSLOQXVETAMKGIW <

盲文密码:

数字盲文:



英文字母盲文:



汉语拼音盲文声母表: 没有全部举出, 随便截了点, 大概知道点



QWE密码：QWE格式密码就是QWERTYUIOP ASDFGHJKL ZXCVBNM 依次表示字母 ABCDEFGHIJKLMNOPQRSTUVWXYZ。



BubbleBabble密码解密/加密：

例：bugku EN-气泡

xivak-notuk-cupad-tarek-zesuk-zupid-taryk-zesak-cined-tetuk-nasuk-zoryd-tirak-zysek-zaryd-tyrik-nisyk-nenad-tituk-nysil-hepyd-tov

套娃解密三次

解密网站：[CTF在线工具-在线BubbleBabble编码|Bubble编码|BubbleBabble解码|BubbleBabble编码原理|BubbleBabble编码算法](#)**元音密码：**元音密码表（1~5开头的数字）

A	B	C	D	E	F	G	H	I	J	K	L	M	N
1	11	12	13	2	21	22	23	3	31	32	33	34	35
O	P	Q	R	S	T	U	V	W	S	Y	Z		
4	41	42	43	44	45	5	51	52	53	54	55		

例：bugku Math&English

你会数学和英语吗?

$$3 \times 7 = 21$$

$$11 \times 3 = 33$$

$$\sin(\pi/6) + \sin(\pi/6) = 1$$

$$2 \times 11 = 22$$

$$3 \times \cos(2\pi) = 3$$

$$22 \times 2 = 44$$

$$6 \times 9 = 54$$

$$2.5 \times 2 = 5$$

$$\tan(\pi) + 1 = 1$$

$$5 \times 7 = 35$$

$$7 \times 9 - 9 = 53$$

$$\ln(e) + 2 = 3$$

$$(6 \times 6) - 1 = 35$$

$$4 \times 10 + \cos(0) = 41$$

$$26 \times 2 = 52$$

$$\ln(e) \times 10 + 3 = 13$$

FLAGISYUANSINPWD

flagisyuansinpwd CSDN @ tjt

7*9-9=54, 算错一个(草率□)算出来的数字跟字母表一一对应

ROT13解密:

ROT13回转十三位, 是一种简易的替换式密码, 也是过去在古罗马开发的凯撒加密的一种变体。

ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz

NOPQRSTUVWXYZABCDEFGHIJKLMnopqrstuvwxyzabcdefghijklm

例: buuctf 看我回旋踢

synt{5pq1004q-86n5-46q8-o720-oro5on0417r1}

解密网站: ROT13 @ <http://www.rot13.de/>