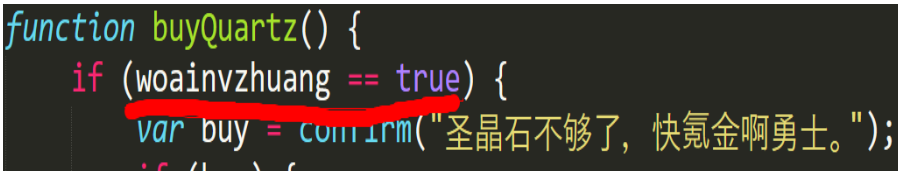
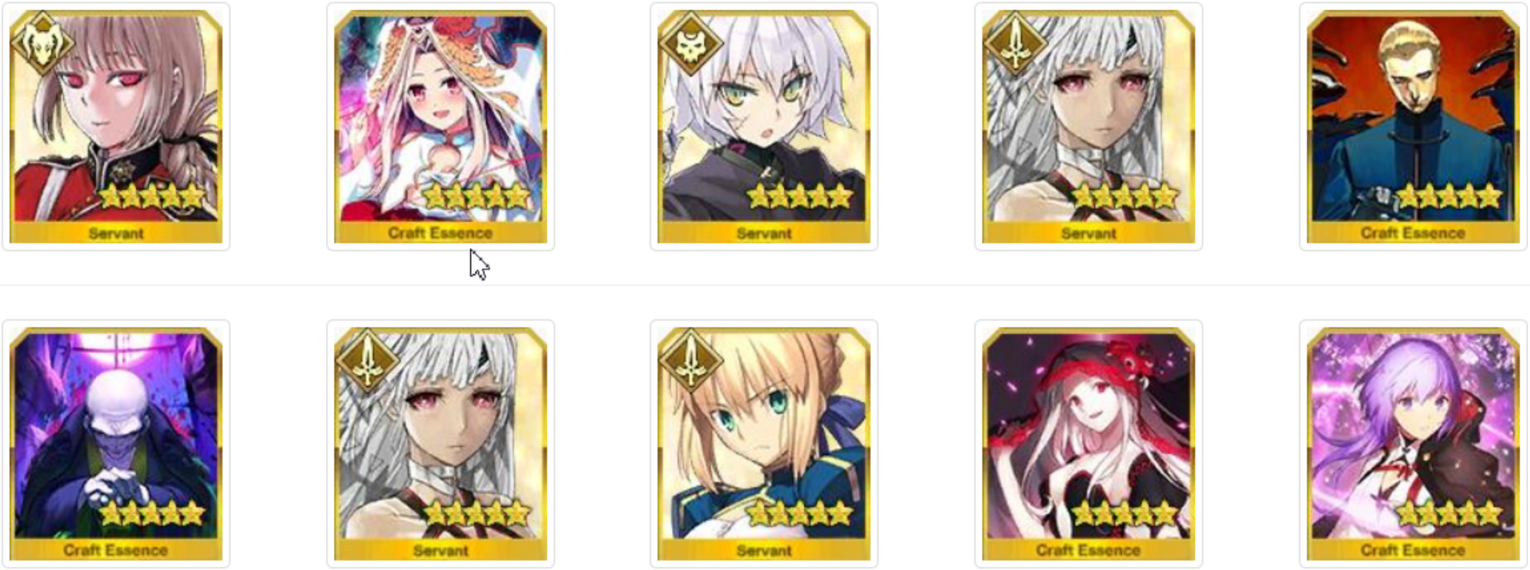
(WEB1)Are you from Europe

其实我是抽到的，然后按f12
发现了SSR=0.00000000000001
自己建一个flag.html
然后clrt+c　　　　然后clrt+v
修改SSR=1
然后：　　　　　发现彩蛋：

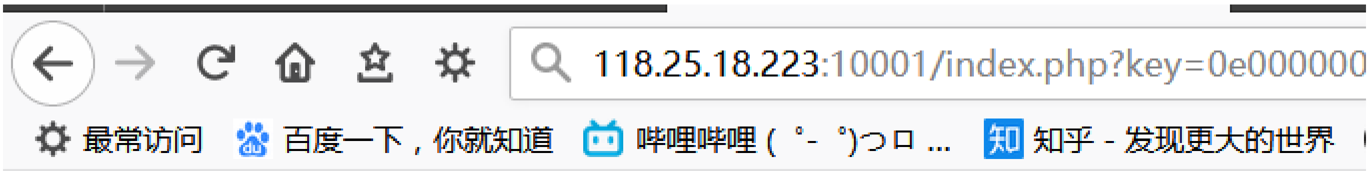


```
function buyQuartz() {
    if (woainvzhuang == true) {
        var buy = confirm("圣晶石不够了，快氪金啊勇士。");
```



(WEB2)special number

打开发现一段代码
解读一下就是这个key要求符合大于等于7位且要有字母和数字，而且要满足其值为0，我首先想到的是0x00000
发现不行，然后0e00000成功
（到现在也不知道0x00000为啥不行）

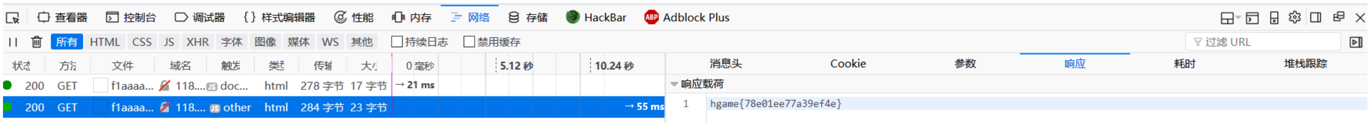


118.25.18.223:10001/index.php?key=0e000000

hgame{pHp_w34k_typing_s000_e4sy}

(web3)can u find me?

点进去发现关键字robot，想到robots协议
于是输入http://118.25.18.223:10003/robots.txt
发现f1aaaaaaaag.php
继续输入http://118.25.18.223:10003/f1aaaaaaaag.php
提示you are not admin，看消息头Cookie：user=guest
改为 user=admin，在响应中发现flag



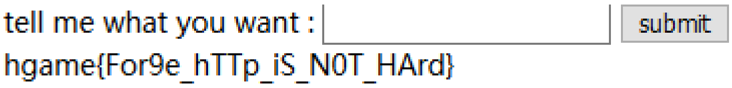
```
状态  方法  文件      域名    触发        类型  传输    大小    0 毫秒   5.12 秒   10.24 秒
200   GET   f1aaaa...  118....  doc...    html  278 字节  17 字节  → 21 ms
200   GET   f1aaaa...  118....  other     html  284 字节  23 字节  → 55 ms
```

```
1  hgame{78e01ee77a39ef4e}
```

(web4)tell me what you want

随意输入一个字符串，发现了需要post
post给他后又要本地登陆
登完后又要改UA然后是改referer最后改cookie得到flag
下面是最后的消息头，右下角为flag

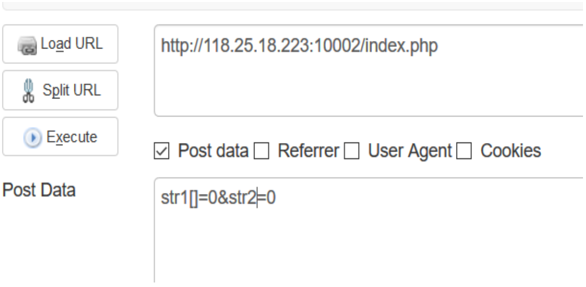
```
POST /index.php?want= HTTP/1.1
Host: 123.206.203.108:10001
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; rv:58.0) Gecko/20100101 Icefox/57.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Referer: www.google.com
Content-Type: application/x-www-form-urlencoded
Content-Length: 8
Cookie: isadmin=1
Connection: close
Upgrade-Insecure-Requests: 1
X-Forwarded-For: 127.0.0.1

want=849
```



hgame{For9e_hTTp_iS_N0T_HArd}

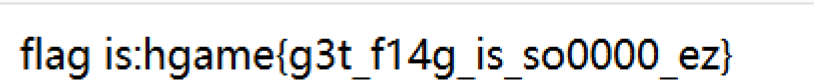
(web5)我们不一样

查找发现strcmp出错是返回0
只要使str1和str2类型不同即可拿到flag



http://118.25.18.223:10002/index.php

str1[]=0&str2=0



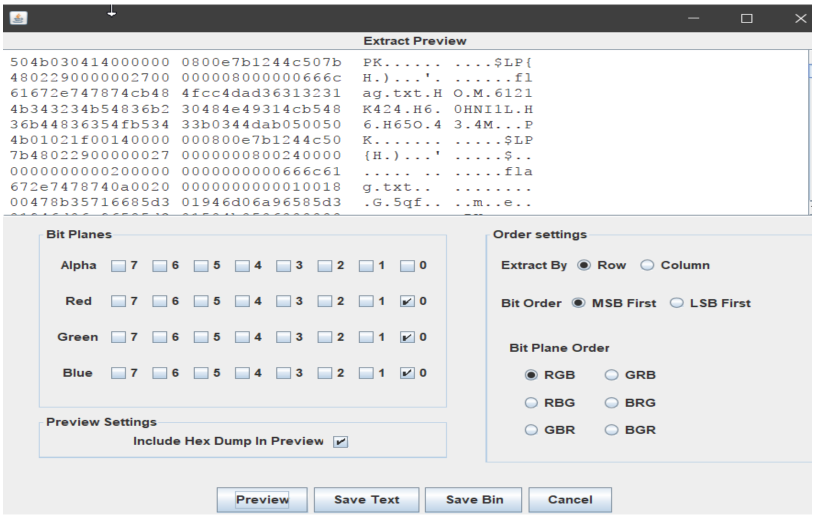
flag is:hgame{g3t_f14g_is_so0000_ez}

(re1)re0

用ida打开文件，F5发现flag
flag： hctf{F1r5t_St5p_Ls_Ea5y}

(misc1)白菜1

这道题想了好久，然后通过排除法想到了想到了用stegsolve analyse ->data exetract RGB都改为0通道



Extract Preview

```
504b030414000000 0800e7b1244c507b  PK......  ....$LP{
4802290000002700 000008000000666c  H.)...'.  ......fl
61672e747874cb48 4fcc4dad36313231  ag.txt.H  O.M.6121
4b343234b54836b2 30484e49314cb548  K424.H6.  0HNI1L.H
36b44836354fb534 33b0344dab050050  6.H65O.4  3.4M...P
4b01021f00140000 000800e7b1244c50  K.......  .....$LP
7b48022900000027 0000000800240000  {H.)...'  .....$..
0000000000200000 0000000000666c61  .....  .. .....fla
672e7478740a0020 0000000000010018  g.txt..   ........
00478b35716685d3 01946d06a96585d3  .G.5qf..  ..m..e..
```

Bit Planes

Alpha	□ 7	□ 6	□ 5	□ 4	□ 3	□ 2	□ 1	□ 0
Red	□ 7	□ 6	□ 5	□ 4	□ 3	□ 2	□ 1	☑ 0
Green	□ 7	□ 6	□ 5	□ 4	□ 3	□ 2	□ 1	☑ 0
Blue	□ 7	□ 6	□ 5	□ 4	□ 3	□ 2	□ 1	☑ 0

Preview Settings

Include Hex Dump In Preview ☑

Order settings

Extract By ● Row ○ Column

Bit Order ● MSB First ○ LSB First

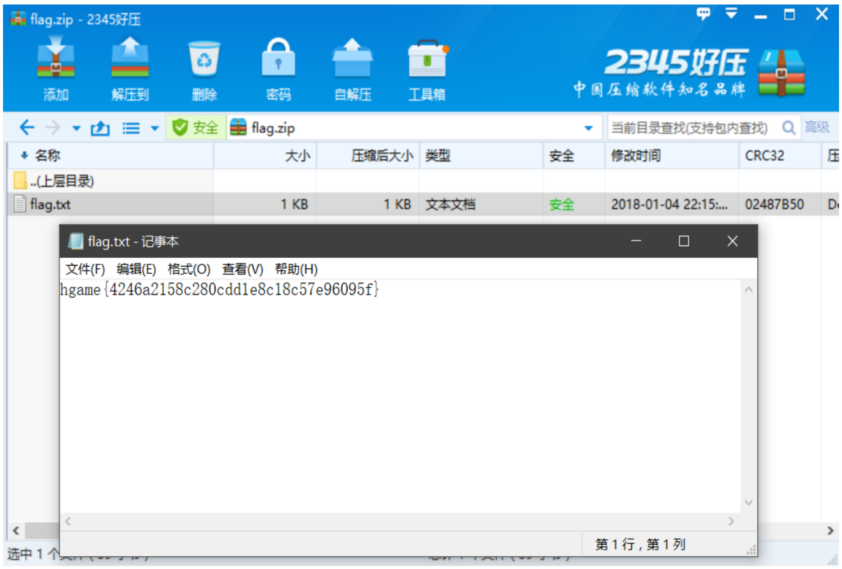
Bit Plane Order

● RGB ○ GRB

○ RBG ○ BRG

○ GBR ○ BGR

发现了PK， flag.txt很明显了，保存二进制文件并加扩展名zip，得到flag

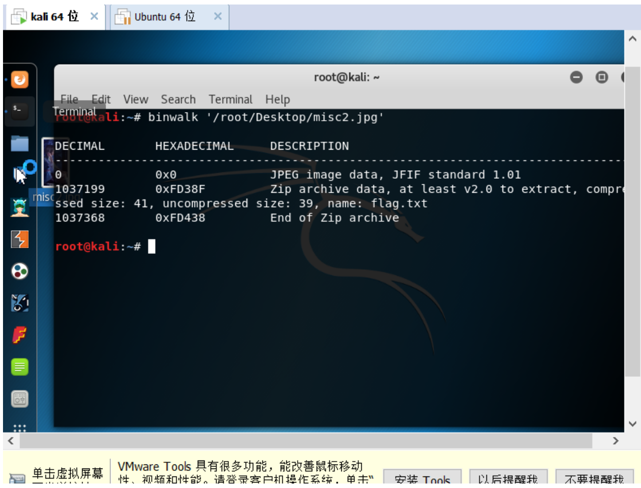


名称	大小	压缩后大小	类型	安全	修改时间	CRC32	压
..(上层目录)							
flag.txt	1 KB	1 KB	文本文档	安全	2018-01-04 22:15:...	02487B50	D

flag.txt - 记事本

```
hgame{4246a2158c280cdd1e8c18c57e96095f}
```

(misc2)白菜2

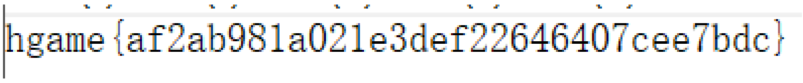


kali 64 位
Ubuntu 64 位
root@kali: ~
File Edit View Search Terminal Help
Terminal
misc

```
root@kali:~# binwalk '/root/Desktop/misc2.jpg'

DECIMAL       HEXADECIMAL     DESCRIPTION
--------------------------------------------------------------------------------
0             0x0             JPEG image data, JFIF standard 1.01
1037199       0xFD38F         Zip archive data, at least v2.0 to extract, compre
ssed size: 41, uncompressed size: 39, name: flag.txt
1037368       0xFD438         End of Zip archive

root@kali:~# 
```

单击虚拟屏幕
VMware Tools 具有很多功能，能改善鼠标移动性、视频和性能。请登录客户机操作系统，单击"
安装 Tools
以后提醒我
不要提醒我

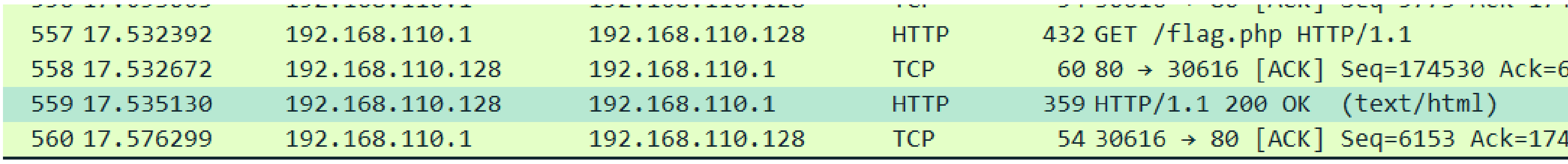
binwalk发现有个zip文件
改扩展名拿到flag



```
hgame{af2ab981a021e3def22646407cee7bdc}
```

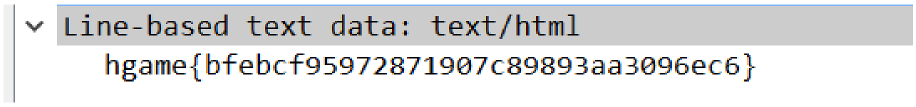
(misc3)pacp1

发现flag.php，点开并没有flag



```
557 17.532392   192.168.110.1     192.168.110.128   HTTP    432 GET /flag.php HTTP/1.1
558 17.532672   192.168.110.128   192.168.110.1     TCP      60 80 → 30616 [ACK] Seq=174530 Ack=6
559 17.535130   192.168.110.128   192.168.110.1     HTTP    359 HTTP/1.1 200 OK  (text/html)
560 17.576299   192.168.110.1     192.168.110.128   TCP      54 30616 → 80 [ACK] Seq=6153 Ack=174
```

然后点559分组找到flag



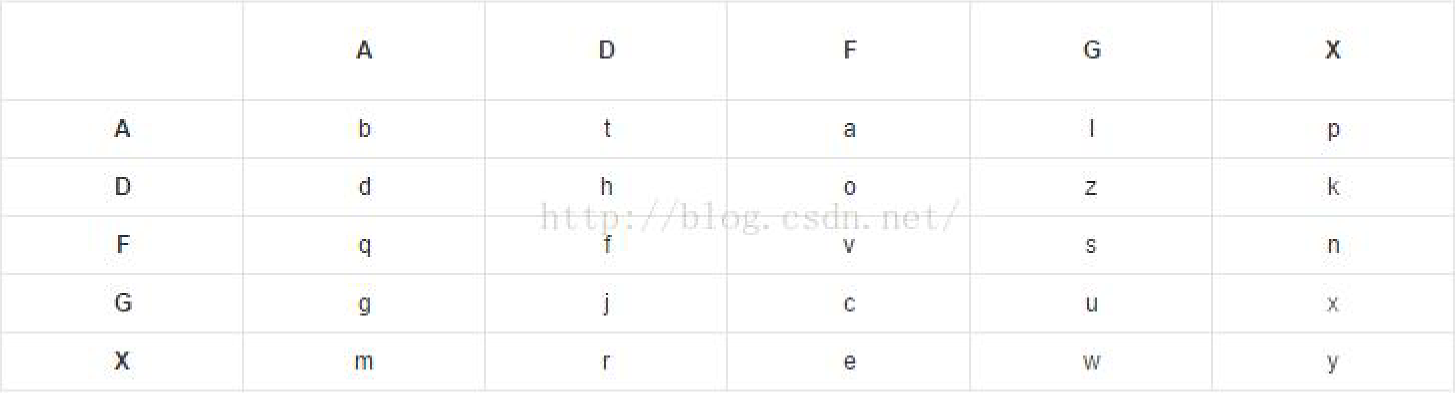
```
∨ Line-based text data: text/html
      hgame{bfebcf95972871907c89893aa3096ec6}
```

(crypto1)easy Caesar

随便找个在线凯撒解密网站，解密提交flag发现是错的
然后就想到了数字也要移动
最后flag：hgame{The_qu1ck_br0wn_4x_jUmps_ovEr_a_La2y_dOg}

(crypto2)Polybius

搜索题目，发现是棋盘密码，对照表格得出flag

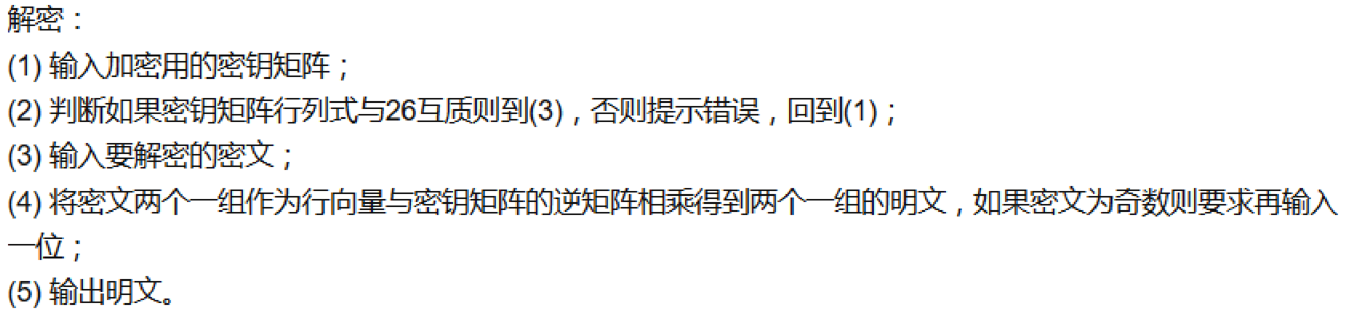


	A	D	F	G	X
A	b	t	a	l	p
D	d	h	o	z	k
F	q	f	v	s	n
G	g	j	c	u	x
X	m	r	e	w	y

flag:hgame{fritz_nebel_invented_it}
这里i，j共用一个格子所以就要多试几次

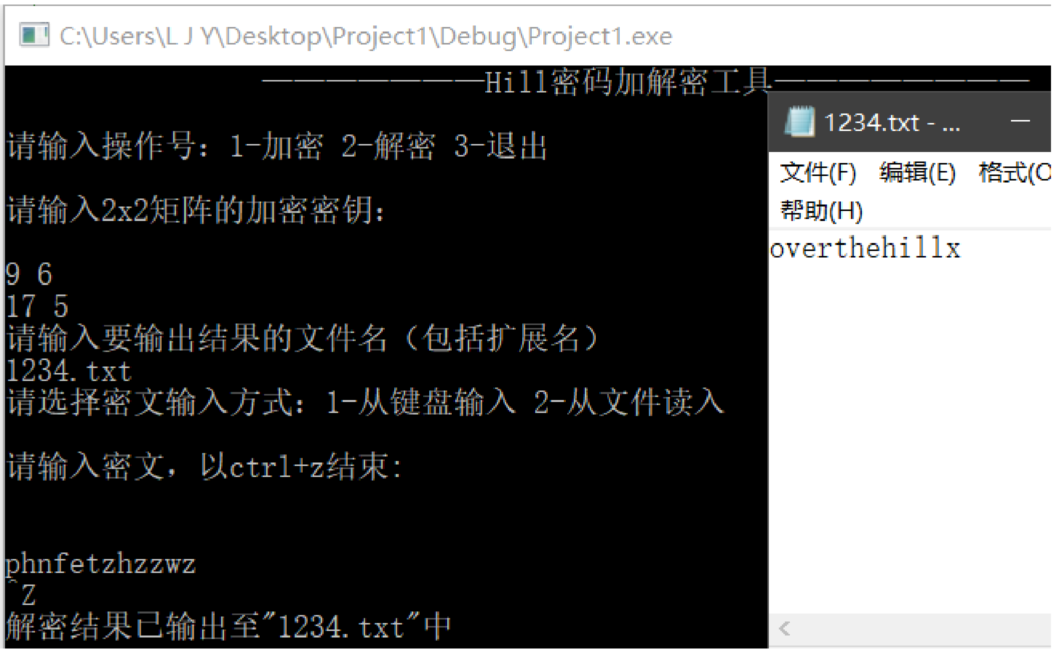
(crypto3)Hill

搜索Hill解密发现解密流程



解密：
(1) 输入加密用的密钥矩阵；
(2) 判断如果密钥矩阵行列式与26互质则到(3)，否则提示错误，回到(1)；
(3) 输入要解密的密文；
(4) 将密文两个一组作为行向量与密钥矩阵的逆矩阵相乘得到两个一组的明文，如果密文为奇数则要求再输入一位；
(5) 输出明文。

利用其c源码得到flag



C:\Users\L J Y\Desktop\Project1\Debug\Project1.exe

```
                ————————Hill密码加解密工具————————————
请输入操作号：1-加密 2-解密 3-退出

请输入2x2矩阵的加密密钥：

9 6
17 5
请输入要输出结果的文件名（包括扩展名）
1234.txt
请选择密文输入方式：1-从键盘输入 2-从文件读入

请输入密文，以ctrl+z结束：


phnfetzhzzwz
^Z
解密结果已输出至"1234.txt"中
```

1234.txt - ...

```
overthehillx
```

(crypot4)confusion

先是通过摩斯密码解码成

MRLTK6KXNVZXQWBSNA2FSU2GGBSW45BSLAZFU6SVJBNDAZSRHU6Q

base32

dW5yWmsxX2h4YSF0ent2X2ZzUHZ0fQ==

base64

unrZk1_hxa!tz{v_fsPvt}

栅栏密码

utnzr{Zvk_1f_shPxvat!}

凯撒

hgame{Mix_1s_fuCking!}