

描述

普通的Vigener

URL <http://plir4axuz.bkt.clouddn.com/hgame2019/orz/ciphertext.txt>

基准分数 150

当前分数 150

直接百度 Vigener

请输入要加密的明文

The Vigenere ciphe is a method of encrypting alphabetic text by using a series of interwoven Caesar ciphers, based on the letters of a keyword. It is a form of polyalphabetic substitution. The cipher is easy to understand and implement, but it resisted all attempts to break it for three centuries, which earned it the description le chiffre indechiffable. Many people have tried to implement encryption schemes that are essentially Vigenere ciphers. In eighteen sixty three, Friedrich Kasiski was the first to publish a general method of deciphering Vigenere ciphers. The Vigenere cipher was originally described by Giovan Battista Bellaso in his one thousand five hundred and fifty-one book La cifra del. Sig. Giovan Battista Bellaso, but the scheme was later misattributed to Blaise de Vigenere in the ninth century and so acquired its present name. flag is gfyuytukxariyydfjplwxsdbzvwqt

加密

无密钥解密

密钥: guess

密钥长度(选填)

有密钥解密

密钥

请输入要解密的密文

Zbi Namyrwik wmhzk cw s eknlay uz ifuxstlata edhnufwlow xwpz vc mkohk s kklmwk uz mfkliagnkh Gswyuy uavbiik huwvuh xzw rylwvxm sz s qycogxx. MI ay u jgis ij hgrsedhnufwlow wmtynmlmzcsf. Lny gahnyv ak kuwg lu orvwxmsfj urv asjpwekhx tmz cx jwycwlvj upd szniehzm xg txyec az zsj lnlw ukhxmjoyw, ozowl wsxhiv az nlw vkmajavnmgf ry gzalzv atxiuzojishfj. Ests twgvfi zsbv xiaxk xg asjpwekhx wfilchloir kunyawk zbel sxy ikkhhxasrfc Namyrwik wmhzkiv. Af kckzlkry kadnc lzyi. Xioyhjaib Oskomoa oqm xzw lcvkl zi tmtcrewz s myrvjaf qwlnih gx jygahnyvafm Pmywtvww uoijwiy. Nlw Noaifwxy gahnyv osy ivayohedde xikuxcfww hs Kagbur Tsznmklg Viddgms af ncw gfk nlqmyurv xopi zmtxvww ghx xalnc gfk vsqc Ru gaxxu hwd. Yck. Yaupef Tgnxakzu Fwdruwg tan xzw ywlwek gek dgnij eomellxcfmikx xg Trumkw jy Zaykhijw oh xzw tcrwln wiflalc sfj ms suwomjwiy csk hxywwfz heew. Ifey ay ajqmenycplmqajzndhrqwpvhtaniz

搜到在线加密解密网站试了一下无密钥解密

Flag 就看到了（感觉是脸滚键盘的 flag）

flag is gfyuytukxariyydfjplwxsdbzvwqt

浪漫的足球圣地[已完成]

描述

无

URL <http://plir4axuz.bkt.clouddn.com/hgame2019/orz/enc.txt>

百度 浪漫的足球圣地 发现了曼切斯特特别显眼

966A969596A9965996999565A5A59696A5A6A59A9699A599A596A595A599A569A5A99699A56996A596A696A996A6A5A696A9A595969AA5A69696A5A99696A595A59AA56A96A9A5A9969AA59A9559

典型的曼切斯特编码

转二进制

按此规则有：

- 编码0101（即0x5），表示原数据为00；
- 编码1001（0x9）表示10；
- 编码0110（0x6）表示01；
- 编码1010（0xA）表示11。

第二种IEEE 802.4（令牌总线）和低速版的IEEE 802.3（以太网）中规定，按照这样的说法，低-高电平跳变表示1，高-低的电平跳变表示0。

- 编码0101（0x5）表示11；
- 编码1001（0x9）表示01；
- 编码0110（0x6）表示10；
- 编码1010（0xA）表示00；

两种规则经实验是第二种 将二进制按照第二标准转化 再转十六进制 再转字符串得 flag

hill[已完成]

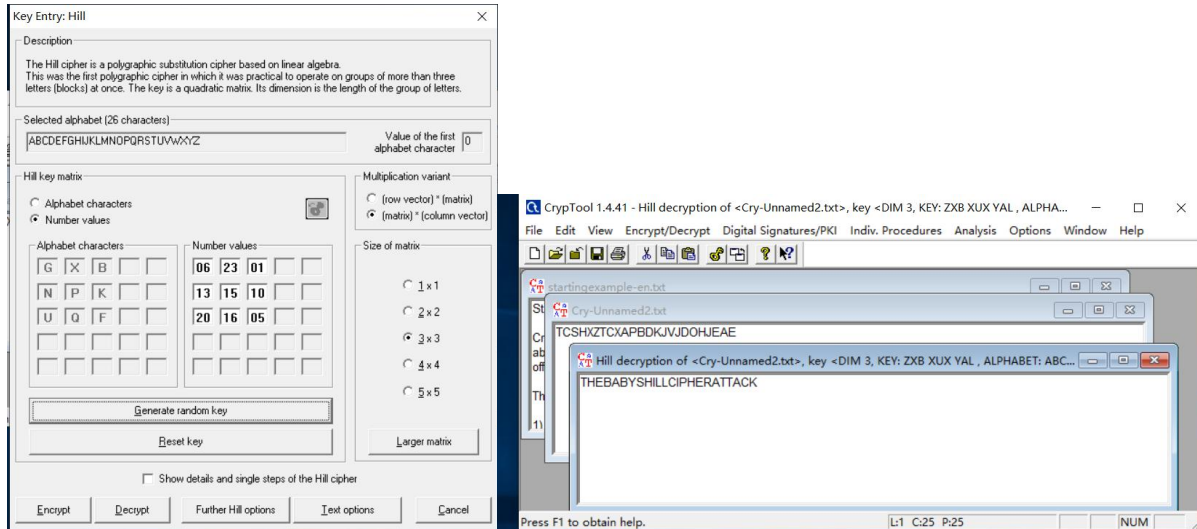
#### 描述

hill密码，秘钥是3x3矩阵，flag的密文是TCSHXZTCXAPBDKJVJDOHJAE，flag中含有BABYSHILL，flag是有意义的英文，最终提交格式: hgame{有意义的英文} hint1: [https://en.wikipedia.org/wiki/Hill\\_cipher](https://en.wikipedia.org/wiki/Hill_cipher) hint2: 模逆元

URL <http://www.example.com>

Hill 密码 知道了密文和部分明文重点在算出加密矩阵

我采用了最笨的方法（毕竟线代不好） 假设 A: 0 将明文对应密文中的连续的九个列出方程组计算九个未知量



最后算出加密矩阵 得到 flag

## Are You Familiar with DNS Records?

#### 描述

well, you know, this is a song-fen-ti, have fun! XD

然并卵的hint: DNS 有很多种不一样的记录类型，其中一种类型如果没有正确设置就可能被其他邮件服务器拒收，flag 就在此域名的第二条此类型记录里

URL <http://project-a11.club/>

看它是个送分题 然而没有轻易的送到我的手上。。。网页打不开让我懵了很久

DNS 记录 一开始用 wireshark 抓包查看然而啥都没有 py 了出题人发现 DNS 可以直接查

```
C:\Users\Director>nslookup
默认服务器:  tzdns1.tzptt.zj.cn
Address:  60.191.134.196

> set type=txt
> project-a11.club
服务器:  tzdns1.tzptt.zj.cn
Address:  60.191.134.196

非权威应答:
project-a11.club      text =
    "flag=hgame{seems_like_you_are_familiar_with_dns}"
project-a11.club      text =
    "v=spf1 include:spf.mail.qq.com ~all"

project-a11.club      nameserver = flglns1.dnspod.net
project-a11.club      nameserver = flglns2.dnspod.net
>
```

这样就看到了 flag。。。

## 初识二维码

### 描述

你知道吗，二维码就算有缺损也能扫出来哦

hint:1.DataURI 2.QRcode基本结构

URL <http://plqfgjy5a.bkt.clouddn.com/%E5%88%9D%E8%AF%86%E4%BA%8C%E7%BB%B4%E7%A0%81.zip>

基准分数 150

当前分数 150

完成人数 37

得到一个压缩包然后解压是个 Data URL 数据 网上在线转化为图片

Input Data URI

```
data:image/png;base64,iVBORw0KGzoAAAANSUhEUgAAAHwAAABSCAYAAACrHtS+AAAAACXBIVWMAAASTAAALEwEampwYAAAKTWLDQ1BqaG90b3Nob3AgSUNDIHB7b2ZpbGUAAHJanVN3WJP3Fj7f92UPVklY8LGXbIEAi0sCMgQWaIQgBhhBASQMWFiaPwFBUrEhVxILVCKidiOKgKLhnQYqIWotVXDjuH9yntX167+3t+9f7y0ec5/z0ec8PgBESJpHmomoAOVKFPDrYH49PSMTJvYACFujgBCAQ5svCZwXFAADwA314fnSwP/wBr28AAgBw1S4kEsfh/406UCZXACCRA0AiEucLAZBSAMguVMgUAMgYALBTs2QKAJQAAGx5fEiIAkoNAOzOST4FANipk9wXANiIHkIAIOBAJkoRyQCQLsAYFWBUiWcWmIAoKxAii4EwK4BgFm2MkcCgLOFAHaOWJAPQGAAGJ1CLMwAIDgCAEMeESODIEwDoDDsv+CpX3CFuEgBAMDL1c2XS9IzFLiV0Bp38vDg4iHiwnyxQmEXKRBMceQinJebIxNI5wNMzgwABr50cH+OD+Q5+bk4eZm52zv9MWi/mvwbvI+JfHf/rvMAgQAE7P79pf5eXWA3DHAAb1v2upWwDaVaBo3/1dMQsIoFoK0Hr5i3k4/EaenoFQvDrdHaoLC+Q1YcG9MOOLPy8z4W/g1372/E4e/tt684BxmKcZrcC1g/1x1W52r1KQ58sEQiFu8+ci/seFf/2QKdHiNLFcLBWKSviIuFAiIcd5uVKKRCH1IeIS6X8vSR+W/QmIdw0ArI2PwE62B7XLBMB+7gECiw5YQnYAQH7zLYwaC5EAEgcOMnn3AACTv/mPQCSBAM2XpOAAALzoGFyo1BdMxggAAESggSqwQQcMwRSswA6cwR28wBcCYQZEQAwkDwQqgbkGwKoRiWQR1UwDrYBLWwAxqgEzrhELTBMTgN5+ASXIHrcBeGYBiewhi8hgkEQcgIE2EhOogRYo7YIs4IF5mOBCJhSDSSgKqg6YgUUSLFyHKkAq1CapFdSCPylXIU0Y1cQPqQ28ggMor8irxHmZSBs1ED1AJ1QLmoHxqKxqBzOXQ0D12A1qJr0Rq0Hj2AtqKnOUvodXQAFyQ0Y4DRMQ5mjN1hXIyHRWCJWBomxxZj5Vg1Vo81Yx1YN3YVG8CeYe8IJAKLgBPSCF6EEMJsgpCQR1hMWE0oJewjtBK6CFcJg4Qxwicik6hPtCV6EvnEeG16sZ
```

Ouput Image



是个奇奇怪怪的二维码。。。 下面开始修复 然而就是扫不出 flag 审题审题（py 学长去）



最后修复出正确的二维码 果然很破损。。。 扫一扫就可以得到二维码了

找得到我嘛？小火汁[已完成]

描述

$$\varepsilon = \varepsilon = \varepsilon = \varepsilon = \varepsilon = \varepsilon = 1 \left( \cdot \right)^{-1}$$

hint: Https

URL <http://plir4axuz.bkt.clouddn.com/hgame2019/orz/safe.pcapng>

基准分数 150

当前分数 150

完成人数 40

Wireshark 打开流量包是 https 的流量包 题目中也没有给密钥日志那就找吧

```
C:\Windows\system32\cmd.exe
155110 0x25DE6 XML document, version: "1.0"
156250 0x2625A XML document, version: "1.0"
156970 0x2652A XML document, version: "1.0"
157794 0x26862 XML document, version: "1.0"
158638 0x26BAE XML document, version: "1.0"
159526 0x26F26 XML document, version: "1.0"
160246 0x271F6 XML document, version: "1.0"
160946 0x274B2 XML document, version: "1.0"
161666 0x27782 XML document, version: "1.0"
163246 0x27DAE XML document, version: "1.0"
180878 0x2C28E Zip archive data, at least v2.0 to extract, compressed size: 1862, uncompressed size: 3586
, name: secret.log
182960 0x2CA80 End of Zip archive, footer length: 22
184966 0x2D286 XML document, version: "1.0"
185666 0x2D542 XML document, version: "1.0"
186510 0x2D88E XML document, version: "1.0"
187210 0x2DB4A XML document, version: "1.0"
187930 0x2DE1A XML document, version: "1.0"
189070 0x2E28E XML document, version: "1.0"
189790 0x2E55E XML document, version: "1.0"
190614 0x2E896 XML document, version: "1.0"
191458 0x2EBE2 XML document, version: "1.0"
192158 0x2EE9E XML document, version: "1.0"
192878 0x2F16E XML document, version: "1.0"
193578 0x2F42A XML document, version: "1.0"
194298 0x2F6FA XML document, version: "1.0"
195878 0x2FD26 XML document, version: "1.0"

C:\Users\Director>
```

用 binwalk 分析了一下文件发现了一个压缩包 但是分离出来的文件是损坏的无法解压

No.	Time	Source	Destination	Protocol	Length	Info
193	61.1436.988852	192.168.61.136	192.168.61.1	FTP-DA..	1514	FTP Data: 1460 bytes (PASV) (RETR /pub/test/secret.zip)
194	61.142567	192.168.61.135	192.168.61.1	TCP	1514	443 → 6701 [ACK] Seq=120673 Ack=1986 win=33536 Len=1460
195	61.142102	192.168.61.135	192.168.61.1	TCP	1514	443 → 6701 [ACK] Seq=119969 Ack=1006 Win=22526 Len=1460
Frame 404: 1514 bytes on wire (12112 bits), 1514 bytes captured (12112 bits) on interface 0						
Ethernet II, Src: Vmware_77:d7:ca (00:0c:29:77:d7:ca), Dst: Vmware_c0:00:01 (00:50:56:c0:00:01)						
Internet Protocol Version 4, Src: 192.168.61.136, Dst: 192.168.61.1						
Transmission Control Protocol, Src Port: 54921, Dst Port: 7331, Seq: 1, Ack: 1, Len: 1460						
0000	00 50 56 c0 00 01 00 0c	29 77 d7 ca 08 00 45 08	·PV·...	·w·...	·E·	
0010	05 dc 99 3c 40 00 40 06	9f fd c0 a8 3d 88 c0 a8	····@·@·	·...	·...	
0020	3d 01 d6 2f 1c 35 f7 31	17 10 7e 91 85 f6 50 10	=··/·5·1·	·...	·P·	
0030	00 e5 b1 99 00 00 50 4b	03 04 14 00 00 00 08 00	·...	·PK·	·...	
0040	cc 69 3c 4e 87 28 96 c5	46 07 00 00 02 0e 00 00	··i·N·(·	·F·	·...	
0050	0a 00 00 00 73 65 63 72	65 74 2e 6c 6f 67 bd 57	·...	·secr et.log W	·	
0060	b9 aa 05 45 10 cd 05 ff	61 c0 54 b0 ab ab aa 97	··E·...	·a·T·	·...	
0070	50 d4 40 70 01 35 97 5a	45 10 05 35 f1 ef 3d 63	P·@·p·5·Z·	E·5·...	·c·	

在流量包中找到了 zip 文件的二进制编码 不过好像被分成了两份。。。

用 UE 将两份二进制编码进行拼接 运气不错得到的压缩包 没有密码解压也正常 得到日志文件  
配置日志文件 再导出对象 HTTP 得到一个压缩包



1 (~\Desktop\HGAME) - GVIM

文件(F) 编辑(E) 工具(T) 语法(S) 缓冲区(B) 窗口(W) 帮助(H)

00000210: 0060 0000 ffe1 00a0 4578 6966 0000 4d4d .`.....Exif..MM  
00000220: 002a 0000 0008 0007 0131 0002 0000 0016 .\*.....1.....  
00000230: 0000 0062 0301 0005 0000 0001 0000 0078 ..b.....x  
00000240: 0303 0001 0000 0001 0000 0000 5110 0001 .....Q...  
00000250: 0000 0001 0100 0000 5111 0004 0000 0001 .....Q.....  
00000260: 0000 0ec3 5112 0004 0000 0001 0000 0ec3 ....Q.....  
00000270: 8298 0002 0000 0017 0000 0000 0000 0000 .....  
00000280: 436c 6970 496d 6747 6574 2076 6572 2e20 ClipImgGet ver.  
00000290: 312e 302e 3200 0001 86a0 0000 b18f 6867 1.0.2.....hg  
000002a0: 616d 657b 436f 6e67 7261 7475 6c61 7469 ame{Congratulati  
000002b0: 6f6e 735f 0000 fffe 0013 596f 755f 476f ons\_.....You\_Go  
000002c0: 745f 5468 655f 466c 6167 7dff db00 4300 t\_The\_Flag}...C.  
000002d0: 0201 0101 0101 0201 0101 0202 0202 0204 .....  
000002e0: 0302 0202 0205 0404 0304 0605 0606 0605 .....  
000002f0: 0606 0607 0908 0607 0907 0606 080b 0809 .....  
00000300: 0a0a 0a0a 0a06 080b 0c0b 0a0c 090a 0a0a .....  
00000310: ffdb 0043 0102 0202 0202 0205 0303 050a ...C.....  
00000320: 0706 070a 0a0a 0a0a 0a0a 0a0a 0a0a 0a0a .....  
00000330: 0a0a 0a0a 0a0a 0a0a 0a0a 0a0a 0a0a 0a0a .....  
00000340: 0a0a 0a0a 0a0a 0a0a 0a0a 0a0a 0a0a 0a0a .....  
00000350: 0a0a 0a0a 0aff c000 1108 032a 05a0 0301 .....\*....  
00000360: 2200 0211 0103 1101 ffc4 001f 0000 0105 .....  
00000370: 0101 0101 0101 0000 0000 0000 0000 0102 .....  
00000380: 0304 0506 0708 090a 0bff c400 b510 0002 .....  
39,1

新建文本文档.txt - 记事本

文件(F) 编辑(E) 格式(O) 查看(V) 帮助(H)

hgame{Congratulations\_You\_Got\_The\_Flag}

解压文件用 vim 打开 得到 flag