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

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 gfyuytukxariyydfjlplwsxdbzwvqt

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]

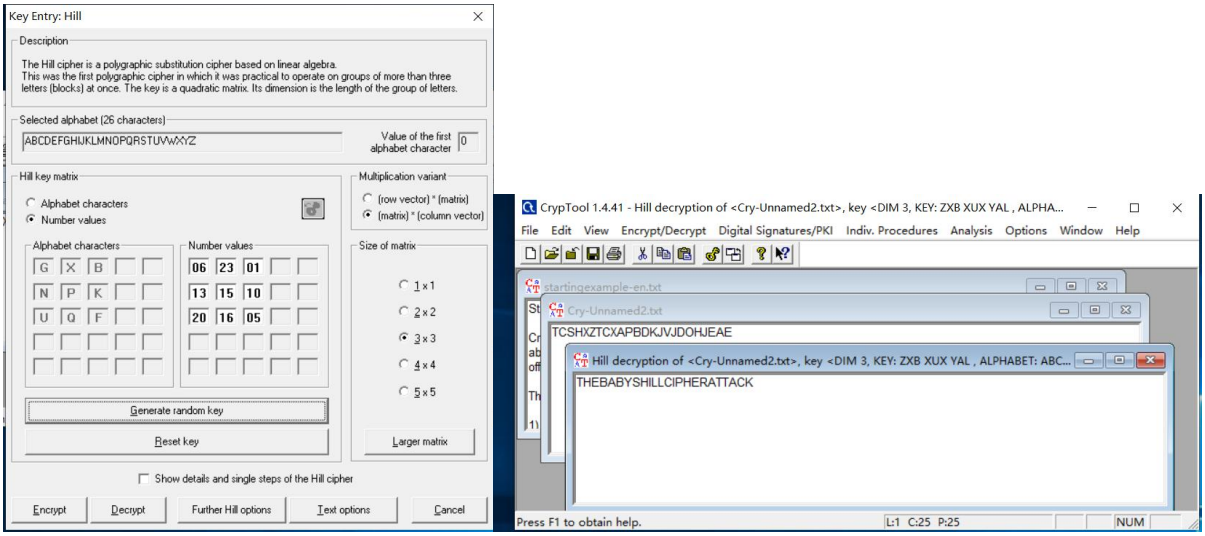
描述

hill密码，秘钥是3x3矩阵，flag的密文是TCSHXZTCXAPBDKJVJDOHJEAE，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 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 = f1g1ns1.dnspod.net
project-a11.club        nameserver = f1g1ns2.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

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

ε=ε=ε=ε=ε=ε= ┌(;￣◇￣)┘

hint: Https

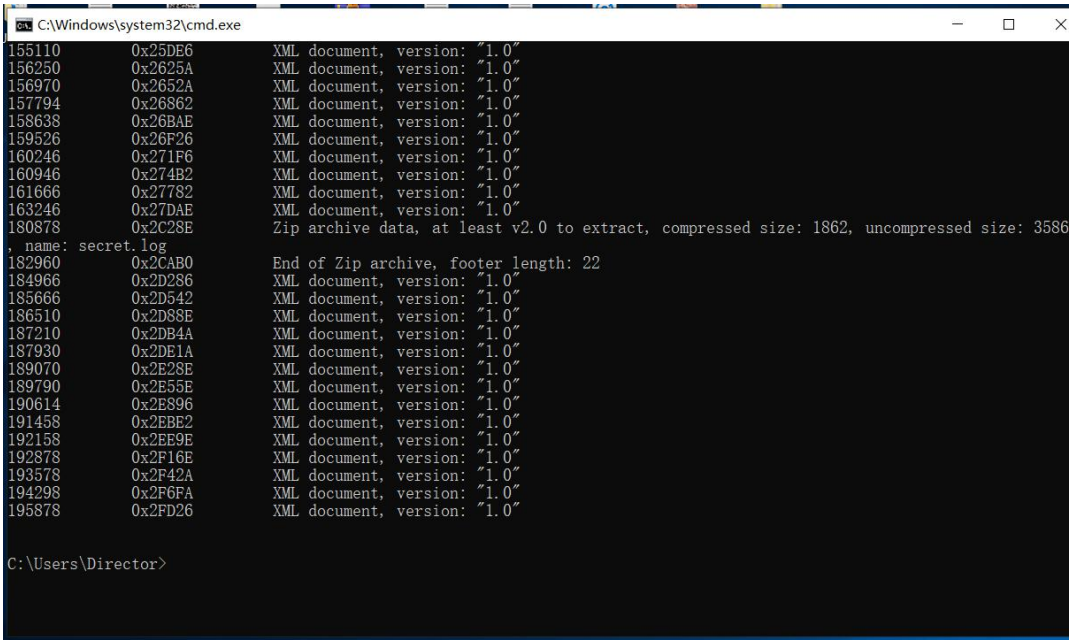
URL http://plir4axuz.bkt.clouddn.com/hgame2019/orz/safe.pcapng

基准分数 150

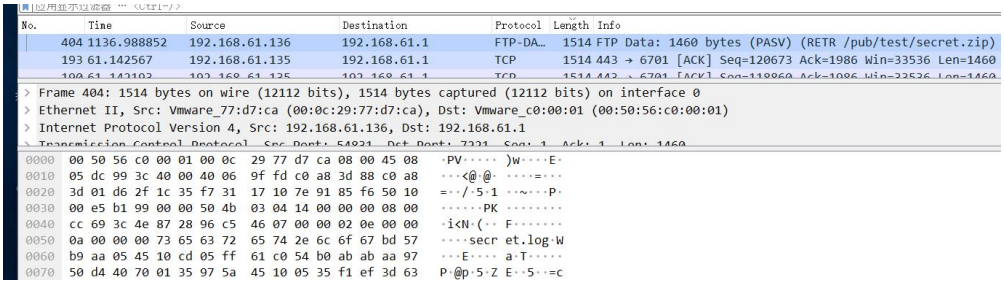
当前分数 150

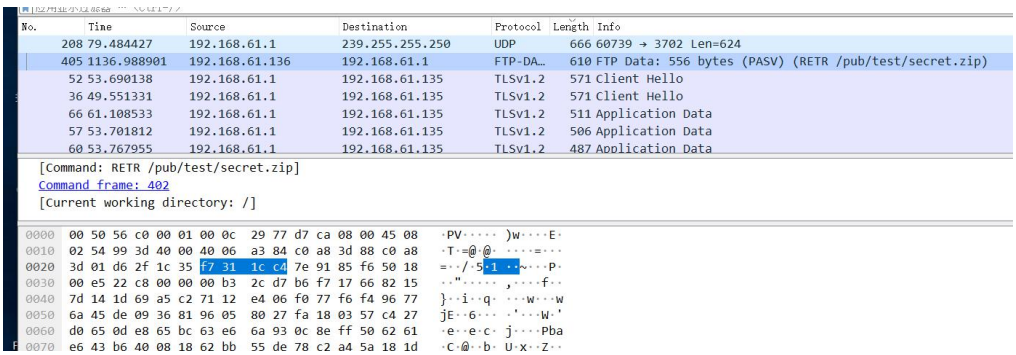
完成人数 40

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



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

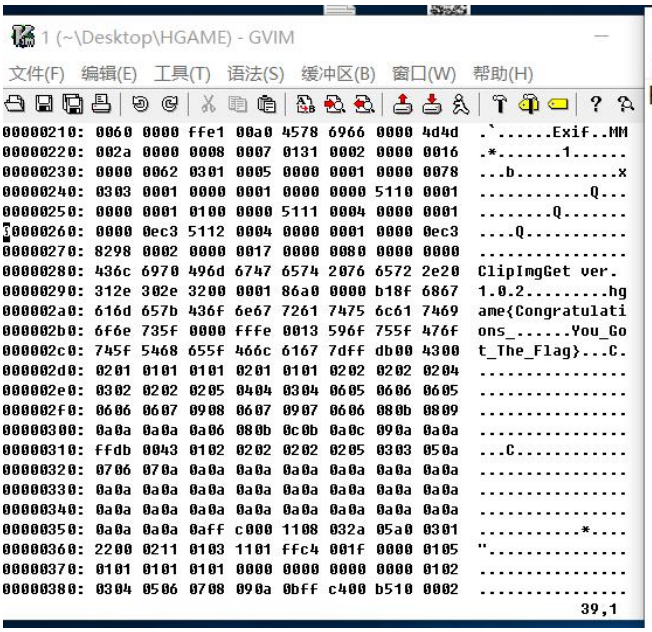




在流量包中找到了 zip 文件的二进制编码 不过好像被分成了两份。。。

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



解压文件用 vim 打开 得到 flag