# HGAME 2022 Week1 writeup by z3



## REVERSE

### easyasm

用ida打开，f5失败，提示只能编译32位。阅读汇编代码可知加密过程为二进制高四位与低四位交换，然后与23异或。由于异或可逆，很容易写出解密代码。在data区翻阅，找到可疑字符串，代入hgame验证前五位通过，解密即可。

## WEB

## MISC

### 这个压缩包，它真的可以打开吗?

压缩包打开需要密码，根据注释猜想密码为六位数字，工具爆破打开压缩包，获得压缩包和两个文本，根据readme 文本猜想字典攻击，使用工具字典攻击，打开压缩包，获得压缩包和文本。查看压缩包，包含图片和文本，注意到内外文本crc 值相同，猜想明文攻击。azpr报错，压缩软件换成7-zip成功，得到图片但没有flag ，尝试压缩包方式（改后缀）打开图片，可以看到是另一张图片但需要密码，尝试伪加密成功（504B0304后第三字节和504B0102后第五字节改为00）

## CRYPTO

### Easy RSA

加密算法为rsa，flag为明文，已知e,p,q,m求c，python代码根据rsa算法先求出d，然后解密得到明文flag

### Matryoshka

解压得到未知点阵文本（其实是盲文），发现只有三种符号，然后没有思路。然后发现摩斯密码其实需要三种符号，猜想摩斯密码，先替换分隔符（确定），然后替换点和杠，得到两种，都提示格式错误。将摩斯密码逆序解密，只得到一种密文，尝试base16 解码得到末尾带等号的密文，此时顺序为维吉尼亚（密码如题），base64 ，栅栏密码（枚举找出？？？？？{ * } 的形式），凯撒解密22，得到flag

## English Novel

解压得到原文和密文，打开代码可以看到是维吉尼亚加密，密钥线索应该在文档中。由于密文顺序被打乱，合并原文，用通配符和空格检索原文找到匹配密文的原文，计算密钥，代码解密flag 文本。由于空格无法解出密钥，使用两段空格不重叠密文分别解密，重叠即可得到flag

# IoT

## 饭卡的uno

没有资料，没有思路。winhex 打开，尝试检索字符串，无果。于是反汇编软件打开，
一眼看到 ame{F1rst_5tep_0F_IOT} 补上两个字母，通过。

# PWN