HGAME WEEK2 WP

好难 TAT　---EkkoSonya

Crypto

WhitegiveRSA

百度搜索RSA 了解了基本的操作

上代码

```
# coding=UTF-8

import binascii
import gmpy2
p = 857504083339712752489993810777
q = 1029224947942998075080348647219
e =  65537
c = 747831491353896780365654517748216624798517769637260742155527

# 1.已知的p和q求出n
n = p * q
print(n)

# 2.根据已知的条件求出d
phi_n = (p-1)*(q-1)
d = gmpy2.invert(e,phi_n)
#print(d)

#求出明文
m = pow(c,d,n)
print("m=\n%s"%m)
s = binascii.unhexlify(hex(m)[2:])
print(s)
```

得到flag

Misc

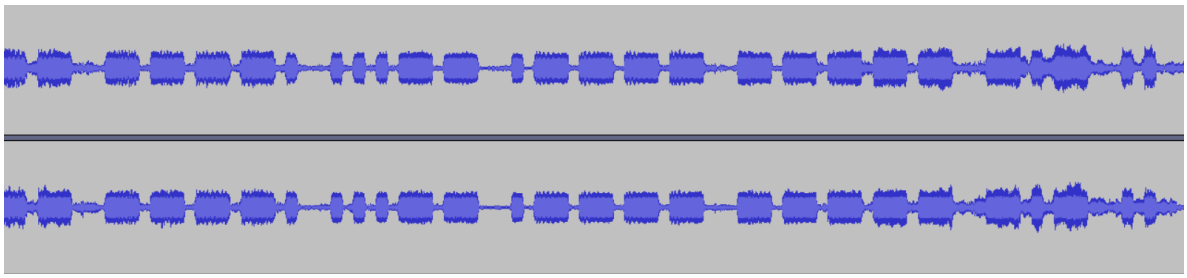
Telegraph：1601 6639 3459 3134 0892

1.把题目复制到搜索引擎 发现是中文电报 带入得到 戴通滤波器？

2.进入听了一遍歌 从1min10s开始左右有一段莫斯

3.点开频谱仪 发现850HZ

emm 就试试用带通滤波器 + 850HZ 滤波

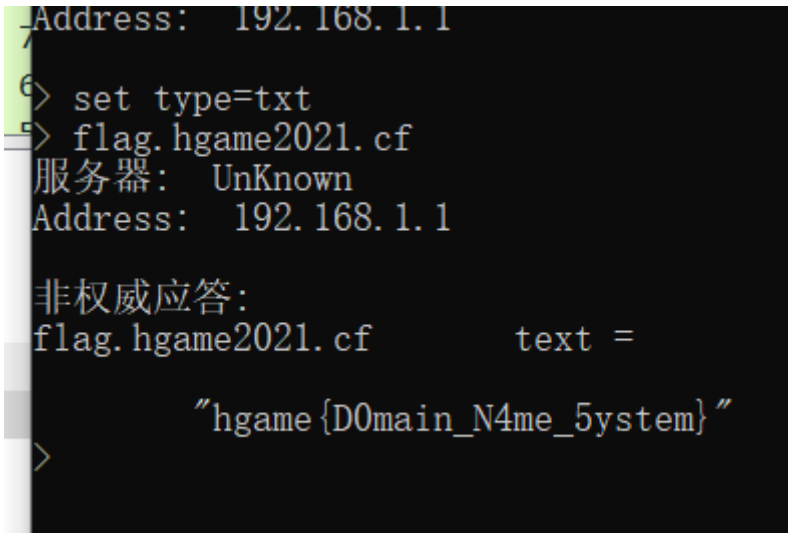


类似这样后写出莫斯电码 在线解码得到flag

DNS

下载发现是pcapng文件 拖入wireshark 发现有一个txt 移出发现 flag并非在这

后查找dns和txt文本所给提示SPF



即得到flag

RE

还是差了点 没做出来 TAT

HelloRE2

1.先拖入ida后观察 发现要输入两次password后再输入flag {%s_%s} 一开始盲猜是这个两个password合并

2.password1还是很好求的 一开始f5代码比较复杂 直接看汇编

发现是输入password1后与ds:xmmword_4030F0的比较

得到password1：2b0c5e6a3a20b189 (是反了一下后的)

3.后来尝试到ollydbg动态 发现完全进不去password2 就很无奈放弃

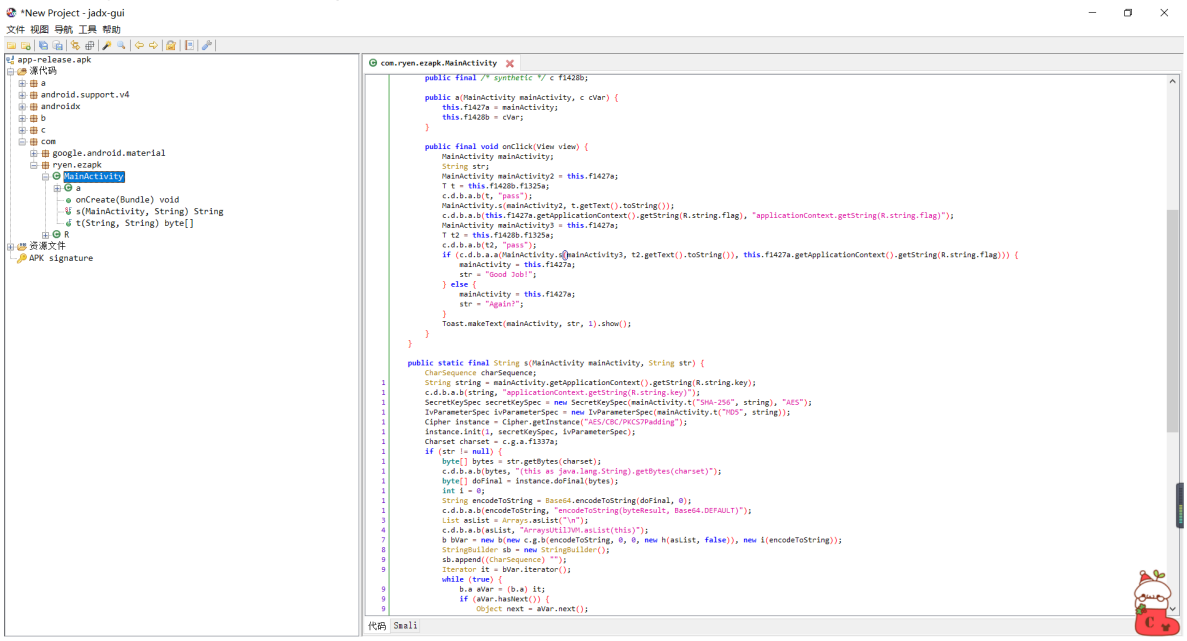
4.重新看password2的代码 发现是调用了win32的API BCrypt的来编码你输入的password2然后再与ds:xmmword_4030E0的比较

5.研究了蛮久的BCrypt的各个编码 不太懂 感觉又有key和iv向量等 很是疑惑

期待wp

EZAPK

不是很懂java 百度搜索了下apk的逆向方法 成功得到



工具并找到MainActivity后尝试看看java源码

```
    }

    public static final String s(MainActivity mainActivity, String str) {
        CharSequence charSequence;
        String string = mainActivity.getApplicationContext().getString(R.string.key);
        c.d.b.a.b(string, "applicationContext.getString(R.string.key)");
        SecretKeySpec secretKeySpec = new SecretKeySpec(mainActivity.t("SHA-256", string), "AES");
        IvParameterSpec ivParameterSpec = new IvParameterSpec(mainActivity.t("MD5", string));
        Cipher instance = Cipher.getInstance("AES/CBC/PKCS7Padding");
        instance.init(1, secretKeySpec, ivParameterSpec);
        Charset charset = c.g.a.f1337a;
```

看到这一段后 感觉又是啥编码后的 还是比较迷糊

TAT