crypt 450

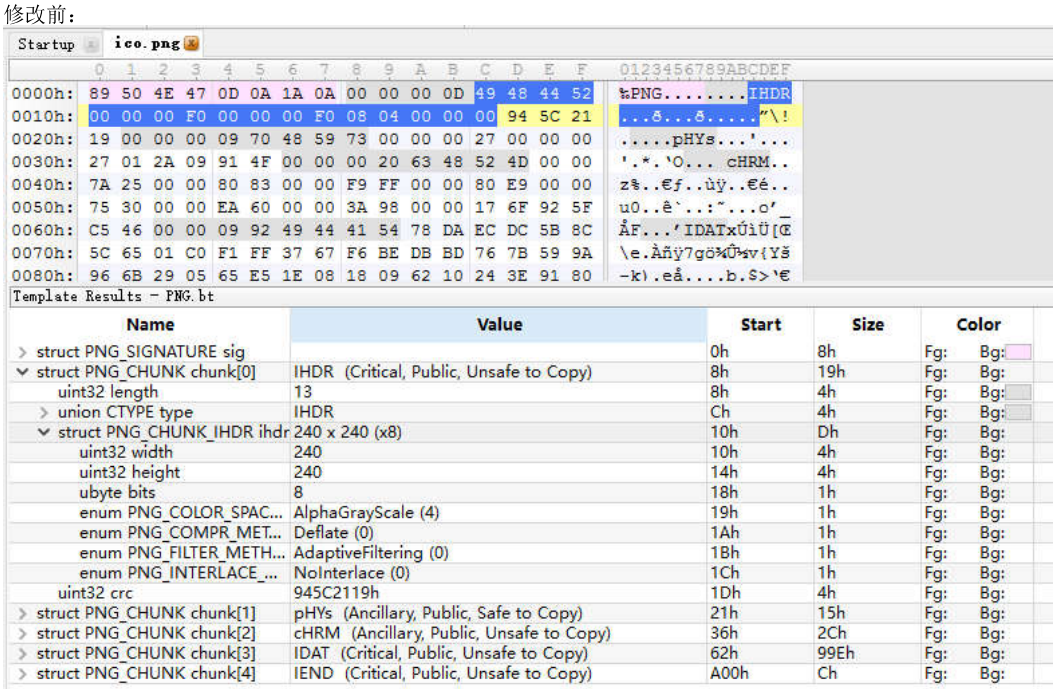
拿到流量包，只有三个http请求：

- 主页(特别加载了网站图标)
- 网站图标(favicon.ico)
- 下载了一个加密的zip文件(Somethingneeded.zip)

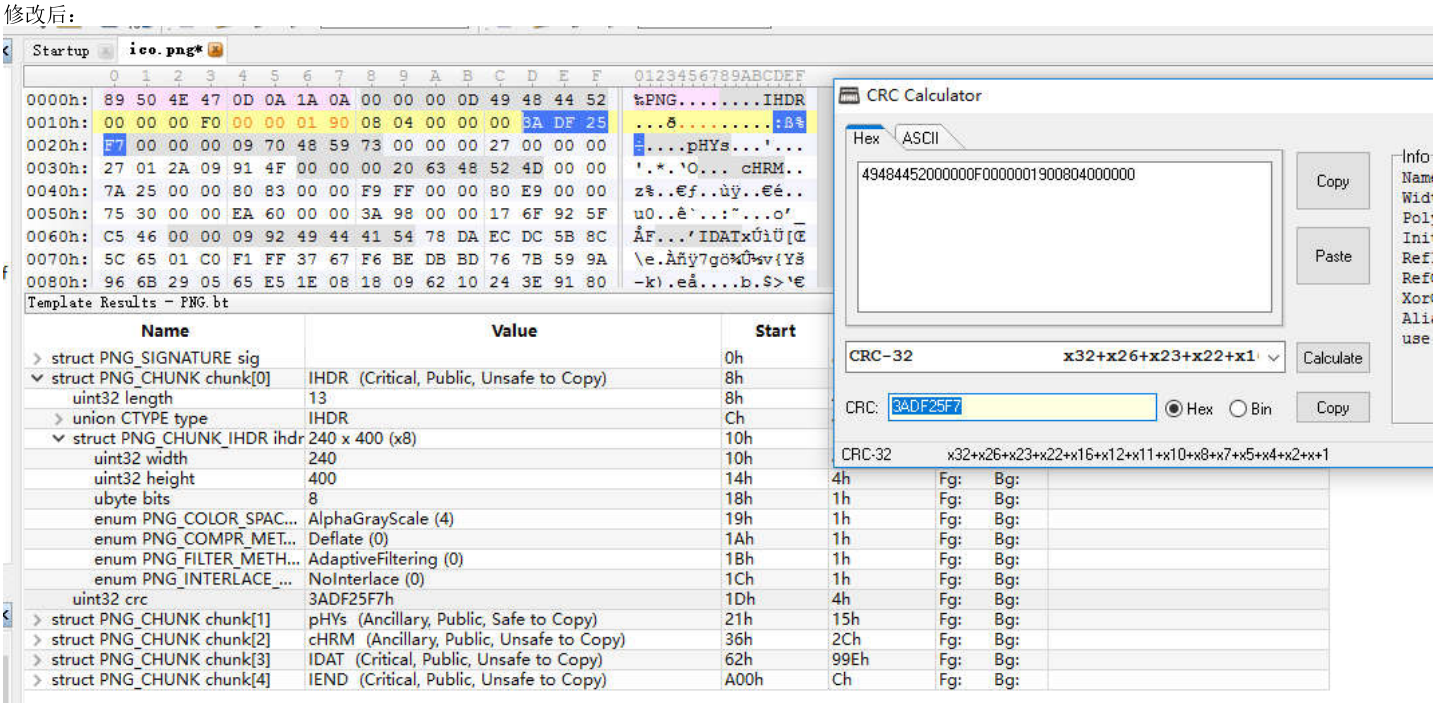
压缩包有密码，爆破不出来也没有提示；主页上就一个下载压缩包的链接，和一个网站图标的请求，然后看favicon.ico。一个简单的隐写，改了文件高度= =没有想到这里会卡主一部分人，估计解压出来压缩包的都卡在密码上，没解压压缩包的，都卡在这个隐写上面了。

用010editor打开图片，并载入png模板。找到文件的宽高字段，修改高度为一个略大的值，比如400，重新计算CRC并用新得到的CRC值替换原来字段的CRC值保存文件，打开就会得到zip加密的key。

修改前：



修改后：



key:3%7@pj!laYqL!XJ8

用得到的key解压压缩包会得到三个文件。

1. 发现RSA公钥中存在低解密指数攻击（加密指数过长）：通过Wiener Attack 攻击公钥n, e ，得到RSA私钥。恢复出RSA明文：
   AES_key:>>JfffOaqYHvuSIkfU
   First sign: ElGamal; First HASH: SHA[in python:>>int(SHA.new(msg).digest().encode('hex'),16)]

2. 使用1.中得到的AES的密钥解密文本，得到：
   ESIGN
   HASH: SHA
   Alice in Sun Sep 25 02:40:07 CST 2016
   in these Signatures, important things r different....but....they r one and the same. indeed.

通过1.中所给消息，知道本次信息传递中使用的是elgamal签名算法。发现几条对消息签名时使用了相同的随机指数（A值相同）。根据A,B,P,以及1.中给出的hash计算方法，解出elgamal的私钥。

1. 通过2.中的AES明文，知道本次信息传递中使用的是ESIGN签名算法。用AES解密后，发现明文是两篇演讲的片段。

发现没有找到flag，回头检查3，通过计算签名s的长度，发现其长度为4094位。长度有些诡异，怀疑用来计算N的私钥有问题。通过以前的积累，或查询资料，发现本次esign中存在阈下信道。通过2.中所给信息，猜测本次阈下信道中的额外私钥r与2.中elgamal签名的私钥相同。对3.中签名信息计算后，得到信息：

1. flag:>>pleas3_b00m_**__b0om_shak4l4ka_lam_****
2. hash:>>b96648cc3f097c6faf581386b97d7e043521abe2369d1141d9a98d4897770ea7
3. map(lambda x:x in string.letters[:26]+string.digits, flag)==[True for x in len(flag)]

通过得到的信息得知：flag的格式、flag的hash值、flag包含的字符。其中，根据散列值长度得知，hash算法应为SHA256。此处有两种解法：

1. 猜测flag的值
2. 爆破

爆破耗时：in python 7966.50890207s