Normal_RSA Writeup

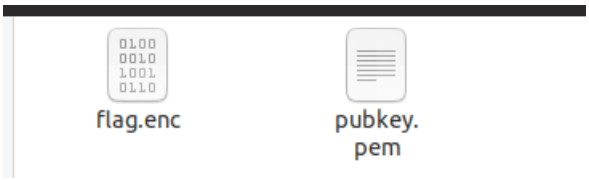
原创

tuck3r 于 2019-08-05 13:05:28 发布 2261 收藏 6

分类专栏： Crypto 文章标签： Crypto RSA Writeup

实验环境：
Ubuntu1904

实验工具：
openssl
rsatool.py（可在https://github.com/adeptex/rsatool或者https://github.com/ius/rsatool（免安装）上下载）
yafu（可在https://github.com/DarkenCode/yafu上下载）
分析过程
1、我们将下载的压缩包crypto7.rar解压
发现有两个文件：



首先我们使用openssl提取出public.pem中的相关参数（关于openssl的相关知识，可以自行google）,命令如下：

```
openssl rsa -pubin -text -modulus -in warmup -in pubkey.pem
```

会得到如下结果：

```
tucker@ubuntu:~/Desktop/Crypto/crypto7$ openssl rsa -pubin -text -modulus -in warmup -in pubkey.pem
RSA Public-Key: (256 bit)
Modulus:
    00:c2:63:6a:e5:c3:d8:e4:3f:fb:97:ab:09:02:8f:
    1a:ac:6c:0b:f6:cd:3d:70:eb:ca:28:1b:ff:e9:7f:
    be:30:dd
Exponent: 65537 (0x10001)
Modulus=C2636AE5C3D8E43FFB97AB09028F1AAC6C0BF6CD3D70EBCA281BFFE97FBE30DD
writing RSA key
-----BEGIN PUBLIC KEY-----
MDwwDQYJKoZIhvcNAQEBBQADKwAwKAIhAMJjauXD2OQ/+5erCQKPGqxsC/bNPXDr
yigb/+l/vjDdAgMBAAE=
-----END PUBLIC KEY-----
```


从中我们可以得到两个大素数的乘积（n）为：
c2636ae5c3d8e43ffb97ab09028f1aac6c0bf6cd3d70ebca281bffe97fbe30dd，转化为十进制则为：
879243482641324068752761405144999371450508936656025929924181716470424916584 61

2、对n进行大整数分解

由于这个乘积（n）长度不超过2^384，因此我们可以考虑使用yafu进行大整数分解或者在网站http://factordb.com/上进行分解（速度应该会更快），可以得到两个素数分别为：
275127860351348928173285174381581152299和
319576316814478949870590164193048041239

（关于yafu，可在以L(1/2)的复杂度进行大整数分解，仅适用于大整数不超过 2^384时，如果数据超过384bits，可以考虑使用连分数（https://zh.wikipedia.org/wiki/连分数）（具体的我也不大懂，读者可以自行google），

3、接下来我们使用rsatool生成私钥文件：

```
python rsatool.py -o private.pem -e 65537 -p 275127860351348928173285174381581152299 -q  319576316814478949870590164193048041239
```

(此处我的电脑运行rsatools，使用pip安装gmpy packet时，出现了一点小bug，并且在Stack Overflow和AskUbuntu上搜寻了半天，仍未解决……所以接下来的步骤我是无能为力了……就靠各位大佬了……如果同样出现上述问题的还请各位大佬指教……）

上述将会生成private.pem文件，即我们刚刚产生的私钥文件。

4、 用private.pem解密 flag.enc

```
openssl rsautl -decrypt -in flag.enc -inkey private.pem
```

我们就可以得到flag了。