2016 年第 19 题

大家好，我是胡一米。这期视频是关于 2016 年看雪 CTF 第 19 题解题资料。

一、简介

1.1 录制说明

视频是基于其他大佬文字 Writeup 录制的，所以在视频操作之前就已知了该题中的各种坑，如反调试等，所以不再演示踩坑过程。

1.2 录制参考

第 19 题主要参看了 HighHand、风间仁以及 AloneWolf 的 Writeup，链接如下：
HighHand:
https://bbs.pediy.com/thread-214562.htm
AloneWolf:
https://bbs.pediy.com/thread-214570.htm
风间仁：
https://bbs.pediy.com/thread-214478.htm

1.3 内容简介

在本期中，主要讨论 4 个问题。这 4 个问题可能与最终的 Key 没有太大的联系，但题目中既然出现了，还是说一说。此 4 个问题分别是：
a. 大数运算的识别
b. RSA 签名
c. RSA Tool、Big Integer Calculator、factordb.com
d. libtommath 大数库

二、视频操作

2.1 静态分析定位关键点

结合其他大佬的分析过程，可以直接定位到关键点。.
a. RSA 签名

```
加密: c = (m^e) mod n
解密: m = (c^d) mod n
```

条件：
签名内容为要求的字符串

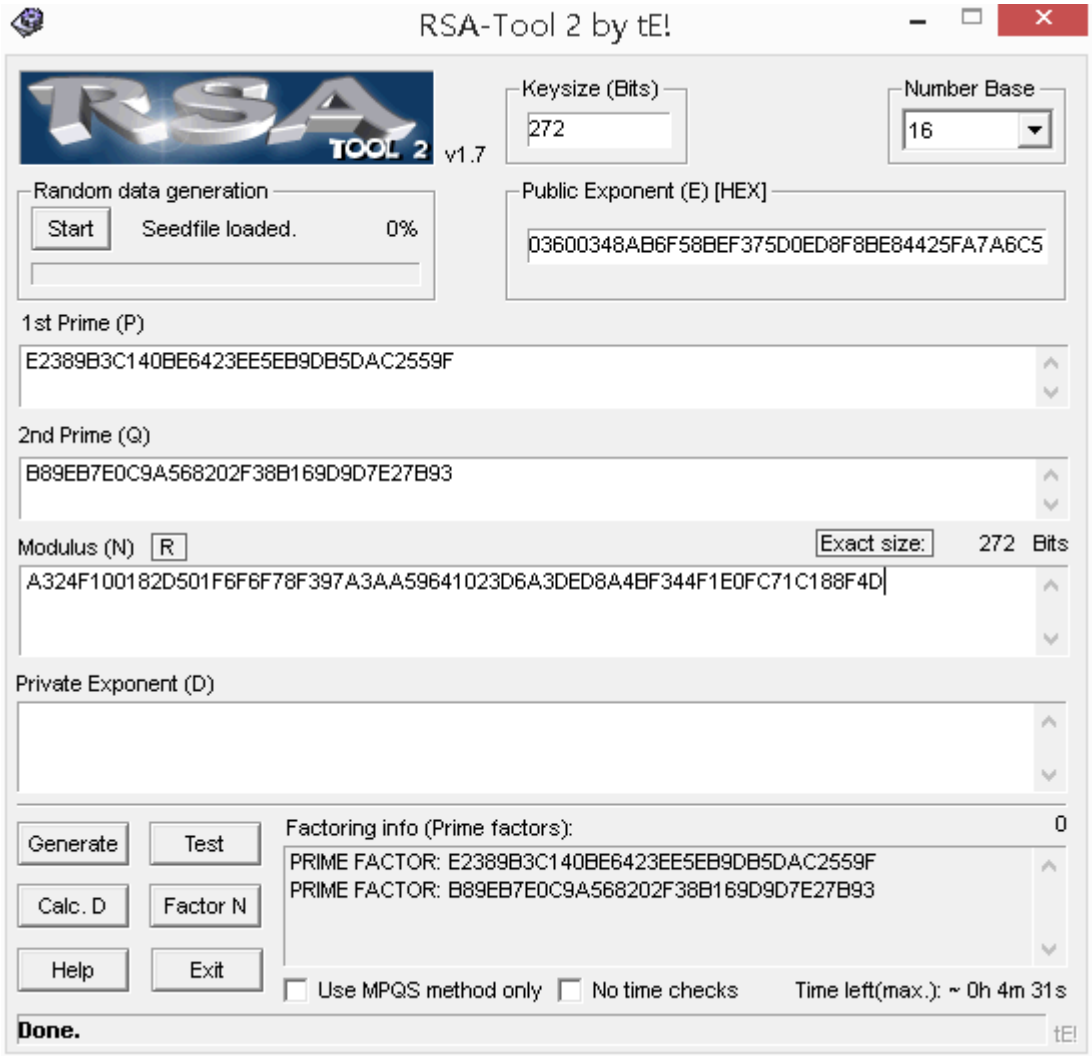
2.2 动态调试其加密过程

通过动态调试，理解程序内存加载过程。
a. 大数运算的识别

8525B546AE766CAD7F7964B1E5DD00DB6C535828F96AFBF1F0CD84440E2E072C9969

可以到 factordb.com

或者用 RSATool



2.3 计算某一个验证码

使用 visual studio 和 libtommath 库。这里直接使用 HighHand 大佬贴出的代码。

三、小结

题目很好。

附录：

录制顺序：29 – 28 – 7 – 19 - ?