RSA原理和手工，工具解密

翻译

cried_cat 于 2018-04-01 09:06:37 发布 3201 收藏 2

2018/3/30

criedcat

密码学writeup

笔者借阅一些网络文献来总结笔者一周来对密码学以及rsa加密方法的认知。

本writeup提纲：1rsa加密理论2手工解密rsa算法3解析解密rsa题目4ctf的rsa

Rsa理论参考链接：

https://blog.csdn.net/dbs1215/article/details/48953589（链接中笔者发现了一些错误，读者请自行去辨别，看链接的文章中正确的内容）

文章已经说的很彻底了，笔者认为，如果说看过rsa加密后自认为解密思路也比较明朗的话，限制人类破解rsa加密的因素，主要是计算机的运行能力。所以才会说，对于计算机而言，找到一种更容易分解质数的算法，才会离破解rsa算法迈进一步。

这里就简单写一写rsa理论概括了。

公钥	（E，N）
私钥	（D，N）
密钥对	（E，D，N）
加密	密文＝明文*EmodN*密文＝明文EmodN
解密	明文＝密文*DmodN*明文＝密文DmodN

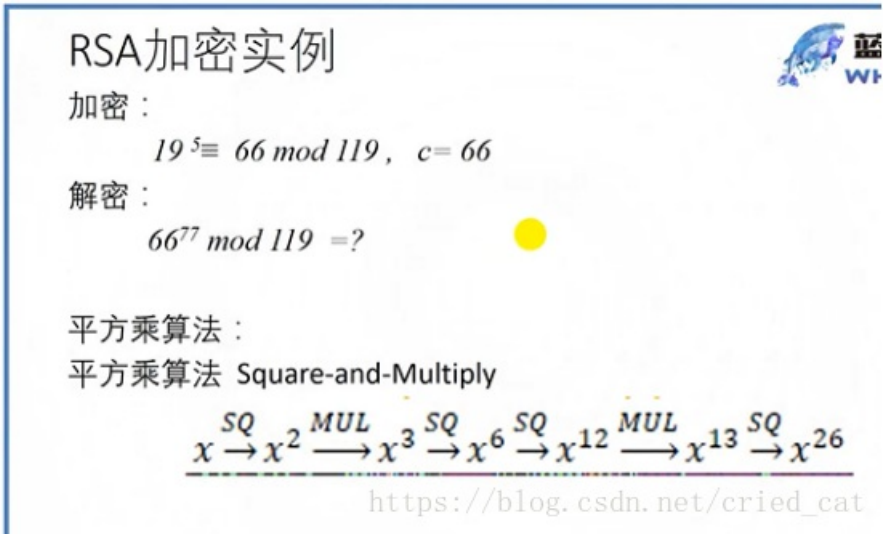
求N	N＝ p ＊ q ；p，q为质数
求L	L＝lcm（p－1，q－1）；L为p－1、q－1的最小公倍数
求E	1 < E < L，gcd（E，L）=1；E，L最大公约数为1（E和L互质）
求D	1 < D < L，E＊D mod L ＝ 1

通过上面的表格，容易知道，rsa加密紧紧依赖着质数分解。

首先笔者觉得有个比较使用的技术：

手工算小数值rsa的算法

题目意图：



比如，我们要加密的数字是十九；

现在我们想办法把密文66的77方还原回19；

而手工的数学关键就是，，

还原这个数字。

我们知道密文，大数，私钥：

数学表达式：

```
平方乘算法：
66^77 mod 119
```

首先还原密钥为二进制：

```
77 = 0b1001101
1 0 0 1 1 0 1
```

第一位的底数为66； 66的平方为4396，然后模119，得到72；

```
1   0   0 1 1 0 1
66  72
```

接着下一个数字是0，0还是做乘方，我们把72平方得5184，再模119，

获得的数就是67；下一个数是1了，1和0的运算不一样，是先乘方再乘x，

所以67的平方再乘66（注意，要乘的不是进阶数，而是基数66），再模119，得到83；

```
1   0   0   1   1 0 1
66  72  67  83
```

；再遇到一，83先做平方，再乘66，模119得到94；最后是0，直接94做平方模119得30；

最后做最后一位1，30方乘66模119最终得到了明文19.

上述是手工方法，接下来是编程思路，详见www.whaledu.com/course/76/task/680/show，个人理解是，把手工的方法编写为程序

带有星号的就是加密的文件，要求我们输入密码，可能是伪加密。

一般有两种思路：1：伪加密，不需要真正输入密码进行解密；2：进行爆破：用进行爆破（只针对zip）；

这个支持字典自动生成

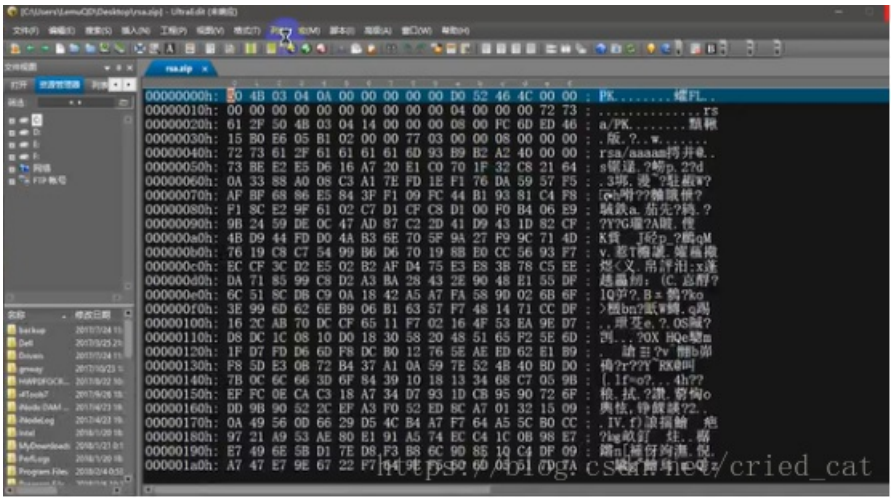
伪加密速度快；

以下介绍两种破解伪加密的算法：

1手动

要掌握文件的

压缩包格式：用winhex来打开文件压缩包



找加密位，

带有pk字段，这就是加密的东西。文件夹，压缩文件本身，两个文件，在这道题中一共是四个pk位；

但是最终找到五个pk

找明显带有0的地方

这里的0014（0x0014）代表压缩方式是怎样压缩的

我们要改动的就是0014后面的两个00；（之前的pk后是两个00）

这里表示了伪加密的位置，把09（加密）变成00就可以了，保存。

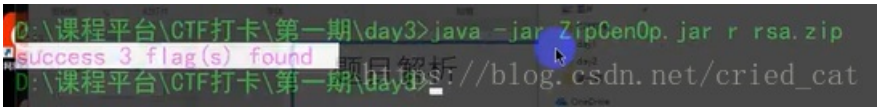
生成新文件，我们可以发现星号不见了，解压成功。

（百度：文件头格式）

2

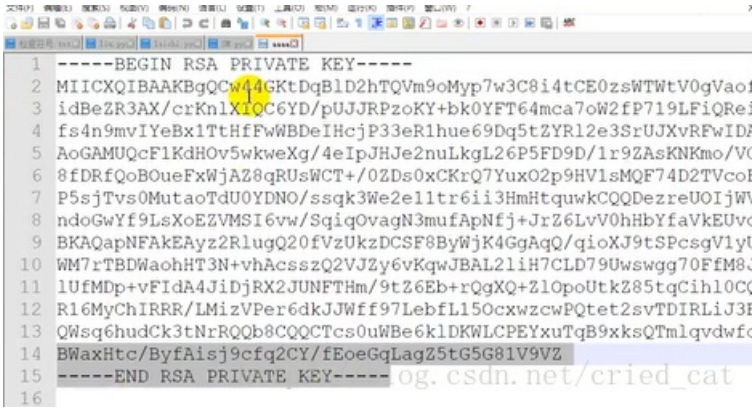
把zip文件放到zipcenop的同目录下即可，输入命令

回车，注意备份，这回直接修改文件

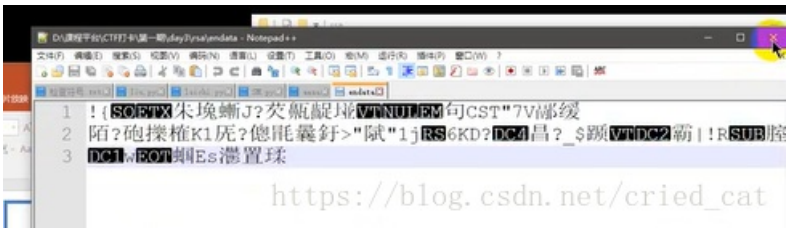


获取三个加密标志位，已去除加密标志。

把aaa打开，



这是rsa私钥文件

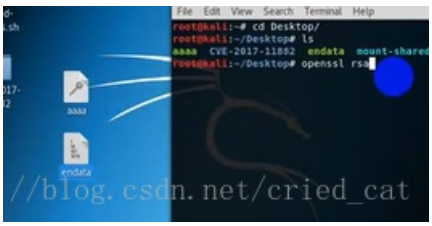


这是密文

接下来，我们用openssl解密

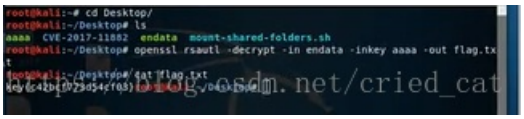
再kali中输入：

则，再当前文件夹下生成了解密后的文件。



把题库的文件拖进kali中，，

其实和上二图中的命令一样；



视频中用cat命令读取了解密文件内容

嗯，以上主要是是rsa手工解密的算法了。

密钥生成

题目链接：

http://daka.whaledu.com:9999/challenges#密钥生成

用rsa-tool算算就知道答案了；

直接把本篇writeup上文的操作转化为行动就出来了题，塔主亲讲过；

咳咳，本周时间仓促，未能做出几道rsa的题目。只能下周来上交解出rsa类的题目来弥补此周的缺陷。希望下周的writeup的rsa题目总结可以弥补此周写作的质量不佳。