buuctf rsarsa·wp

原创

connamon 于 2022-03-29 22:18:08 发布 3550 收藏
文章标签： 网络安全

本文链接：https://blog.csdn.net/sml1918451478/article/details/123833709

题目： **rsarsa**

题目来源： buuctf（BUUCTF在线评测 (buuoj.cn)）

分析过程

1、复习一下rsa的原理

算法描述

播报 编辑

RSA算法的具体描述如下： [5]

（1）任意选取两个不同的大素数p和q计算乘积 $n = pq, \varphi(n) = (p-1)(q-1)$ [5] ；

（2）任意选取一个大整数e，满足 $gcd(e, \varphi(n)) = 1$ ，整数e用做加密钥（注意：e的选取是很容易的，例如，所有大于p和q的素数都可用） [5] ；

（3）确定的解密钥d，满足 $(de) mod \varphi(n) = 1$ ，即 $de = k\varphi(n) + 1, k \geq 1$ 是一个任意的整数；所以，若知道e和 $\varphi(n)$ ，则很容易计算出d [5] ；

（4）公开整数n和e，秘密保存d [5] ；

（5）将明文m（m<n是一个整数）加密成密文c，加密算法为 [5]

$$c = E(m) = m^e mod n$$

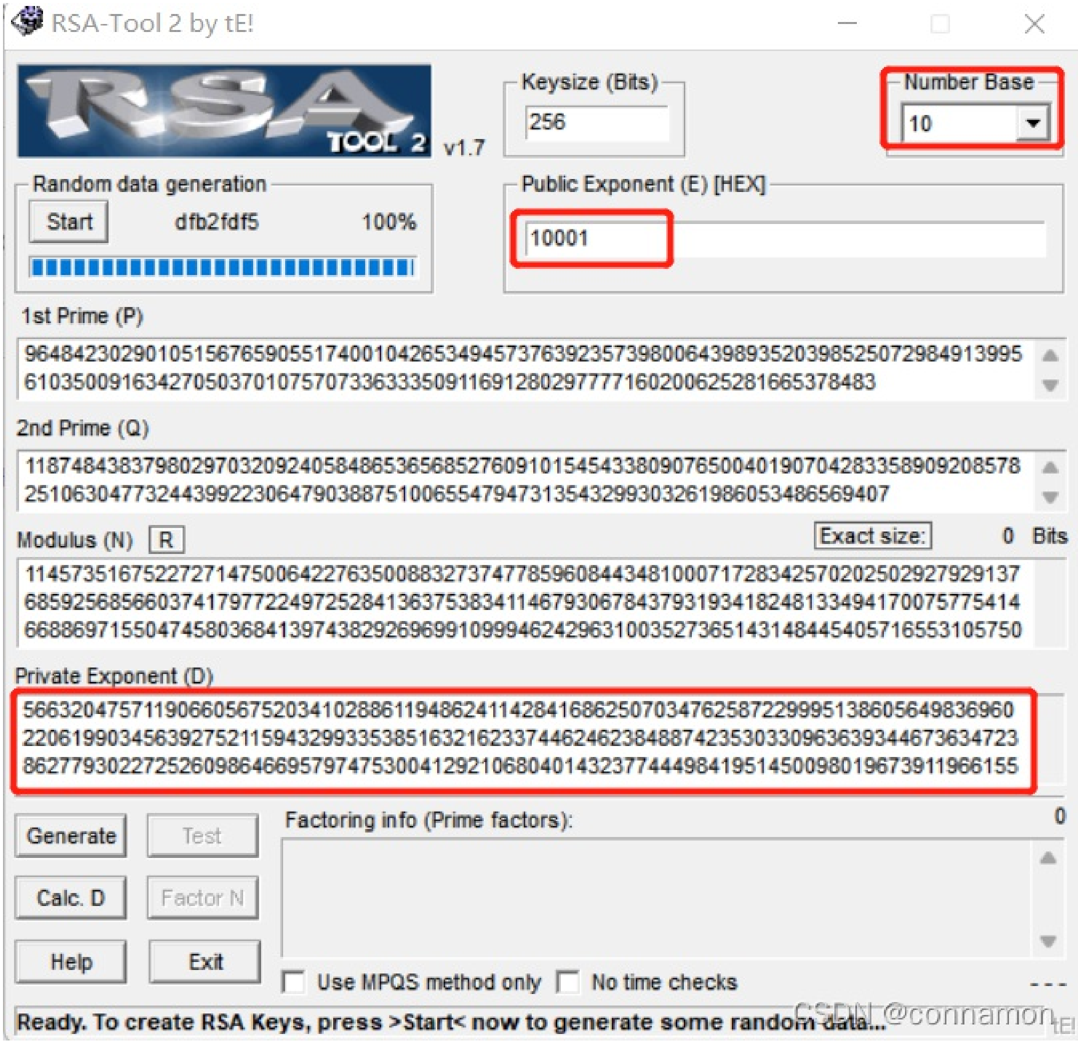
（6）将密文c解密为明文m，解密算法为 [5]

$$m = D(c) = c^d mod n$$

然而只根据n和e（注意：不是p和q）要计算出d是不可能的。因此，任何人都可对明文进行加密，但只有授权用户（知道d）才可对密文解密 [5] 。

2、根据题目给的p、q、e、c扔进rsatool计算（其中e要转化成16进制）

rsatool2下载链接：链接：百度网盘 请输入提取码
提取码：upnr



3、最后python上pow根据公式求解铭明文

```
n=11457351675227271475006422763500883273747785960844348100071728342570202502
C=83208298995174604174773590298203639360540024871256126892889661345742403314
d=56632047571190660567520341028861194862411428416862507034762587229995138605
M = pow(C,d,n)    #快速求幂取模运算
print(M)
```

CSDN @connamon

知识点总结： rsa原理

rsa加解密工具RSATool的使用：https://blog.csdn.net/ss7xz/article/details/116352120