**《计算机网络安全》实验报告**

**实验（5）非对称密码-RSA实验**

学生姓名： 陈华豪 学 号： 6130116238 专业班级： 网络工程161班

实验类型：■ 验证 □ 综合 □ 设计 实验日期：  实验成绩：

**实验目的**

通过实际编程了解非对称密码算法RSA的加密和解密过程，加深对非对称密码算法的认识。

**试验内容**

1. 学生通过实验能深入、透彻地理解RSA算法的基本原理

2. 能使用RSA对文件进行加密；

3.根据给出的RSA算法简单实现的C代码源程序。

**3．实验过程**

3．1实验环境

VPC1(虚拟PC）：操作系统类型：windows XP

实验环境描述：Windows xp

软件描述：gcc（linux）、VC（windows）C语言编译环境。

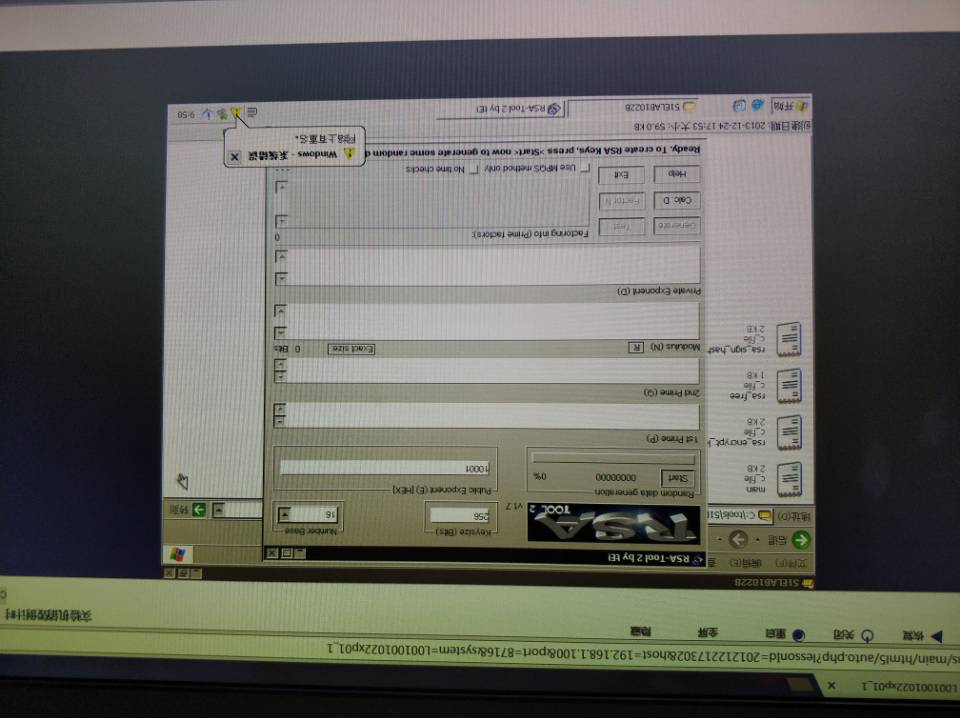
3．2关键实验步骤及配置

1、 学生单击进入实验场景，单击L001001022xp01\_1中的“打开控制台”按钮，进入目标主机。

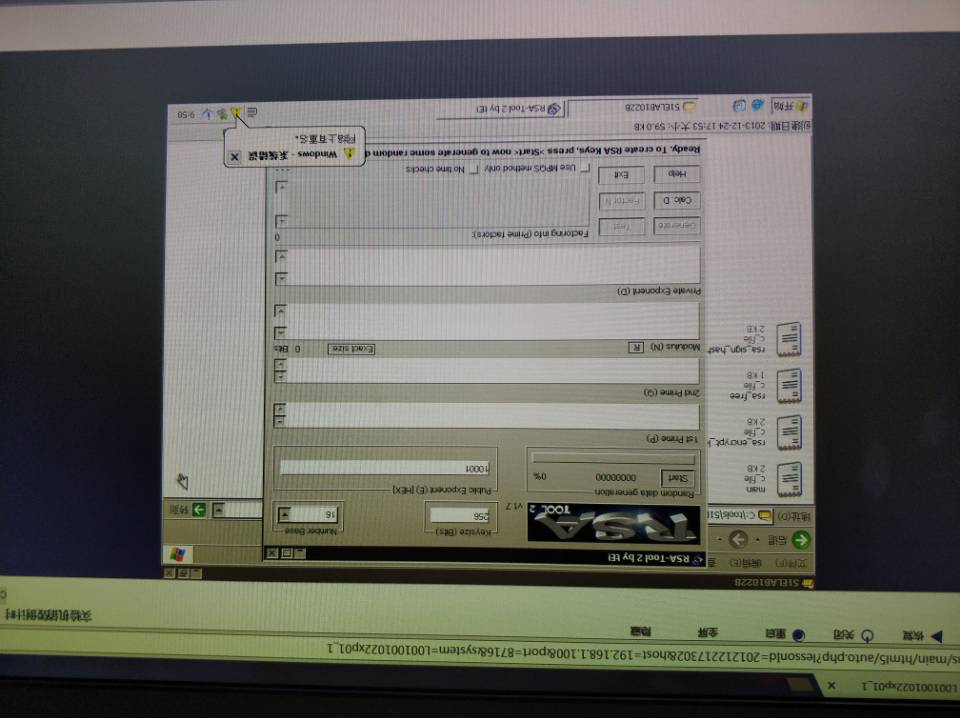
2、使用默认的用户名：administrator，密码：123456登录到windows xp系统。

3.点击进入目标主机上的目录“C:\tools\51elab1022B”。

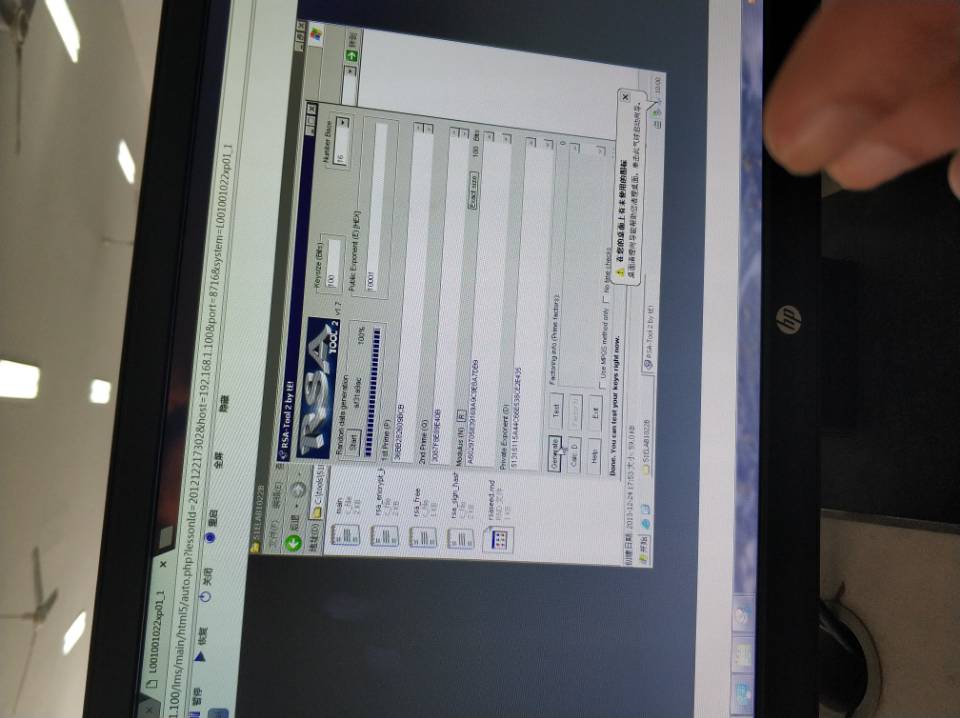
4.点击打开“RSATool”，出现如下界面。



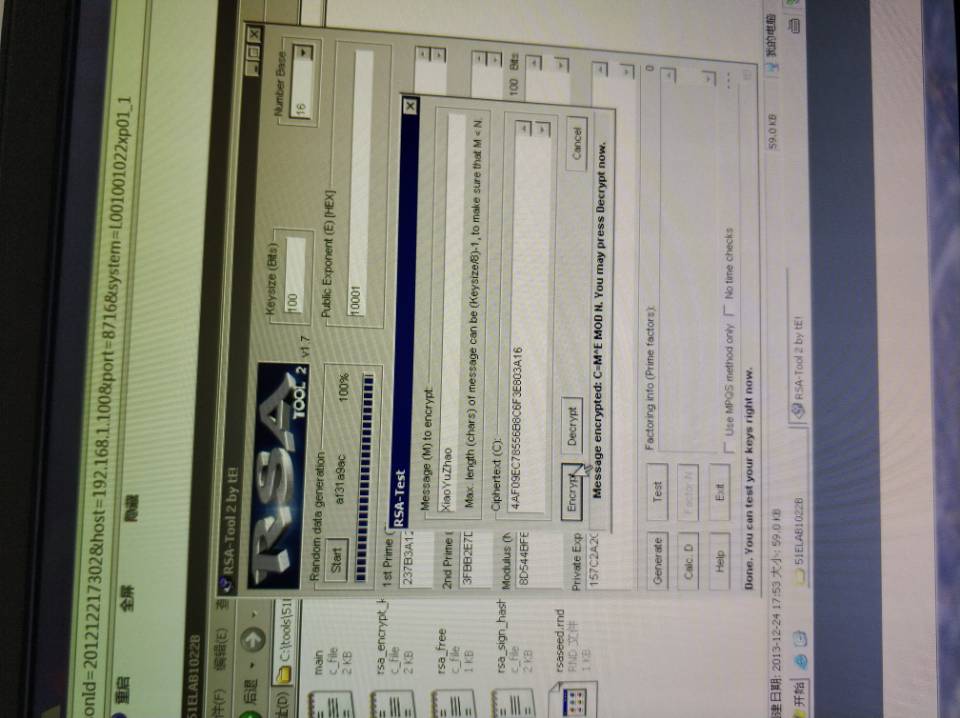
5.单击“Start”按钮，然后随意移动鼠标直到提示信息框出现，以获取一个随机数种子。



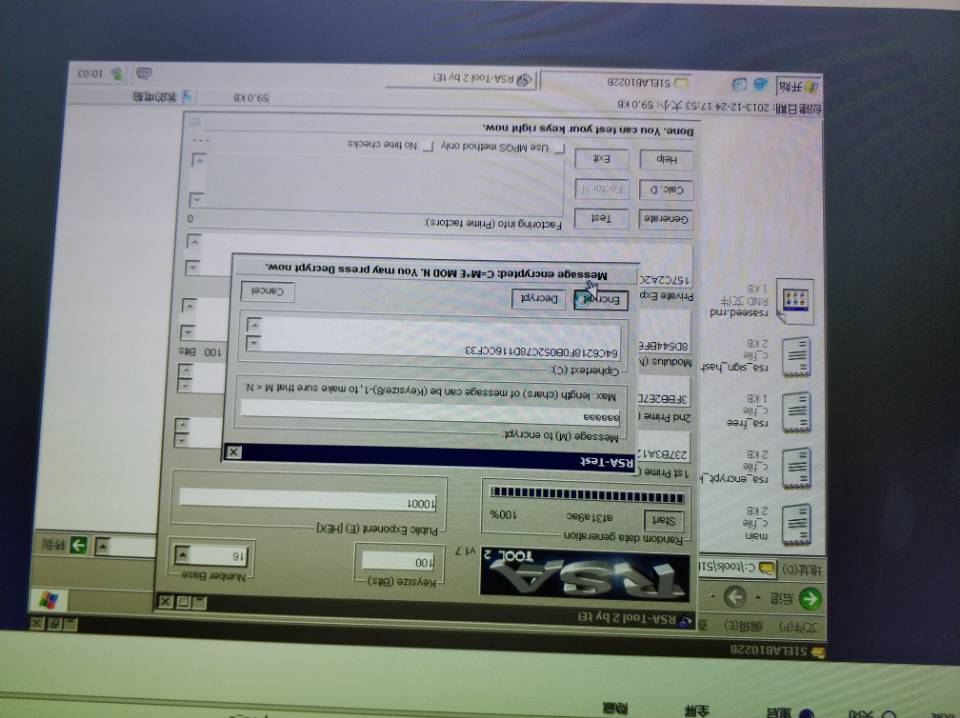
6.在“Keysize”中输入你想要的密钥的长度，从32到4096，位数越多安全性也高，但运算速度越慢，一般选择1024位足够了，单击“Generate”按钮生成。

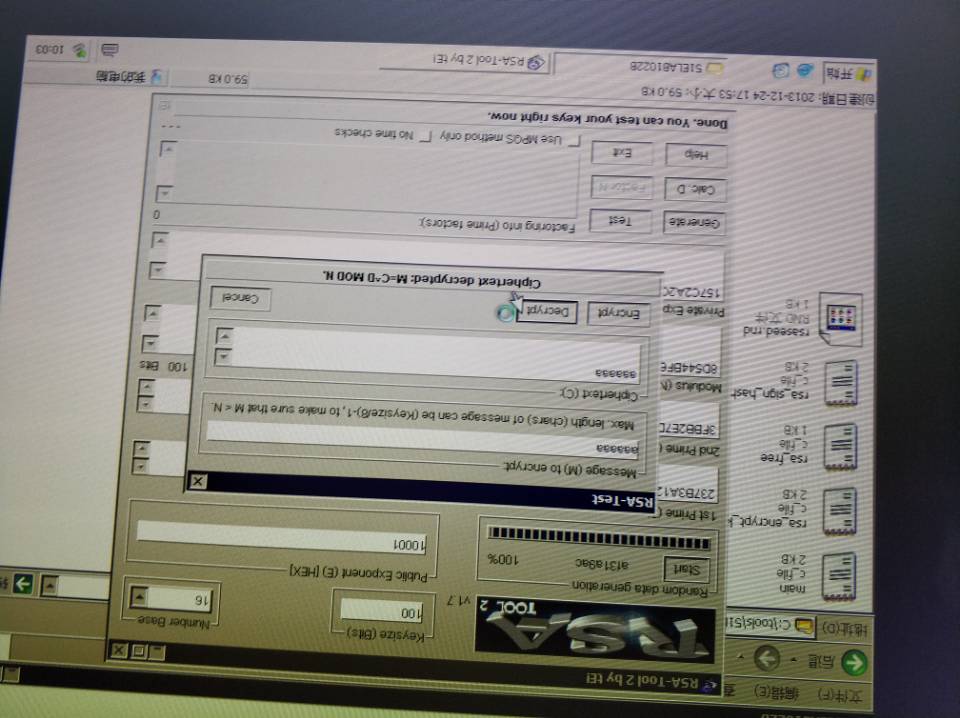


7.单击“Test”按钮测试，在“Message to encrypt”编辑框中随意输入一段文本，然后单击“Encrypt”按钮加密，再单击“Decrypt”按钮解密，看解密后的结果是否和所输入的一致，如果一致表示所生成的RSA密钥可用，否则需要重新生成。



**实验结果**





**实验总结**

通过rsa算法加密信息破解难度大，通过计算顺着容易逆向难的特点保证了破破译的困难性和加密的简单性。