**《计算机网络安全》实验报告**

**实验（8）DSA签名算法实验**

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**

通过对数字签名软件的使用，加深对数字签名原理和过程的了解。实验会给出有关数字签名技术的典型协议。结合这些协议充分理解DSA和ECDSA数字签名技术。

**试验内容**

使用DSAToolv13.exe工具对文件进行加密和解密

了解DSA算法的原理

**3．实验过程**

3．1实验环境

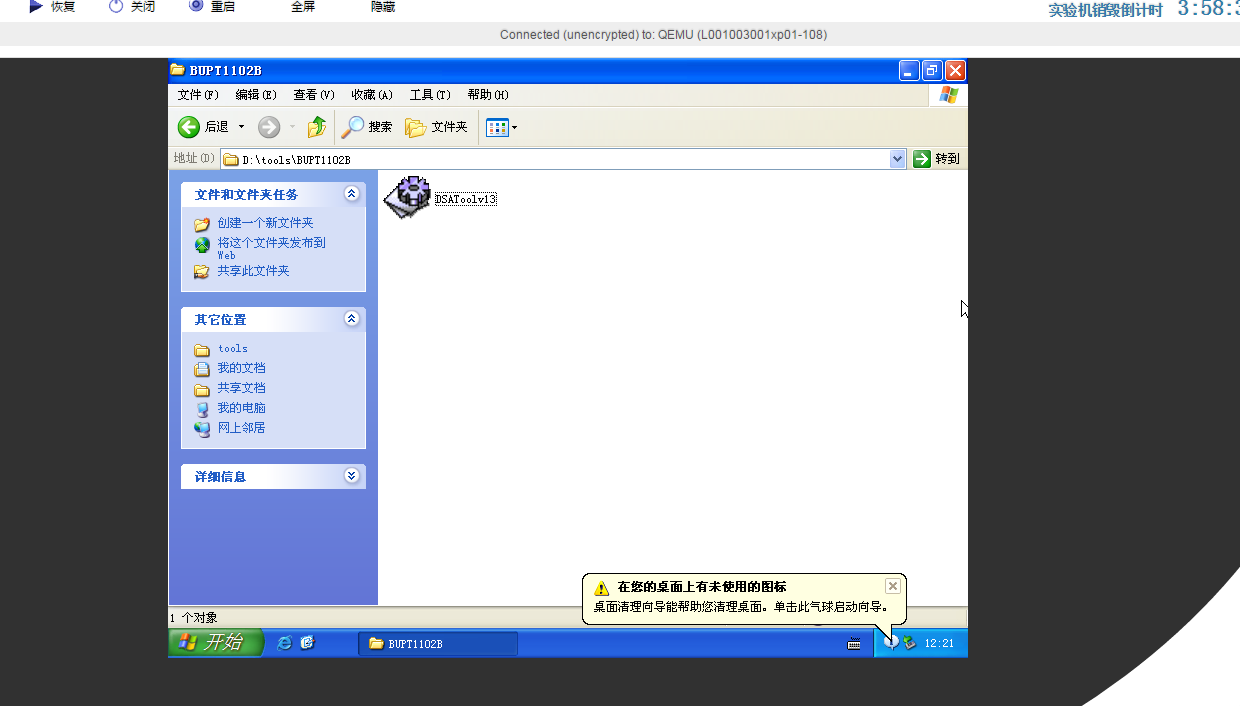
Windows xp 操作系统

DSAToolv13.exe工具

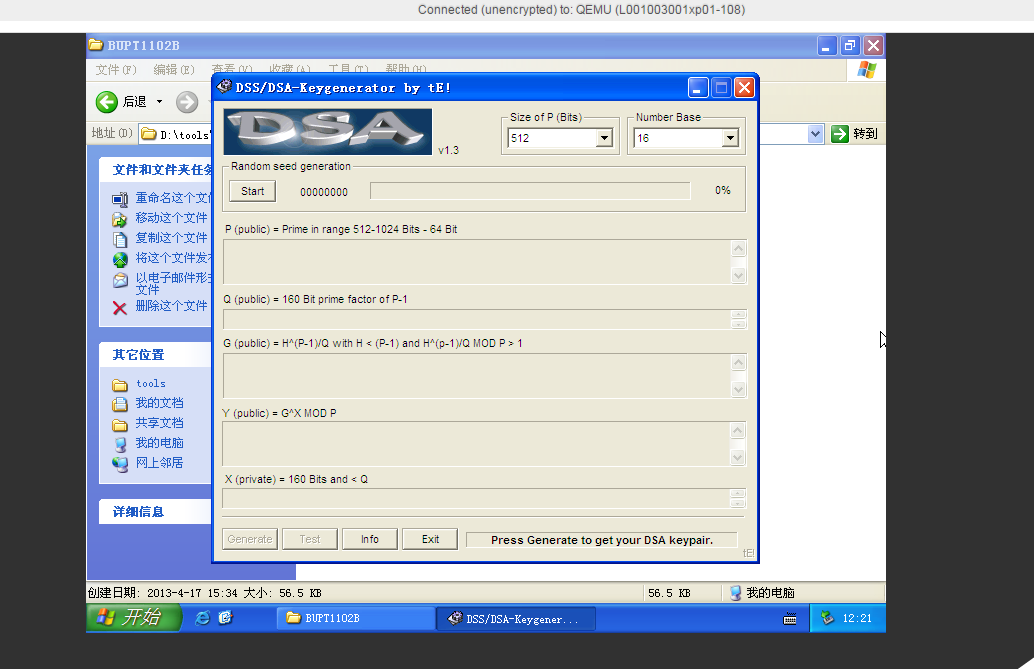
3．2关键实验步骤及配置

1 、打开控制台，进入虚拟环境。

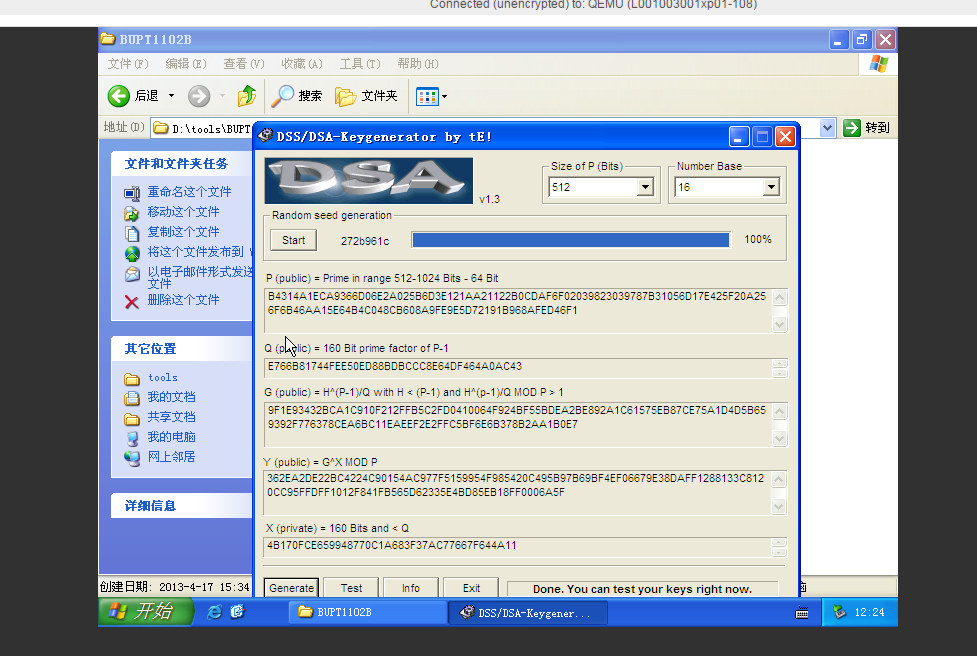
2、在D:\tools\51elab目录下找到DSAToolv13.exe程序，双击运行。



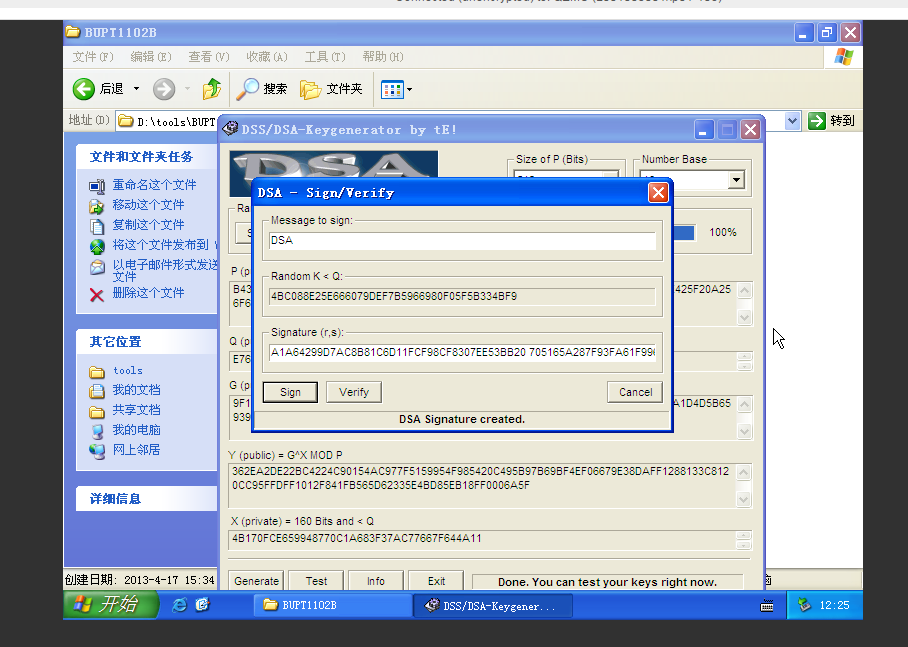
3、先点击“Start”，在弹出的对话框中选择“是”，并随意在框架内移动鼠标，生成一个随机数种子。



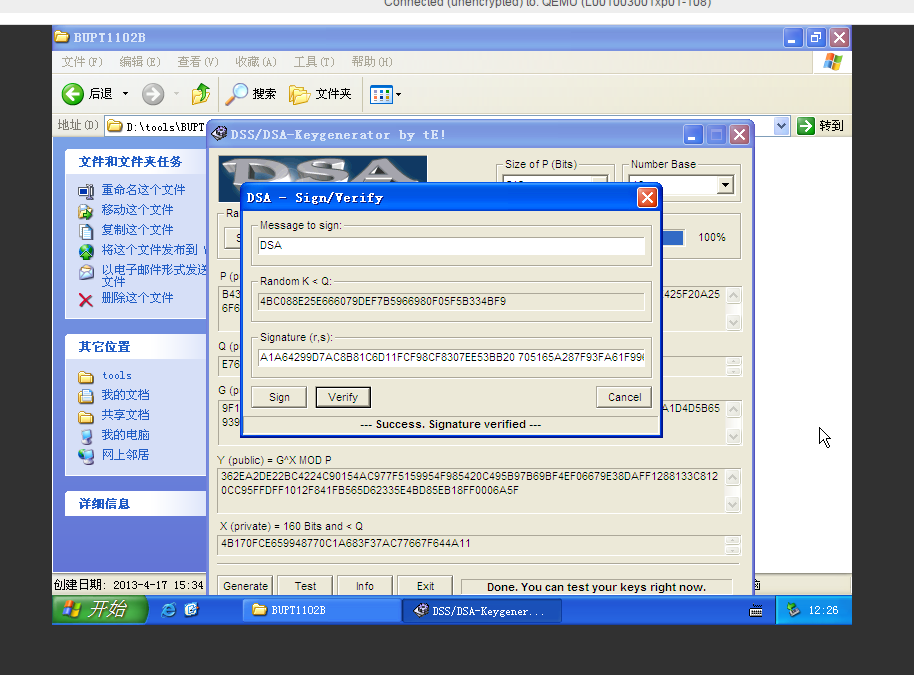
4、随机数种子生产完毕后，会在DSAToolv13.exe同目录下产生一个新文件dsaseed.rnd。若之前已经存在此文件则直接点击“Generate”按钮。



5、从前面的DSA算法原理可知界面中各项数据的含义。下面点击“Test”，在第一行输入要签名的消息“This is DSA”，单击“Sign”用产生的密钥对消息进行签名。

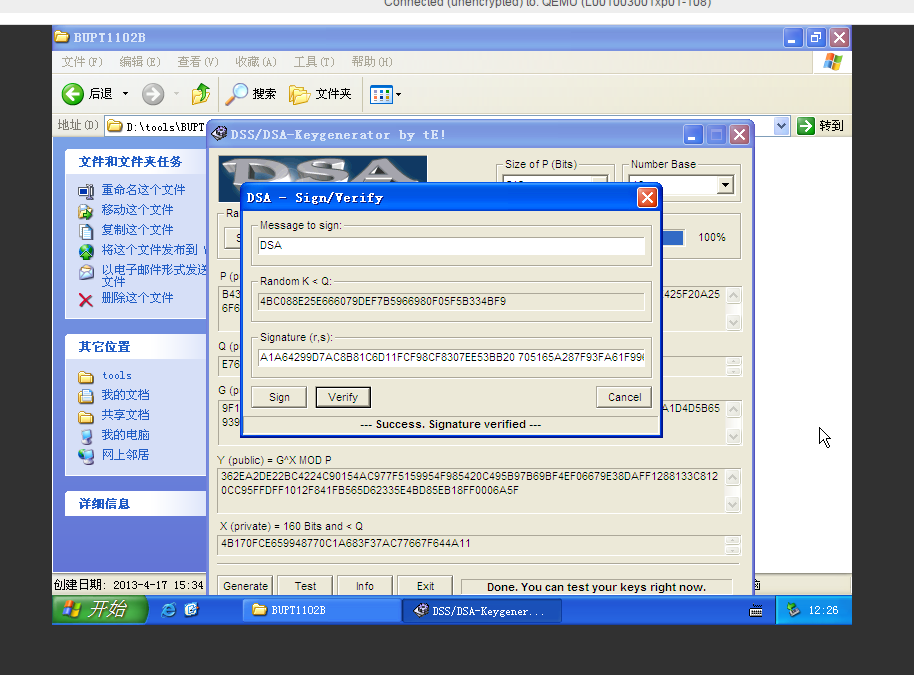


6、单击“Verify”可以对签名进行验证。



**实验结果**

同上



**实验总结**

网上有成熟的加密软件，方便运用，且因为加密原理本身的强大性，小软件可以实现高安全。