**《信息安全概论》实验报告**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **姓名** | **谢双骏** | | **年级** | | **2019级** |
| **学号** | **20194196** | | **专业、班级** | | **计算机科学与技术01班** |
| **实验名称** | **PGP加密软件文的使用** | | | | |
| **实验时间** | **2022.11.26** | **实验地点** | | **线上** | |
| **实验成绩** |  | **实验性质** | | **□验证性 □设计性 □综合性** | |
| 教师评价：  □算法/实验过程正确； □源程序/实验内容提交 □程序结构/实验步骤合理；  □实验结果正确； □语法、语义正确； □报告规范；  评语：  评价教师签名（电子签名）： | | | | | |
| **一、实验目的**   1. 掌熟悉公开密钥体制，熟悉数字签名 2. 熟悉使用PGP的基本操作 | | | | | |
| **二、实验项目内容**   1. 创建一私钥和公钥对 2. 与别人交换使用 3. 对公钥进行验证并使之有效 4. 对E-MAIL进行加密和数字签名对E-MAIL进行解密和验证 | | | | | |
| **三、实验原理**  PGP加密软件是美国Network Associate Inc.出产的免费软件，可用它对文件、邮件进行加密，在常用的WINZIP、[Word](http://www.d9soft.com/article/304/ArticleList304_1.htm" \o "" \t "_blank)、ARJ、[Excel](http://www.d9soft.com/article/305/ArticleList305_1.htm" \o "" \t "_blank)等软件的加密功能均告可被破解时，选择PGP对自己的私人文件、邮件进行加密不失为一个好办法。除此之外，你还可和同样装有PGP软件的朋友互相传递加密文件，安全十分保障。 | | | | | |
| 1. **实验过程或算法** 2. **安装**   PGP的安装很简单，和平时的软件安装一样，只须按提示一步步“Next”完成即可。其中在以下的画面你可以选择要安装的选件，如果选择了“PGPnet Virtual Private Networking”虚拟网，再选择相应的Plugin，如“PGP Microsoft Outlook Express Plugin”，就可以在Outlook Express中直接用PGP加密邮件，这里指的是加密邮件的内容，具体操作我们在后面会详细说到。   1. **生成密钥** 2. 用菜单key>new key开始生成密钥   **1**   1. 输入全名和邮件地址。虽然真实的姓名不是必须的，但是输入一个你的朋友看得懂的名字会使他们在加密时很快找到想要的密钥。   **2**   1. 重复输入你的密码。   **3**   1. 接下来PGP会花一点点时间来生成你的密钥   **4**   1. 询问你是否想把你的公共密钥发送到[服务器](http://www.d9soft.com/query.asp?t=m&q=服务器" \o "" \t "_blank)上去，一般我们是不会这么做的，因此一直“下一步”就可以完成了。   **5**   1. 生成完成的密钥   **6**   1. 导出密钥   **7**   1. 导出后的密钥   **8**   1. **加密、解密** 2. 加密 3. 只须选中该文件，然后点击右键中PGP的Encrypt   QQ截图20221123120914   1. 选择使用公钥加密   QQ截图20221123120924  QQ截图20221123120936   1. 最后选择保存位置即可。   QQ截图20221123121014QQ截图20221123121020   1. 解密时双击扩展名为pgp的文件或选中并点击右键中的PGP>Decrypt，在图中的下框输入密码即可。   QQ截图20221123121448QQ截图20221123121458QQ截图20221123121614   1. **邮件签名和加密** 2. 输入邮件内容   QQ截图20221123145423   1. 添加数字签名   QQ截图20221123145436   1. 加入数字签名后的内容   QQ截图20221123145520   1. 使用公钥进行加密   QQ截图20221123145601   1. 使用公钥进行加密后的密文   QQ截图20221123145624   1. 接受到的密文邮件   QQ截图20221123145701   1. 对密文邮件进行解密后的内容   QQ截图20221123145727   1. 验证签名，state为good signature，没有问题，说明内容没有篡改   QQ截图20221123145755   1. 对密文进行篡改，解密失败   QQ截图20221123145912  QQ截图20221123145928   1. 对解密后的内容进行篡改，state为bad signature，发现签名已经失效   QQ截图20221123150011  QQ截图20221123150024 | | | | | |
| 1. **实验过程中遇到的问题及解决情况** 2. 在发送public key的时候，注意一定不要加密发送，直接发送即可，不然public key是不可以使用的 3. 老师给的安装包不能加密邮件的内容，后来在网上查找到了gpg desktop版本完成实验中邮件签名加密的部分 | | | | | |