山东大学 软件 学院

信息安全导论 课程实验报告

|  |  |  |  |
| --- | --- | --- | --- |
| 学号：201600301079 | 姓名： 崔玉峰 | | 班级： 2016级软件4班 |
| 实验题目： 实验四公钥算法应用之PGP | | | |
| 实验学时：4 | | 实验日期： 2018/ | |
| 实验目的： 实验内容 使用PGP或GPG，完成如下内容。 加密原理 查询资料，了解PGP原理，并用自己的语言重新表述。 密钥管理 导入、导出公钥、私钥。 加密(以及签名)文件 （1）文件加密，为了存储。  （2）文件加密，为了交换。 加密(以及签名)邮件 （1）发送匿名、加密邮件  （2）发送署名、不加密邮件  （3）发送署名、加密邮件 | | | |
| 硬件环境：  PC  CPU : intel-i5  RAM: 8G | | | |
| 软件环境：  虚拟机：VMWARE  操作系统：ubuntu 18.04.5 64位 | | | |
| 实验步骤与内容：   1. **PGP加密原理：**   PGP（Pretty Good Privacy）优良保密协议，是一款基于RSA公钥加密体系的加密软件。   1. **Linux下GPG安装：** 2. **执行apt-get install gnupg 进行安装** 3. **执行dpkg-query -l | grep gnupg查看安装情况：**    **密钥管理：**  1. **生成公钥密钥对** 2. **通过gpg --gen-key命令生成公钥** 3. **输入真实姓名，邮箱等信息，设置密码。** 4. **提示移动鼠标以产生随机数**        1. **查看公钥密钥对**   执行gpg -K命令查看生成的公钥密钥对：     1. **导出公钥：**   执行命令：gpg --export -a cuiyufeng > cuiyufeng.key  导出公钥cuiyufeng.key文件可以发给通讯的另一方。     **加密解密文件：**  1. **加密文件** 2. 准备加密文件main.txt      1. 执行命令 gpg -e -r **cuiyufeng** -o **Emain.txt main.txt**   UserID: **cuiyufeng**  输出文件：**Emain.txt**  加密文件**： main.txt**         1. 查看生成文件：       生成二进制文件所以用记事本打开乱码。   1. **解密文件：** 2. 执行解密命令gpg -d --passphrase **123456789** -o **Dmain.txt Emain.txt**   密码： 123456789  输出文件： Dmain.txt  需要解密文件： Emain.txt   1. 查看解密结果：          **签名文件：**  1. **执行命令 gpg --sign main.txt为文件签名** | | | |
| 结论分析与体会： | | | |