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    GPG | | | |
| 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DES,RSA公钥加密体系的混合加密软件。通过对称加密算法(DES.AES)对数据进行加密,通过非对称加密算法（RSA）对对称加密的密钥进行加密，即保证了加密的速度，由提高了交换密钥时的安全性。   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来生成KEY      1. **查看公钥密钥对**   执行gpg -K命令查看生成的公钥密钥对：  可以看到两个公钥密钥对，其中一个是我之前测试时生成的。     1. **导出公钥：**   执行命令：gpg --armor --export -a cuiyufeng > cuiyufeng.gpg  导出公钥 cuiyufeng.gpg文件可以发给通讯的另一方。    cuiyufeng.gpg:     1. **导入公钥：**   通讯的对方执行命令gpg --import cuiyufeng.gpg可以将密钥导入。 **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：          **签名验证文件：**  1. **文件签名 ：** 2. 执行命令 gpg --sign main.txt为文件签名   2) 提示输入密码：     1. 生成签名文件：      1. 可以生成单独的签名文件方便交换和验证：   gpg --detach-sign main.txt   1. **验证文件签名 ：**   执行命令gpg --verify main.txt.sig main.txt | | | |
| 结论分析与体会：    通过实验了解了pgp加密软件的使用，并且可以对一些文件进行加密和解密，并且对于pgp的原理也有了理解，也算将所学的算法知识应用于实践。 | | | |