江苏科技大学

课程实验报告

课　程：　无线网与移动终端安全技术

课　题：　Linux 环境搭建与 GPG 文件加解密

学　院：　计算机学院

姓　名：　陈四贵

班　级：　1822107101

学　号：　182210710119

指导老师：　张迪明

目　　录

一、实验目的

1.熟悉 linux 操作系统的基本使用方法，掌握命令行交互界面下的基础命令和软件包管理;
2.掌握基于 GPG 工具的非对称加密算法的使用方法，能够熟练完成对指定文件的加密和解密工作。

二、实验流程

1.安装 Firefox、Chrome、360 安全浏览器（非必需，但从兼容性考虑建议安装）；

2.配置浏览器网络代理;

> 1.地址：218.3.140.153
> 2.端口：23128

3. 登录实验平台;

> http://192.168.2.11:9000/。

4. 创建实验平台基础系统;

> 1.novnc 初始密码 password
> 2.系统管理员密码 resu

5. 熟悉 linux 系统;
6. 验证 GPC 加密工具。

三、基础验证

1. 安装 GPG;

```
sudo apt install gnupg
```

2. 创建密钥;

```
gpg --full-generate-key
```

3. 创建实验对象文件并填充任意信息；

```
touch /tmp/test.txt
或
nano /tmp/test.txt
```

4. 加密文件；

```
gpg -e -r  “Your Name” /tmp/test.txt
```

5. 解密文件。

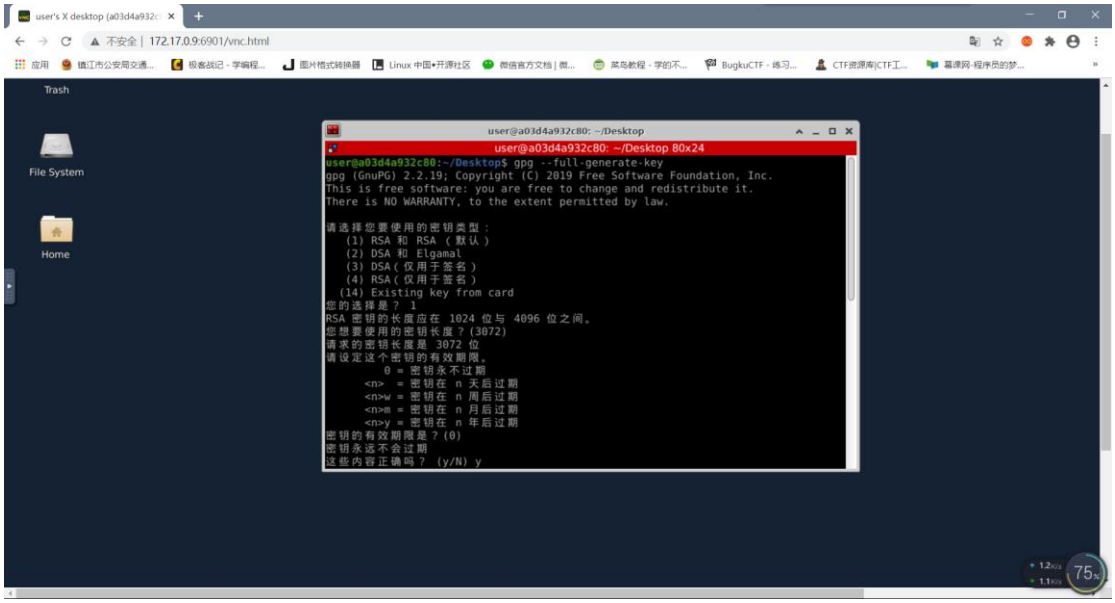
```
gpg -d /tmp/test.txt.gpg
```

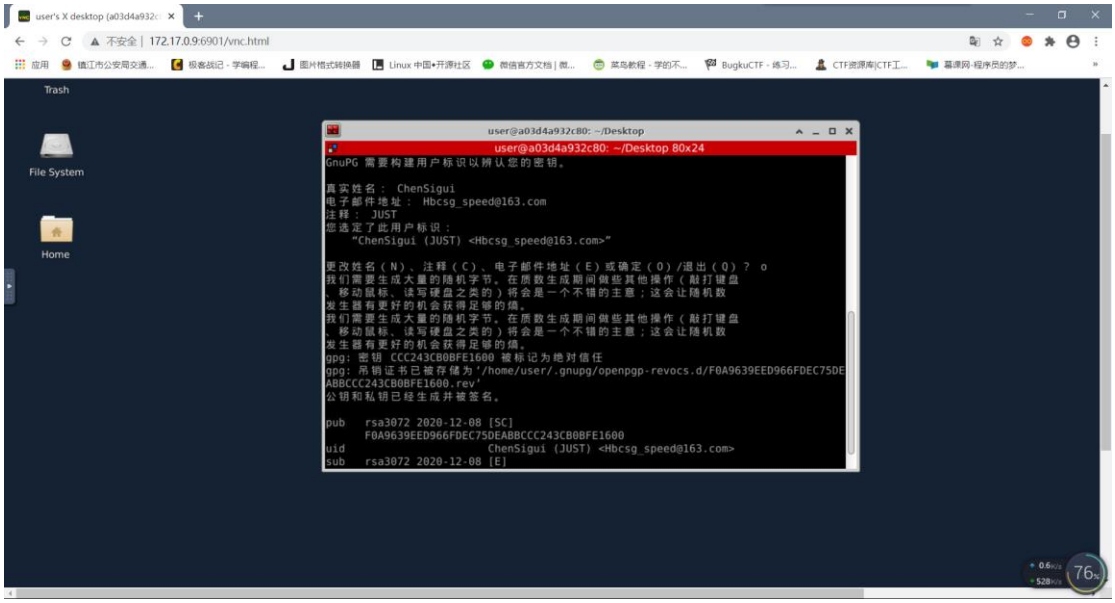
四、进阶验证

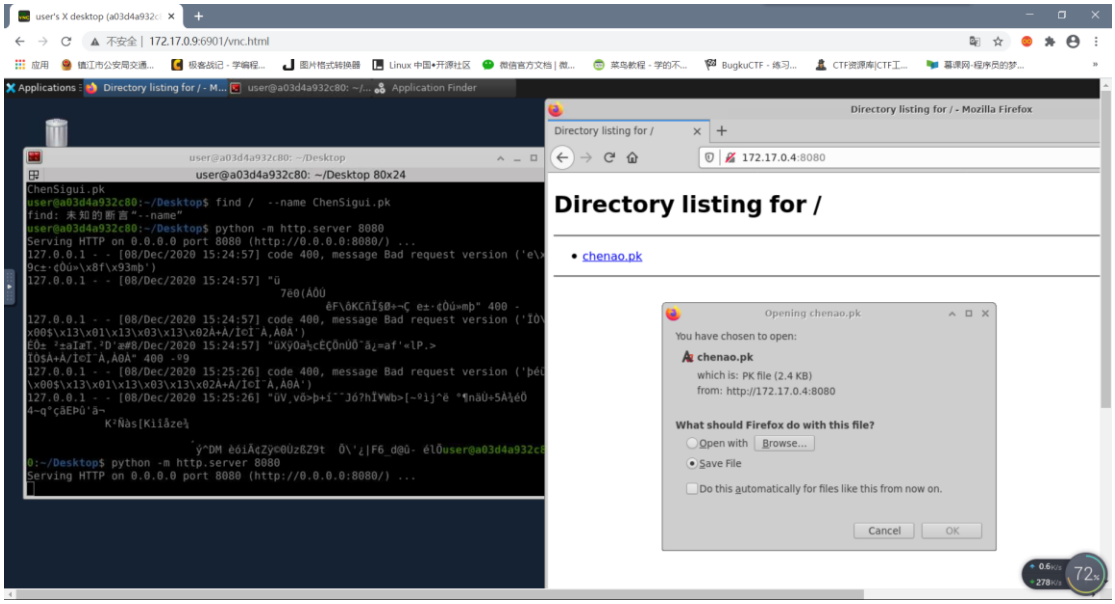
问：若 A 向 B 发送加密文件，B 如何才能正确解密？反之又如何？请两人一组完成该实验。

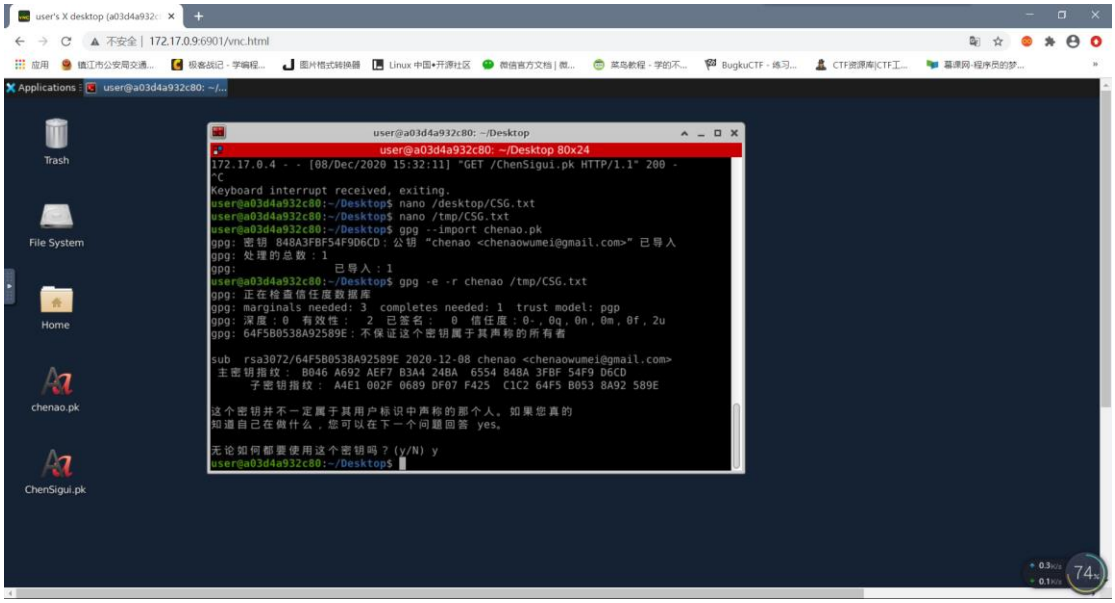
答：合作伙伴 IP 地址：172.17.0.4（182210710118 陈鳌）
4.1 在终端运行”gpg --full-generate-key”;
4.2 选择 RSA 和 RSA（默认），密钥长度 3072，密钥永不过期;
4.3 依据自身实际情况设置真实姓名、电子邮件地址、注释等;
4.4 按要求移动鼠标，生成密钥公钥和私钥并对其签名;
4.5 在终端运行”gpg --armor --export ChenSigui>ChenSigui.pk”生成自己的公钥文件;
4.6 在终端运行”find / --name ChenSigui.pk”查找自己生成的公钥文件，若出现未知的断言可输入 ls 命令，若无异常则成功生成;
4.7 在终端运行”python -m http.server 8080”后，并打开浏览器输入合作伙伴的 IP 地址，后加端口 8080，下载对方的公钥文件;
4.8 在终端输入”gpg --import chenao.pk”，导入对方的公钥;
4.9 在终端输入”nano /tmp/CSG.txt”，创建文本文件，编辑明文;
4.10 在终端输入”gpg -e -r chenao CSG.txt “，使用对方的公钥加密自己的文件，得到 CSG.txt.gpg 文件;
4.11 再次建立通讯，下载对方加密过的文件;
4.12 输入”gpg -d ca.txt.gpg”，解密对方加密的文件，得到明文。

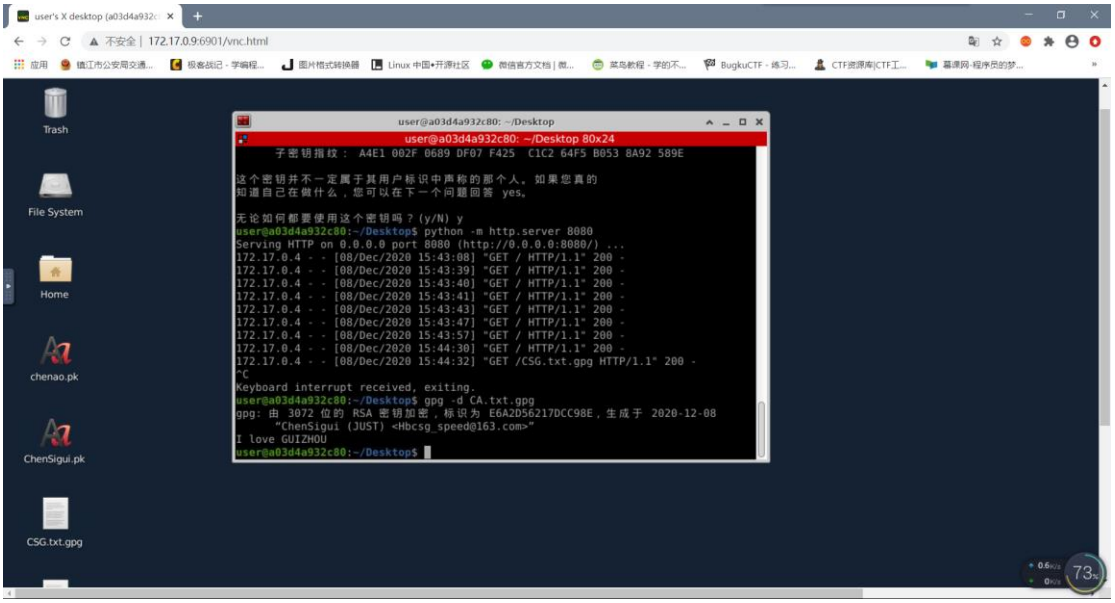
具体步骤图示如下：


user's X desktop (a03d4a932c80:0)
172.17.0.9:6901/vnc.html
Trash
File System
Home
user@a03d4a932c80: ~/Desktop
user@a03d4a932c80: ~/Desktop 80x24
user@a03d4a932c80:~/Desktop$ gpg --full-generate-key
gpg (GnuPG) 2.2.19; Copyright (C) 2019 Free Software Foundation, Inc.
This is free software: you are free to change and redistribute it.
There is NO WARRANTY, to the extent permitted by law.
请选择您要使用的密钥类型：
(1) RSA 和 RSA （默认）
(2) DSA 和 Elgamal
(3) DSA（仅用于签名）
(4) RSA（仅用于签名）
(14) Existing key from card
您的选择是？ 1
RSA 密钥的长度应在 1024 位与 4096 位之间。
您想要使用的密钥长度？(3072)
请求的密钥长度是 3072 位
请设定这个密钥的有效期限。
0 = 密钥永不过期
<n> = 密钥在 n 天后过期
<n>w = 密钥在 n 周后过期
<n>m = 密钥在 n 月后过期
<n>y = 密钥在 n 年后过期
密钥的有效期限是？(0)
密钥永远不会过期
这些内容正确吗？ (y/N) y
75%


user's X desktop (a03d4a932c80:0)
172.17.0.9:6901/vnc.html
Trash
File System
Home
user@a03d4a932c80: ~/Desktop
user@a03d4a932c80: ~/Desktop 80x24
GnuPG 需要构建用户标识以辨认您的密钥。
真实姓名： ChenSigui
电子邮件地址： Hbcsg_speed@163.com
注释： JUST
您选定了此用户标识：
"ChenSigui (JUST) <Hbcsg_speed@163.com>"
更改姓名（N）、注释（C）、电子邮件地址（E）或确定（O）/退出（Q）？ o
我们需要生成大量的随机字节。在质数生成期间做些其他操作（敲打键盘
、移动鼠标、读写硬盘之类的）将会是一个不错的主意；这会让随机数
发生器有更好的机会获得足够的熵。
我们需要生成大量的随机字节。在质数生成期间做些其他操作（敲打键盘
、移动鼠标、读写硬盘之类的）将会是一个不错的主意；这会让随机数
发生器有更好的机会获得足够的熵。
gpg: 密钥 CCC243CB0BFE1600 被标记为绝对信任
gpg: 吊销证书已被存储为'/home/user/.gnupg/openpgp-revocs.d/F0A9639EED966FDEC75DE
ABBCCC243CB0BFE1600.rev'
公钥和私钥已经生成并被签名。
pub rsa3072 2020-12-08 [SC]
F0A9639EED966FDEC75DEABBCCC243CB0BFE1600
uid ChenSigui (JUST) <Hbcsg_speed@163.com>
sub rsa3072 2020-12-08 [E]
76%


user's X desktop (a03d4a932c80:0)
172.17.0.9:6901/vnc.html
Applications
Directory listing for / - M...
Application Finder
user@a03d4a932c80: ~/Desktop
user@a03d4a932c80: ~/Desktop 80x24
ChenSigui.pk
user@a03d4a932c80:~/Desktop$ find / --name ChenSigui.pk
find: 未知的断言"--name"
user@a03d4a932c80:~/Desktop$ python -m http.server 8080
Serving HTTP on 0.0.0.0 port 8080 (http://0.0.0.0:8080/) ...
0:~/Desktop$ python -m http.server 8080
Serving HTTP on 0.0.0.0 port 8080 (http://0.0.0.0:8080/) ...
Directory listing for / - Mozilla Firefox
Directory listing for /
172.17.0.4:8080
Directory listing for /
chenao.pk
Opening chenao.pk
You have chosen to open:
chenao.pk
which is: PK file (2.4 KB)
from: http://172.17.0.4:8080
What should Firefox do with this file?
Open with Browse...
Save File
Do this automatically for files like this from now on.
Cancel
OK
72%





五、实验记录

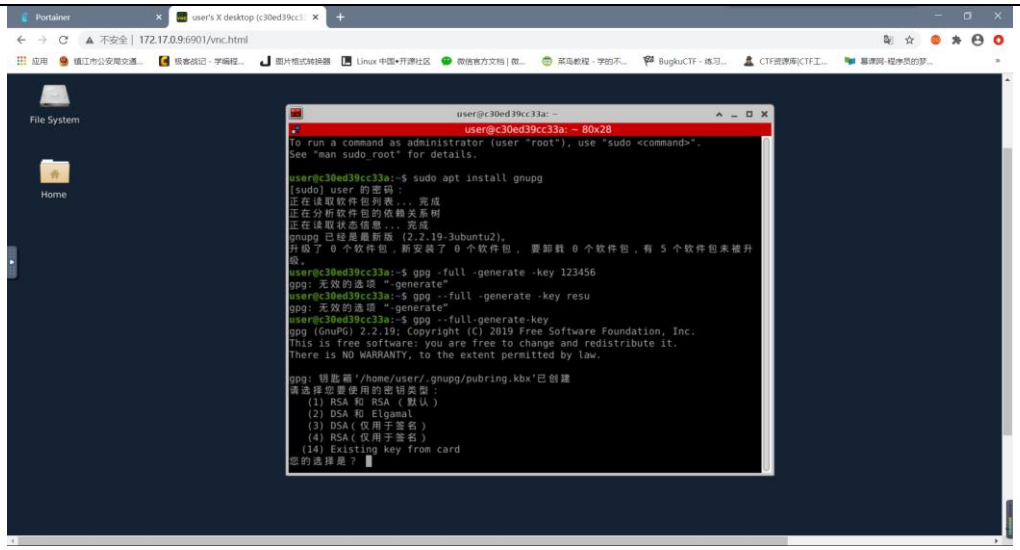
1.使用“sudo apt install gnupg”命令安装 GPG；

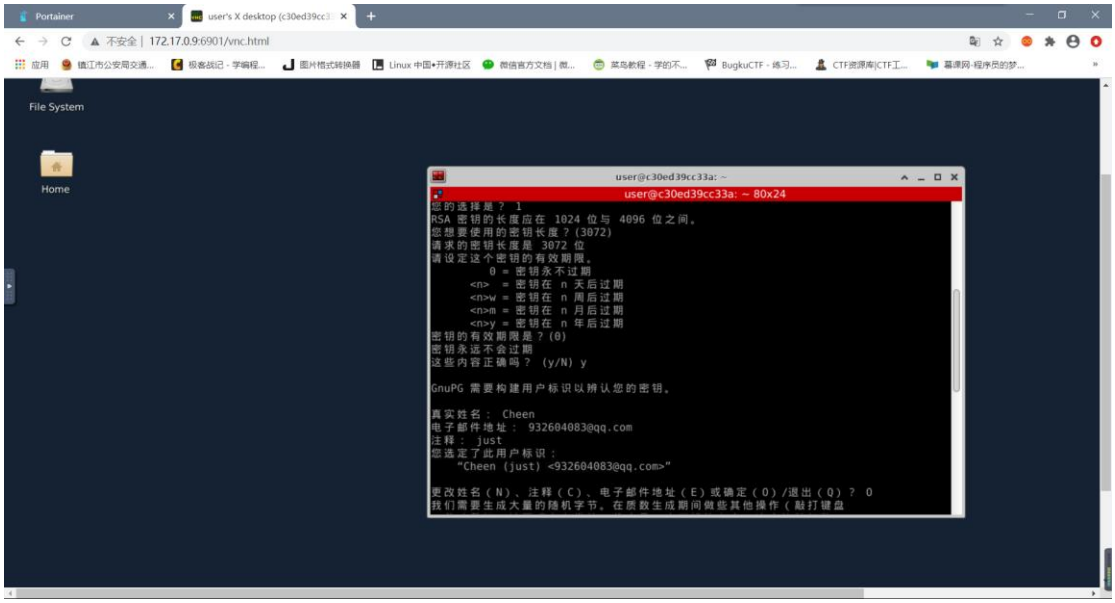
2.使用” gpg –full-generate-key”命令创建密钥，这个密钥应牢记于心，后续加密、解密会用到；

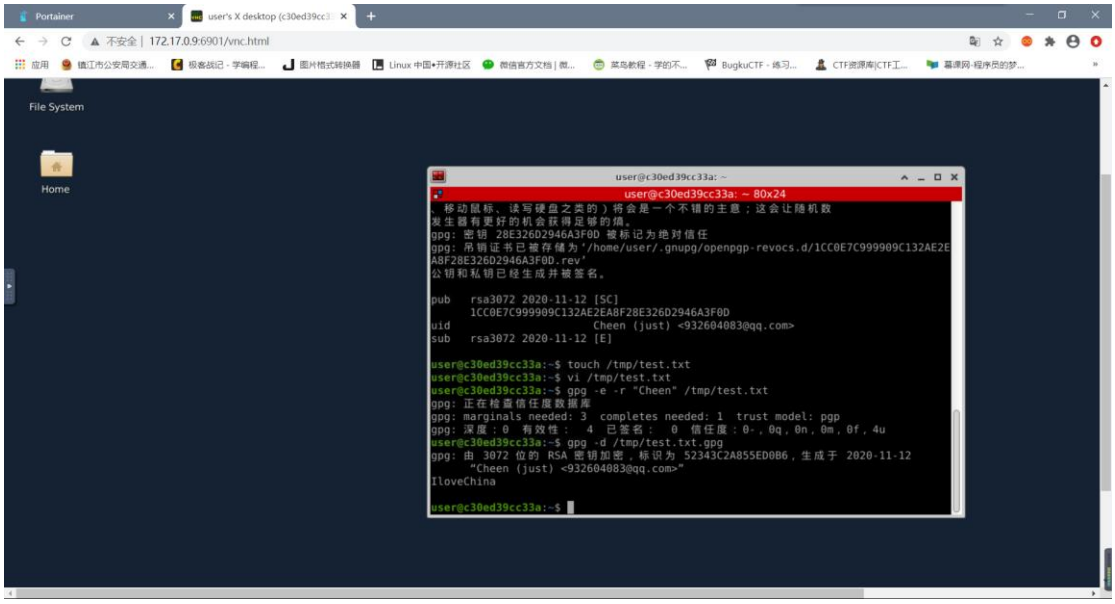
3.使用“touch /tmp/test.txt”命令创建文件，再使用 vim 编辑器对其填充任意消息，用于保存明文（加密文件）；

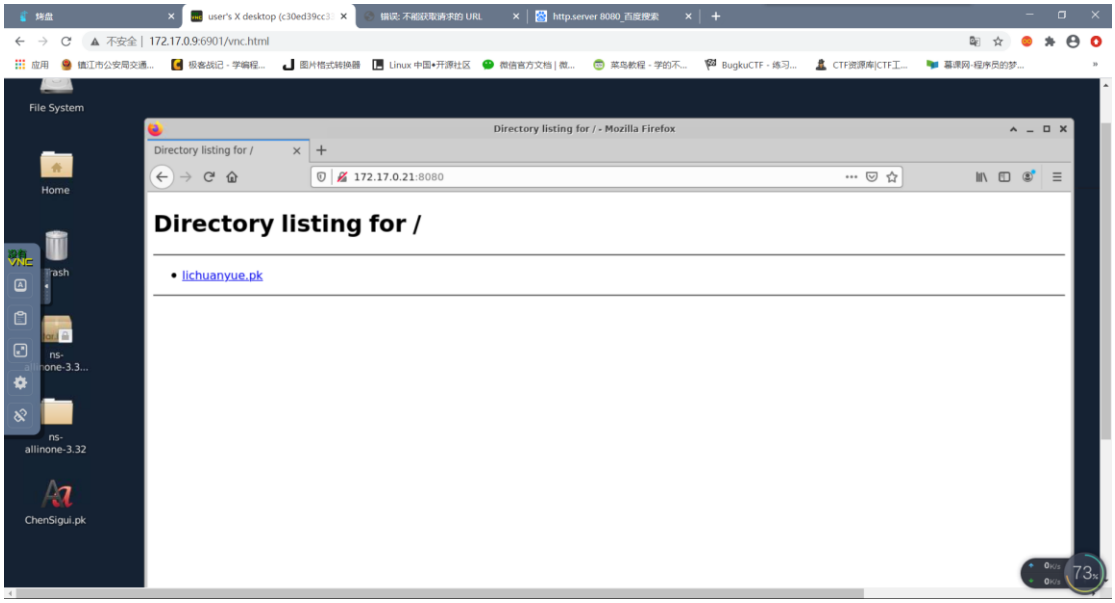
4.使用”gpg -e -r “Your Name” /tmp/test.txt”命令加密文件，注意，这里的 Your name 是我们之前创建密钥时输入的用户标识；

5.使用” gpg -d /tmp/test.txt.gpg”命令解密文件。


Portainer
user's X desktop (c30ed39cc3
不安全 | 172.17.0.9:6901/vnc.html
File System
Home
user@c30ed39cc33a: ~
user@c30ed39cc33a: ~ 80x28
To run a command as administrator (user "root"), use "sudo <command>".
See "man sudo_root" for details.
user@c30ed39cc33a:~$ sudo apt install gnupg
[sudo] user 的密码：
正在读取软件包列表... 完成
正在分析软件包的依赖关系树
正在读取状态信息... 完成
gnupg 已经是最新版 (2.2.19-3ubuntu2)。
升级了 0 个软件包，新安装了 0 个软件包，要卸载 0 个软件包，有 5 个软件包未被升级。
user@c30ed39cc33a:~$ gpg -full -generate -key 123456
gpg: 无效的选项 "-generate"
user@c30ed39cc33a:~$ gpg --full -generate -key resu
gpg: 无效的选项 "-generate"
user@c30ed39cc33a:~$ gpg --full-generate-key
gpg (GnuPG) 2.2.19; Copyright (C) 2019 Free Software Foundation, Inc.
This is free software: you are free to change and redistribute it.
There is NO WARRANTY, to the extent permitted by law.
gpg: 钥匙箱'/home/user/.gnupg/pubring.kbx'已创建
请选择您要使用的密钥类型：
(1) RSA 和 RSA（默认）
(2) DSA 和 Elgamal
(3) DSA（仅用于签名）
(4) RSA（仅用于签名）
(14) Existing key from card
您的选择是？


Portainer
user's X desktop (c30ed39cc3
不安全 | 172.17.0.9:6901/vnc.html
File System
Home
user@c30ed39cc33a: ~
user@c30ed39cc33a: ~ 80x24
您的选择是？ 1
RSA 密钥的长度应在 1024 位与 4096 位之间。
您想要使用的密钥长度？(3072)
请求的密钥长度是 3072 位
请设定这个密钥的有效期限。
0 = 密钥永不过期
<n> = 密钥在 n 天后过期
<n>w = 密钥在 n 周后过期
<n>m = 密钥在 n 月后过期
<n>y = 密钥在 n 年后过期
密钥的有效期限是？(0)
密钥永远不会过期
这些内容正确吗？ (y/N) y
GnuPG 需要构建用户标识以辨认您的密钥。
真实姓名： Cheen
电子邮件地址： 932604083@qq.com
注释： just
您选定了此用户标识：
"Cheen (just) <932604083@qq.com>"
更改姓名（N）、注释（C）、电子邮件地址（E）或确定（O）/退出（Q）？ O
我们需要生成大量的随机字节。在质数生成期间做些其他操作（敲打键盘


Portainer
user's X desktop (c30ed39cc3
不安全 | 172.17.0.9:6901/vnc.html
File System
Home
user@c30ed39cc33a: ~
user@c30ed39cc33a: ~ 80x24
移动鼠标、读写硬盘之类的）将会是一个不错的主意；这会让随机数
发生器有更好的机会获得足够的熵。
gpg: 密钥 28E326D2946A3F0D 被标记为绝对信任
gpg: 吊销证书已被存储为'/home/user/.gnupg/openpgp-revocs.d/1CC0E7C999909C132AE2EA8F28E326D2946A3F0D.rev'
公钥和私钥已经生成并被签名。
pub rsa3072 2020-11-12 [SC]
1CC0E7C999909C132AE2EA8F28E326D2946A3F0D
uid Cheen (just) <932604083@qq.com>
sub rsa3072 2020-11-12 [E]
user@c30ed39cc33a:~$ touch /tmp/test.txt
user@c30ed39cc33a:~$ vi /tmp/test.txt
user@c30ed39cc33a:~$ gpg -e -r "Cheen" /tmp/test.txt
gpg: 正在检查信任度数据库
gpg: marginals needed: 3 completes needed: 1 trust model: pgp
gpg: 深度：0 有效性： 4 已签名： 0 信任度：0-，0q，0n，0m，0f，4u
user@c30ed39cc33a:~$ gpg -d /tmp/test.txt.gpg
gpg: 由 3072 位的 RSA 密钥加密，标识为 52343C2A855ED0B6，生成于 2020-11-12
"Cheen (just) <932604083@qq.com>"
IloveChina
user@c30ed39cc33a:~$



六、实验小结

1.linux 操作系统下，终端输入密码时显示屏上并不会显示，密码输完后回车即可；
2.两个 linux 操作系统的通信比较复杂，需要双方在终端运行”python -m http.server 8080”后，并打开浏览器输入合作伙伴的 IP 地址，后加端口 8080，方能进行通讯。此外，我们最好将想要通讯的文件放到桌面上，以免对方看不见相应文件；
3.linux 系统有时比较迟缓，拖拽出的文件不一定能实时显现文件，此时我们刷新一下就好了。