**西安电子科技大学**

**计算机与网络安全 课程实验报告**

**实验名称 PGP邮件加密实验**

网络与信息安全 学院 2118021 班

成 绩

姓名 学号 同作者

实验日期 2024 年 05 月 24 日

|  |
| --- |
| 指导教师评语：  指导教师：  年 月 日 |
| **实验报告内容基本要求及参考格式**  一、实验目的  二、实验所用仪器（或实验环境）  三、实验基本原理及步骤（或方案设计及理论计算）  四、实验数据记录（或仿真及软件设计）  五、实验结果分析及回答问题（或测试环境及测试结果） |

## 一、实验目的

1.熟悉非对称加密算法。

2.掌握私钥和公钥再签名和加密中的应用。

3.了解 PGP 工具的操作

## 二、实验原理

PGP 加密系统是采用公开密钥加密与传统密钥加密相结合的一种加密技术。 它使用一对数学上相关的钥匙，其中一个(公钥)用来加密信息，另一个(私钥) 用来解密信息。

PGP 采用的传统加密技术部分所使用的密钥称为“会话密钥”(sek)。每次使 用时，PGP 都随机产生一个 128 位的 IDEA 会话密钥，用来加密报文。公开密钥 加密技术中的公钥和私钥则用来加密会话密钥，并通过它间接地保护报文内容。

PGP 中的每个公钥和私钥都伴随着一个密钥证书。它一般包含以下内容:

1) 密钥内容(用长达百位的大数字表示的密钥)

2) 密钥类型(表示该密钥为公钥还是私钥)

3) 密钥长度(密钥的长度，以二进制位表示)

4) 密钥编号(用以唯一标识该密钥)

5) 创建时间

6) 用户标识 (密钥创建人的信息，如姓名、电子邮件等)

7) 密钥指纹(为 128 位的数字，是密钥内容的提要表示密钥唯一的特征)

8) 中介人签名(中介人的数字签名，声明该密钥及其所有者的真实性，包括中介人的密钥编号和标识信息)

PGP 把公钥和私钥存放在密钥环(KEYR)文件中。PGP 提供有效的算法查找用户需要的密钥。PGP 在多处需要用到口令，它主要起到保护私钥的作用。由于 私钥太长且无规律，所以难以记忆。PGP 把它用口令加密后存入密钥环，这样用 户可以用易记的口令间接使用私钥。PGP 的每个私钥都由一个相应的口令加密。

PGP 主要在 3 处需要用户输入口令:

需要解开收到的加密信息时，PGP 需要用户输入口令，取出私钥解密信息 当用户需要为文件或信息签字时，用户输入口令，取出私钥加密 对磁盘上的文件进行传统加密时，需要用户输入口令

**公钥、私钥加密特性**

在 PGP 系统里经常遇到公钥、私钥，大家如果不理解就无法使用了。公钥、

私钥只是个代号而已，我们这里称它们为 a 钥、b 钥。a、b 钥就像一对密码本， 但是它很特殊:

1) 用 a 加密的东西只能用 b 来解，b 加密的东西只能用 a 解。

2) a 不能解密 a 自己加密的东西。b 不能解密 b 自己加密的东西。

3) a 有且仅有一个 b 与自己配对。b 有且仅有一个 a 与自己配对。不存在第三者。

如果我们把 a 留给自己用，把 b 发给大家(别人)，那 a 就称为“私钥”()，b 就称为“公钥”。当然，反过来那 b 就称为“私钥”，a 就称为“公钥”。系统只 是自动给了个名称，防止你以后乱不清到底是把 a 当公钥发给别人了，还是把 b 当公钥发给别人了。

## 三、实验要求

实验前认真预习公钥，私钥以及数字签名原理，对称加密和非对称加密算法，PGP 的原理以及使用方法，在进行实验时，应注意爱护机器，按照试验指导书的 要求的内容和步骤完成实验，尤其应注意认真观察试验结果，做好记录;实验完成后应认真撰写实验报告。

## 四、实验步骤

1. 使用PGP生成创建密钥并导出公钥和签名

首先启动PGP，在文件目录下，打开新建PGP密钥。





2.输入全名和邮箱地址。命名为bill，地址为zhifenghan.mail@gmail.com



3.之后输入自己设定的私钥，此处私钥不少于8个字符，我设置为包含我的名字的一串字符zfhan123

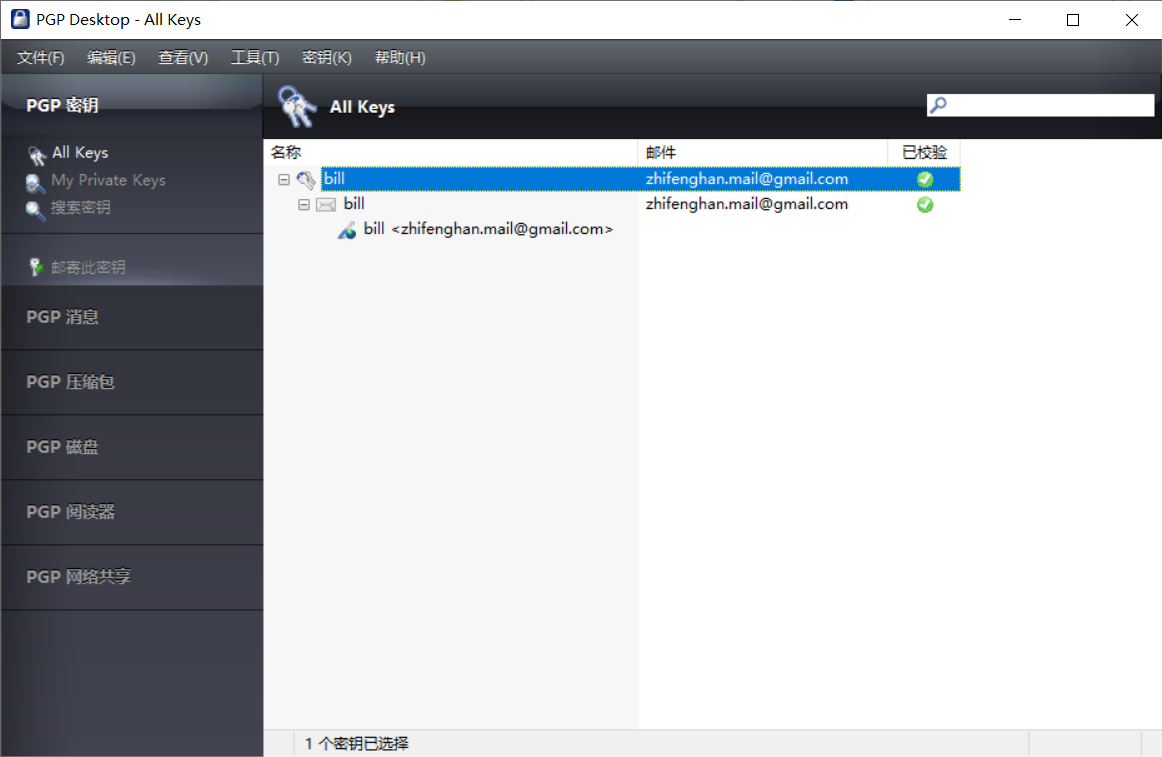


4.之后密钥生成完成。

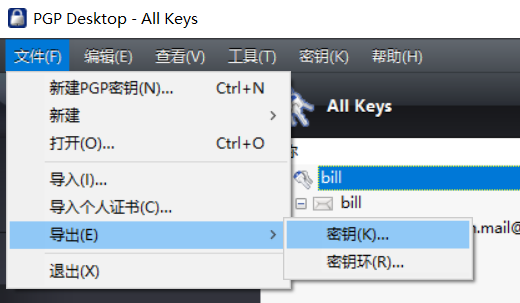




5.在PGP主页面，可以看到已经刚才生成的密钥记录。



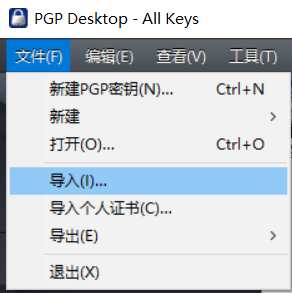
6.之后导出密钥。打开文件 -> 导出 -> 密钥，以默认文件名将bill.asc文件保存在桌面上。

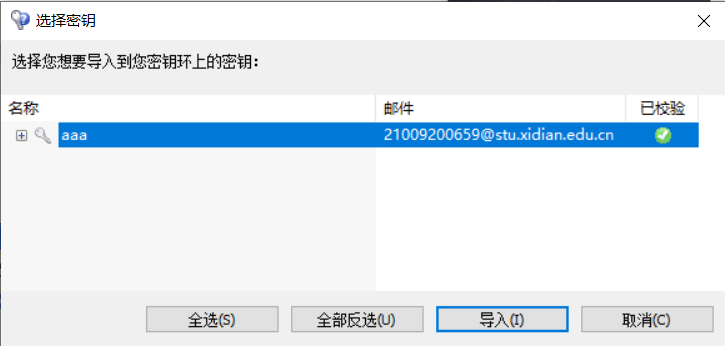
 

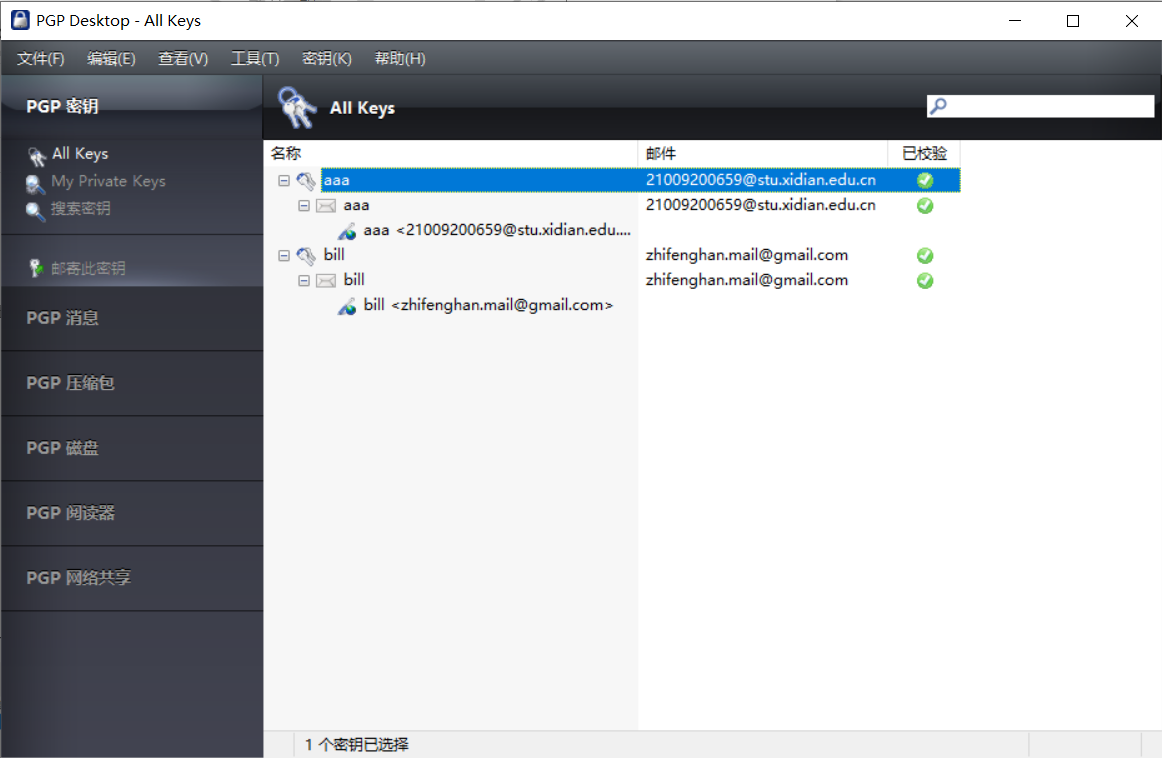
7.采用相同方式，在另一台计算机上创建新密钥并导出。名字为aaa，邮箱为21009200659@stu.xidian.edu.cn（本人学生邮箱），私钥为pgptest2。



8.接下来导入密钥。打开文件并选择导入。导入成功后，在主界面可以看到两个密钥，包括最开始创建的bill和新导入的aaa。

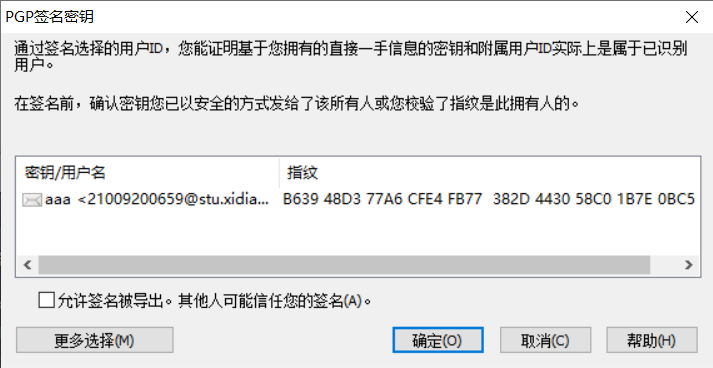


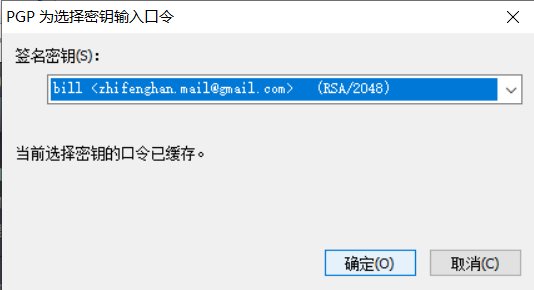




9.选择密钥 -> 签名，选择公钥aaa，密钥输入口令选择bill。

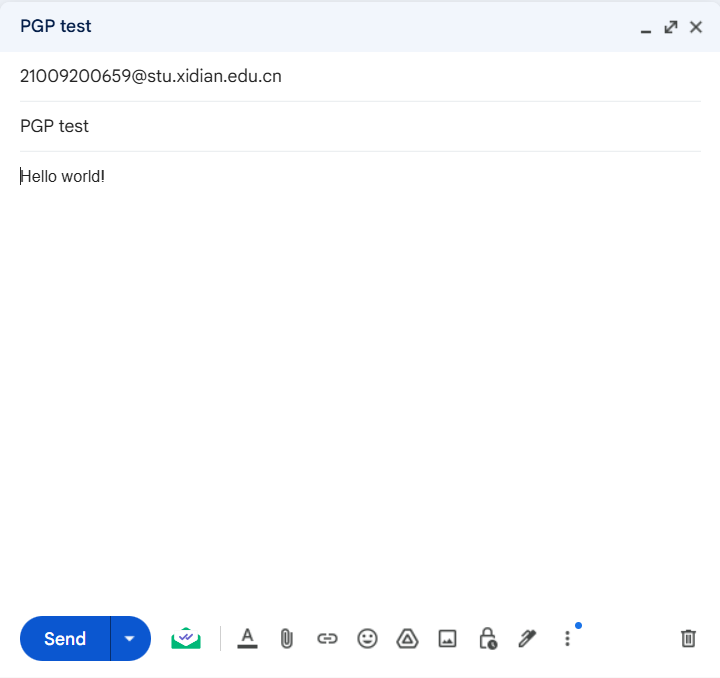




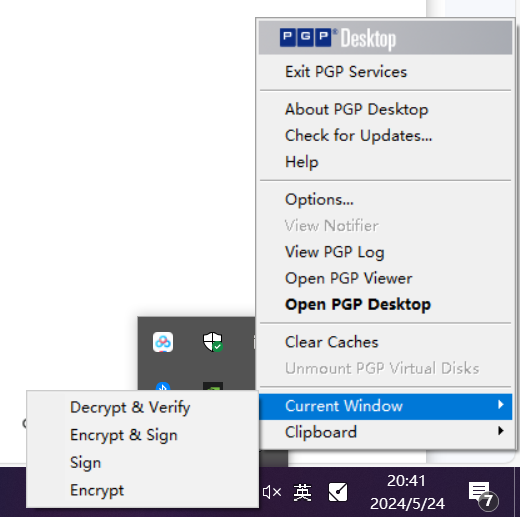


10. 切换回第一台计算机，以相同的方式将第二台计算机的公钥(bill.asc)导入并签名。 下面开始用PGP加密邮件，并发送邮件。

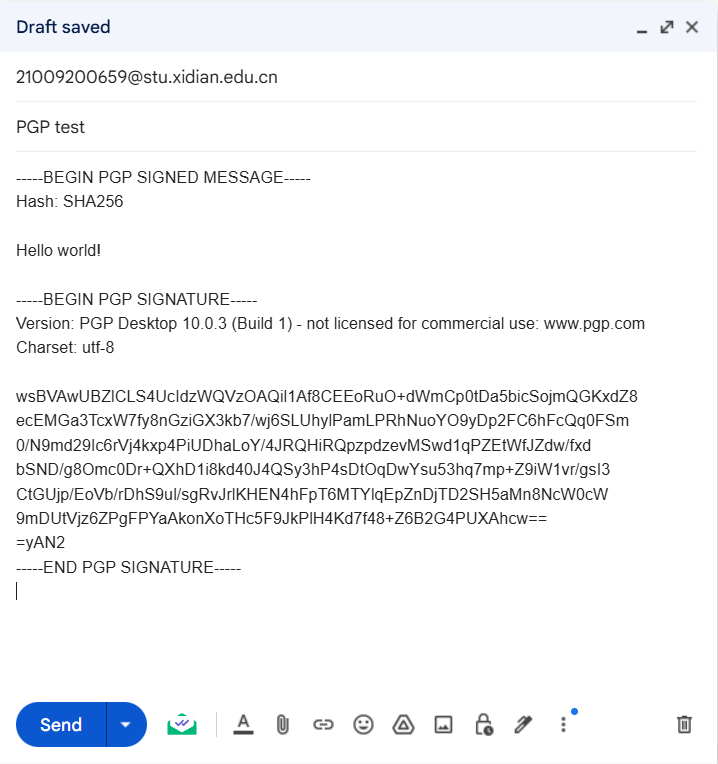
11.打开gmail，创建邮件发送给21009200659@stu.xidian.edu.cn，内容设置为hello world！



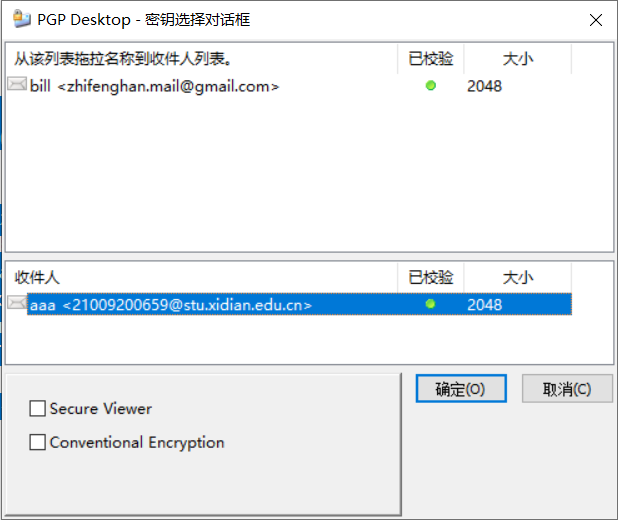
12.在发送之前，选择sign。



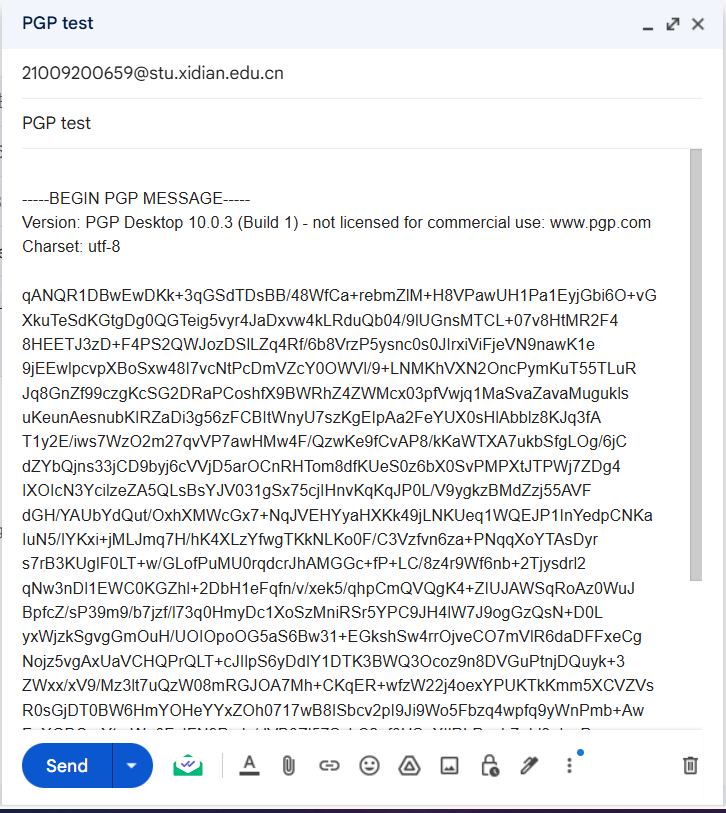
签名后的邮件如图所示



13.对邮件内容加密，此处需要选择使用公钥aaa，以供第二台PC解密

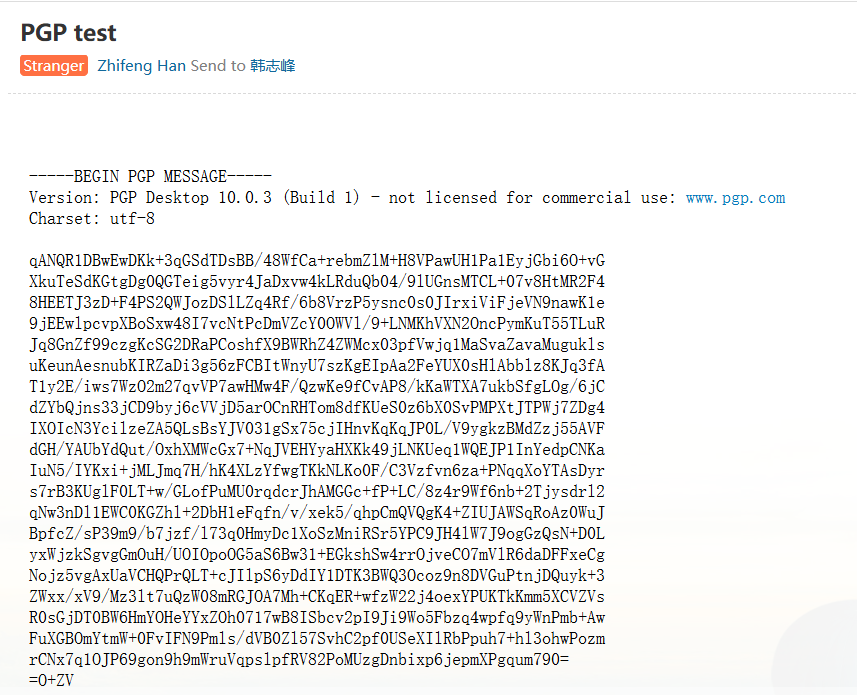


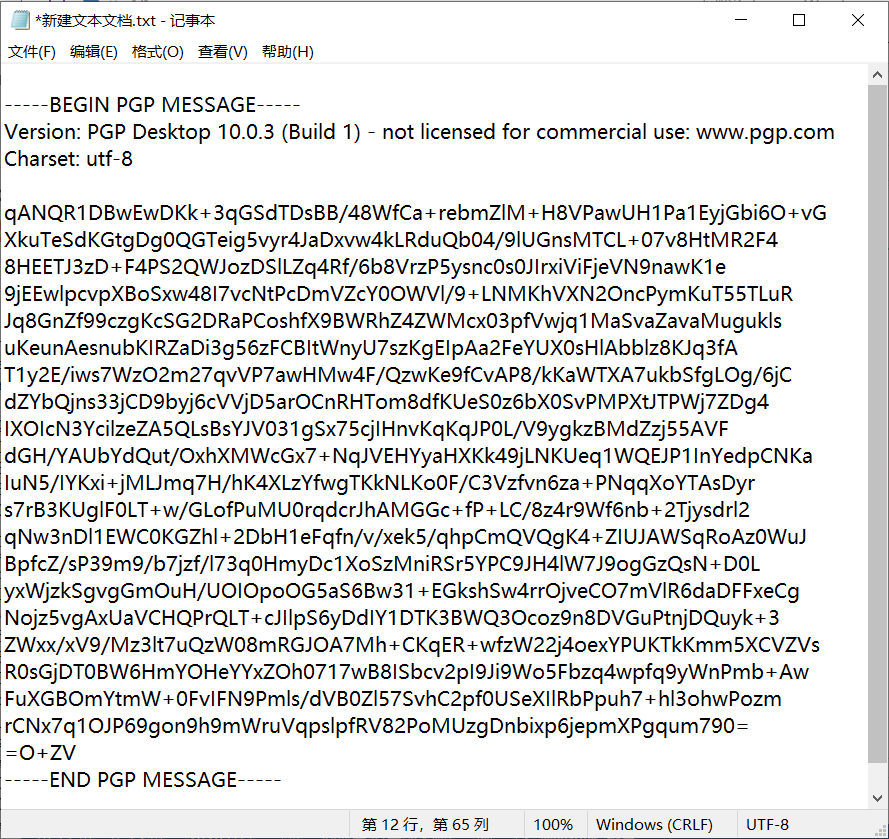
加密后的邮件如图所示：



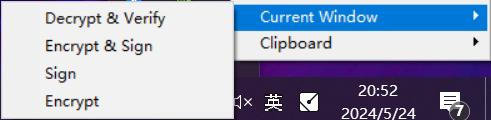
16.发送邮件

17.转发到另一个邮箱后，需要进行解密，此处复制到txt文件中。





18.对邮件解密和验证签名，选择decrypt & Verify



19.输入私钥zfhan123，即可得到结果

