安全电子邮件 PGP 实验报告

班级：　　学号：　　姓名：

一、实验名称

二、实验目的

三、实验内容与要求

四、实验过程

安装 gpg4win-3.1.4，参考工具使用方法进行：

1）生成密钥对、导出公钥、导入其他人公钥；

alsPP

密钥对创建成功。

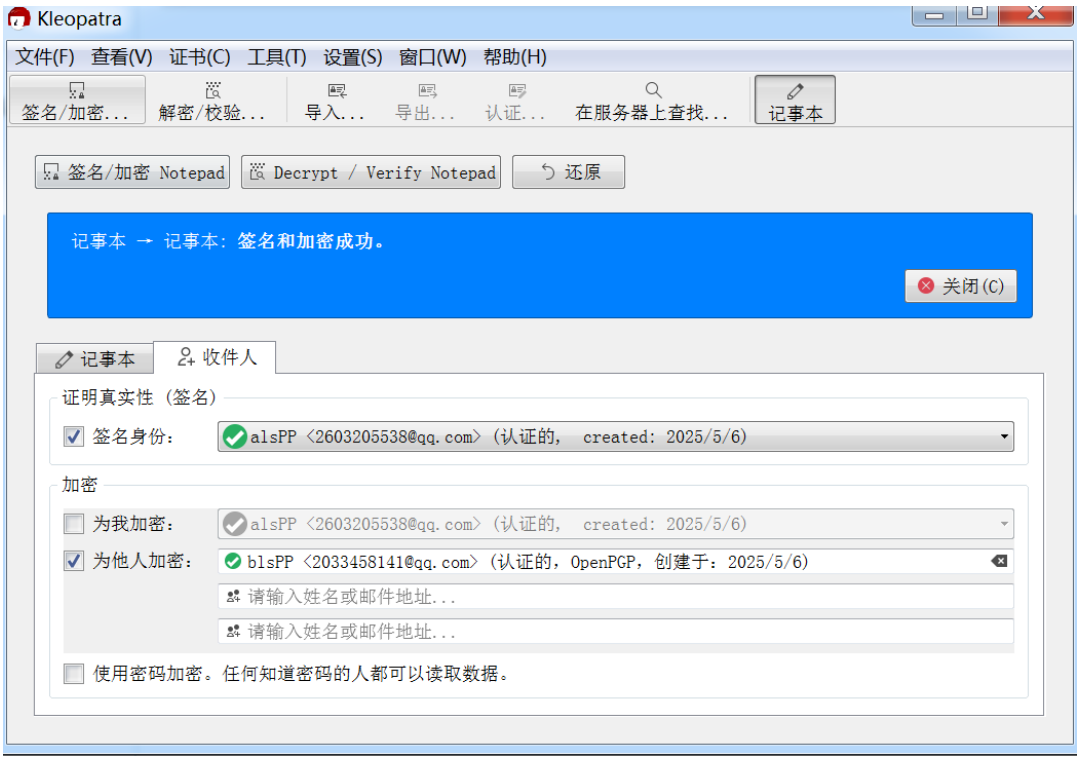
指纹：6941D4BAB75C3A9AA3C4C282AC9D19DF2B20F409

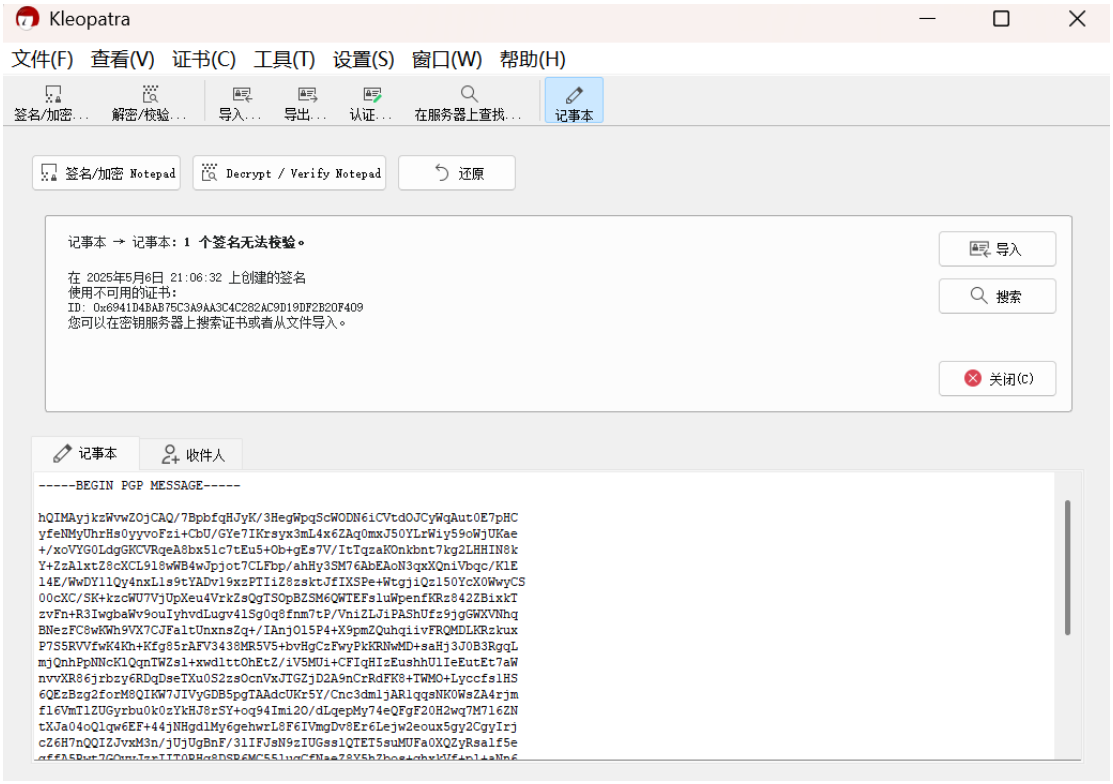
blsPP

密钥对创建成功。

指纹：32BA1CEB2E9C8AF541ACE66EA7D2F8B522D082ED

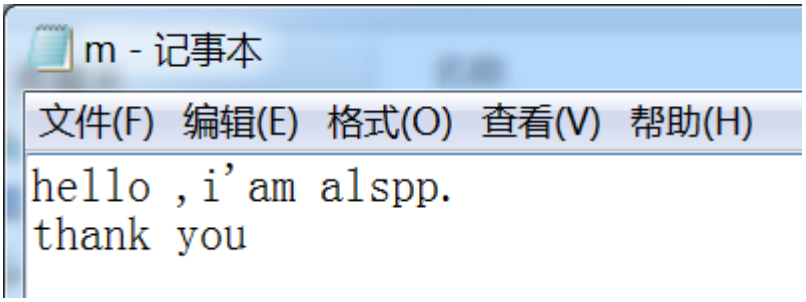
2）利用 Kleopatra 记事本进行邮件内容签名和加密、验证和解密；

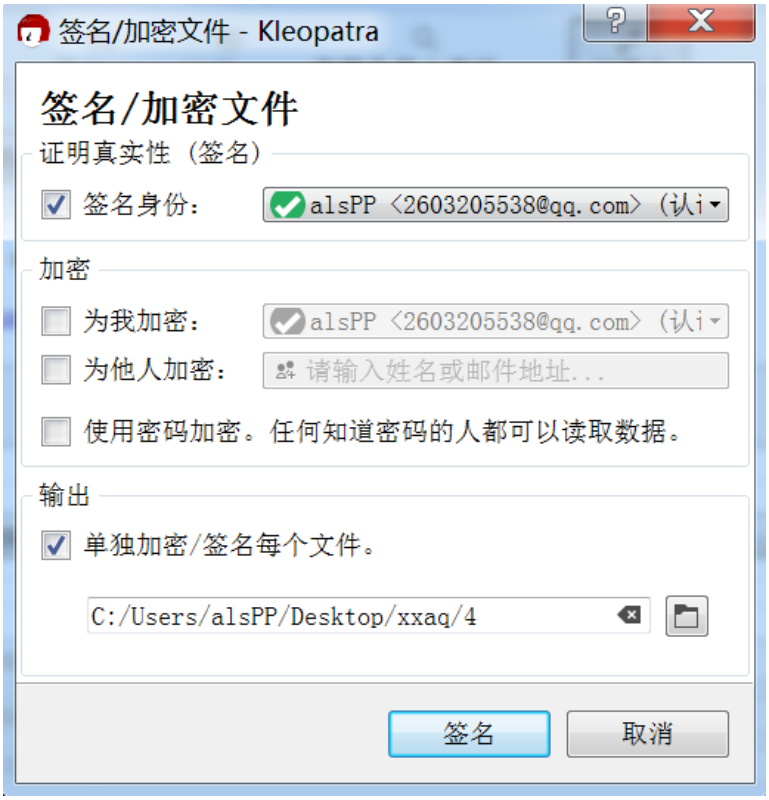


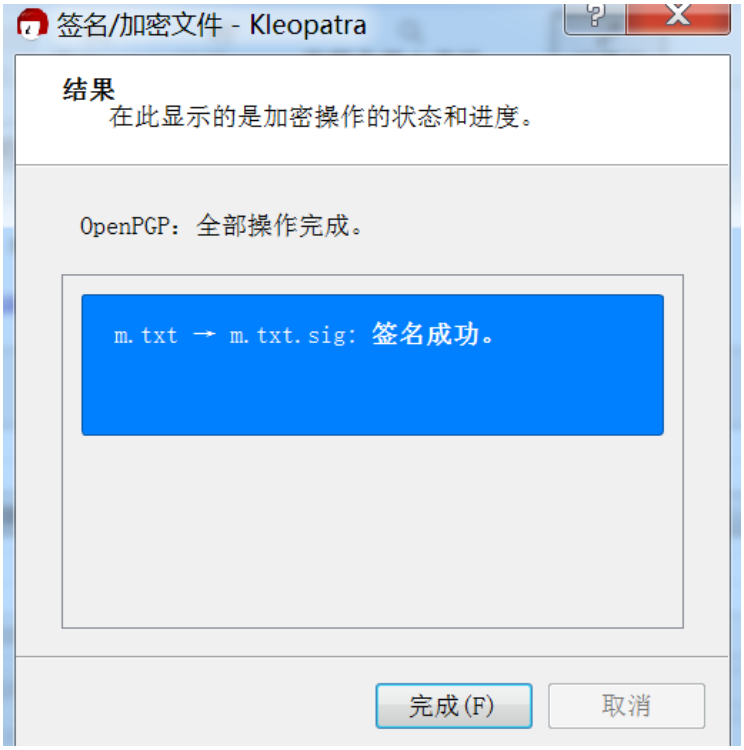


3）利用文件方式进行签名和加密、验证和解密。

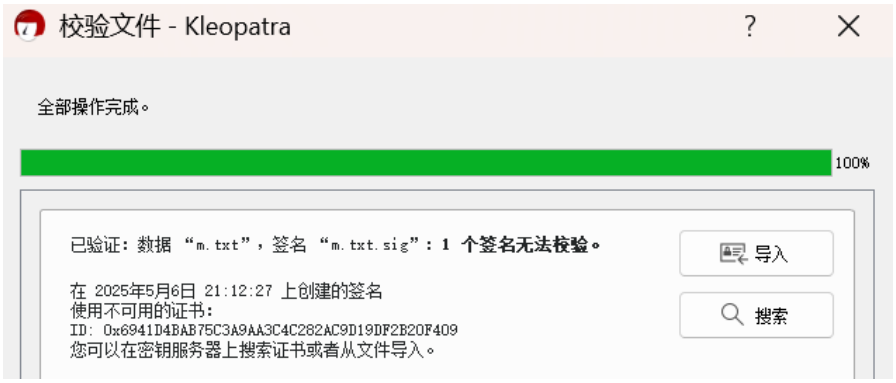
文件签名用于对文件本身进行保护，如果原始文件被人篡改，可以证明不是原作者本人。此功能常用于软件发布，很多软件开发者为了防止自身发布的软件被反编译注入有害代码，特使用签名方式保护软件本身。





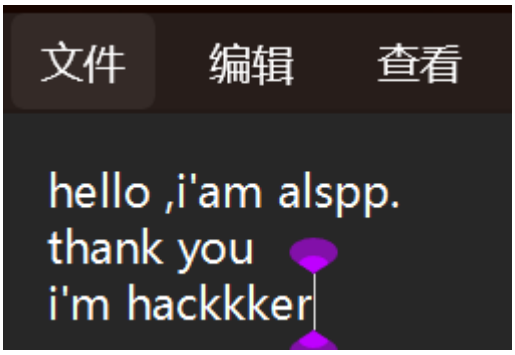


现在，我们可以把签名文件和原始文件发给目标接受者。
在文件没有改动时，验证文件如下：



没有导入 alsPP 的公钥时会出现“1 个签名无法校验

在文件改动后，验证文件如下：



自己用两个邮箱（或者两位同学互相配合），一个作为发送方，另一个作为接收方，完成邮件加密签名后发送，接收方再验证签名和解密。

五、实验结果分析

六、思考与心得体会