**《计算机网络安全》实验报告**

**实验（2）使用PGP软件进行加解密**

学生姓名： 陈华豪 学 号： 6130116238 专业班级： 网络工程161班

实验类型：■ 验证 □ 综合 □ 设计 实验日期：  实验成绩：

**实验目的**

为了能够让重要文件或邮件等信息安全地通过网络传播，通常对这些文件和邮件采用加密和数字签名技术，这样即使文件或邮件被非法用户获取。通过对PGP的使用来理解掌握加密和数字签名这两种在Internet上广泛应用的技术。PGP使用两个密钥来管理数据：一个用以加密，称为公钥（Public Key）；另一个用以解密，称为私钥（Private Key）。公钥和私钥是紧密联系在一起的，公钥只能用来加密需要安全传输的数据，却不能解密加密后的数据；相反，私钥只能用来解密，却不能加密数据。

**试验内容**

（1）PGP密钥生成。

（2）PGP密钥发布。

（3）PGP加密邮件。

（4）用PGP实现数字签名。

**3．实验过程**

3．1实验环境

Win10

下载PGP软件。用户可以到PGP公司的中文官方网站（www.pgp.com.cn）上下载中文版软件，软件分为32位版本和64位版本。

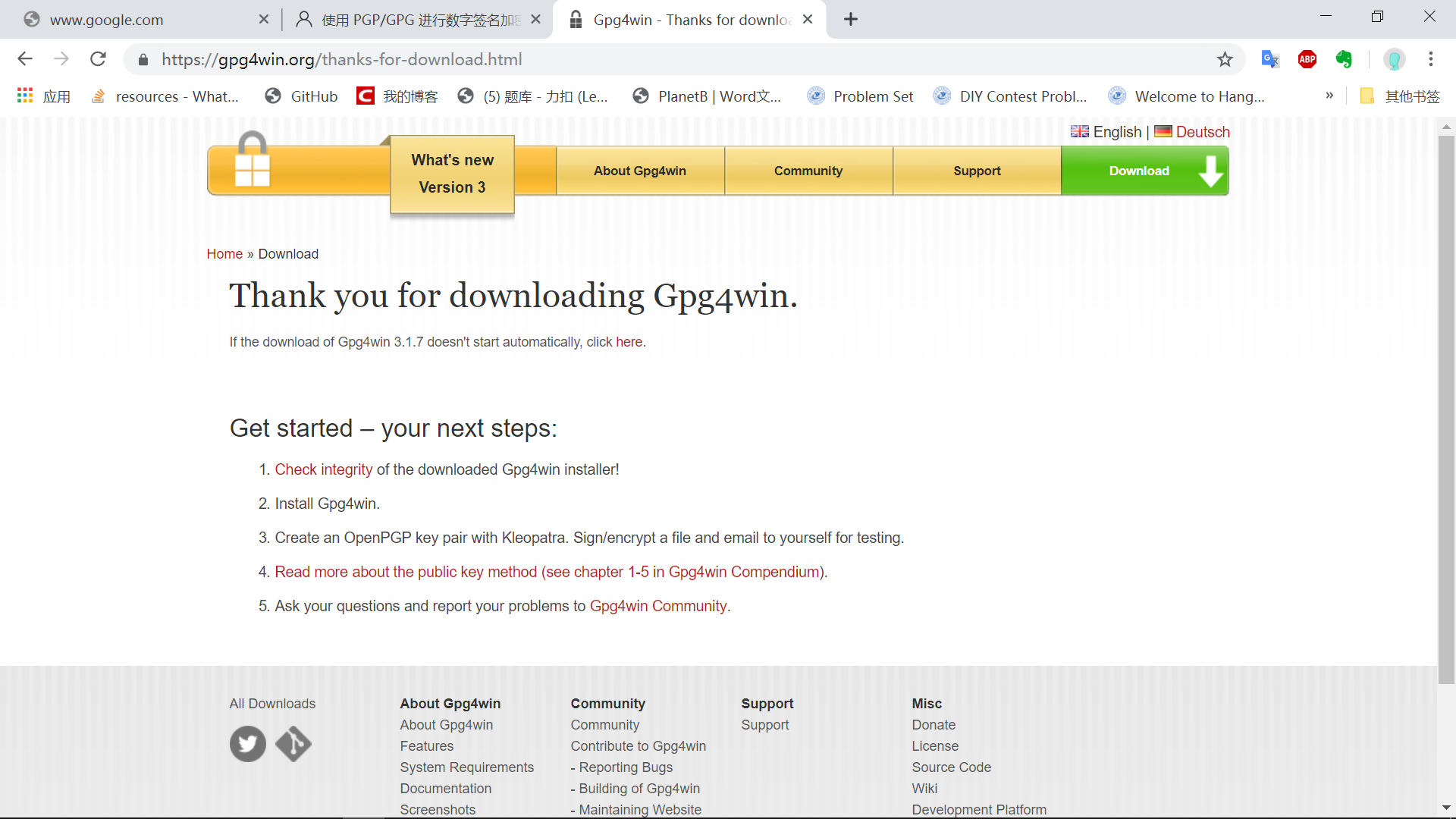
3．2关键实验步骤及配置

（1）搜集相关资料

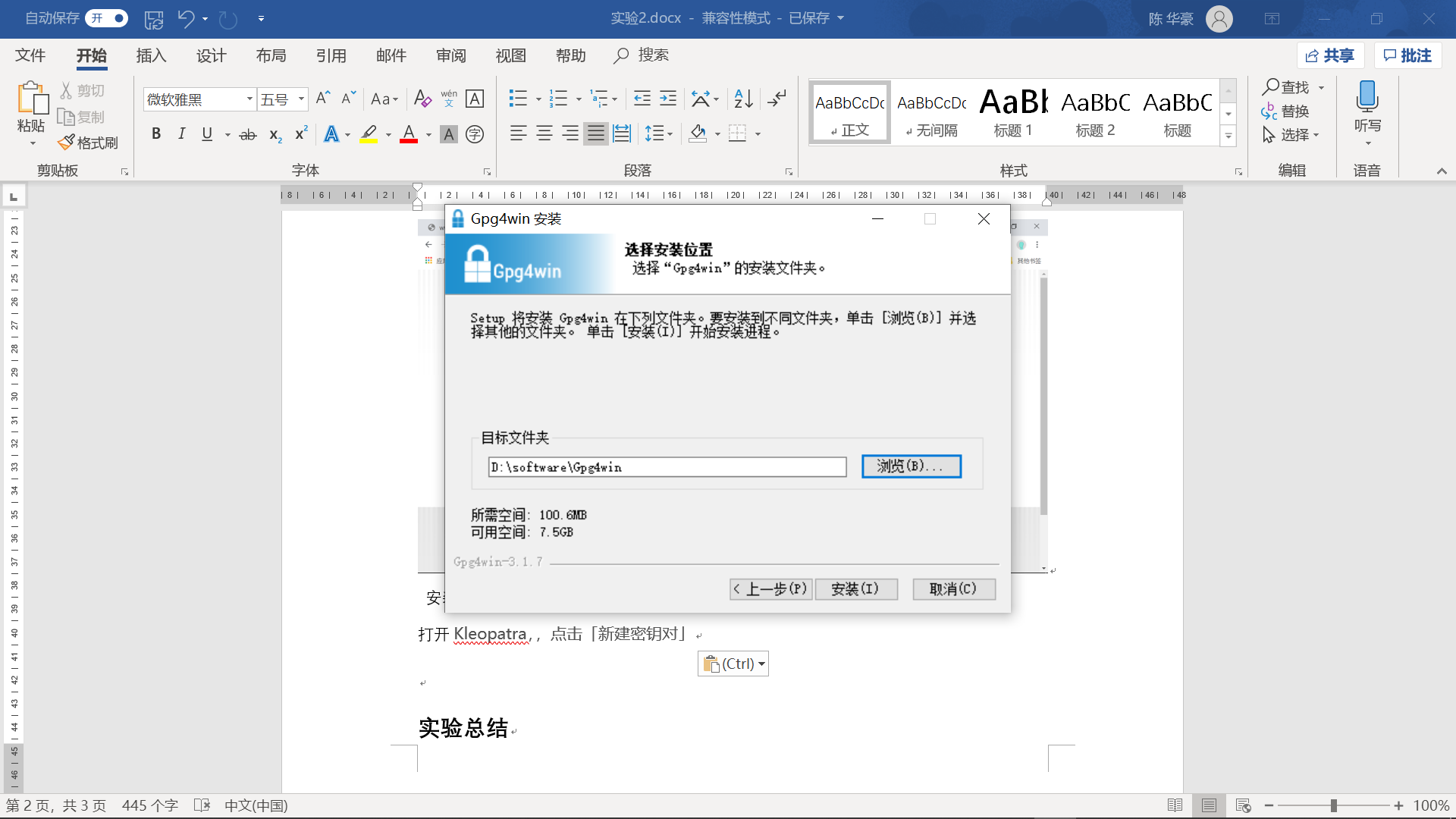
<http://www.pgp.cn/index.htm>

**实验结果**

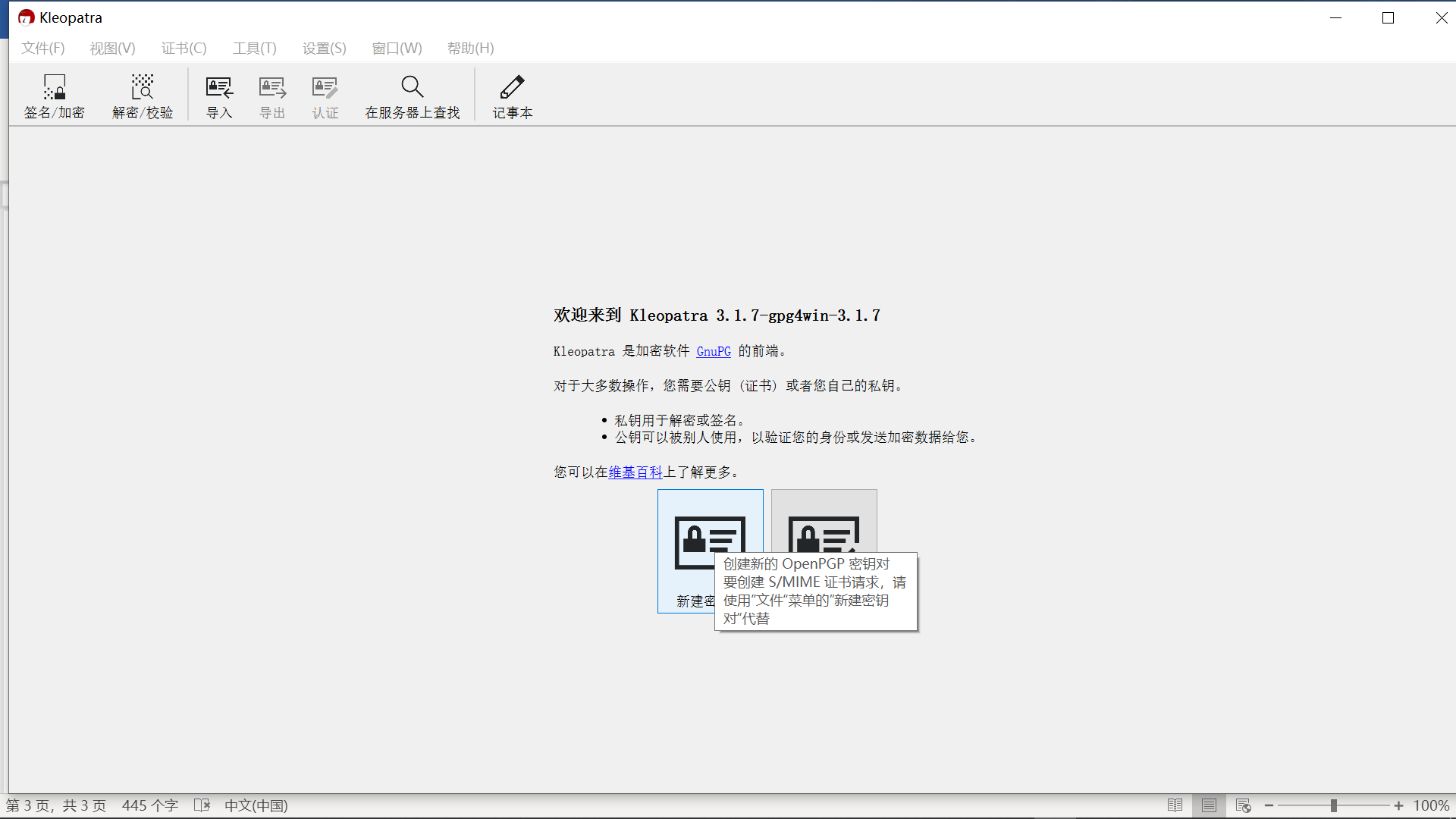
下载gpg4win



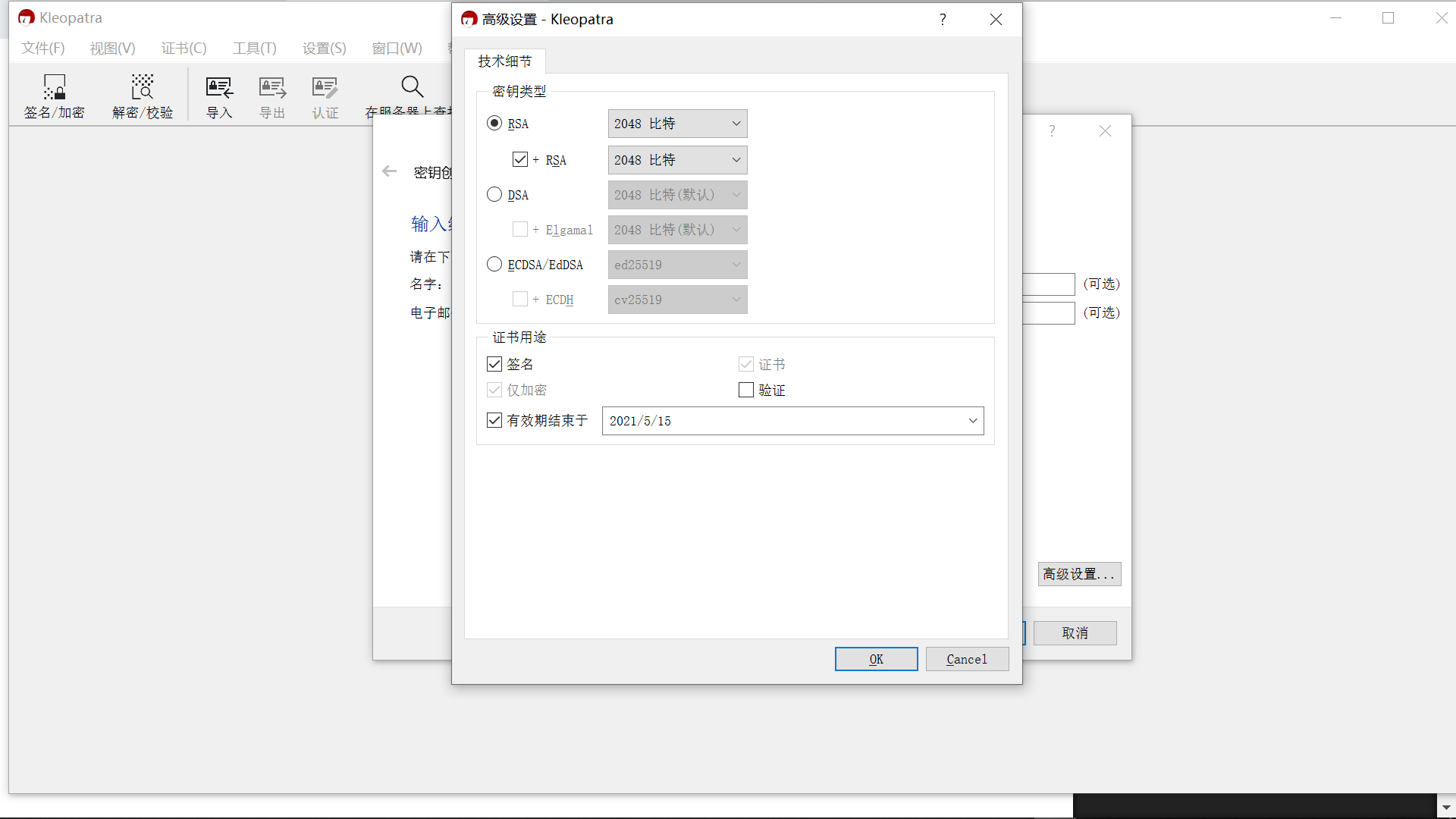
安装到合适位置



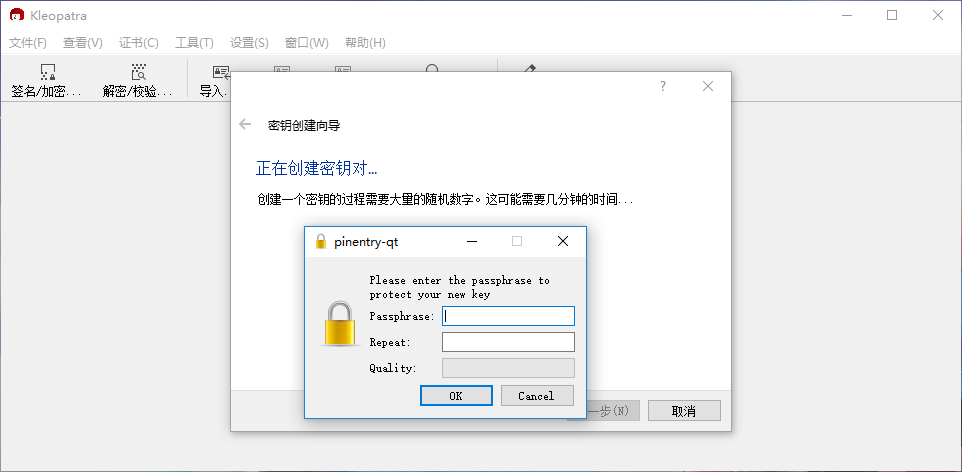
打开Kleopatra，，点击「新建密钥对」



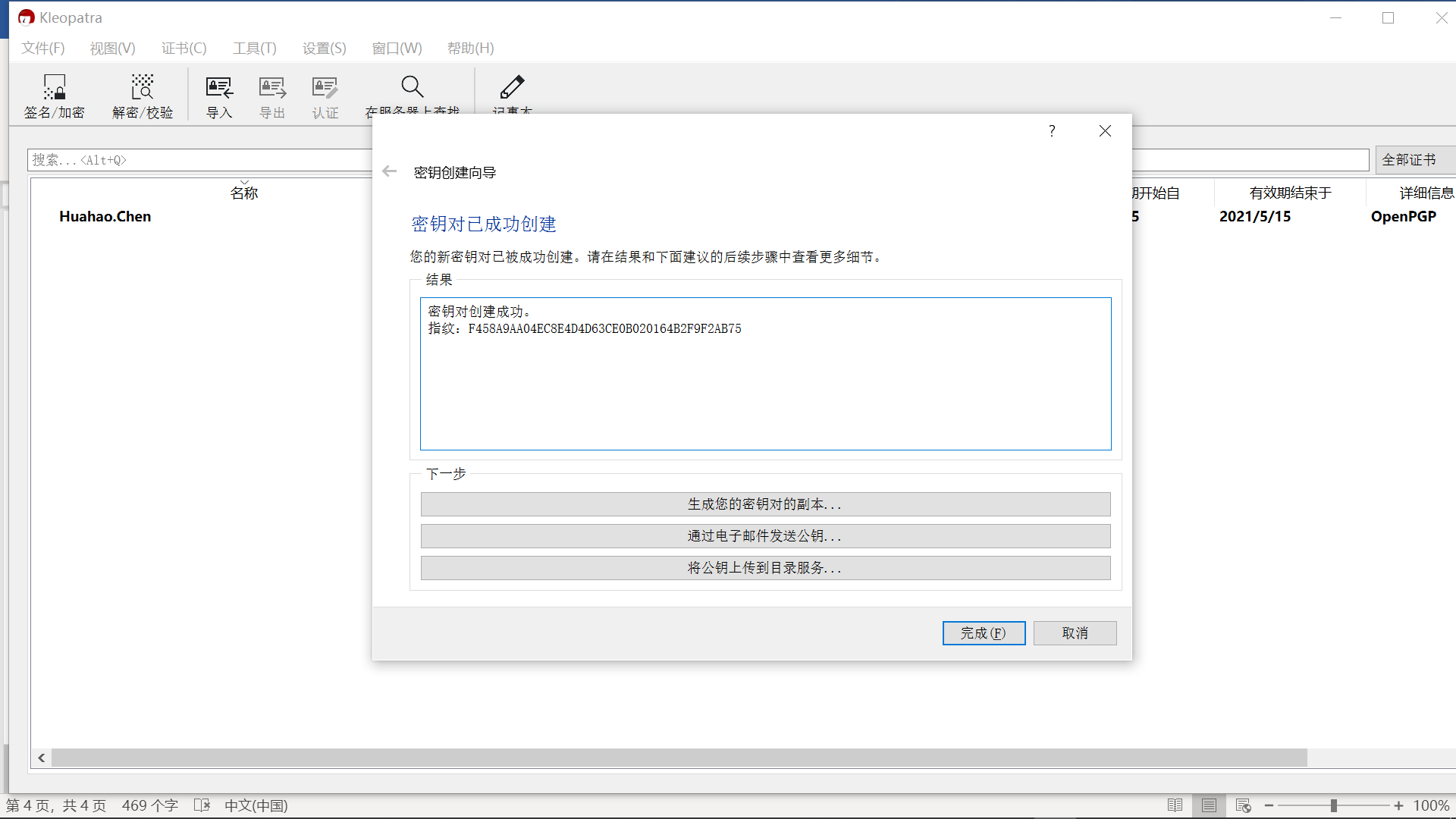
加密配置，可选加密方式

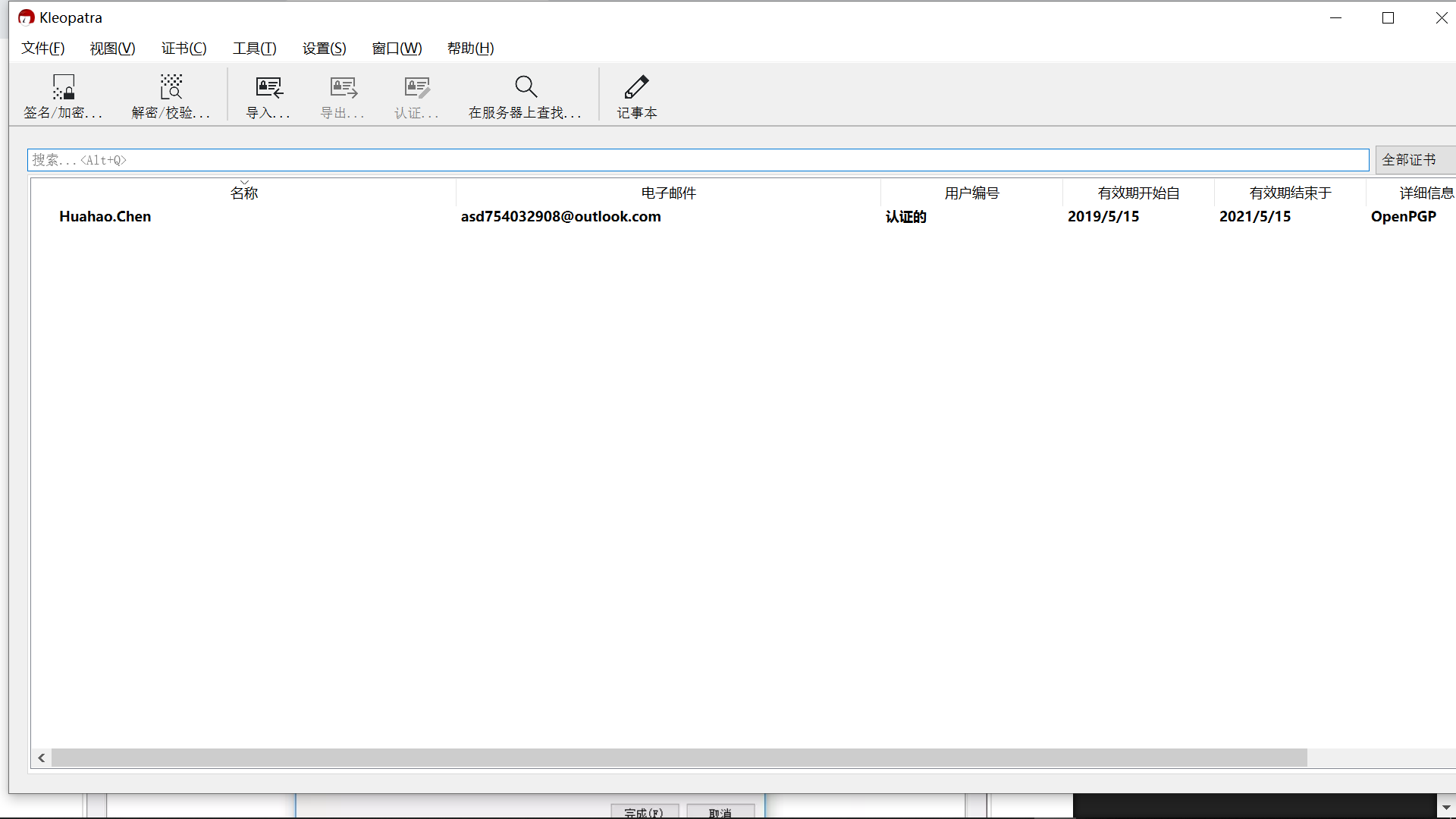


输入一个密码，用来加密密钥

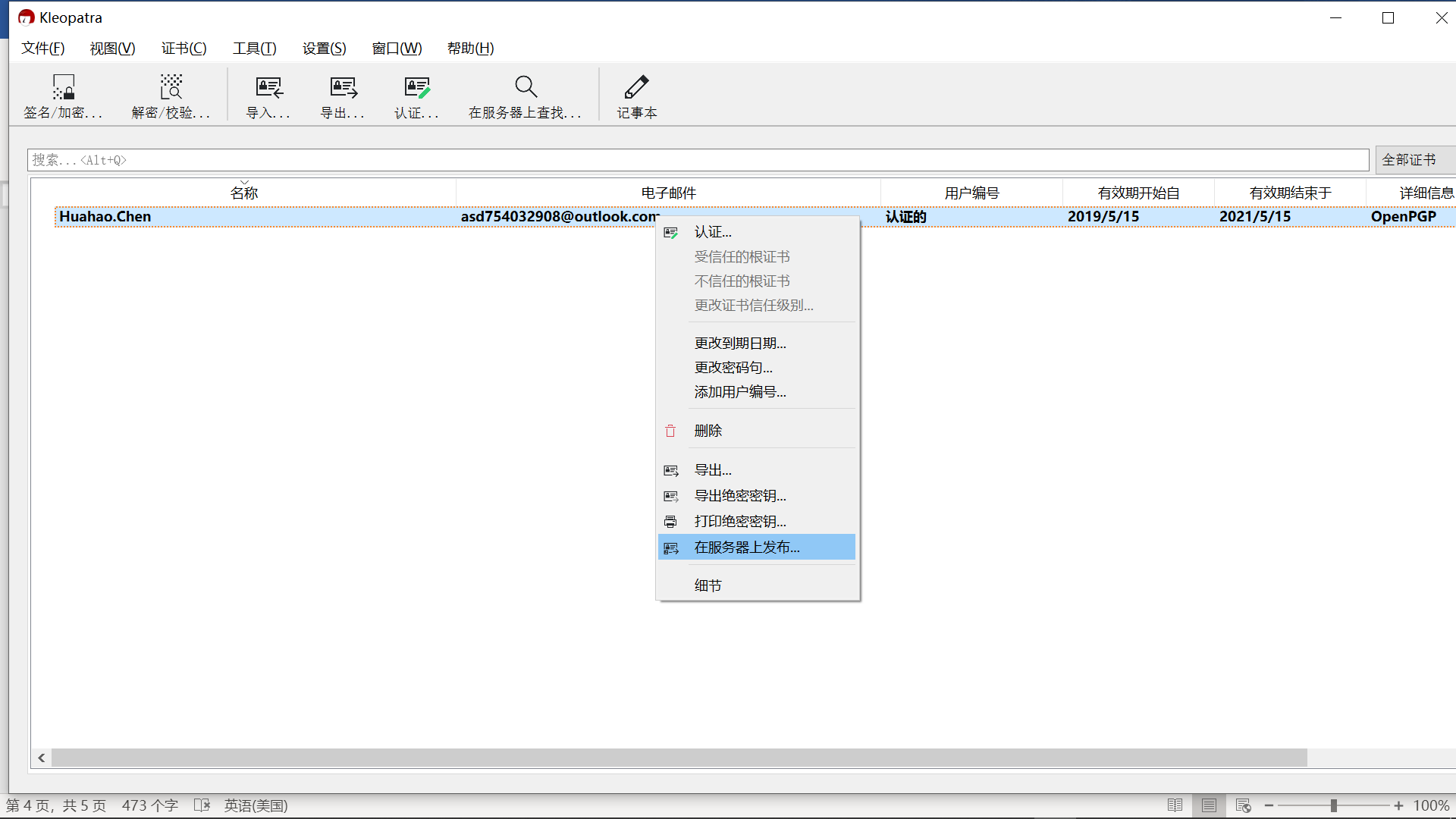


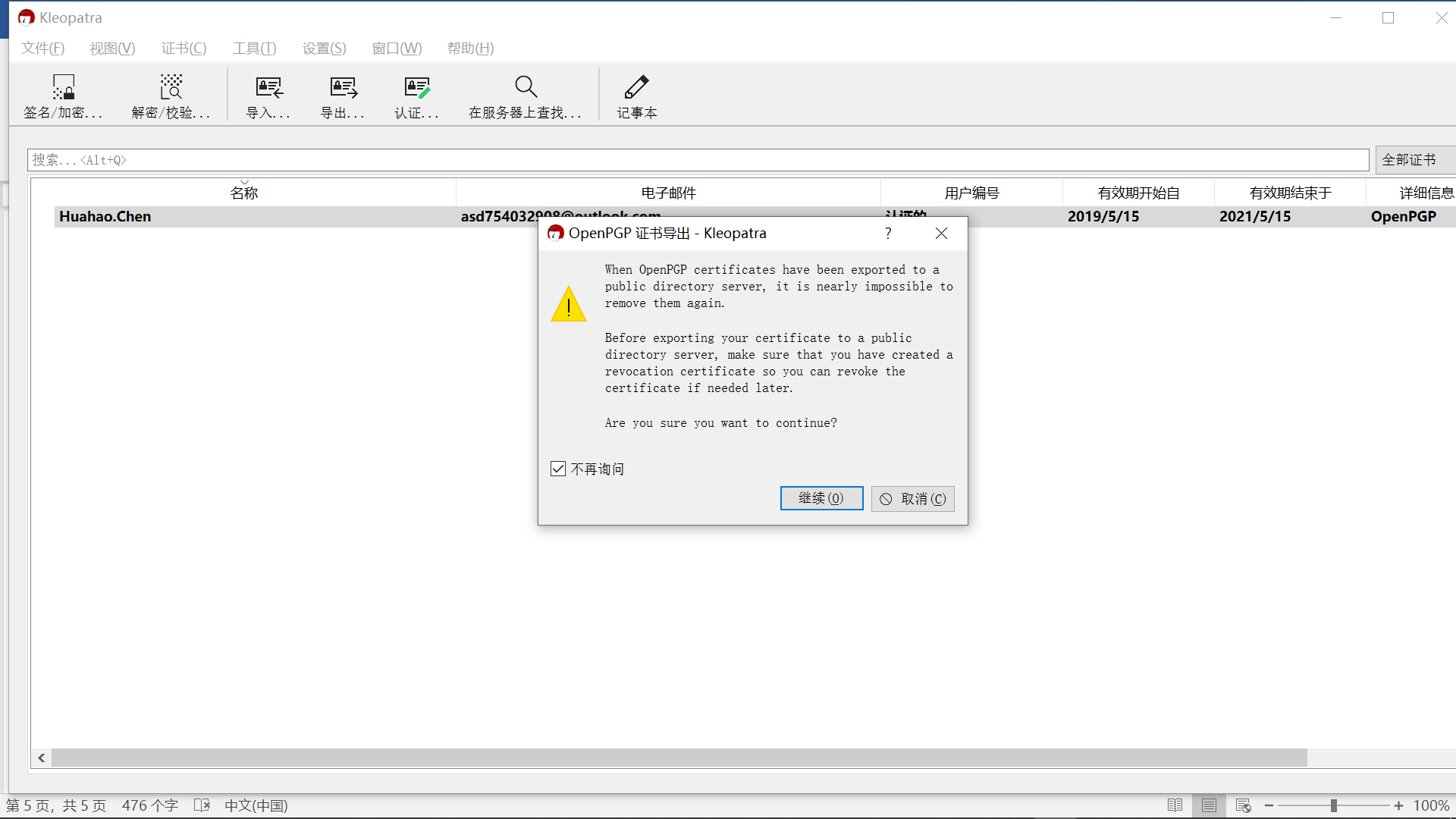
创建成功



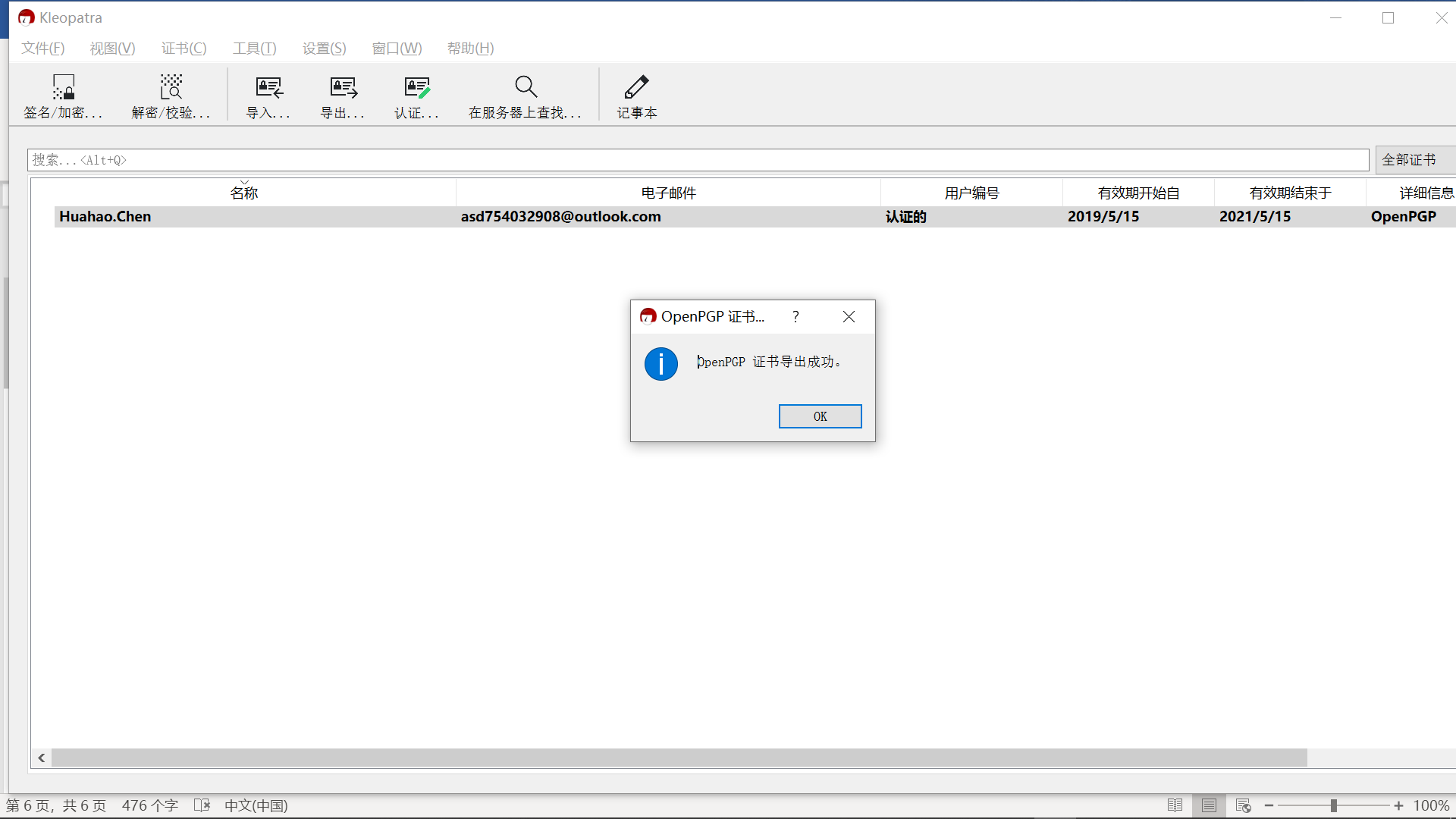


发布：

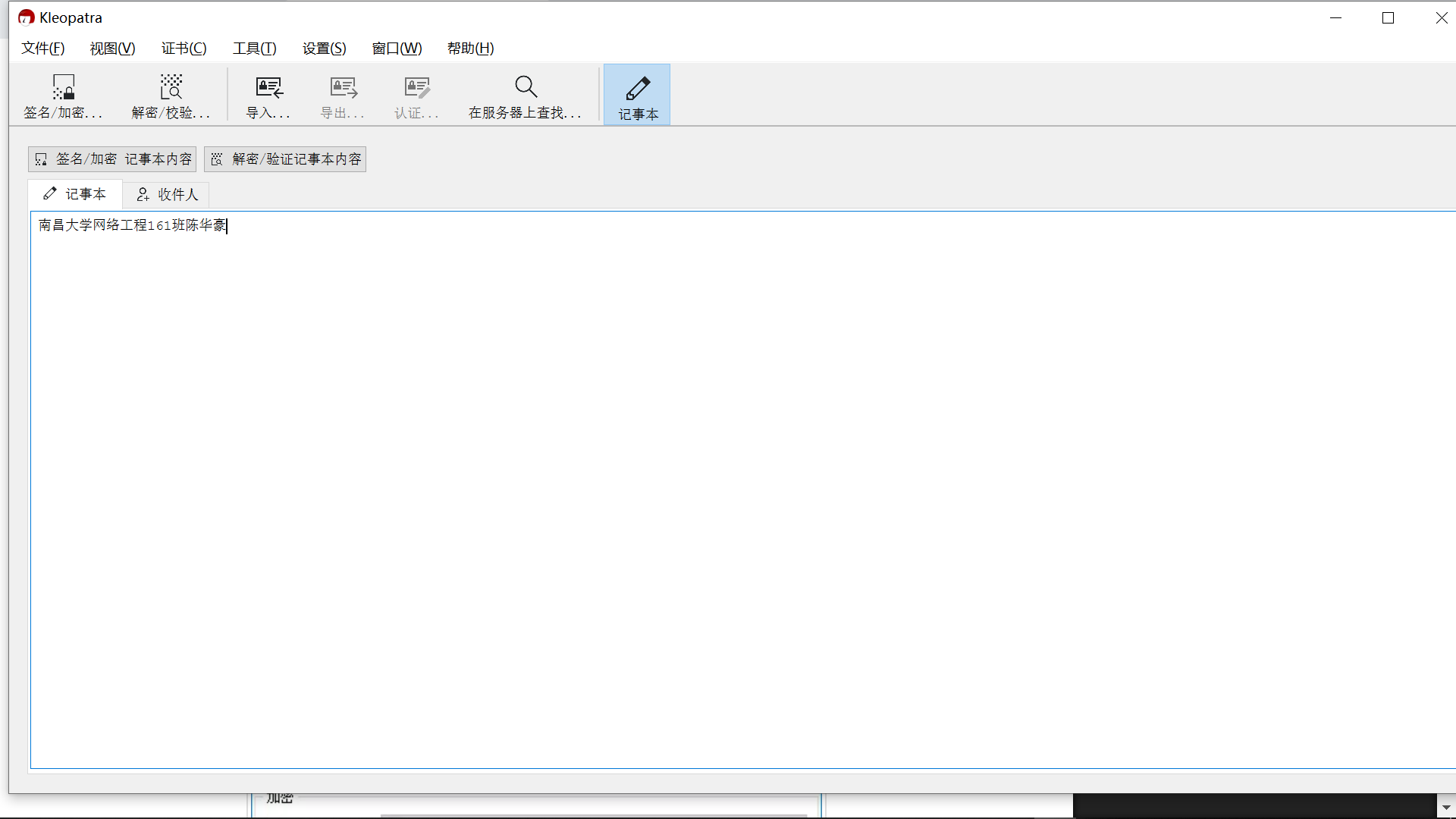




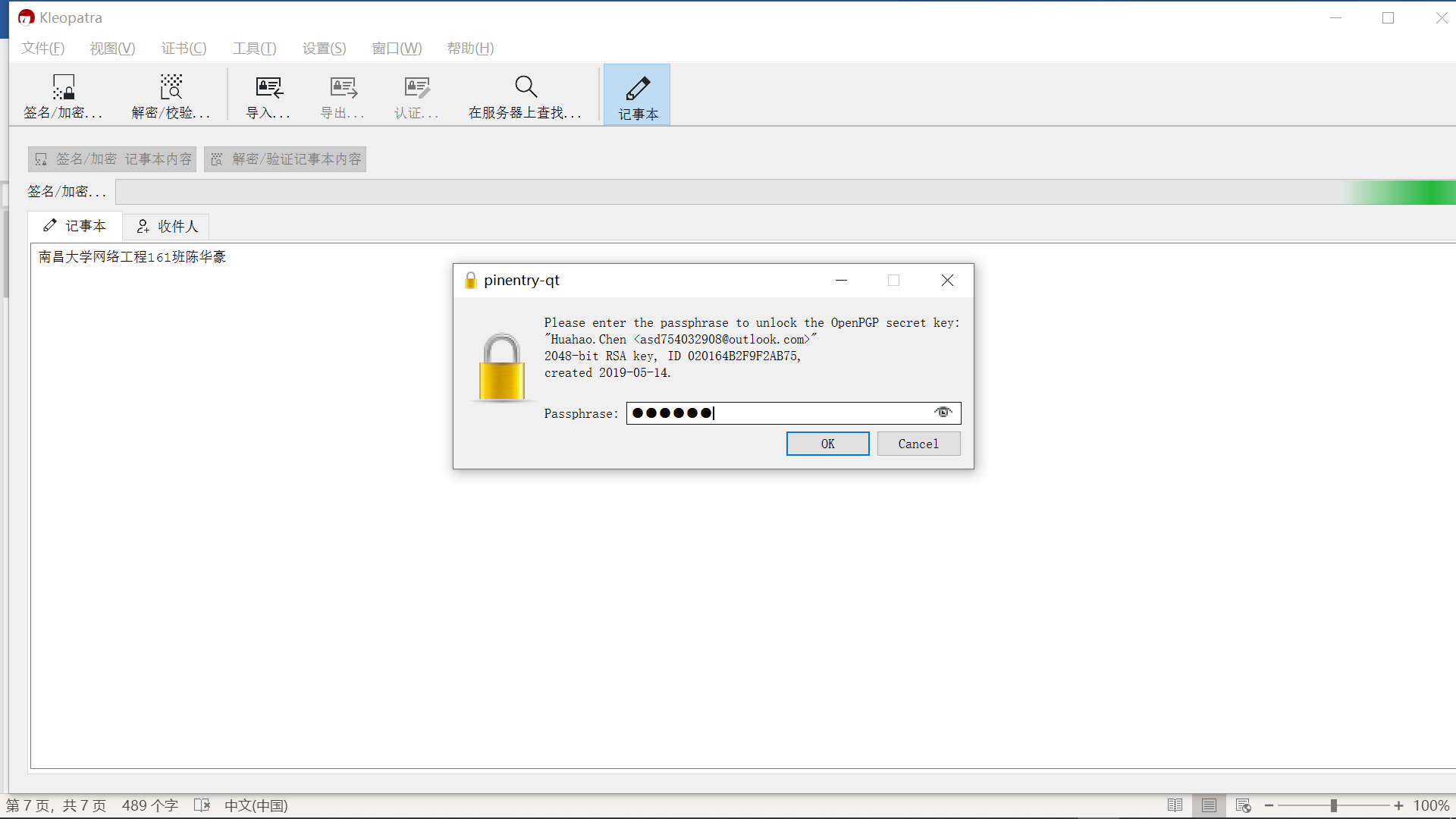
发布成功：



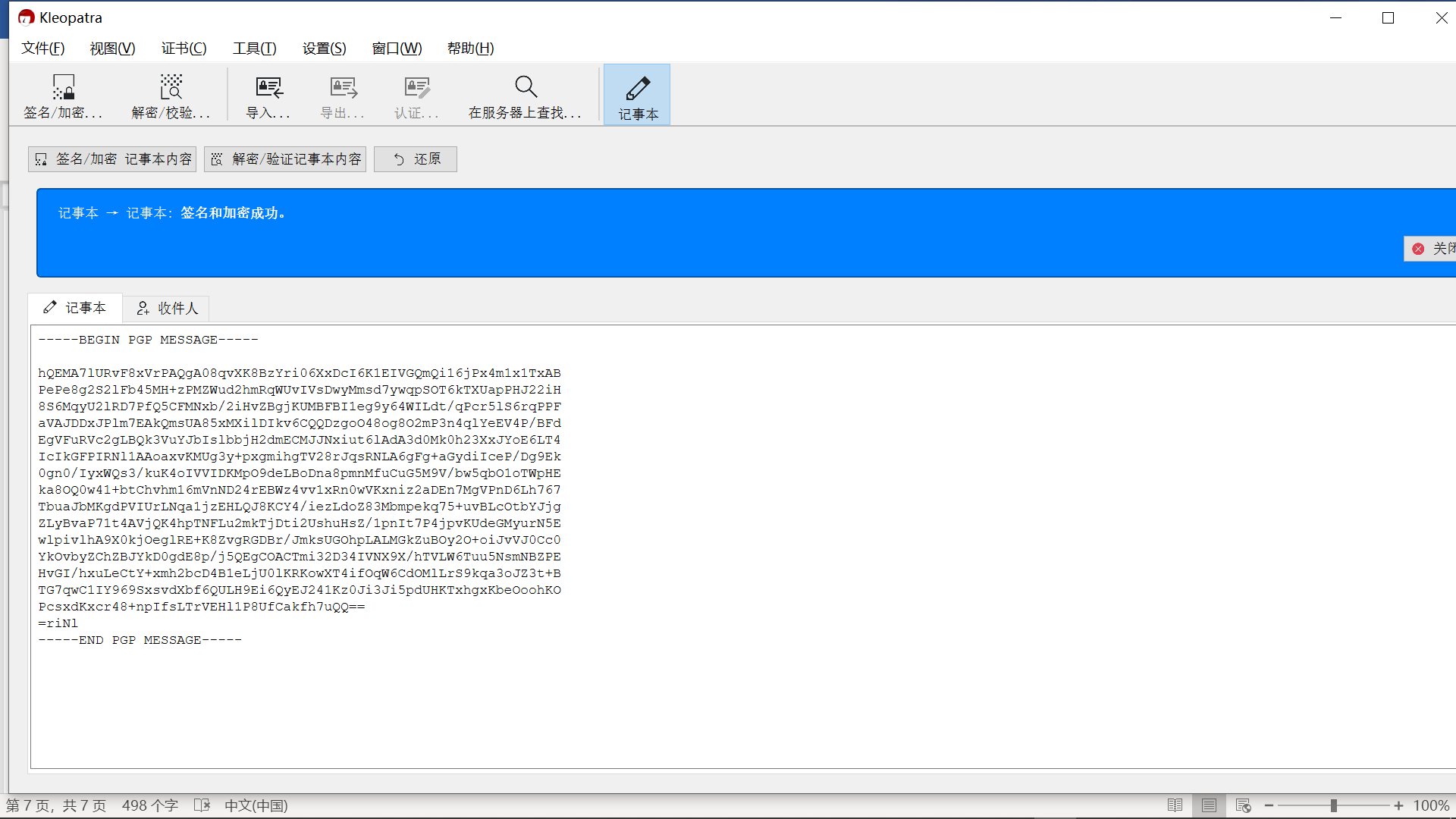
撰写邮箱草稿文本



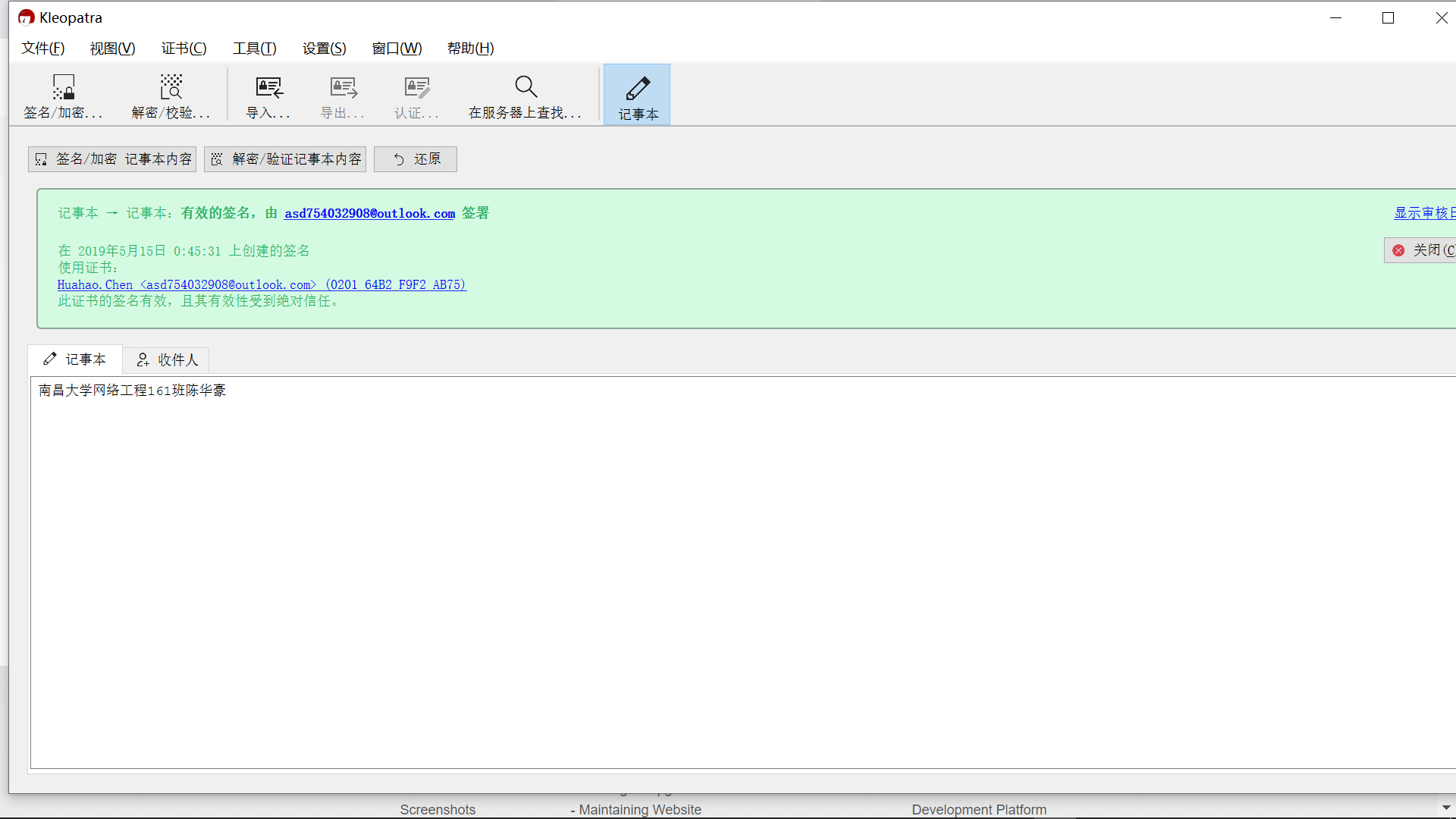
点击加密记事本内容



提示加密成功



点击解密/验证记事本内容，提示解密成功



解密成功

**实验总结**

网上浏览资料认识到pgp原本是一个1991年开发出的商业程序，开发者是美国的Phil Zimmermann。那时候美国法律规定高强度加密技术属于军用技术不许出口海外，因此开发者收到了政府对它的指控，但开发者巧妙地利用了出版物收言论自由保护的相关法律，将pgp源码写入自己通过MIT出版社出版的书中，以此化解指控。

PGP开发者后来同意IETF 制定一项公开的互联网标准，称作 OpenPGP，任何支持这一标准的程序也被允许称作 OpenPGP。

这次实验，打开的实验指导给出的网站网页不美观于是我想到了了解其他支持openpgp协议的相关软件。最后决定使用gpg4win这款软件进行本次试验。

实验过程中看到生成秘钥后可以通过将公钥发布到服务器的方式来让其他人用我的公钥与我秘密通信，体验了一次基于互联网的加密通信之旅，收获很大。