密码学加解密及数字签名

实 验 报 告

实验名称　密码学加解密及数字签名

班　　级　信安 20-2

姓　　名　李天昊

学　　号　20101110201

指导教师　徐　刚

2020 年 11 月 9 日

实验一 密码学加解密及数字签名

一、实验目的

1. 通过对 PGP 软件的使用，进一步加深对非对称加密算法 RSA 的认识和掌握熟悉及掌握。

2. 实现掌握 PGP 加密文件的原理和过程；

3. 学会使用 PGP，包括密钥的生成、密钥的导入和导出、对文件内容进行加密和解密。

二、实验环境

1. 文件接收方：（物理机，李天昊）

DEVICE NAME : Thinkpad T480s

PROCESSOR : Intel(R) Core(TM) i7-8650U CPU @ 1.90GHz 2.11 GHz

SYSTEM TYPE : 64-bit operating system,x64-based processor

SYSTEM EDITION : Windows 10 Professional

VERSION : 2004

OS BUILD : 19041.572

2. 文件发送方：（虚拟机，David）

DEVICE NAME : V-WinXP

PROCESSOR : (inter VT)Intel(R) Core(TM) i7-8650U CPU @ 1.90GHz 2.11 GHz

SYSTEM TYPE : 32-bit operating system,x64-based processor

SYSTEM EDITION : Windows XP Professional SP3

VERSION : /

OS BUILD : 5.1.2600 Service Pack 3 Build 2600

三、实验要求

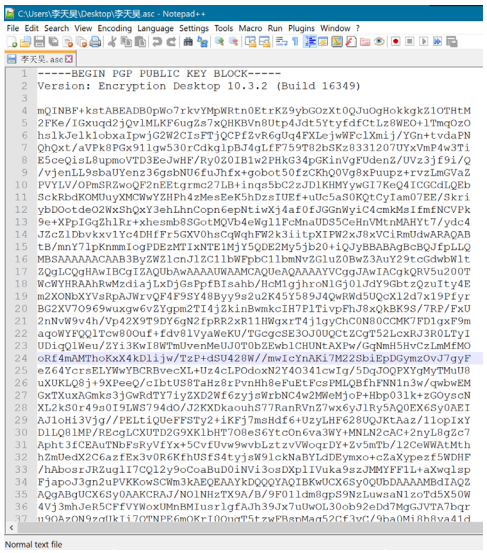
利用 PGP 软件，完成以下操作：

1、密钥管理：（1）生成公钥/私钥对；（2）密钥的导出；（3）密钥的导入。

2、文件操作：（1）加密/解密文件；（2）签名/验证文件；（3）加密和签名/解密和验证文件。

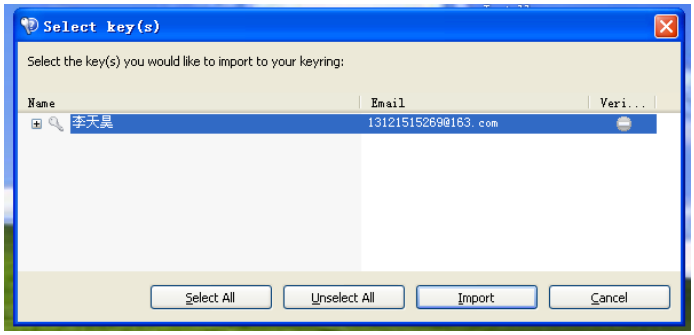
四、实验步骤和结果

1.物理机 PGP 软件内**生成公钥/私钥对，导出公钥**并使用公共信道发送给虚拟机；

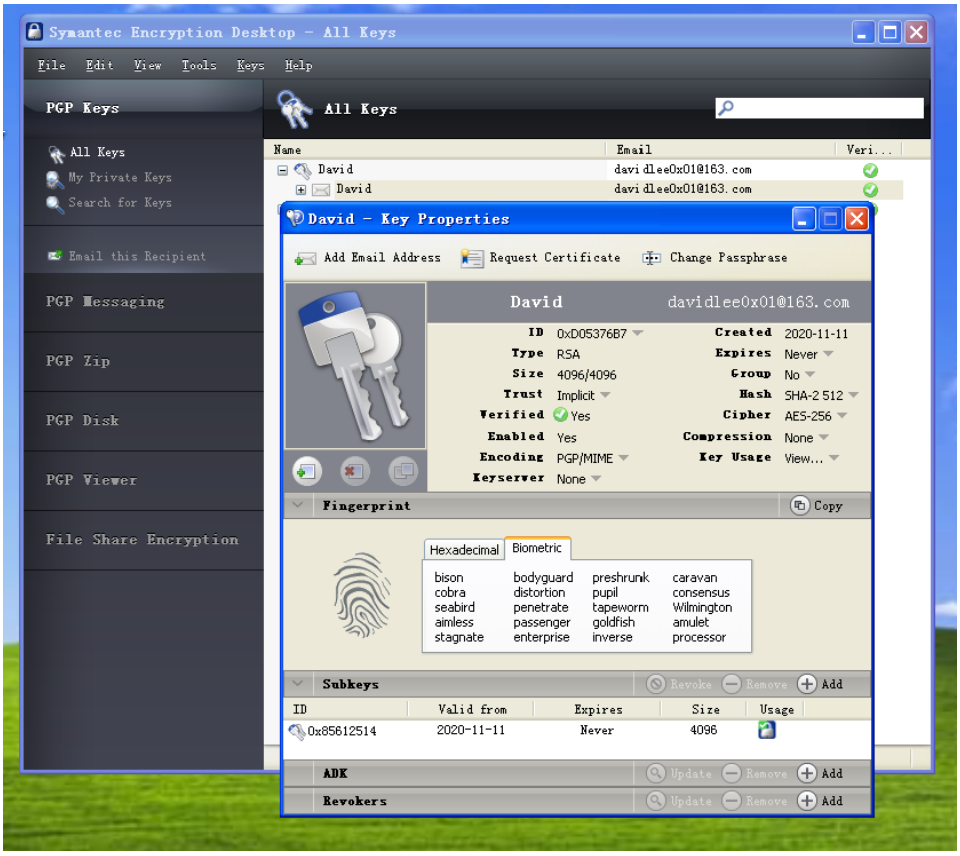


“李天昊”的密钥属性　　“李天昊”公钥的一部分

2. 虚拟机**导入并校验公钥**，并添加至钥匙环；

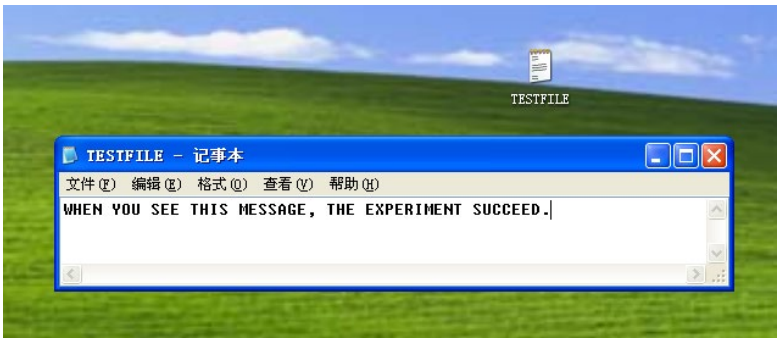


“David”成功接收了“李天昊”发送的公钥



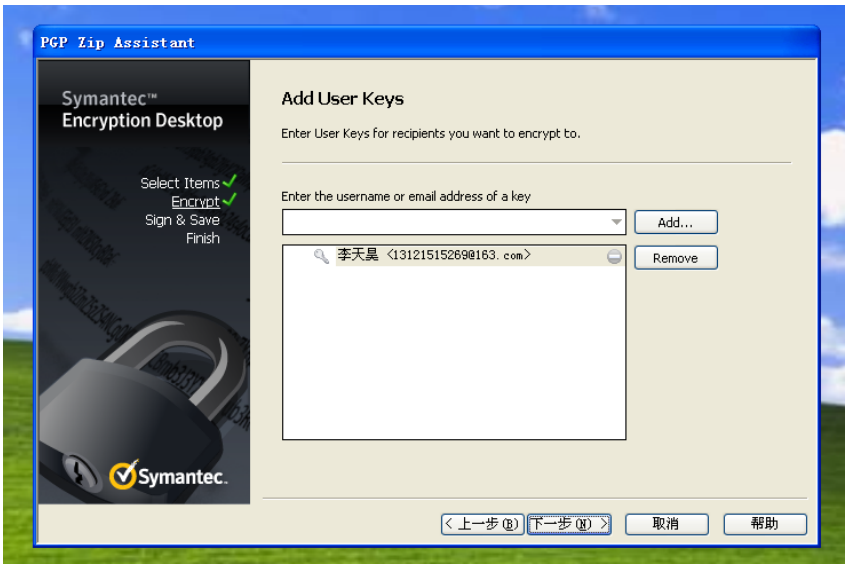
“David”成功校验了“李天昊”发送的公钥，并添加到钥匙环中

3. 虚拟机生成文件，准备加密；

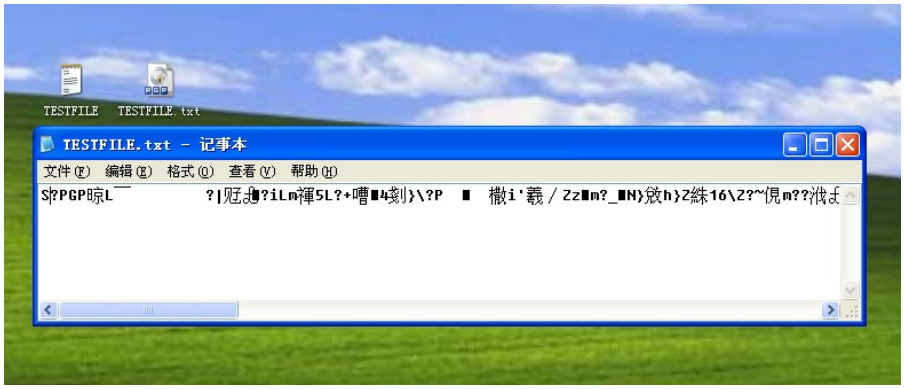


“David”生成的文本文档

4. 虚拟机使用物理机公钥，生成**加密文档**，并使用公共信道发送给物理机；

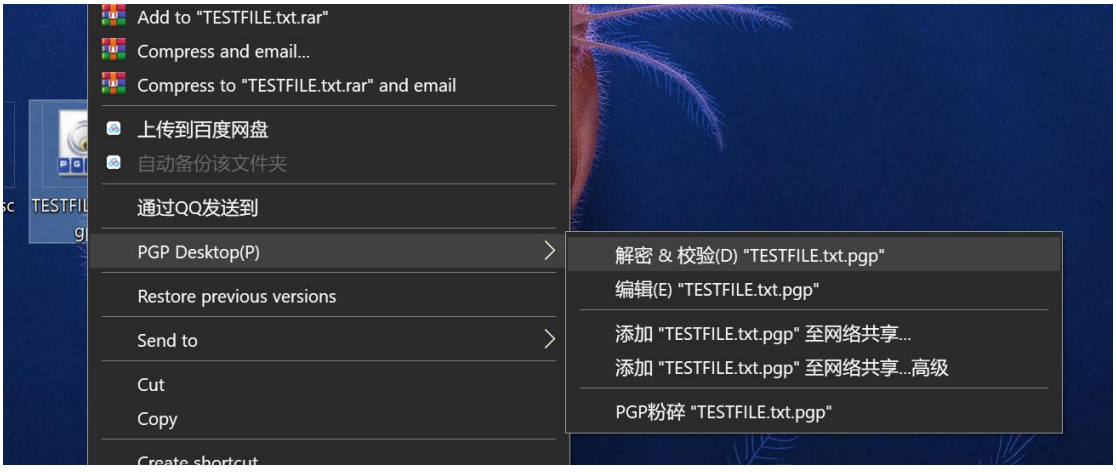


选择接收人为“李天昊”

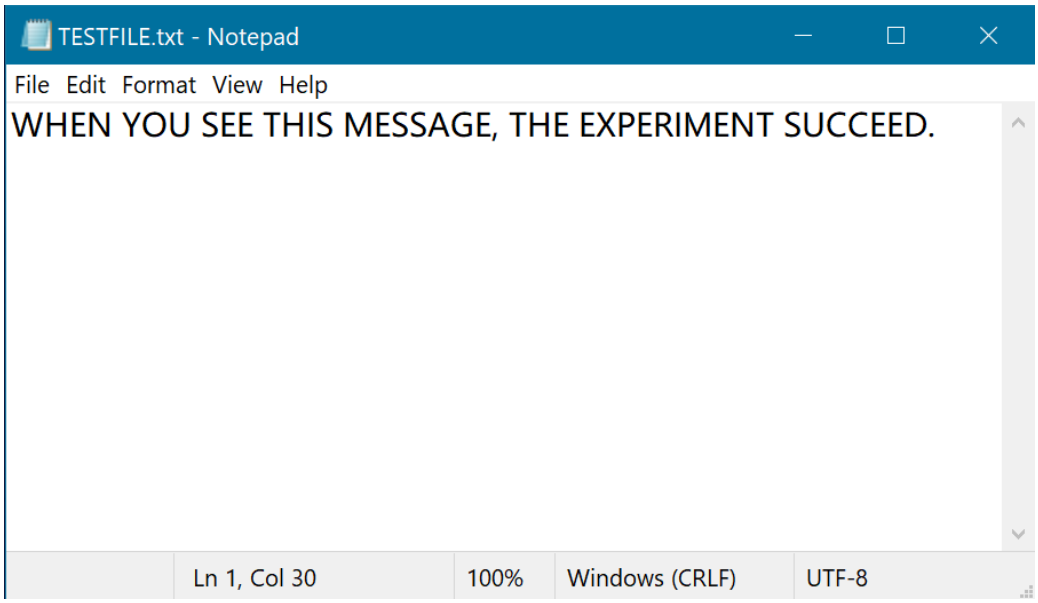


加密后的文档，显示乱码，可以相对安全地在公共信道传输

5. 物理机接收加密文件，使用私钥**解密**并查看原文。



使用“李天昊”的私钥解密并校验. pgp 加密文件



解密成功，“李天昊”成功得到“David”发送的原文

五、实验心得和思考

数据可以通过各种方式传输，微信、QQ、邮件等，传输过程中的信息安全很难得以保证。这时候，需要加密传输，而非对称加密算法很好地保证了加密传输过程。