

实验 2 密码学及其应用

中国科学技术大学 曾凡平
(2020 年 3 月 26 日星期四)

2.1 实验目的

1. 掌握 OpenSSL 的命令；
2. 掌握在 C 程序中使用 OpenSSL 的方法；
3. 掌握 PGP 的使用。

2.2 实验内容

1. 使用 OpenSSL 的常用命令；
2. 利用 OpenSSL 编程实现 RSA 加密、解密；
3. 用 PGP 实现加密和解密。

2.3 实验步骤

本实验是用了 Windows 2003 虚拟机。因为要下载教学资源，需要将虚拟网卡的连接方式设置为“网络地址转换(NAT)”模式，以便可以从虚拟机访问因特网，如下图所示。（也可新增一个“网络地址转换(NAT)”模式的虚拟网卡）

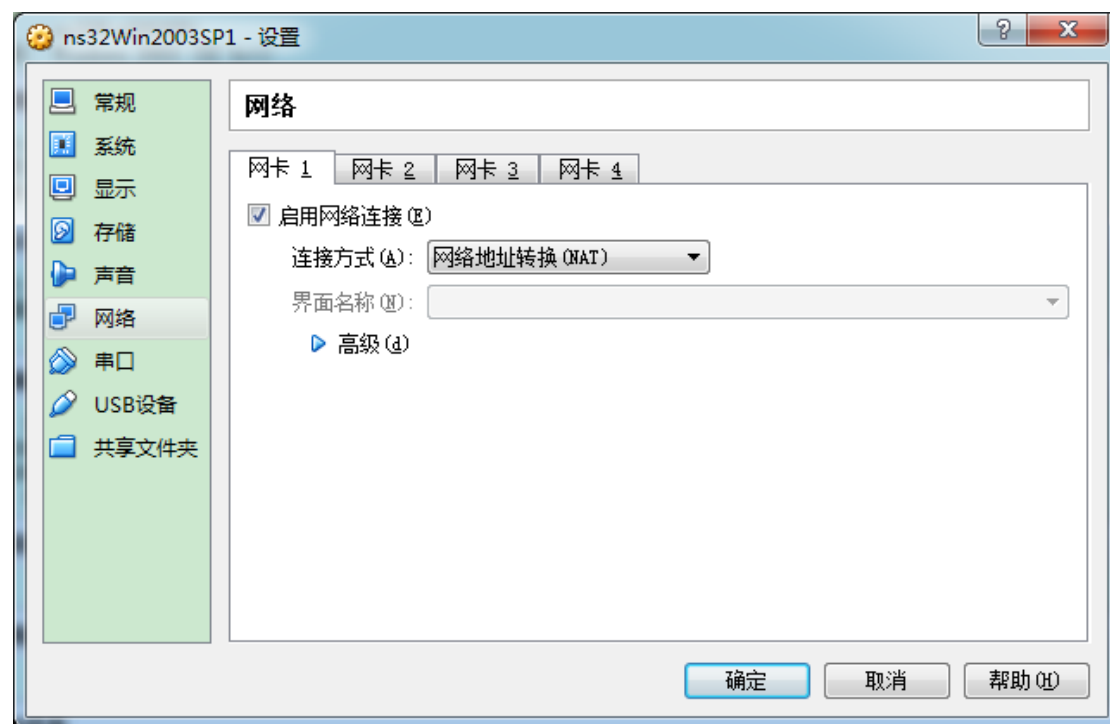


图 1 设置虚拟机环境中的虚拟网卡“网络地址转换(NAT)”模式

启动该虚拟机，设置本地网卡为自动获取 IP 地址模式，则虚拟机可以访问因特网了。

从课程网站下载 cryptoDemo.zip，从课程网站指定的链接下载 openssl，Win32Openssl 和 gpg4Win 到目录 C:\work\ns\chapter03。将文件解压缩，完成后的目录如下图所示：

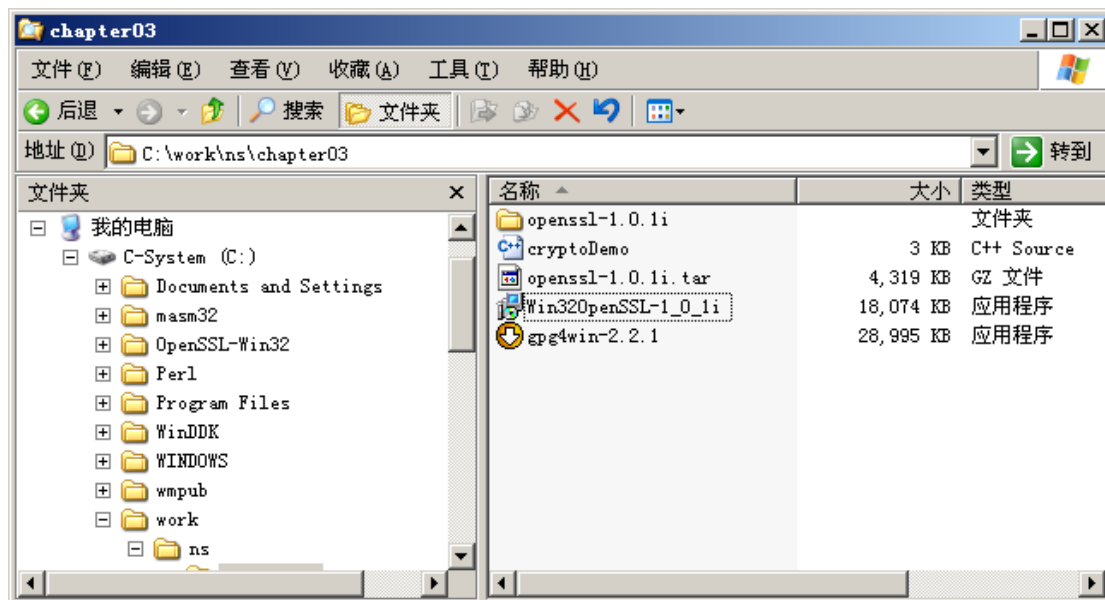


图 2 实验代码所在的目录

2.3.1 使用 OpenSSL 的常用命令

点击 Win32openSSL-1_0_1i 对应的安装文件，安装完后可以看到目录 C:\OpenSSL-Win32，其中包含了 OpenSSL 的各类文件。如下图所示：

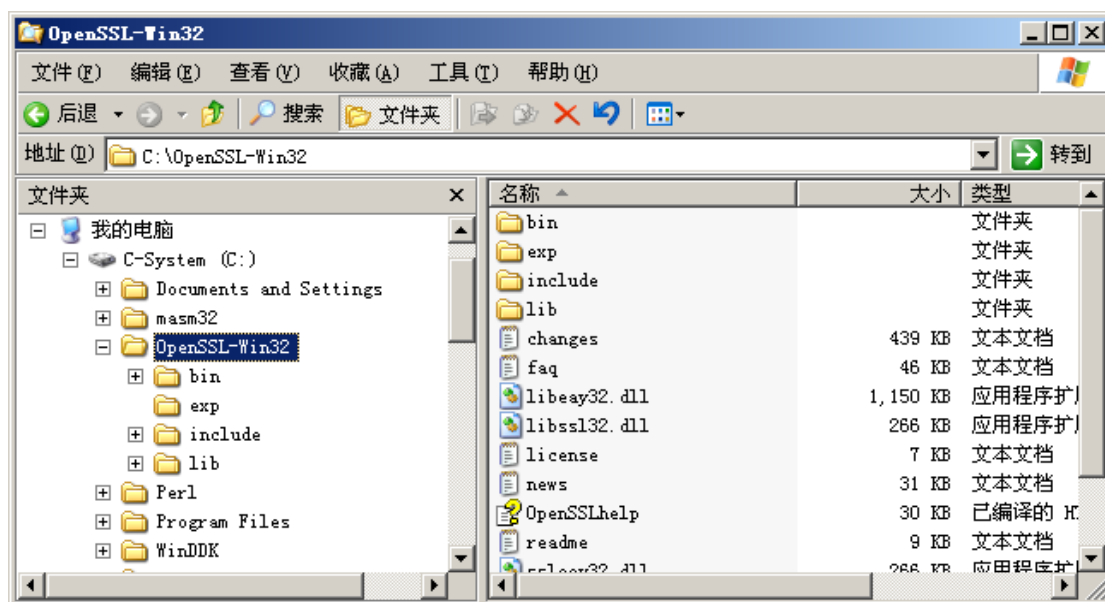
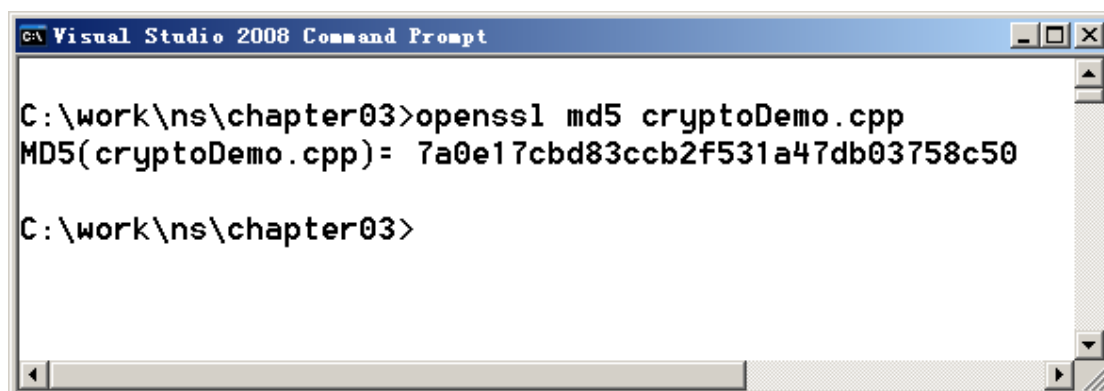


图 3 OpenSSL-Win32 的路径

将 C:\OpenSSL-Win32\bin 添加到环境变量 path 中，将 C:\OpenSSL-Win32 下的 include 和 lib 目录拷贝到 C:\Program Files\Microsoft Visual Studio

9.0\VC 中。

参考第 2 章 PPT 的“在命令行下使用 OpenSSL”的相关内容，测试其中的相关命令，如下图所示：



```
C:\work\ns\chapter03>openssl md5 cryptoDemo.cpp
MD5(cryptoDemo.cpp)= 7a0e17cbd83ccb2f531a47db03758c50

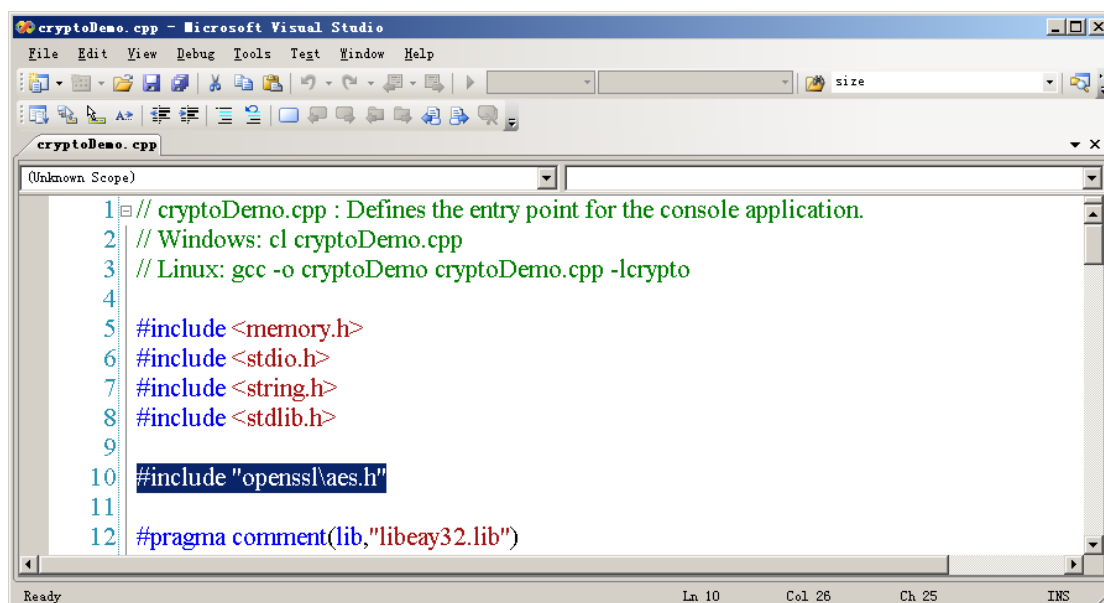
C:\work\ns\chapter03>
```

图 4 MD5 的运行结果

2.3.2 利用 OpenSSL 编程实现 AES 的加密、解密

OpenSSL 提供了对 AES 的支持，实例程序 cryptoDemo.cpp 实现了对字符串的加密和解密。

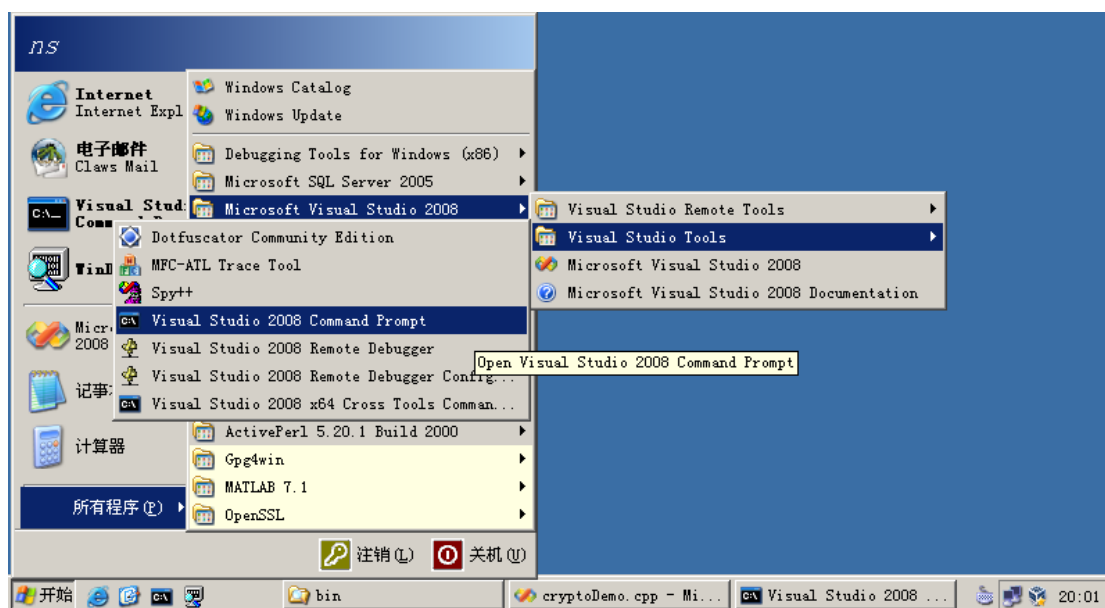
将该程序的第 10 行代码改成 `#include "openssl/aes.h"`，如下图所示：



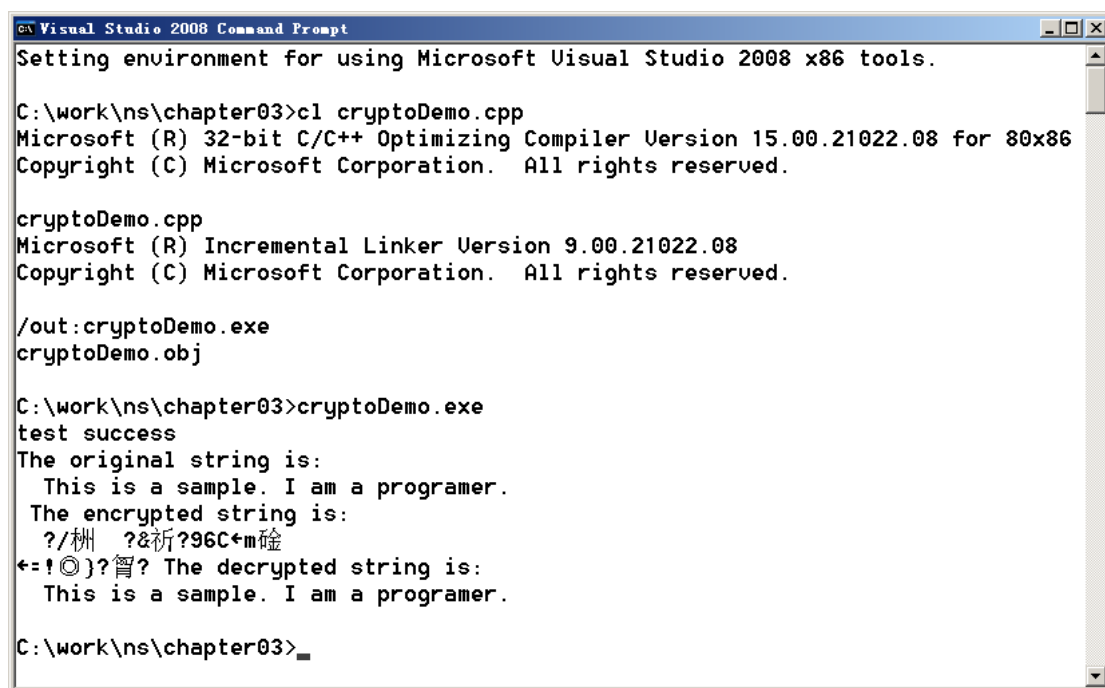
```
1 // cryptoDemo.cpp : Defines the entry point for the console application.
2 // Windows: cl cryptoDemo.cpp
3 // Linux: gcc -o cryptoDemo cryptoDemo.cpp -lcrypto
4
5 #include <memory.h>
6 #include <stdio.h>
7 #include <string.h>
8 #include <stdlib.h>
9
10 #include "openssl/aes.h"
11
12 #pragma comment(lib, "libeay32.lib")
```

图 5 修改 cryptoDemo.cpp 的第 10 行源代码

启动 Visual Studio 2008 Command Prompt 编译环境，如下图所示：



编译和运行 cryptoDemo.cpp，如下图所示：



如果你在做实验时出现如上图所示的信息，则说明实验结果正确。

2.3.3 用 PGP 实现加密和解密

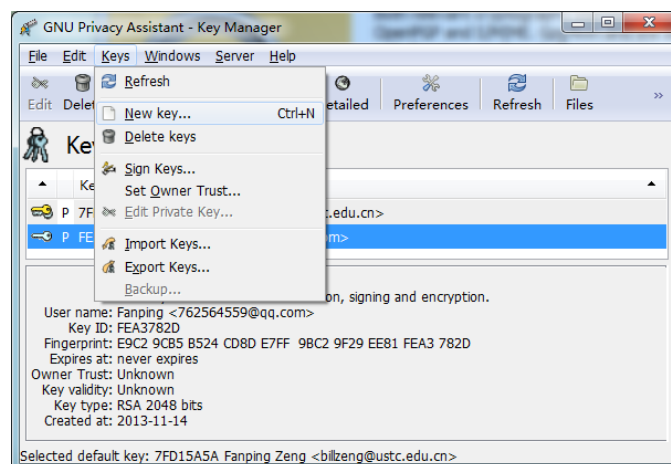
安装 Gpg4win2.2.3，界面如下：



选择安装所有的组件，安装结束后认真阅读 README.en 文件。按以下步骤使用加密和解密功能。

步骤 1：产生一对 RSA 密钥

启动 GPA（Windows7 下以管理员身份运行），产生一对密钥，如下图所示。



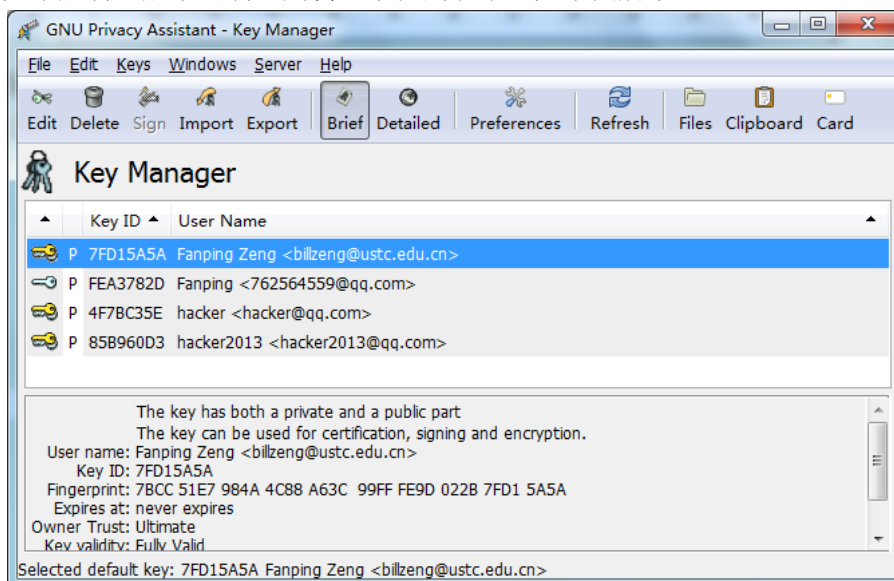
输入用户名，比如：hacker。



再输入电子邮件地址，如图所示：

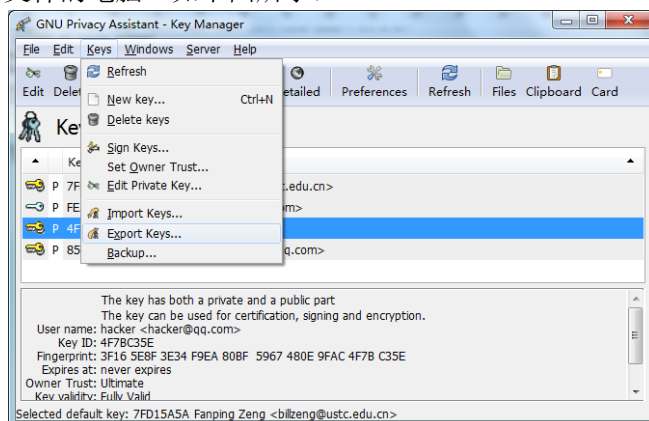


接下来输入 passphrase，然后就会生成 2048 位的公钥/私钥对（注意：可能要等待一段时间）。如果成功生成了密钥，则会显示在列表中。如下图所示：



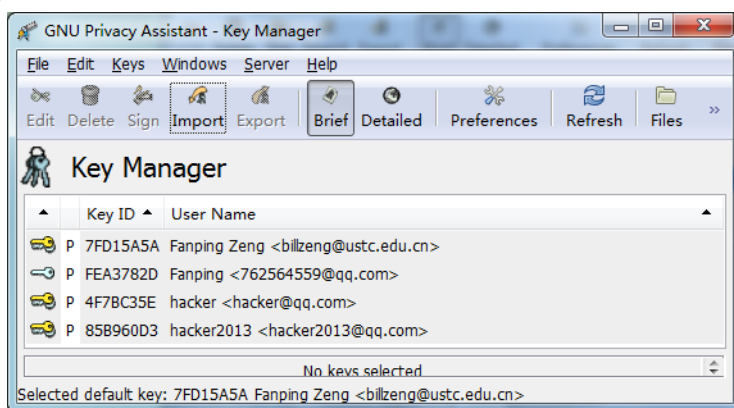
步骤 2: 互换公钥

将公钥导出(Export Keys)到一个文件中(假定文件名为 pub-hacker-2013.key), 传递给需要给自己发送加密文件的电脑。如下图所示:



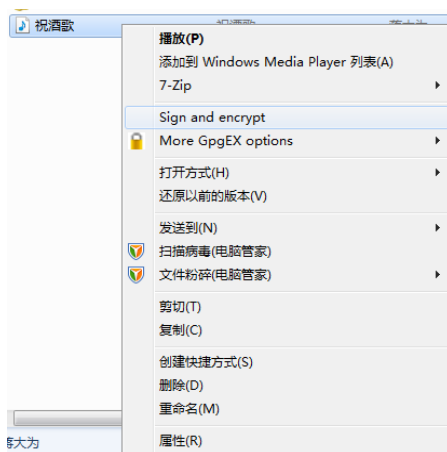
如果要将私钥也导出, 则选择“Backup...”。

对方收到公钥文件(pub-hacker-2013.key)后, 将公钥导入到本机。如果导入成功, 将在本机的 GPA 中列出该公钥。如图所示导入了 ID 号为 FEA3782D、邮件地址为 762564559@qq.com 的公钥。

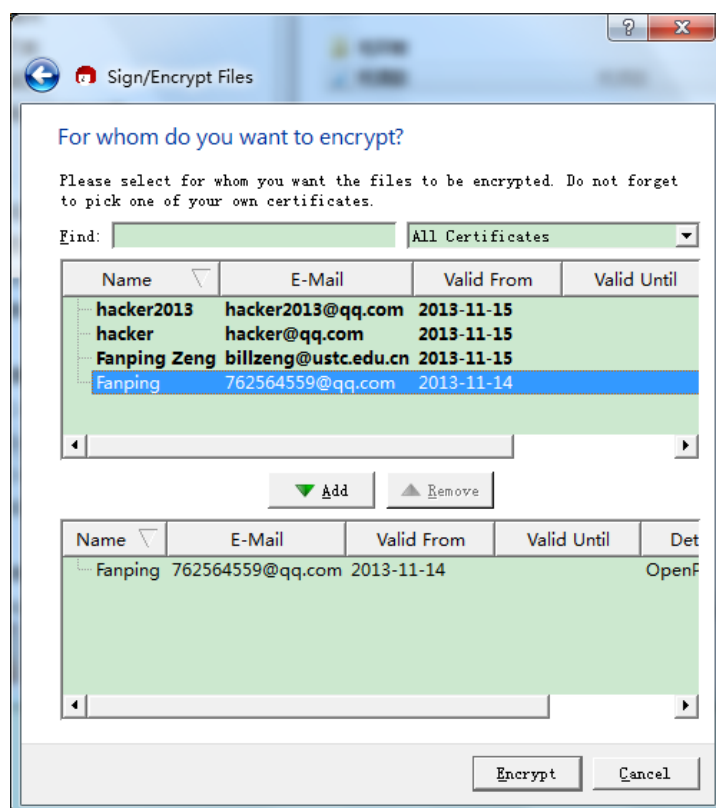


步骤 3: 向对方发送加密文件

启动资源管理器, 选择要加密的文件, 右击该文件将弹出如下菜单:



选择 Sign and encrypt。选择要接收该加密文件的用户(与公钥对应的私钥持有者):



点击 Encrypt 按钮将加密指定的文件，得到扩展名为 gpg 的加密文件，将该文件发送给私钥持有者。私钥持有者对其解密(需要输入 passphrase)后可以恢复出原文件。

2.4 上机实践(自己练习，不考核)

从课程网站下载“太阳岛上.mp3”，以 2 人为一组进行 PGP 实验。各自生成公钥/私钥对，导出公钥并发送给对方，双方用对方的公钥加密音乐文件并将加密的文件发送给对方。

如果能用自己的私钥解密文件，则可以用媒体播放器播放出音乐，由此可以检验实验是否成功。