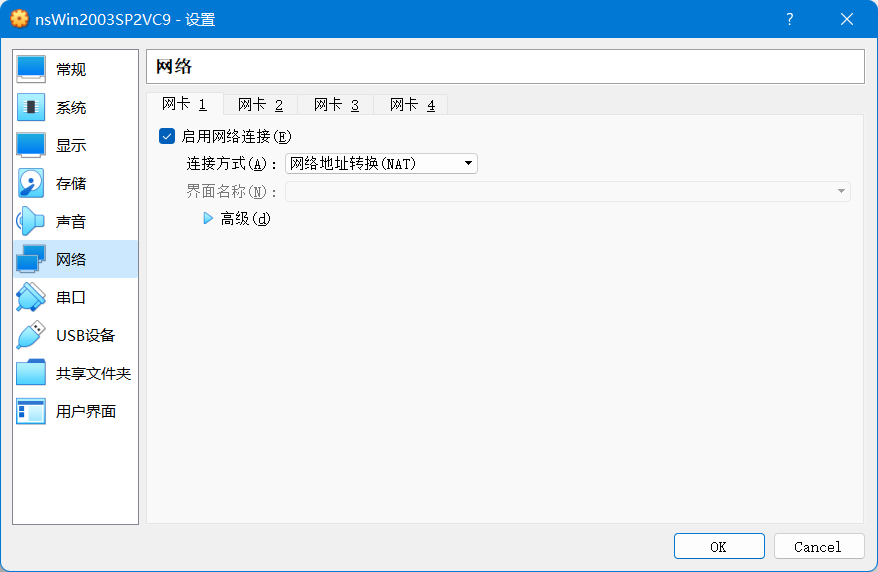
**实验 2 密码学及其应用**

李远航 PB20000137

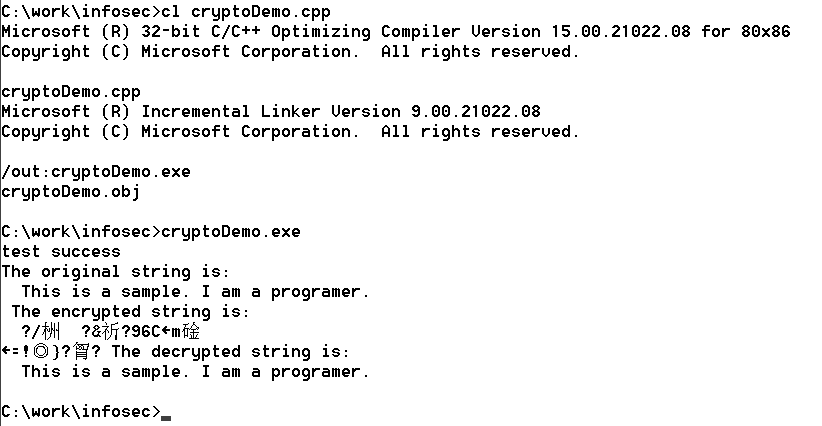
1. **实验目的**
2. 掌握 OpenSSL 的命令；
3. 掌握在 C 程序中使用 OpenSSL 的方法；
4. 掌握 PGP 的使用。
5. **实验内容**
6. 使用 OpenSSL 的常用命令；
7. 利用 OpenSSL 编程实现 AES 加密、解密；
8. 用 PGP 实现加密和解密。
9. **实验步骤**
10. 将虚拟网 卡的连接方式设置为“网络地址转换(NAT)”模式



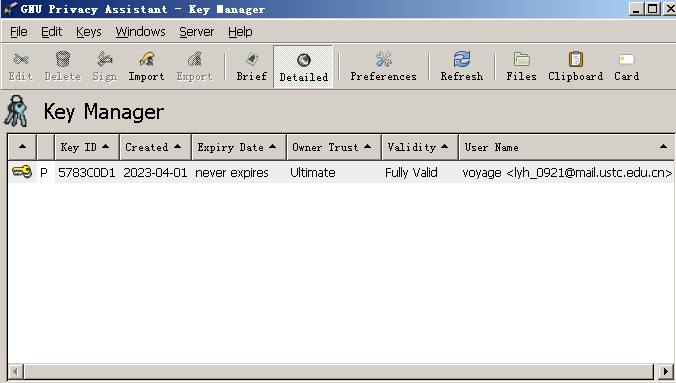
1. 安装OpenSSL-Win32并添加环境变量



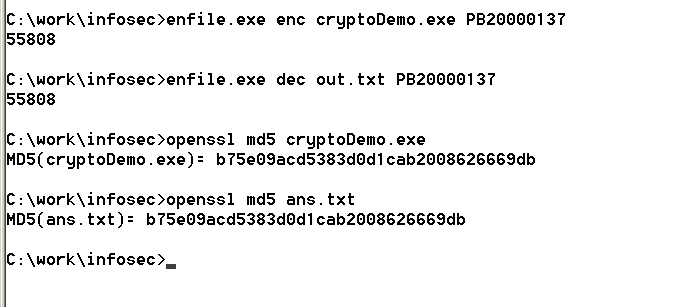
1. 利用 OpenSSL 编程实现 AES 的加密、解密



1. 用 PGP 实现加密和解密



1. **实验内容**



使用方法：

enfile.exe [enc/dec] [文件路径] [passwd]

选择enc作为参数时程序将加密后的文件out.txt 存储在程序运行目录下，选择dec作为参数时，程序将解密后的文件 ans.txt 存储在程序运行目录下

如图所示，将cryptoDemo.exe文件用学号PB20000137加密再解密，得出的两个文件md5值完全相同，可见顺利完成了对文件的加密和解密

1. **实验收获**
2. 亲身实践了加密解密算法
3. 对信息安全有了更深的理解
4. 提升了调试代码的能力