实验 2 密码学及其应用

PB19111708 杨云皓

2.1 实验目的

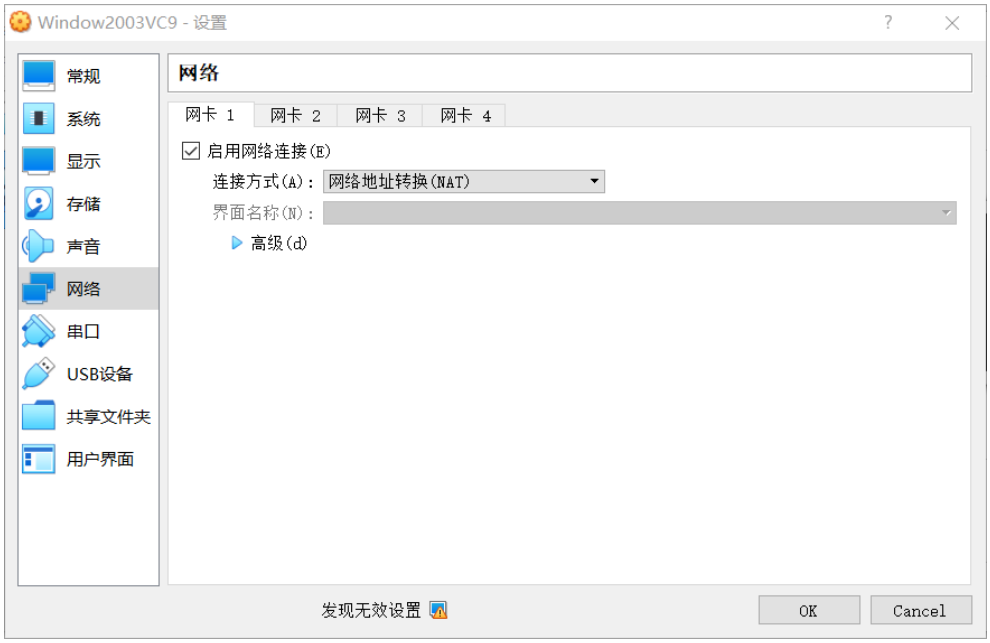
1．掌握 OpenSSL 的命令;
2．掌握在 C 程序中使用 OpenSSL 的方法;
3．掌握 PGP 的使用。

2.2 实验内容

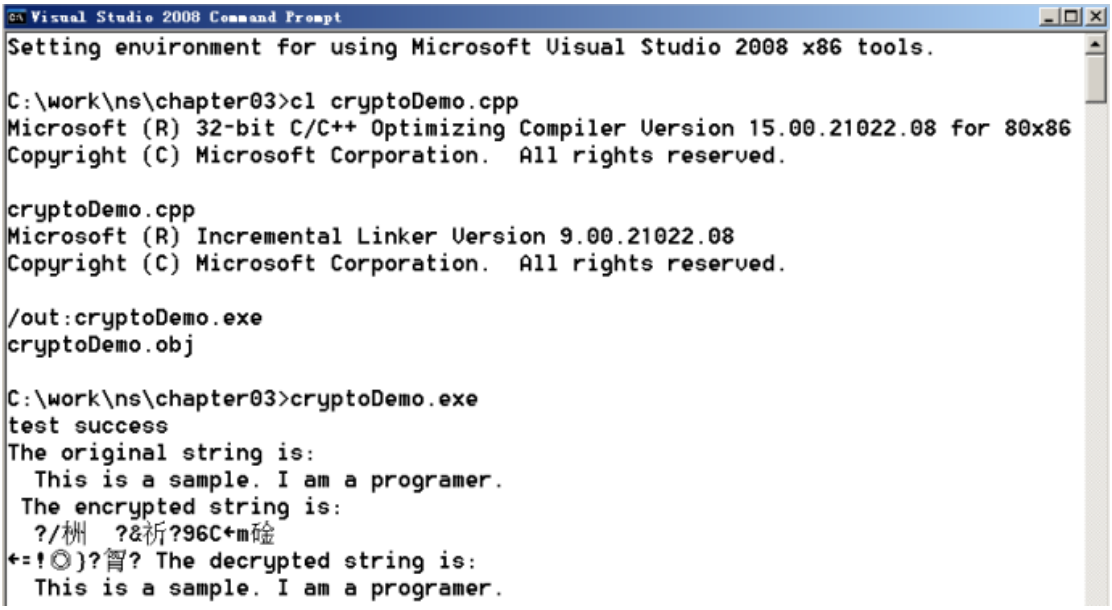
1．使用 OpenSSL 的常用命令;
2．利用 OpenSSL 编程实现 AES 加密、解密;
3．用 PGP 实现加密和解密。

2.3 实验步骤

1.将虚拟网卡的连接方式设置为“网络地址转换(NAT)”模式



2. 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。
3. 利用 OpenSSL 编程实现 AES 的加密、解密
   将该程序的第 10 行代码改成 #include "openssl\aes.h"
4. 编译和运行 cryptoDemo.cpp



5. 用 PGP 实现加密和解密

（1）产生一对 RSA 密钥

（2）互换公钥

（3）向对方发送加密文件

2.4 实验内容

修改例程 cryptoDemo.cpp 为 encfile.cpp：从命令行接受 3 个字符串类型的 参数：参数 1，参数 2，参数 3。参数 1=enc 表示加密，参数 1=dec 表示解密； 参数 2 为待加密、解密的文件名；参数 3 为密码。 以文件 cryptoDemo.cpp 为测试文件，以你的学号为密码，验证你的程序 encfile.cpp 的正确性。

```
C:\work\ns\chapter03>cl encfile.cpp
Microsoft (R) 32-bit C/C++ Optimizing Compiler Version 15.00.21022.08 for 80x86
Copyright (C) Microsoft Corporation.  All rights reserved.

encfile.cpp
Microsoft (R) Incremental Linker Version 9.00.21022.08
Copyright (C) Microsoft Corporation.  All rights reserved.

/out:encfile.exe
encfile.obj

C:\work\ns\chapter03>encfile.exe enc cryptoDemo.cpp PB19111708
test success
The original string is:
  // cryptoDemo.cpp : Defines the entry point for the console application.
// Windows: cl cryptoDemo.cpp
// Linux: gcc -o cryptoDemo cryptoDemo.cpp -lcrypto

#include <memory.h>
#include <stdio.h>
#include <string.h>
#include <stdlib.h>

#include "aes.h"

#pragma comment(lib,"libeay32.lib")

void testAes(char inString[], int inLen, char passwd[], int pwdLen)
{
        int i,j, len, nLoop, nRes;
        char enString[1024];
        char deString[1024];

        unsigned char buf[16];
        unsigned char buf2[16];
        unsigned char aes_keybuf[32];
        AES_KEY aeskey;

        // 准备32字节(256位)的AES密码字节
        memset(aes_keybuf,0x90,32);
        if(pwdLen<32){ len=pwdLen; } else { len=32;}
```

```
 The encrypted string is:
  鼹1  U螵江DT? The decrypted string is:
  // cryptoDemo.cpp : Defines the entry point for the console application.
// Windows: cl cryptoDemo.cpp
// Linux: gcc -o cryptoDemo cryptoDemo.cpp -lcrypto

#include <memory.h>
#include <stdio.h>
#include <string.h>
#include <stdlib.h>

#include "aes.h"

#pragma comment(lib,"libeay32.lib")

void testAes(char inString[], int inLen, char passwd[], int pwdLen)
{
        int i,j, len, nLoop, nRes;
        char enString[1024];
        char deString[1024];

        unsigned char buf[16];
        unsigned char buf2[16];
        unsigned char aes_keybuf[32];
        AES_KEY aeskey;

        // 准备32字节(256位)的AES密码字节
        memset(aes_keybuf,0x90,32);
        if(pwdLen<32){ len=pwdLen; } else { len=32;}
        for(i=0;i<len;i++) aes_keybuf[i]=passwd[i];
        // 输入字节串分组成16字节的块
        nLoop=inLen/16; nRes = inLen%16;
        // 加密输入的字节串
        AES_set_encrypt_key(aes_keybuf,256,&aeskey);
        for(i=0;i<nLoop;i++){
                memset(buf,0,16);
                for(j=0;j<16;j++) buf[j]=inString[i*16+j];
                AES_encrypt(buf,buf2,&aeskey);
                for(j=0;j<16;j++) enString[i*16+j]=buf2[j];
        }
        if(nRes>0){
                memset(buf,0,16);
                for(j=0;j<nRes;j++) buf[j]=inString[i*16+j];
                AES_encrypt(buf,buf2,&aeskey);
```