1. **需求**
2. 问题重现：Alice和Bob是一对好朋友，他们远隔千山万水，无法面对面地交流，只能通过Internet进行信息交互，如果数据传输的环境很安全，Alice和Bob就会很顺利地收到对方的消息，可是网络上有一个人Eve，他经常会做一些窃取Alice与Bob通信内容的事情，也会拦截并篡改他们之间的通信内容，甚至会假冒Alice或Bob给对方发送信息，这就使得Alice和Bob常常因此而饱受困扰，必须有合适的方法或工具让他们之间能够安全地进行信息交互。请你为他们设计一个工具套件，以便能够在非安全的互联网环境下进行安全的信息交互。

# （2）问题分析：可以从两个方面进行分析，即信息传输功能的实现和信息安全性的实现。信息传输功能的实现即工具可以通过Internet传输消息，信息安全性的实现可以分为机密性，完整性和真实性三个方面完成Alice和Bob之间安全的信息交互。

# ①机密性：机密性（Confidentiality）指只有授权用户可以获取信息或即使其他用户获得了传输的数据也不能获得其中的信息。机密性可以通过密码学中的加解密算法来实现，其中分为两个部分，即安全分配密码算法的密钥和在信息发送端与接收端对需要传输的信息进行加密和解密。解决了问题中提到的Eve窃取信息的问题，即Eve即使窃取了通信内容也会不知道密码算法的密钥而无法破译数据包中隐藏的信息。

# ②完整性：完整性（Integrality）指信息在输入和传输的过程中，不被非法授权修改和破坏，保证数据的一致性。完整性可以通过密码学中的消息验证码算法来实现，其中分为两个部分，即消息验证码算法的密钥和在信息发送端与接收端对需要传输的消息验证码进行附加和校验。解决了问题中Eve假冒Alice或Bob给对方发送信息的问题，即通信系统可以识别出消息是非被Eve篡改。

# ③真实性：真实性（Truth）指由于某种机制的存在，人们不能假冒自己的身份或传输虚假的数据。不可否认性可以通过共同的私钥进行实现，因为机密性和完整性均涉及到密钥传输的安全问题，故选用DH协议可以有效地在不安全信道进行共同私钥的交互，基于离散对数的数学难题，Eve无法获得私钥即难以假冒身份进行通信。

（3）需求及目标：

1. 实现Alice和Bob之间的信息交互。（信息可以本地发送，本地接受但在必须经过网络传输）

2. 在Alice和Bob之间安全地进行会话密钥分发。

3. 用分发的密钥key和AES加密算法，实现Alice和Bob之间的加密数据传输，构造不少于4条测试数据消息进行正确性测试。

4. 对Alice和Bob之间发送的消息进行完整性保护和校验，防止消息篡改。

5. 采用Huffman或其他压缩算法，对网络传输信息进行压缩编码。

6. 能够支持多种信息（短消息、文件、图像等）安全传输。

7. 有良好的人机交互界面。

1. **设计框架**

存储结构；抽象数据类型；涉及的函数或操作的规格说明；重要的函数调用关系，可以通过调用关系图表达。

本题涉及数据结构及函数较多，以下仅对关键数据结构和封装函数进行说明。

关键数据结构说明：

union b4w

{

unsigned char bytes[4];

unsigned int word;

};

用于记录AES分组状态的数据

typedef union \_uint128\_t {

struct {

uint64\_t low;

uint64\_t high;

};

unsigned char byte[DH\_KEY\_LENGTH];

} uint128\_t;

用于记录DH分配密钥的数据，用于大数计算

关键函数说明：

void key\_allocate\_ser(); //dh协议共享密钥

void commuciation\_ser();//服务器通信函数

void commuciation\_ser\_double();//服务器双人通信函数

DWORD WINAPI serEventThread(LPVOID lpParameter);//服务器事件处理线程

DWORD WINAPI recvMsgThread\_double(LPVOID lpParameter);//服务器事件处理线程

void file\_exchange\_ser();//服务器文件传输函数

void DH\_generate\_key\_pair(DH\_KEY public\_key, DH\_KEY private\_key); //DH协议生成公私钥对函数

void DH\_generate\_key\_secret(DH\_KEY secret\_key, const DH\_KEY my\_private, const DH\_KEY another\_public); //DH协议计算共同私钥函数

void hmac\_md5(unsigned char\* out, unsigned char\* data, int dlen, unsigned char\* key, int klen); //计算缓冲区data的hmac\_md5值

void hmac\_md5\_file(char\* filename, unsigned char\* out, unsigned char\* key, int klen);// //计算文件filename的hmac\_md5值

void LZSS\_compress(char\* filename, char\* newfilename); //LZSS算法压缩filename

void LZSS\_uncompress(char\* filename, char\* newfilename); //LZSS算法解压filenmae

void AES\_ECBEncrypt(b4w\* Messenger, b4w\* key, int len); //ECB模式下对len个分组的数据进行AES加密函数

void AES\_ECBDecrypt(b4w\* Messenger, b4w\* key, int len); //ECB模式下对len个分组的数据进行AES解密函数

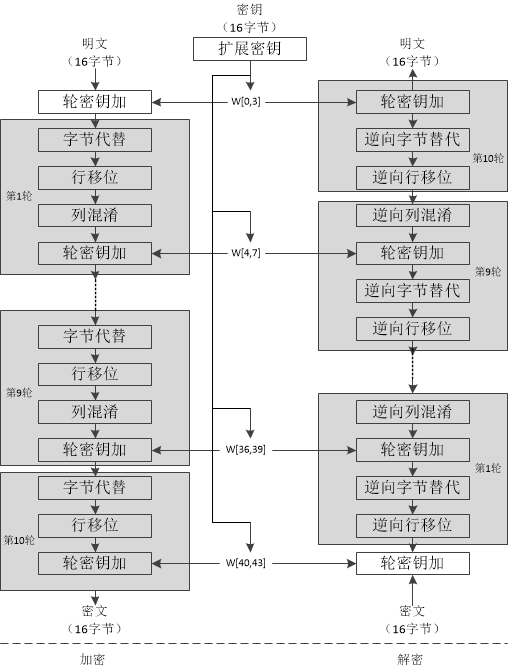
void AES\_ECBEncrypt\_text(unsigned char\* text, unsigned char\* key, int size); //ECB模式下对text文本数据进行AES加密函数--使用PKCS7填充空缺

void AES\_ECBDecrypt\_text(unsigned char\* text, unsigned char\* key, int size);//ECB模式下对text文本数据进行AES解密函数--使用PKCS7填充空缺

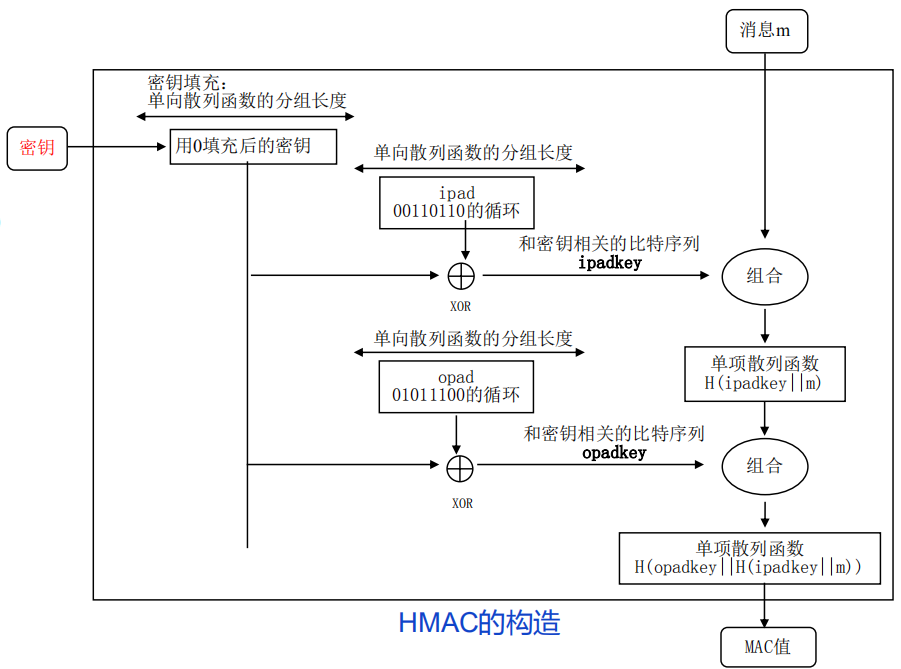
void AES\_ECBDecrypt\_file(char\* filename, char\* filename2, unsigned char\* key);//ECB模式下对filename文件进行AES加密函数--使用PKCS7填充空缺

void AES\_ECBEncrypt\_file(char\* filename, char\* filename2, unsigned char\* key);//ECB模式下对fileneme进行AES加密函数--使用PKCS7填充空缺

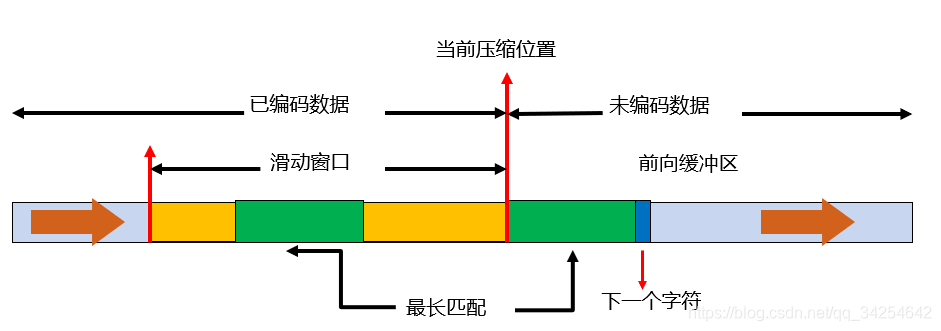
1. **主要算法的基本思想、实现框架。**
2. AES算法实现中使用迭代法和SP网络（SP网络是密码算法中的特殊算法结构），通过对轮函数（字节代换、行位移、列混合和轮密钥加）和密钥扩展算法的迭代实现由简单到高强度密码的升级，并通过位运算实现了数学上的有限域加法乘法求逆等操作，在S盒置换中还运用了穷举法的思想，将所有可能的模逆运算结果写入S盒表格中直接调用，采用空间换时间的思想，提高了性能。此外，在由对AES分组的加密到对文本和文件的加密，我们采用了ECB模式和PKCS7填充方法进行进一步完善对文本和文件的加密和解密。



1. DH协议使用离散对数的思想进行安全密钥交换，在大数模幂运算中使用滑动窗口法，每次处理一个窗口大小，通过逐次平方，依次计算以达到快速模幂运算的目的。实现了在非安全网络下通信双方密钥的安全建立，从而使通信双方能够使用这个密钥进行消息的加密解密，从而实现通信的安全。
2. MD5算法同样采用迭代法和分组思想：MD5码以512位分组来处理输入的信息，且每一分组又被划分为16个32位子分组，经过大量迭代处理和位运算后，算法的输出由四个32位分组组成，将这四个32位分组级联后将生成一个128位散列值，直到所有的数据均被使用。
3. HMAC\_md5消息验证码使用单向散列函数来构造消息认证码的方法，同样使用迭代法和循环异或(位运算）调用哈希函数md5进行加密得到消息验证码，只有使用相同的数据和相同的密钥才能得到相同的HMAC码，以达到保证完整性的效果。



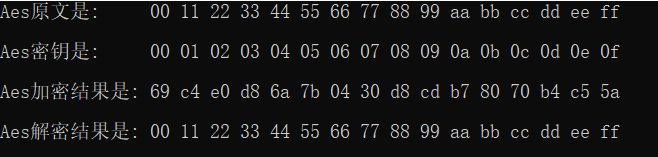
1. LZSS压缩算法由LZ77改进而来，使用滑动窗口压缩算法，该算法将一个虚拟的，可以跟随压缩进程滑动的窗口作为词典，要压缩的字符串如果在该窗口中出现，则输出其出现位置和长度，没出现则原样输出字符。



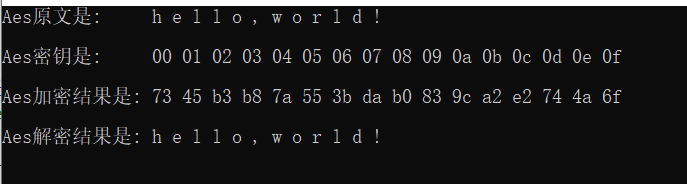
4. 测试

（1）AES文本数据及文件数据加解密测试：

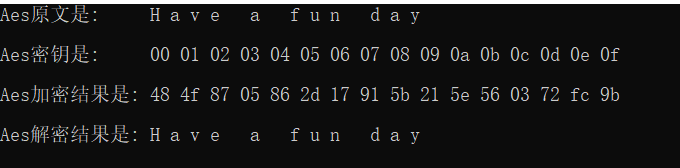
AES标准向量测试：



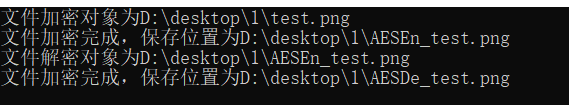
AES文本测试其一：

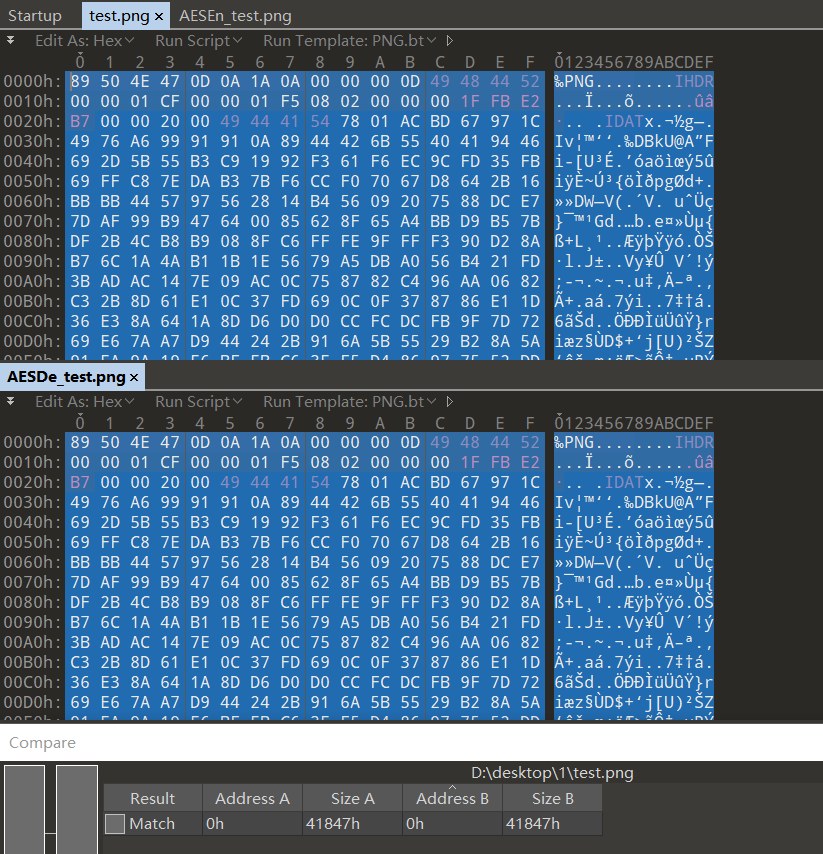


AES文本测试其二：



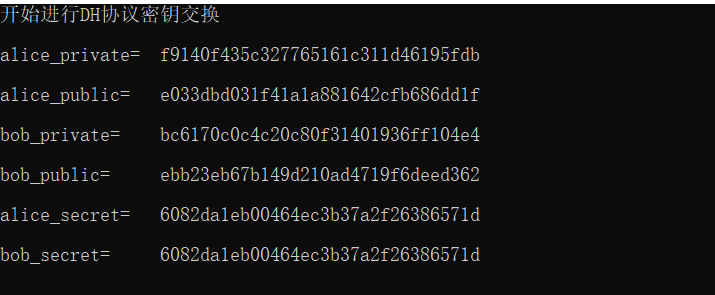
AES文件测试：



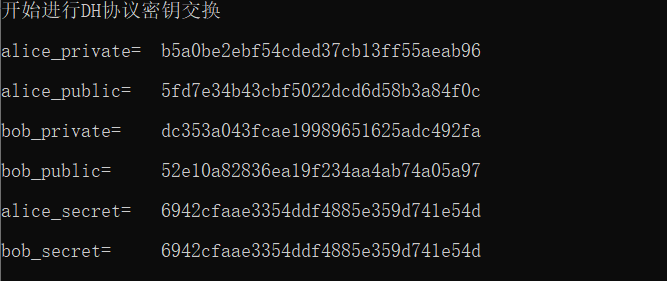


1. DH协议分配密钥实现：

随机分配密钥其一：

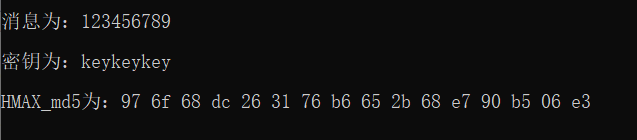


随机分配密钥其二：

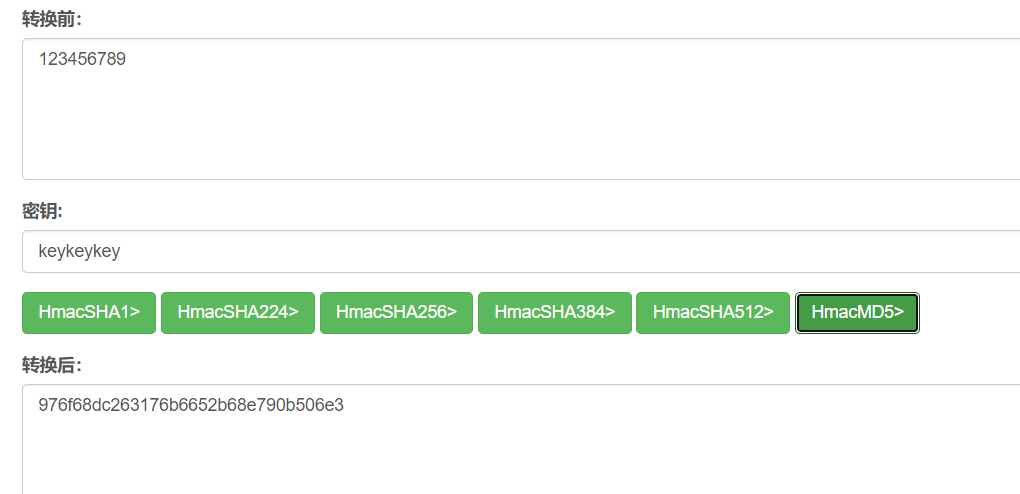


1. HMAC\_md5消息验证码测试：

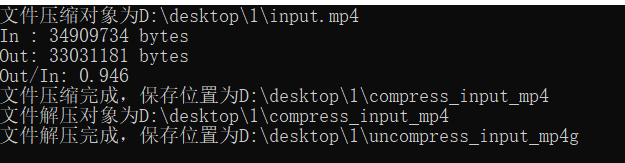
本地测试：



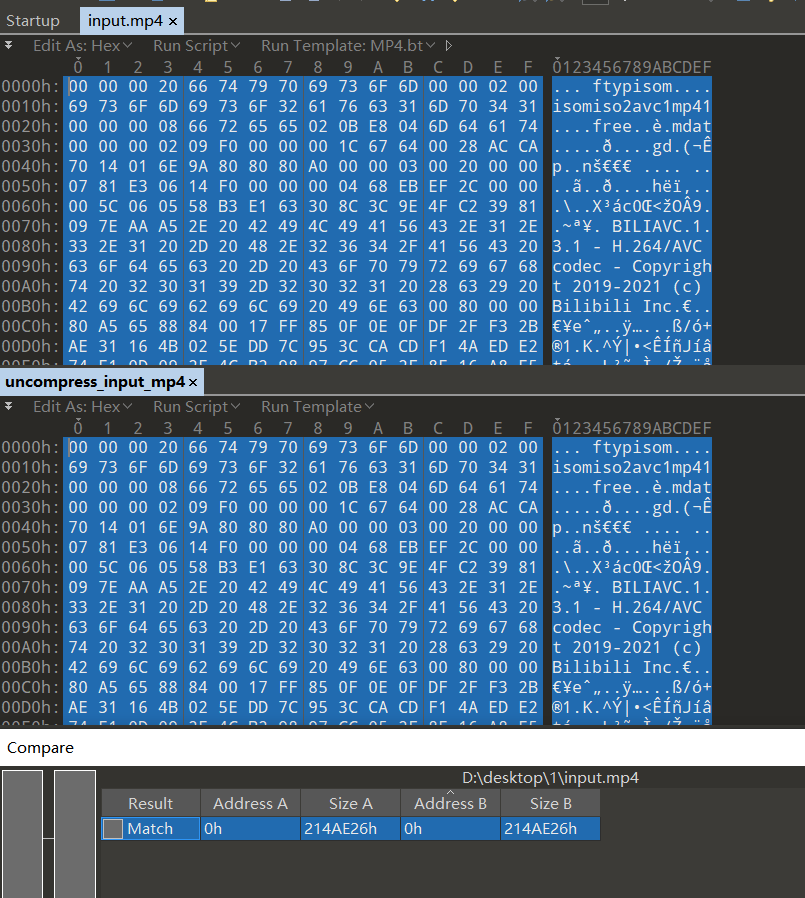
在线网站对比：



（4）LZSS算法文件压缩解压测试：



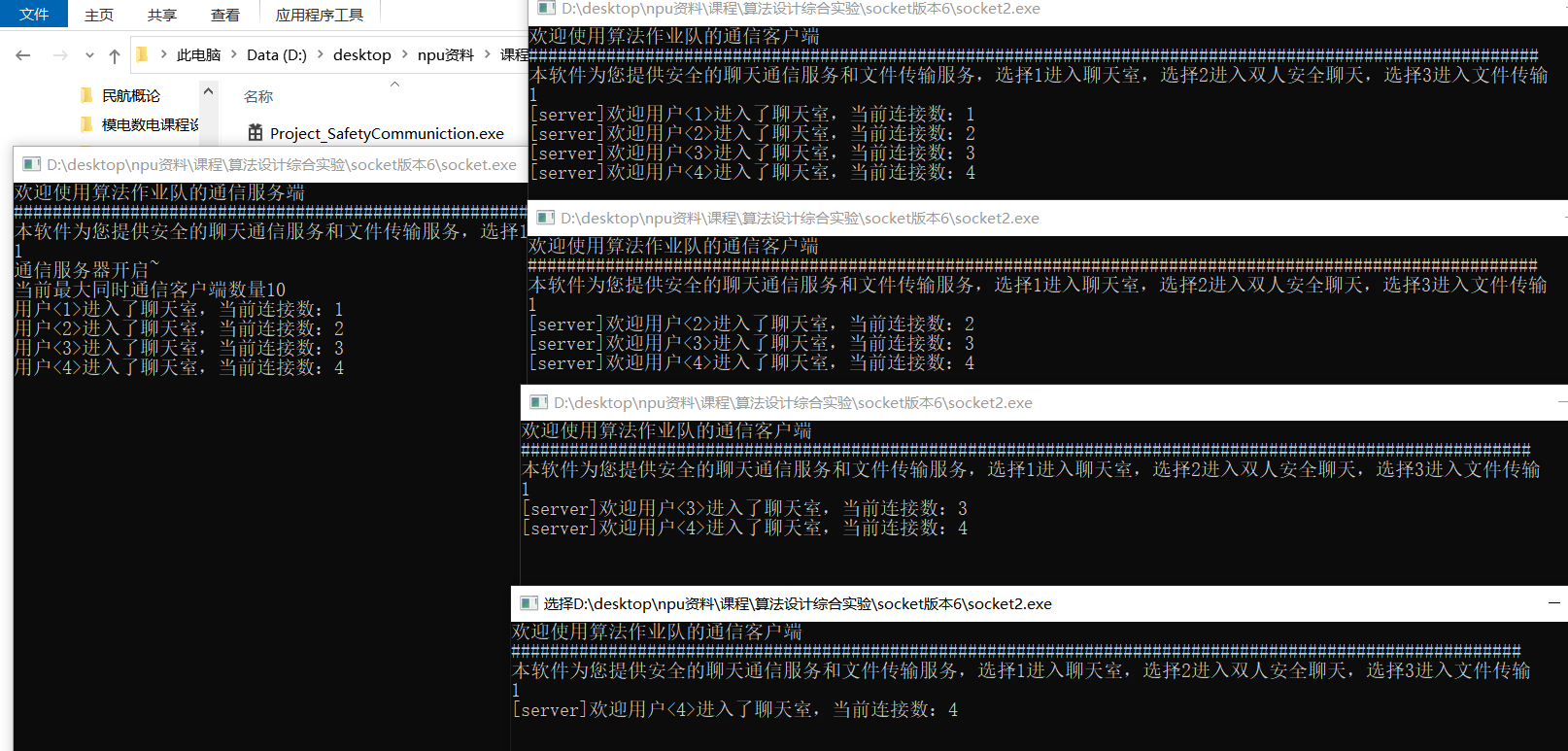
原文件和解压后文件对比：



1. 性能分析及结果

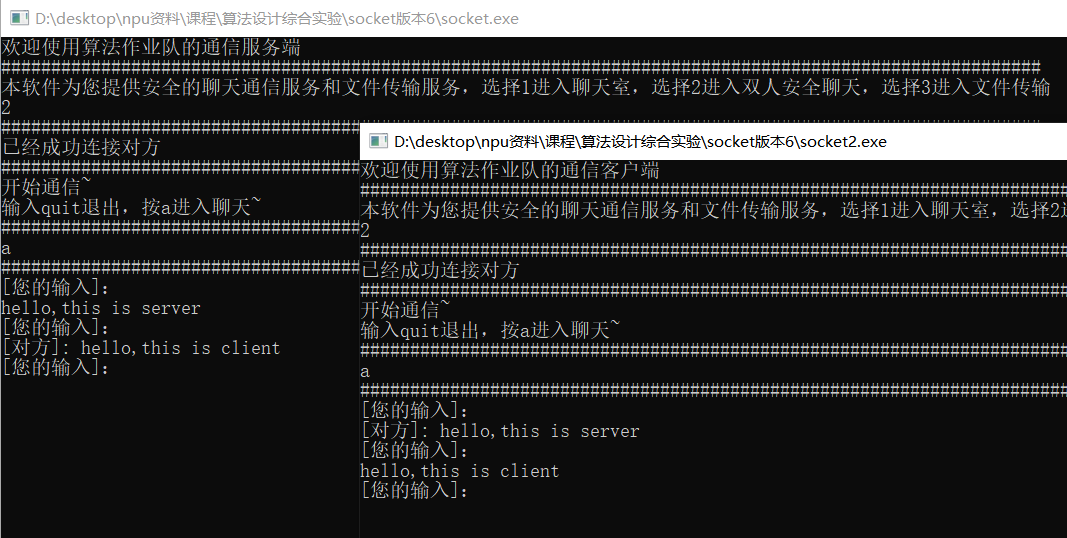
SOCKET编程通信实现了三个功能，功能1需要在服务器开启的情况下同时10个客户端进行通信，加上服务器就是11个机器同时聊天，不安全，无加密和完整性验证，无压缩；功能2是需要在服务器开启的情况下服务器和1个客户端聊天，安全，有加密，有完整性验证，无压缩；功能3是需要在服务器开启的情况下服务器和1个客户端进行文件传输，安全，有加密，有完整性验证，有压缩；

功能一：不安全的多人聊天室测试



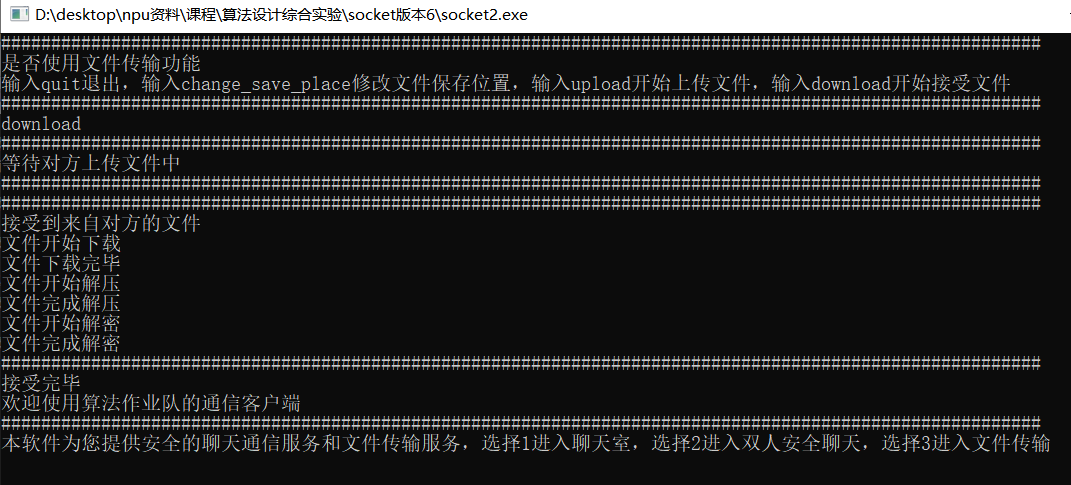
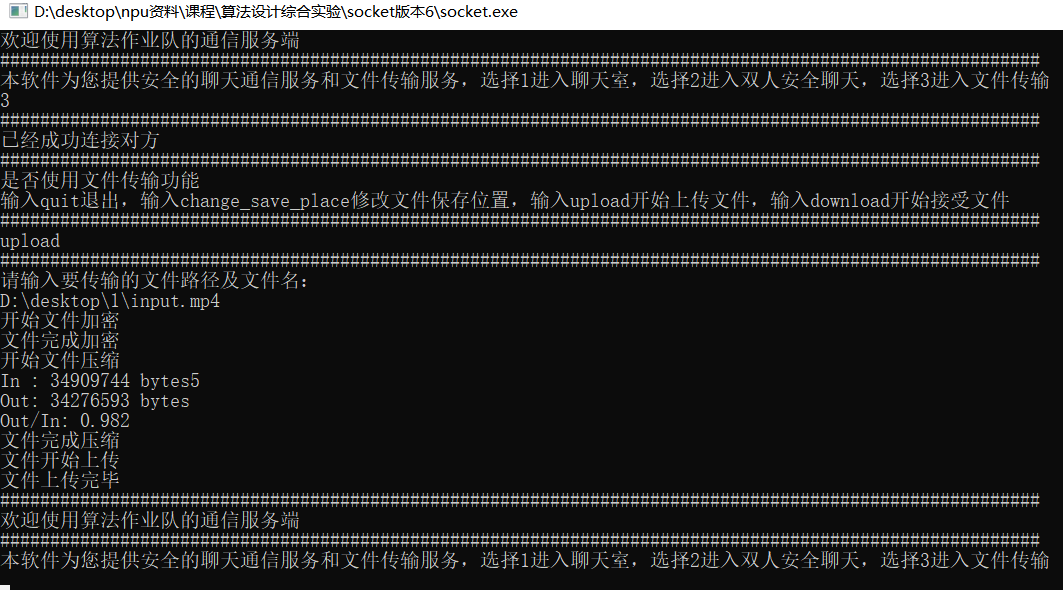


功能二：安全的双人聊天测试



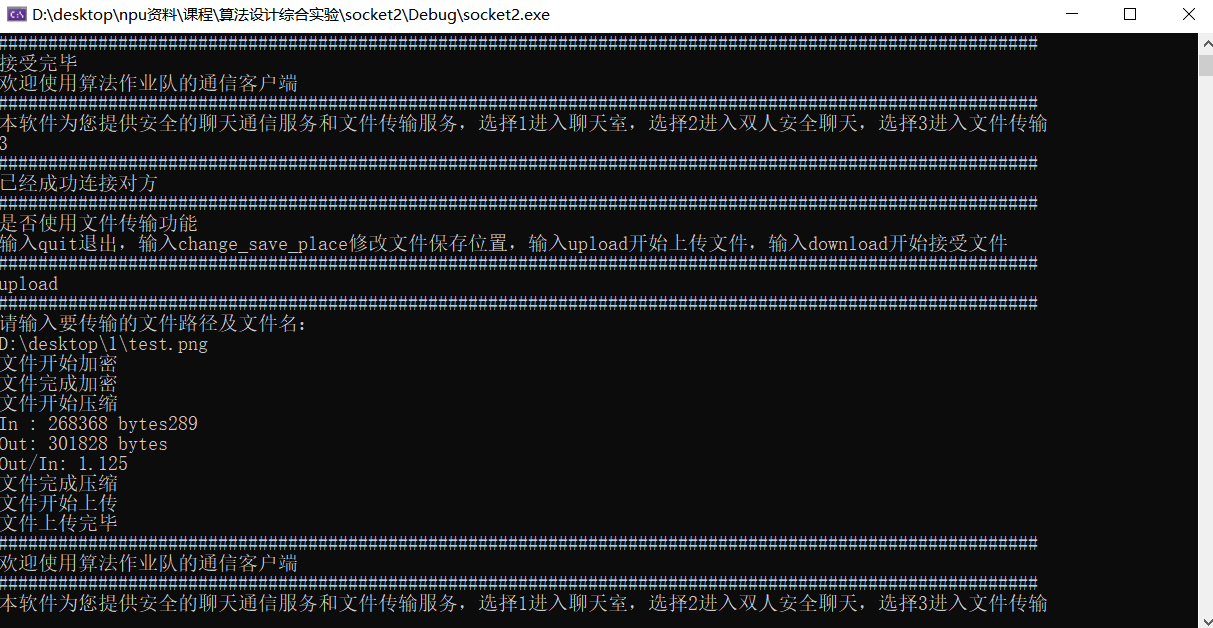
功能三：安全的双人文件传输测试

其一（视频）：

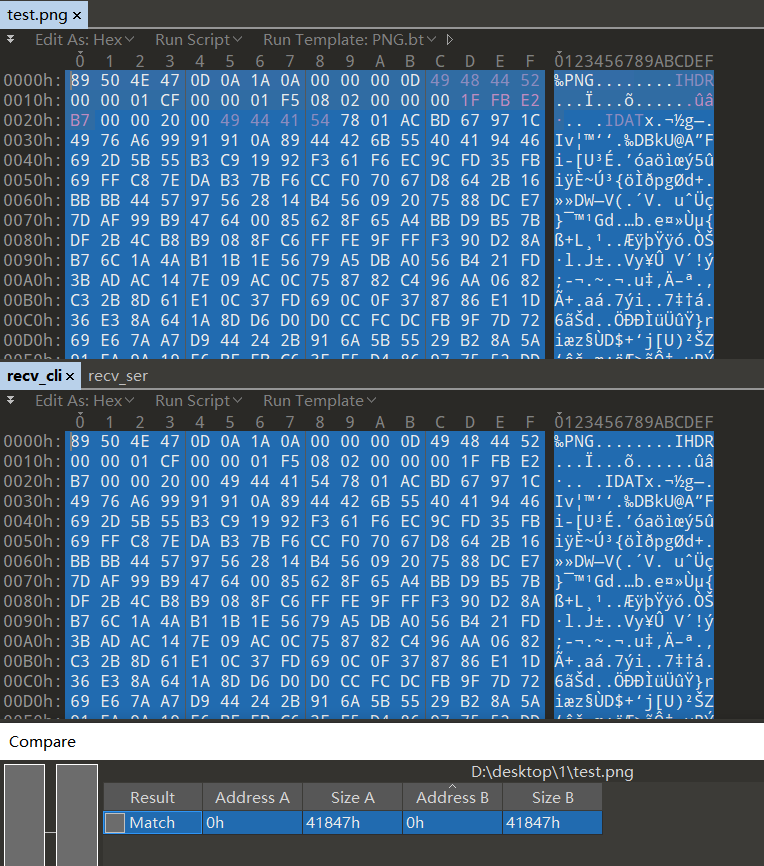


其二（图片）：





文件比较：



客户端图形化界面：

