密码学大作业

1. **通信保密协议的设计**

假设条件：假设通讯双方为A和B，并假设发方拥有自己的RSA公钥PKA和私钥SKA ，同时收方拥有自己的RSA公钥PKB和私钥SKB ，同时收发双方已经通过某种方式知道了双方的公钥。

实现过程中使用了之前编写的生成大素数、RSA加密解密算法、AES加密解密算法，并在这次的作业中利用socket编程使用TCP协议进行双方的通信，通信双方分别是客户端A和服务端B。

**协议流程：**

1. A使用B的RSA公钥PKB和n对AES加解密算法的会话密钥进行加密，之后发送给B。
2. B收到了加密的消息，并用自己的RSA私钥SKB和n进行解密，获得AES加解密算法的会话密钥key1。
3. B利用会话密钥key1，使用AES加密消息“OK”，并发送给A。
4. A使用会话密钥key1，解密接收到的消息，得到了“OK”消息，说明双方交换AES加密解密算法会话密钥成功。
5. 之后双方可以利用会话密钥key1并用AES算法加密消息之后通信：任一方输入要发送的消息，使用AES算法加密，之后发送；接收方收到加密的消息，经过AES算法解密，获得消息内容。
6. **通讯双方程序实现的功能**
7. **利用RSA作业中的生成大素数算法为双方生成公钥和私钥**

先为双方生成A的RSA公钥PKA和私钥SKA ，以及B的RSA公钥PKB和私钥SKB ，并且双方都互相知道对方的公钥。

（1）公钥：生成两个512bit的大素数p和q，n是二者的乘积，即n＝p\*q，使。

为欧拉函数。随机选取正整数e，使其满足，即e和互

素，则将（n，e）作为公钥。

图1－3 子密钥的生成流程

1. 私钥：求出正数d，使其满足，则将（n，d）作为私钥。

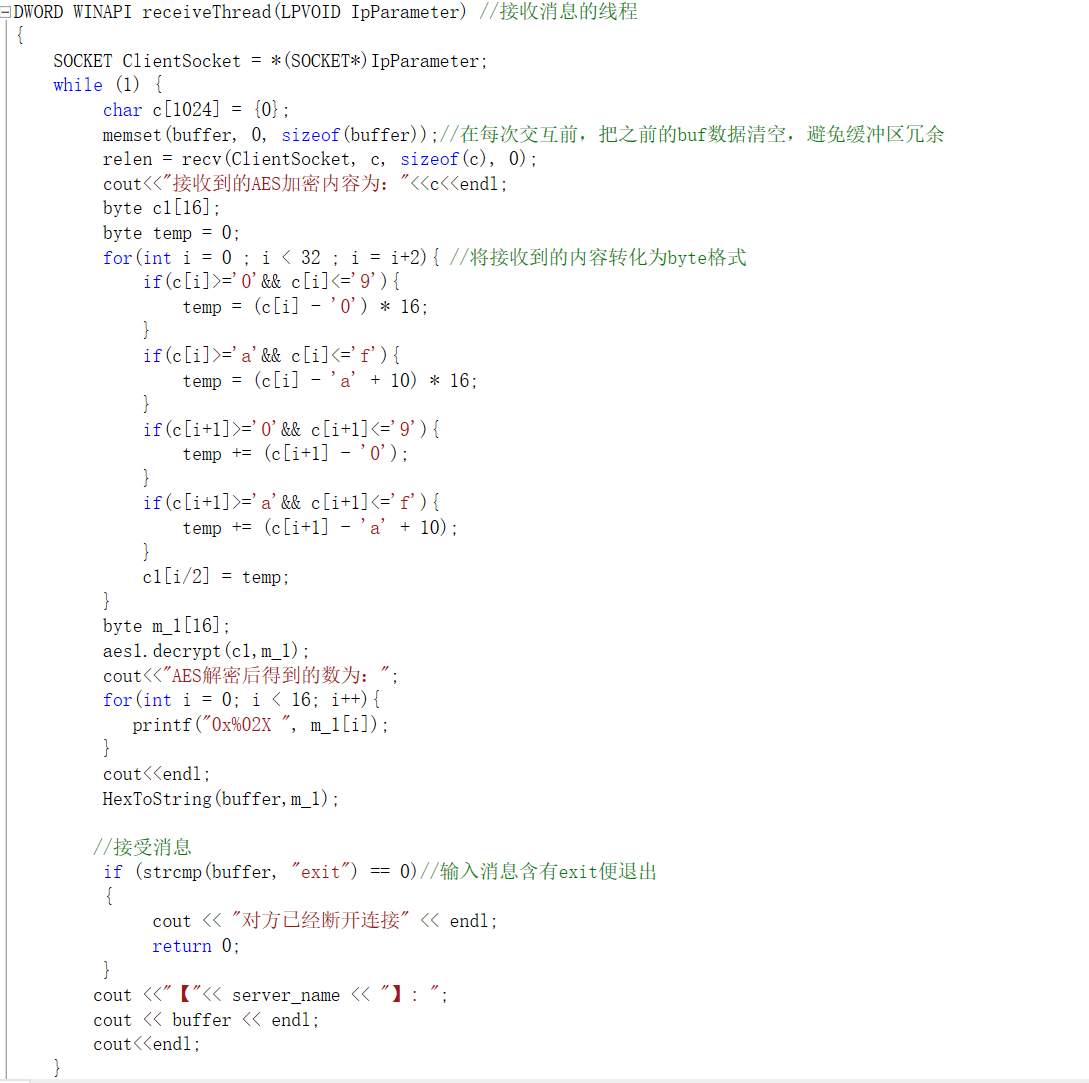
公钥和私钥生成后，利用大数数据结构BigInt存储在双方，以便之后RSA加密解密时使用。

1. **双方通信部分**
2. 首先是双方通信的连接：服务端B监听连接，当客户端A发送连接请求，B监听到请求时，连接成功，连接成功后首先互通双方的名称。
3. 交换密钥的过程：A用B的RSA公钥，利用RSA加密算法对AES会话密钥key1加密，并发送给B。B接收到加密的消息后，用自己的RSA私钥，利用RSA解密算法进行解密，获得AES会话密钥key1。B用AES会话密钥key1，利用AES加密算法加密“OK”，将加密后的消息发送给A。A用key1利用AES解密算法解密后，获得消息“OK”，双方交换密钥的过程结束。
4. 双方通信程序：双方的通信发送消息和接收消息的流程是一样的。都是在主程序中设置一个while循环进行发送消息，并增加一个接收消息的线程，接收消息的线程中也是一个while循环不断循环来接收消息。

发送消息：在while循环中，检测键盘输入消息，输入消息可以是大写字母小写字母或者数字。之后将输入的消息转为16进制数字，并利用AES算法，使用会话密钥key1进行加密，将加密后的16进制密文转化为字符串，并进行发送。如果键盘输入的消息为”exit”，那么程序在3秒之后断开连接，并退出主程序。客户端A的发送消息的主线程如下图所示：



接收消息：在接收消息的线程中，有一个while循环不断的循环检测是否有消息接收。将接收到的消息，先从字符串类型转化为16进制数字，再利用AES算法，使用会话密钥key1进行解密，将解密后的16进制数字明文转化为字符串，获得真实的消息。输出对方的名称+真实的消息。如果解密并转化后的字符串是”exit”，则输出提示“对方已断开连接”，并退出接收消息线程（实际上当知道对方断开连接后，这边也输入”exit”，于是再主程序中，过3秒后断开连接，退出主程序）。客户端A的接收消息的线程如下图所示：



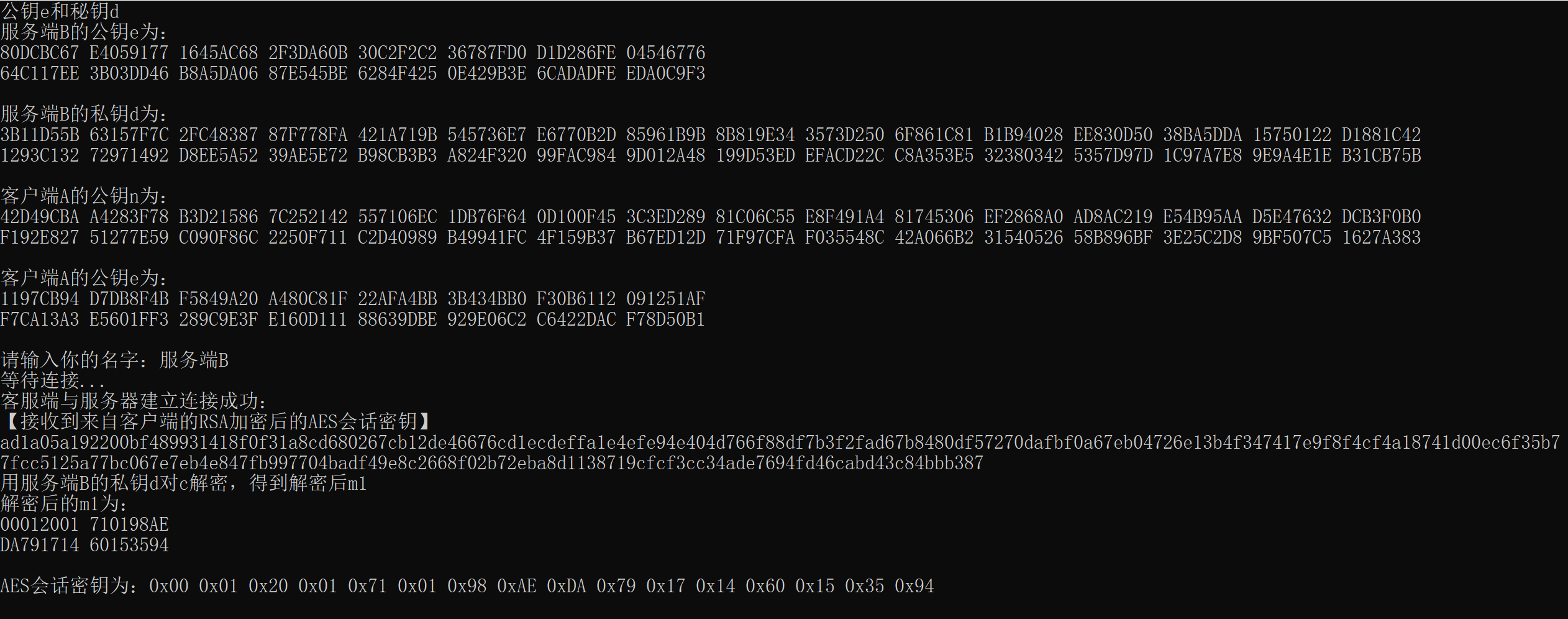
三、结果展示

程序开始，展示双方知道的信息，并输入自己的名称。

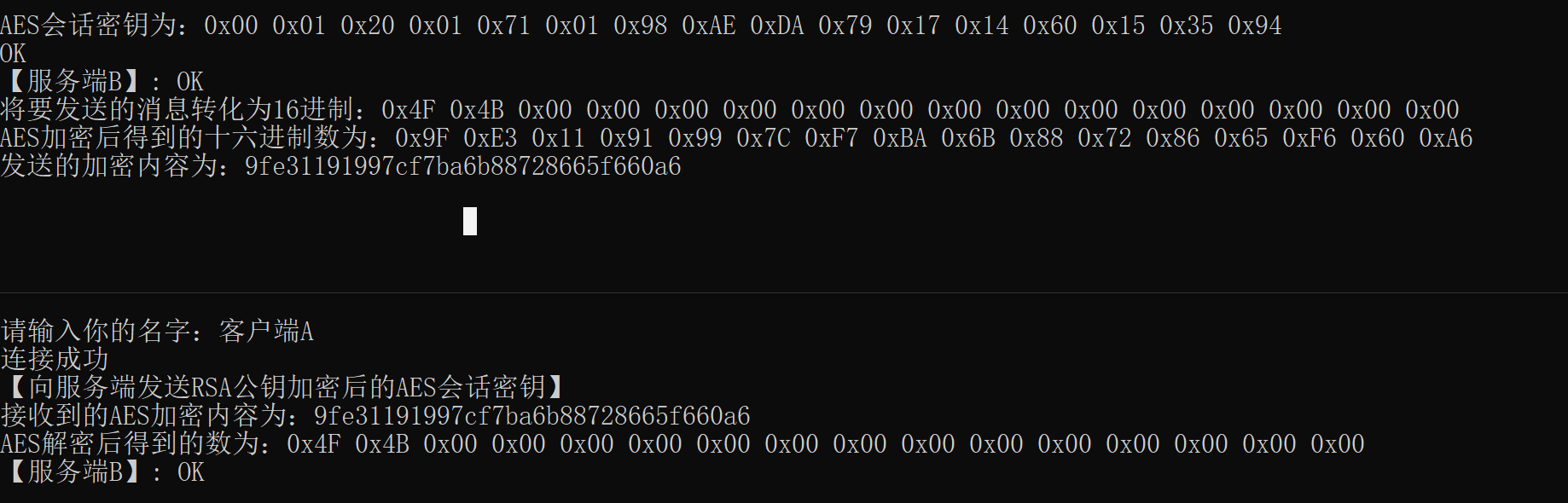
客户端A展示如下：首先，知道的信息有B的RSA公钥和自己的RSA公钥私钥，以及AES会话密钥，输入完名称后，向服务端发送连接请求，连接成功后向B发送用B的RSA公钥加密后的AES会话密钥。



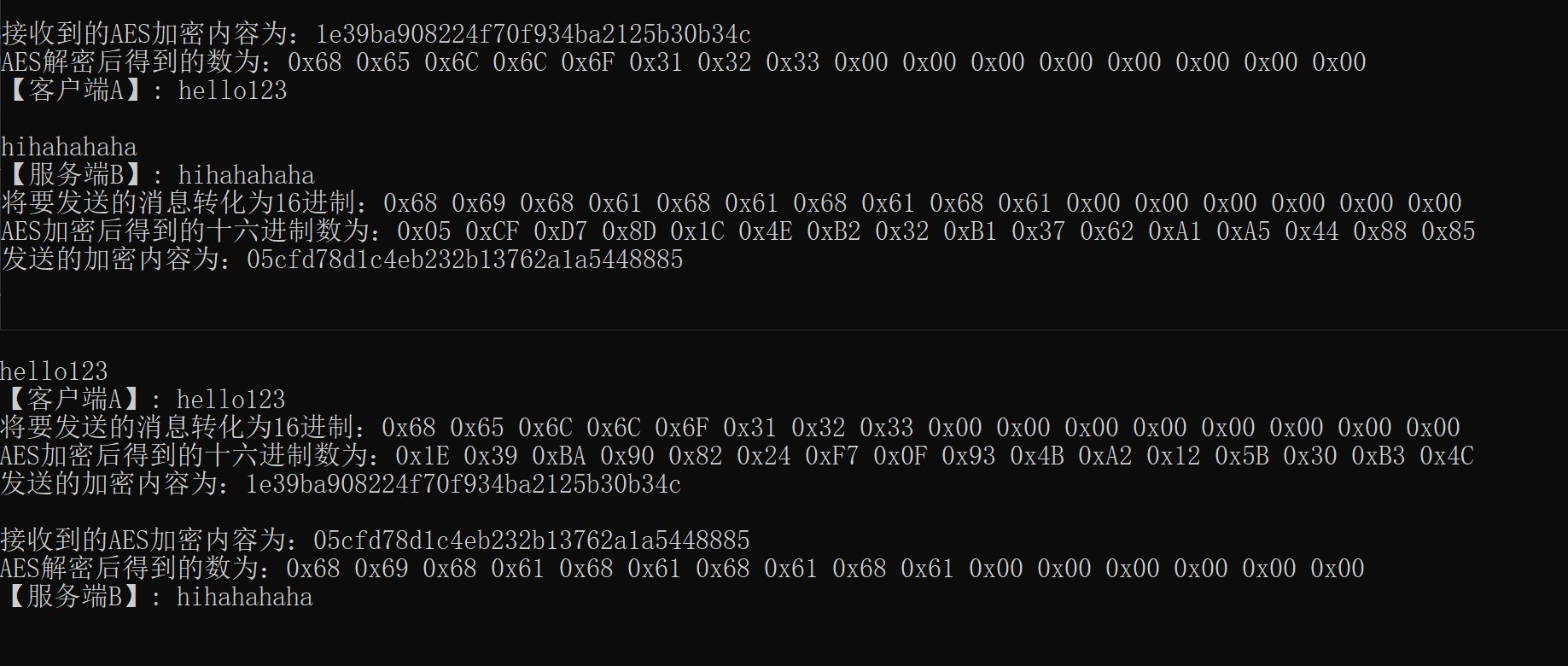
服务端B展示如下：知道自己的RSA公钥私钥，知道客户端A的RSA公钥，在输入完名称后，监听连接，连接成功后，接收来自A发送的RSA加密后的AES会话密钥，利用自己的RSA私钥解密后，获得AES会话密钥内容。



服务端B，输入”OK”，发送时使用AES进行加密：上半部分展示为服务端B，下半部分展示为客户端A。

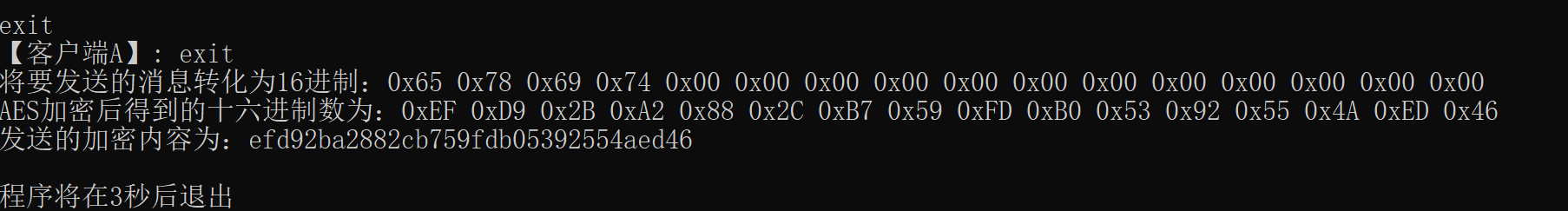


通信内容展示：上半部分展示为服务端B，下半部分展示为客户端A。客户端A这边输入”hello123”,AES加密后发送。服务端B接收到消息，解密得到信息。B输入”hihahahaha”，AES加密后发送。客户端A接收到消息，解密得到信息。



退出程序：一方输入”exit”信息，另一方接收后知道对方下线，也输入”exit”退出程序。

客户端A先输入”exit”:



服务端B也输入”exit”:

