# Network Security

## Homework 4

CHANG LIU

chang.liu@jhu.edu

April. 9, 2012

**1. After writing the program, write out an explanation of how a man in the middle attack would exploit this system.**

Suppose Trudy wishes to intercept the communication between Client and Server. As in our system, the client sends the server its public key during the first handshake. Trudy could intercept the message from client, get the Server's public key and then send a forged message to Server claims to be from the Client, but instead includes Trudy's public key.

The Server believing this public key sent by Trudy to be Client's, encrypts the symmetric key with Trudy's public key and sends the enciphered symmetric key along with any further keys encrypted by the symmetric key back to the Client.

Trudy again intercepts the message from the Server, deciphers the message using her private key, and thus she could get the symmetric key, and further deciphers any other keys in the message that are encrypted by the symmetric key. Trudy can then alter the message or symmetric key if she wants, and re-enciphers it using the public key Client originally sent to Server. When Client receives the newly enciphered message, it believes it came from the Server.

Having the symmetric key and being able to decipher and encrypt any messages between Server and Client using her own private/public key, Trudy can read any messages sent between the Server and Client, and even alter them.

In this way, Trudy exploits this system by the man in the middle attack.

**2. What technology would be needed to make sure that the client and the server know for sure that they are talking to each other and not a man in the middle?**

To make sure the Server and Client are talking to each other and not a man in the middle, we can use the Certificate Authority to safely delivery the public key instead of sending it via an unsecured connection.