ASSIGNMENT IV

Date of evaluation: 27.04.2015, 1.00 pm – 3.0 pm

This programming assignment is based on the extended Needham Schroeder Mediated-Authentication Scheme. Write socket programs that run on three nodes (can be three processes on the same machine also), ***Alice***, ***Bob***, and the ***KDC***. You may use one of C, C++, C#, Python, or Java for your programs.

Assume that Alice initiates the authentication exchange. Please ensure the following.

- The challenges are at 64 bits long.
- The secret key encryption scheme is 3DES.
- You need to set up two keys for each 3DES based secure communication between two parties (Alice and KDC, Bob and KDC, Alice and Bob).
- Use a unique number for identifying a user instead of IP addresses and port numbers.

When the initial two-message handshake is not used the extended version of Needham Schroeder reduces to the original version. For the original version of Needham Schroeder scheme first use the Electronic Code Book (ECB) for encrypting multiple blocks and demonstrate how ***Trudy*** is successful in impersonating Alice by causing a reflection attack. Remove this vulnerability by using Cipher Block Chaining (CBC) instead of ECB. In creating the reflection attack, you can assume that the information that Trudy needs to eavesdrop is available to her (i.e., you can make that information available to Trudy in your program, you do not need to sniff that information in real time).

Include print commands in your code to show

- one successful authentication (extended Needham Schroeder),
- the reflection attack (original Needham Schroeder), and
- the difference in CBC vs ECB outputs for the last two messages (original Needham Schroeder).

For this assignment you could take the help of existing tools such as Openssl for 3DES related functions.