Needham-Schroeder Symmetric Key Protocol establishes a shared session key between two parties on a network with the purpose of protecting further communication between these two parties. In my implementation, we let Alice and Bob represent the two parties wishing to establish communication, and the Key Distribution Center (KDC) acts as the server trusted by both parties with generating and distributing keys. The variables required to initiate and carry out this protocol are as follows:

**IDA** : Alice’s identifier, 16-bit random number in my implementation

**IDB** : Bob’s identifier, similar construction

**N1** : random 32-bit nonce value generated by Alice. Conventionally, nonces are timestamps, but because this code will run so quickly, I use random values to ensure they are different each time.

**N2** : random 32-bit extra nonce generated by KDC to help secure against replay attacks (see Lecture SlideDeck 3.2, slide 15)

**Ka** : private key shared by Alice and the KDC, from Computational Diffie-Hellman (CDH)

**Kb** : private key shared by Bob and the KDC, from instance of CDH

**Ks** : random 10-bit session key generated by the KDC for end use between Alice and Bob