Needham-Schroeder Protocol

Implement the Needham-Schroeder Protocol including three entities Alice (A), Bob(B) and Key Distribution Center (KDC). Assume that there is secure communication between A and KDC, and B and KDC.

a) Register A to KDC where symmetric key is established between A and KDC.
b) Register B to KDC where symmetric key is established between B and KDC.
c) Generate session key between A and B via KDC.
d) A and B should send an acknowledgment message to each other once the session key is established.

Steps for Needham-Schroeder Protocol:

Step 1: $A \rightarrow KDC : A, B, N_A$

Step 2: $KDC \rightarrow A : \{N_A, K_{AB}, B, \{K_{AB}, A\}_{K_B}\}_{K_A}$

Step 3: $A \rightarrow B : \{K_{AB}, A\}_{K_B}$

Step 4: $B \rightarrow A : \{N_B\}_{K_{AB}}$

Step 5: $A \rightarrow B : \{N_B - 1\}_{K_{AB}}$

where K_A: Symmetric key known to A and KDC
K_B: Symmetric key known to B and KDC
K_{AB}: Session key between A and B
N_A: Nonce generated by A
N_B: Nonce generated by B