For next Thursday's class, you'll need to use BAN logic to prove that the following protocol provides mutual authentication. That is, by the end of the protocol,

A believes $A \overset{K}{\leftrightarrow} B$

B believes $A \overset{K}{\leftrightarrow} B$

A believes B believes $A \overset{K}{\leftrightarrow} B$

B believes A believes $A \overset{K}{\leftrightarrow} B$

A believes $\sharp(A \overset{K}{\leftrightarrow} B)$

B believes $\sharp(A \overset{K}{\leftrightarrow} B)$

The protocol to be analyzed is as follows:

$A \rightarrow B : A, N_A$

$B \rightarrow S : B, \{A, N_A, N_B\}_{K_{BS}}$

$S \rightarrow A : \{B, N_A, N_B, K_{AB}\}_{K_{AS}}, \{A, B, N_A, N_B, K_{AB}\}_{K_{BS}}$

$A \rightarrow B : \{A, B, N_A, N_B, K_{AB}\}_{K_{BS}}, \{A, B, N_A, N_B, K_{AB}\}_{K_{AB}}$

$B \rightarrow A : \{A, B, N_A - 1, N_B - 1, K_{AB}\}_{K_{AB}}$

Just follow the same steps as the example in class:

1. List the assumptions. Model these after those used in the proof of the Needham-Schroder secret key protocol discussed in class, without the bogus assumptions.
2. Transform the protocol messages into their logical forms.
3. Apply the rules to each message (and your assumptions) until you have established the desired goals. For each rule, be sure to state what rule it was that you used and where each of the statements above the bar came from (an assumption, a message, or the result of some other rule application).

You won't be required to turn in your solutions, but you should be ready to come to the board and provide a specific part of the solution. Feel free to work in groups, but make sure that you understand your group's solution well enough to present any part of it yourself along with reasonable justifications.