Answer to exercise 2.2

You were asked to consider the Andrew Protocol:

Msg 1. $a \to b : a, \{n_a\}_{shared(a,b)}$
Msg 2. $b \to a : \{n_a + 1, n_b\}_{shared(a,b)}$
Msg 3. $a \to b : \{n_b + 1\}_{shared(a,b)}$
Msg 4. $b \to a : \{k_{ab}, n_c\}_{shared(a,b)}$.

An attack on the Andrew Protocol

One problem with this protocol is that a receives no guarantee of the freshness of k_{ab}.

Suppose the intruder has seen an old run, and remembered the component $\{K_{ab}, N_c\}_{shared(A,B)}$ from message 4, and subsequently compromised the key. Then he can replay this component in a subsequent run:

Msg 1. $A \to B : A, \{N_a\}_{shared(A,B)}$
Msg 2. $B \to A : \{N_a + 1, N_b\}_{shared(A,B)}$
Msg 3. $A \to B : \{N_b + 1\}_{shared(A,B)}$
Msg 4. $B \to I_A : \{K'_{ab}, N'_c\}_{shared(A,B)}$
Msg 4′. $I_B \to A : \{K_{ab}, N_c\}_{shared(A,B)}$.

Another attack on the Andrew Protocol

Another problem with this protocol is a lack of explicitness. If we assume that $shared(A, B) = shared(B, A)$ (i.e. A and B use the same key regardless of who initiates the protocol) then the following "mirror attack" is possible:

Msg α.1. $A \to I_B : A, \{N_a\}_{shared(A,B)}$
Msg β.1. $I_B \to A : B, \{N_a\}_{shared(A,B)}$
Msg β.2. $A \to I_B : \{N_a + 1, N_b\}_{shared(A,B)}$
Msg α.2. $I_B \to A : \{N_a + 1, N_b\}_{shared(A,B)}$
Msg α.3. $A \to I_B : \{N_b + 1\}_{shared(A,B)}$
Msg β.3. $I_B \to A : \{N_b + 1\}_{shared(A,B)}$
Msg β.4. $A \to I_B : \{K_{ab}, N_c\}_{shared(A,B)}$
Msg α.4. $I_B \to A : \{K_{ab}, N_c\}_{shared(A,B)}$

Fixing the Andrew Protocol

- The obvious way to assure a of the freshness of k_{ab} is to include the nonce n_a in the key delivery message in place of n_c.
- The obvious way to prevent the mirror attack is to explictly include an identity in one of the messages.

Msg 1. $a \to b : a, \{n_a, a\}_{shared(a,b)}$
Msg 2. $b \to a : \{n_a + 1, n_b\}_{shared(a,b)}$
Msg 3. $a \to b : \{n_b + 1\}_{shared(a,b)}$
Msg 4. $b \to a : \{k_{ab}, n_a\}_{shared(a,b)}$.