Exercise 4

1. Replace the 2nd message by

\[ A \rightarrow B: \exists, r_B, \Sigma A (B/r_B). \]

2. \[ P^{p-1} = 1 \]
\[ \gcd(k, p-1) = 1 \]
\[ k k^{-1} = 1 \mod (p-1) \]

If \( m_1 = m_2 \mod (p-1) \), then

\[ L^{m_1} = L^{m_2} \]

because

\[ L^{m_1 + r(p-1)} = L^{m_1} (L^{p-1})^r = L^{m_1} \]

Thus \( \lambda = L k^{-1} = (L k)^{p-1} \).
3.  
1. $A \rightarrow C : E_C(A, K_{AB} || N_A)$
2. $C_A \rightarrow B : E_B(A, K'_{AB} || N_A)$
2'. $B \rightarrow C_A : E_A(K_{BA} || N_A, N_B)$
2. $C \rightarrow A : E_A(K_{BA} || N_A, N_B)$
3. $A \rightarrow C : N_B$
3'. $C_A \rightarrow B : N_B$

4. I can force B to reaccept the key again simply by allowing him to receive a sufficiently up-to-date message from S containing the key.

The protocol has been proved correct under assumption that each principal will recognize and reject their own messages. This will prevent these attacks.
5.  
1. \( A \to B: g^{r_A} \)
2. \( B \to A: g^{r_B} \)

\[ K_{AB} = (g^{r_B})^{x_A} = y_B^{r_A} = y_B^{x_A} \]

\[ K_{AB} = g^{r_B} = (y_A^{r_B})^{x_A} = (y_B^{r_A})^{x_B} \]

Forward secrecy?

I: \( x_A \) and \( x_B \) compromised.

Then the attacker knows \( r_A, r_B, g, y_A, y_B \) and can calculate the key. No forward secrecy.

If only \( x_A \) is compromised, but not \( x_B \), then \( A \) cannot compute the key. So partial forward secrecy.
5 (continues).

II: $X_A \times X_B$ compromised. Then $A$ knows

$$X_A (X_B) \rightarrow g^{X_A X_B}$, $g^{X_B X_A}$, $g$. 

$A$ can calculate $(g^{X_B X_A})^{X_A^{-1}} = g^{X_A}$, and similarly $g^{X_B}$, but there is no way to calculate $g^{X_A X_B}$. Thus $II$ has forward secrecy and of course also partial forward secrecy.