Solution to problem 1a [10 points]

We prove Inv (mKey ncf α).

Informal argument [4 points]

It suffices to show that any mKey-term in α is a secure encryption using mKey (because of axiom 2). The messages sent by A or B contain three kinds of fields: (1) ids (A, B); (2) challenges (nL values); and (3) responses (enc(mKey,nR) values). Only the response field involve mKey, and these are secure encryptions using mKey because the attacker cannot write to chan.

Proof [6 points]

The conjunction of C1–C4 is invariantly complete, and C1 implies (mKey ncf α).

| C1 : (y in α.inpts(mKey)) ⇒ (y seu mKey) [2 points] |
| C2 : (y in chan.inpts(mKey)) ⇒ (y seu mKey) [2 points] |
| C3 : A.nL.inpts(mKey) = [] [1 point] |
| C4 : B.nL.inpts(mKey) = [] [1 point] |

Details:

<table>
<thead>
<tr>
<th>initial step</th>
<th>C1</th>
<th>C2</th>
<th>C3</th>
<th>C4</th>
</tr>
</thead>
<tbody>
<tr>
<td>A.1</td>
<td>C2, C3, C1</td>
<td>C2, C3</td>
<td>true</td>
<td>C4</td>
</tr>
<tr>
<td>B.1</td>
<td>C2, C4, C1</td>
<td>C2, C4</td>
<td>C3</td>
<td>true</td>
</tr>
<tr>
<td>B.2</td>
<td>C1</td>
<td>C2</td>
<td>C3</td>
<td>C4</td>
</tr>
</tbody>
</table>
Solution to problem 1b [10 points]

We prove \( \text{Inv} \) for all \( i \) in \( \text{hst.keys: hst[i] = [B,nB,nA] \Rightarrow [A,nA,nB] in hst[0..i-1]} \) 

Informal argument [4 points]

Because the attacker cannot write \( \text{chan} \), the protocol’s behavior is simple to describe:

0. \( A \) sends \([A,B,1]\)
1. \( B \) receives \([A,B,1]\) and sends \([B,A,1,\text{enc(mKey,1)}]\).
2. \( A \) receives above msg, adds \([A,1,1]\) to \( \text{hst} \), and sends \([A,B,\text{enc(mKey,1)}]\) and \([A,B,2]\).
3. \( B \) receives first msg above, adds \([B,1,1]\) to \( \text{hst} \).
4. Repeat steps 1, 2, 3 with the \( nR \) and \( nL \) values in the messages increased by 1.

So just before \([B,nB,nA]\) is added to \( \text{hst} \), the last entry in \( \text{hst} \) is \([A,nA,nB]\).

Proof [6 points]

The conjunction of \( D_0 \) and \( D_1 \) is invariantly complete. Hence \( \text{Inv} D_0 \) holds, and this is what we want to establish.

\[
\begin{align*}
D_0 : & \quad \forall i \in \text{hst.keys: hst[i] = [B,nB,nA] \Rightarrow [A,nA,nB] in hst[0..i-1]} \\
D_1 : & \quad (E_1 \lor E_2 \lor E_3), \text{ where} \\
E_1 : & \quad (B \text{ at } 1 \text{ and chan } = [[A,B,A.nL]]) \quad \text{[2 points]} \\
E_2 : & \quad (B \text{ at } 2 \text{ and } B.nR = A.nL \text{ and chan } = [[B,A,B.nL,\text{enc(mKey,B.nR)}]]) \quad \text{[2 points]} \\
E_3 : & \quad (B \text{ at } 2 \text{ and } B.nR < A.nL \text{ and } ([A,B,nR,B.nL] \text{ in hst}) \text{ and chan } = [[A,B,B.nR,\text{enc(mKey,B.nL)}], [A,B,A.nL]]) \quad \text{[2 points]}
\end{align*}
\]

Details:

\[
\begin{array}{|c|c|c|}
\hline
\text{initial step} & D_0 & D_1 \\
\hline
A.1 & true & \text{true} \\
\hline
B.1 & D_0 & D_1 (E_2 \text{ before ensures } E_3 \text{ after}) \\
\hline
B.2 & D_0, D_1 (E_3 \text{ before}) & D_1 (E_3 \text{ before ensures } E_1 \text{ after}) \\
\hline
\end{array}
\]
Solution to problem 2a [10 points]

We prove $\text{Inv} \langle \text{mKey ncf } \alpha \rangle$.

Informal argument [4 points]

(Almost the same as for problem 1a.)

It suffices to show that any $\text{mKey}$-term in $\alpha$ is a secure encryption using $\text{mKey}$ (because of axiom 2). The messages sent by A or B contain three kinds of fields: (1) ids (A, B); (2) challenges ($nL$ values); and (3) responses ($enc(\text{mKey}, nR)$ values). Only the response field involve $\text{mKey}$, and these are secure encryptions using $\text{mKey}$ because even though the attacker can write to $\text{chan}$, the $\text{mKey}$ values it can write are themselves secure encryptions using $\text{mKey}$.

Proof [6 points]

(Predicates are the same as for problem 1a.)

The conjunction of $C_1$–$C_4$ is invariantly complete, and $C_1$ implies ($\text{mKey ncf } \alpha$).

$$
\begin{align*}
C_1 & : (y \text{ in } \alpha \cdot \text{inpts} (\text{mKey})) \Rightarrow (y \text{ seu } \text{mKey}) & [2 \text{ points}] \\
C_2 & : (y \text{ in } \text{chan. inpts} (\text{mKey})) \Rightarrow (y \text{ seu } \text{mKey}) & [2 \text{ points}] \\
C_3 & : A.nL \cdot \text{inpts} (\text{mKey}) = [] & [1 \text{ point}] \\
C_4 & : B.nL \cdot \text{inpts} (\text{mKey}) = [] & [1 \text{ point}]
\end{align*}
$$

Details: (The only difference from the table in 1a is the “attacker write” row.)

<table>
<thead>
<tr>
<th></th>
<th>$C_1$</th>
<th>$C_2$</th>
<th>$C_3$</th>
<th>$C_4$</th>
</tr>
</thead>
<tbody>
<tr>
<td>initial step</td>
<td>true</td>
<td>true</td>
<td>true</td>
<td>true</td>
</tr>
</tbody>
</table>
| A.1     | $C_2$ | $C_3$ | $C_4$ | true | $C_4$
| B.1     | $C_2$ | $C_3$ | $C_4$ | $C_3$ | true |
| B.2     | $C_2$ | $C_3$ | $C_4$ | $C_4$ |
| attacker write | $C_1$ | $C_2$ | $C_3$ | $C_4$ |

Solution to problem 2b [10 points]

We disprove $\text{Inv}$ forall $i \text{ in hst.keys: } \text{hst}[i] = [B,nB,nA] \Rightarrow [A,nA,nB] \text{ in hst}[0..i-1])$

Informal argument [4 points]

In B’s message, $[B,A,nB,enc(\text{mKey},nA)]$, nA equals nB (assuming the attacker does nothing). So the attacker can make up the response to B without A receiving the message.

Proof [6 points]

Counter-example evolution:

- Initial step
  - After: $[A,B,1]$ in chan; hst = [].
- B.1
  - After: $[B,A,1,enc(\text{mKey},1)]$ in chan; $B.nL = B.nR = 1$; hst = [].
- Attacker, using $enc(\text{mKey},1)$ field in above message, sets chan to $[[B,A,enc(\text{mKey},1)]]$.
- B.2
  - After: $[B,A,1,enc(\text{mKey},1)]$ in chan; hst = $[[B,1,1]]$. Assertion’s predicate not satisfied.
Solution to problem 3 [15 points]

(Taken from my 414 spring 2010 exam 1.)

Part a. [5 points]
- $A$ interacts with CA offline. [2 points]
- $A$ generates its public-key pair [$\text{pub}_A$, $\text{pri}_A$] and gives CA its $\text{pub}_A$. [2 points]
- $A$ gets CA’s public key $\text{pub}_CA$ and (optionally) certificate for $A$ issued by CA, $\text{cert}_A$. [2 points]

Part b. [3 points]
- $C$ can impersonate $A$ to $B$ until $A$’s certificate expires (1 year at worst) [3 points]

Part c. [6 points]
- $A$ interacts offline with CA [2 points]
- $A$ generates a new public key pair (as in part a) [2 points]
- CA adds $A$’s old certificate’s serial number in the next CRL it issues [2 points]
- Assume $B$ uses latest CRL. Then $C$ can impersonate $A$ to $B$ until $A$’s old certificate’s expiry time or until next CRL is issued, which is within 1 hour of contacting CA, whichever is earlier. [2 points]

Part a
- 2 point for missing CA’s public key.
- 1 point for missing certificate.

Part b
- 2 point for not referring explicitly to expiry time

Part c
- 3 point for not using CRL
Solution to problem 4a [5 points]

No, an attacker who can only read cannot obtain data because A and B establish a Diffie-Hellman key.

Solution to problem 4b [10 points]

Yes, an attacker who can read and write chan can obtain data, by doing the classic man-in-middle attack.

- Initial step: \([A,B,A.tL]\) in chan.
- Attacker removes message. Generates random \(Z_{nL}\), sets \(ZtL\) to \(g^{ZnL} \mod p\), sends \([A,B,ZtL]\).
- B.1: sets \(B.key_{DH}\) to \(g^{ZnL} \cdot B.nl\) \(\mod p\), sends \([B,A,B.tL]\).
- Attacker removes message. Sends \([B,A,ZtL]\).
  - Sets \(ZB\) to \(g^{ZnL} \cdot B.nl\) \(\mod p\) (DH key shared with B).
  - Sets \(ZA\) to \(g^{ZnL} \cdot A.nl\) \(\mod p\) (DH key shared with A).
- A.1 sends \([A,B,'DATA',\text{enc}(A.key_{DH}, data)]\).
- Attacker reads message. Uses \(ZA\) to decrypt field 4.