Solution to 1 [20 points]

Solution to part a [10 points]

We prove it.

The predicates below are from homework 5A. $G_1$ is the conjunction of $A_1$ and $A_2$ (5A part 1). $G_1$ is the conjunction of $B_1$ and $B_2$ (5A part 2). $C_2$–$C_5$ are as in 5A part 3.

$G_1$: \((\forall y \in \alpha . \text{inpts}(A.mKey)) \lor (\forall y \in \alpha . \text{inpts}(A.mKey))) \Rightarrow (y \text{ seu } A.mKey)\)

$G_2$: \((\forall y \in \alpha . \text{inpts}(B.mKey)) \lor (\forall y \in \alpha . \text{inpts}(B.mKey))) \Rightarrow (y \text{ seu } B.mKey)\)

$C_2$: \((\forall y \in \alpha . \text{inpts}(A.mKey) \lor \text{chan.inpts}(A.mKey))\)
and \(y = \text{enc}(A.mKey, p) \text{ and p.size} = 4)\)
\(\Rightarrow ([p[2] \text{ ncf } \alpha]) \text{ and } (p[3] \text{ seu } Z.mKeyB \text{ and } p[3] = \text{enc}(Z.mKeyB,[p[2],A]))\)

$C_3$: \((\forall y \in \alpha . \text{inpts}(B.mKey) \lor \text{chan.inpts}(A.mKey))\)
and \(y = \text{enc}(B.mKey, q) \text{ and q.size} = 2)\)
\(\Rightarrow ([q[0] \text{ ncf } \alpha])\)

$C_4$: \((A.kAB \text{ defined}) \land (\forall y \in \alpha . \text{inpts}(A.kAB)))\)
\(\Rightarrow (\forall y \text{ seu } A.kAB) \lor (\forall y \text{ seu } A.mKey) \lor (\forall y \text{ seu } B.mKey)\)

$C_5$: \((B.kAB \text{ defined}) \land (\forall y \in \alpha . \text{inpts}(B.kAB)))\)
\(\Rightarrow (\forall y \text{ seu } B.kAB) \lor (\forall y \text{ seu } A.mKey) \lor (\forall y \text{ seu } B.mKey)\)

Solution to part b [10 points]

We prove it.

The predicates below are from homework 7A (with the same labels).

$D_1$: \((\text{A at } 2) \Rightarrow ([..]A.kAB \text{ not in hst})\)

$D_2$: \((\text{B at } 2) \land (\text{enc}(A.kAB,B.n3-1) \text{ in chan/} \alpha)\)
\(\Rightarrow (|[B,B.kAB] \text{ not in hst}) \land ([A,B.kAB] \text{ in hst})\)

$D_3$: \((\text{A at } 1) \land (\text{enc}(A.mKey,[A.n1,B,k,tkt]) \text{ in chan/} \alpha)\)
\(\Rightarrow ([..]k \text{ not in hst})\)

$D_4$: \((A.mKey \text{ ncf } \alpha) \land (B.mKey \text{ ncf } \alpha)\)
and \((A.kAB \text{ defined}) \Rightarrow (A.kAB \text{ ncf } \alpha)\)
and \((B.kAB \text{ defined}) \Rightarrow (B.kAB \text{ ncf } \alpha)\)

$F_0$: \((\forall i \in \text{hst.keys, } i \neq 0 \land \text{hst}[i] = [B,k]) \Rightarrow \text{hst}[i-1] = [A,k]\)

$F_1$: \((\text{B at } 2) \land (\text{enc}(A.kAB,B.n3-1) \text{ in chan/} \alpha)\)
\(\Rightarrow \text{hst.last} = [A,B.kAB]\)

$F_2$: \((\text{A at } 2) \land (\text{enc}(A.kAB,[A.n2-1,.]) \text{ in chan/} \alpha)\)
\(\Rightarrow (\text{enc}([..],B.n3-1) \text{ not in chan/} \alpha)\)
Solution to 2 [20 points]

We disprove both assertions.

Counter-example evolution (from homework 7B)

1. Initial step: A send \([A,Z,B,n1]\).

2. Z.1 step: receive \([A,Z,B,n1]\), send \([Z,A,\text{enc}(kAZ,[n1,B,k,tkt])]\) with \(tkt = \text{enc}(kBZ,[k,A])\).

   After: \(A.kAB = k\)

4. Attacker getPwdA: add \(kAZ\) to \(\alpha\), set A.mKey and Z.mKeyA to random value.
   After: \(kAZ\) and \([Z,A,\text{enc}(kAZ,[n1,B,k,tkt])]\) are in \(\alpha\). From these attacker gets \([n1,B,k,tkt]\), from which it gets \(k\).

   \textbf{Part a predicate does not hold in this state}

4. Attacker: send message \([A,B,tkt,\text{enc}(k,9)]\). B.1: receive above message, send message \([B,A,\text{enc}(k,[9,n3])]\).
   Attacker: receive above message, send message \([A,B,\text{enc}(k,n3−1)]\).
   B.2: receive above message, add \([B,k]\) to hst.

   \textbf{Part b predicate does not hold in this state}
Solution to 3 [10 points]

Solution to part a [2 points]

Attacker cannot obtain \( W \) by offline-dictionary attack because the only quantities that are encrypted using \( W \), i.e., \( \text{enc}(W,c_B) \) and \( \text{enc}(W,n_B+1) \), are themselves encrypted using the Diffie-Hellman key, which is a strong key.

Solution to part b [8 points]

Attacker can obtain \( W \) by offline-dictionary. First, it does the classic man-in-the-middle attack, from which it obtains \( \text{enc}(W,c_B+1) \) and \( \text{enc}(W,c_B) \). It can then do an offline-dictionary attack on these two quantities.

Details of the man-in-the-middle attack [4 points]:

- It intercepts \( A \)'s initial message, say \([A,B,1,t_A]\).
- It generates a DH random number \( n_Z \) and sets \( t_Z = g^{n_Z} \mod p \). It sends \([A,B,1,t_Z]\). It constructs the DH key shared with \( A \), i.e., \( k_{AZ} = t_A^{n_Z} \mod p \).
- It intercepts \( B \)'s response message, say \([B,A,t_B,\text{enc}(k_BZ,\text{enc}(W,c_B))]\).
- It constructs the DH key shared with \( B \), i.e., \( k_{BZ} = t_B^{n_Z} \mod p \). It decrypts the last field of the message using \( k_{BZ} \) and then encrypts it with \( k_{AZ} \). It sends \([B,A,t_Z,\text{enc}(k_AZ,\text{enc}(W,c_B))]\). It now has \( \text{enc}(W,c_B) \).
- It intercepts \( A \)'s response message, say \([A,B,\text{enc}(k_AZ,\text{enc}(W,c_B+1))]\).
- It decrypts the last field of the message using \( k_{AZ} \), thereby obtaining \( \text{enc}(W,c_B+1) \).
- It now has \( \text{enc}(W,c_B+1) \).

Details of the dictionary attack [4 points]:

- Let \( p = \text{enc}(W,c_B+1) \) and \( q = \text{enc}(W,c_B) \).
  - For candidate password, obtain candidate key \( c_W \) and check for \( \text{dec}(c_W,p) = \text{dec}(c_W,q)+1 \) until match.
Solution to 4 [10 points]

**Part a:** A authenticates B when its ssl receives $\text{enc}(K, [\text{another keyed hash of handshake}])$. B authenticates A at end of authentication handshake involving $\mathcal{W}$.

**Part b:** No. Messages between client A and its ssl are not encrypted.

**Part c:** A tcp message in the data exchange phase would have:
- ip/tcp header: not encrypted.
- ssl header: encrypted.
- ssl payload: encrypted.

**Part c:** No. Because the data between ssl and tcp are encrypted.