

In each problem below:

- Program Protocol refers to the program defined in the note titled *Modeling and Analyzing Authentication Protocols*.
- If you answer that the assertion holds, come up with an argument why every state of every evolution satisfies the assertion's predicate.
- If you answer that the assertion does not hold, come up with a counter-example evolution, i.e., an evolution that ends in a state that does not satisfy the assertion's predicate.

Problem 1. [15 points]

Does assertion $Inv B_3$ hold for program Protocol, where

$$B_3 : (\text{exists}(A.S) \Rightarrow \psi(A.S))$$

Problem 2. [15 points].

Does assertion $Inv B_4$ hold for Protocol, where

$$B_4 : \text{forall}(i \text{ in } \text{hst.keys}: [B,S] = \text{hst}[i] \Rightarrow ([A,S] \text{ in } \text{hst}[0..i-1]))$$