Topics in Concurrency

This question assumes familiarity with the process language SPL and its event-based semantics. In the following SPL process, Auth, agents can behave as initiator or responder in parallel with an attacker Spy. Letting \( A \) and \( B \) range over agent names, define

\[
\text{Init}(A, B) \equiv \text{out new } x \{x, A\}_{P_{ub}(B)}. \text{in}\{x\}_{P_{ub}(A)}. \text{nil}
\]

\[
\text{Resp}(B) \equiv \text{in}\{x, X\}_{P_{ub}(B)}. \text{out}\{x\}_{P_{ub}(X)}. \text{nil}
\]

\[
\text{Auth} \equiv \parallel_{i \in \{\text{init}, \text{resp}, \text{spy}\}} P_{i}
\]

where

\[
P_{\text{init}} \equiv \parallel_{A, B} \text{Init}(A, B), \quad P_{\text{resp}} \equiv \parallel_{A!\text{Resp}(A)}, \quad \text{and } P_{\text{spy}} \equiv !\text{Spy}
\]

(a) Explain briefly and informally the behaviour of \( \text{Init}(A, B) \) and \( \text{Resp}(B) \), for agent names \( A \) and \( B \). Describe diagrammatically the reachable events of \( \text{Init}(A, B) \) and \( \text{Resp}(B) \), taking care to specify the pre- and postconditions, and actions of the events. [5 marks]

(b) Write down an SPL process for the attacker Spy; the process should be able to compose, decompose, encrypt under public keys, and decrypt with leaked private keys. Draw the reachable events of Spy. [5 marks]

Assume a sequence of event-transitions

\[
\langle \text{Auth}, s_0, t_0 \rangle \xrightarrow{e_1} \cdots \langle p_{r-1}, s_{r-1}, t_{r-1} \rangle \xrightarrow{e_r} \langle p_r, s_r, t_r \rangle \cdots
\]

from the configuration \( \langle \text{Auth}, s_0, t_0 \rangle \), of which it is assumed that the names in \( \text{Auth} \) and the output messages \( t_0 \) are included in the name-set \( s_0 \). Suppose that the event \( e_r \) is the input of a message \( \{m\}_{P_{ub}(A)} \) by agent \( A \) as initiator. Define a property of subsets of messages \( t \) by

\[
Q(t) \text{ iff } \forall M \in t. \ m \sqsubset M \Rightarrow \{m, A\}_{P_{ub}(B)} \sqsubseteq M,
\]

where, for instance, \( m \sqsubset M \) means \( m \) is a submessage of \( M \).

(c) Explain briefly why \( Q(t_0) \) is true and \( Q(t_{r-1}) \) is false. [6 marks]

(d) Describe, without proof, the possible form(s) of the earliest event \( e_i \) for which \( Q(t_{i-1}) \) is true while \( Q(t_i) \) is false. [4 marks]