2002 Paper 9 Question 15

Topics in Concurrency

This question assumes familiarity with the process language **SPL** and its event-based semantics. Suppose that there are three agents A, B, S which run at most once (so with no replication) according to the scheme:

$$
\begin{aligned}
A &\to B: \ A \\
B &\to A: \ n \quad \text{(a nonce)} \\
A &\to B: \ \{n\}_{Key(A,S)} \\
B &\to S: \ \{A,\ \{n\}_{Key(A,S)}\}_{Key(B,S)} \\
S &\to B: \ \{A,\ n\}_{Key(B,S)}
\end{aligned}
$$

The symmetric key $Key(A, S)$ is shared between A and S, and the symmetric key $Key(B, S)$ between B and S.

(a) Express the agents A, B and S as processes in **SPL**. [3 marks]

(b) Describe diagrammatically the reachable events of A, B and S, taking care to specify the pre- and postconditions, and actions of the events (you may, however, omit descriptions of the control conditions). [5 marks]

(c) The agents communicate in the presence of an attacker which can decrypt and encrypt messages with available keys, and compose and decompose messages. Draw the four kinds of events (decryption, encryption, composition, decomposition), taking care to specify the nature of their pre- and postconditions. [2 marks]

Let P be the Petri net obtained as the union of the events of A, B, S and the attacker.

(d) Let $Q(\mathcal{M})$ be the property of net P's markings $\mathcal{M}$ which holds when no output message in $\mathcal{M}$ has either key $Key(A, S)$ or $Key(B, S)$ as a submessage. Explain why the property Q holds at all reachable markings of P provided it holds at its initial marking. [6 marks]

(e) Assume that Q holds at the initial marking. Draw, without proof, the dependency on events of agents A, B and S which shows that if B inputs a message $\{A,\ n\}_{Key(B,S)}$, then A has previously input a message n. [4 marks]