12 Topics in Concurrency (JMH)

This question is on an authentication protocol using a key server and symmetric keys. $Key(X,Y)$ represents the symmetric key used to encrypt messages sent by $X$ to $Y$, and symbols $K$ and $K'$ are used as variables over keys. SPL terms representing a key server $S$, an initiator $A$ and responder $B$ are:

\[
S = !(in \{X,Y\}_{Key(X,S)}) \cdot out \{Key(X,Y), Key(Y,X), Y\}_{Key(S,X)}
\]
\[
A = out \{A,B\}_{Key(A,S)} \cdot in \{K,K',B\}_{Key(S,A)} \cdot out \{m\}_K \cdot in \{m,m\}_{K'}
\]
\[
B = out \{B,A\}_{Key(B,S)} \cdot in \{K',K,A\}_{Key(S,B)} \cdot in \{\psi\}_K \cdot out \{\psi,\psi\}_{K'}
\]

(a) (i) The capabilities assumed of an attacker when public-key cryptography is used for authentication, as when studying the Needham-Schröder-Lowe protocol, are that it can pair messages, split paired messages, encrypt messages under a public key and decrypt messages under a public key if it has access to the private key.

Give four SPL processes $Spy_1, \ldots, Spy_4$ representing these capabilities. [4 marks]

(ii) Give a further two processes $Spy_5, Spy_6$ representing the capability of an attacker to encrypt and decrypt messages when symmetric-key cryptography is used. [2 marks]

(b) Let $P_{Spy} = !(\big|_{i \in \{1,\ldots,6\}} Spy_i)$. Draw the events of the Petri net for

$$P_{Spy} \parallel S \parallel A \parallel B.$$ 

For $P_{Spy}$, only show those from $Spy_5$ and $Spy_6$. [7 marks]

(c) Secrecy of the message $m$ can be viewed as $m$ never being output directly to the network by either the participants in the protocol or the attacker.

Give a reasonable general condition on the set of messages initially assumed to have been output to the network for which secrecy of $m$ holds. You may assume that if $Key(X,Y) = Key(X',Y')$ then $X = X'$ and $Y = Y'$.

Describe the principles underlying a proof of the secrecy of the message $m$. [7 marks]