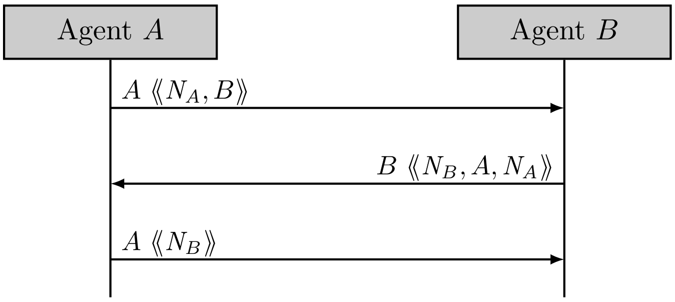
3 Protocol Verification

Consider the following protocol where $X\ \langle\!\langle M \rangle\!\rangle$ denotes a message M digitally signed by agent X:


Agent A
Agent B
$A\ \langle\!\langle N_A, B \rangle\!\rangle$
$B\ \langle\!\langle N_B, A, N_A \rangle\!\rangle$
$A\ \langle\!\langle N_B \rangle\!\rangle$

The aim of the protocol is to establish authentication between two agents. In particular, at the end of the protocol, agent B needs to be sure that nonce N_A was indeed send by agent A and also not replayed by someone else.

3.1 Tasks

T3.1 Formalize the protocol in OFMC.

T3.2 State the security property required and formalize it as a goal in OFMC.

T3.3 The protocol does not meet its goal. Provide a counterexample.

T3.4 One simple fix is to encrypt all the messages. Provide an alternative fix of the protocol and verify in OFMC that the property now holds.