INTRODUCTION TO COMPUTATIONAL LOGIC
HOMEWORK 5
DUE DATE: DECEMBER 16, 2020

In this homework, we will build a NuSMV model to reconstruct the man-in-the-middle attack to the Needham-Schroeder authentication protocol. Consider a simplified public-key Needham-Schroeder protocol:

(1) $A \to B$: $\{N_a, A\}_{K_b}$
(2) $B \to A$: $\{N_a, N_b\}_{K_a}$
(3) $A \to B$: $\{N_b\}_{K_b}$

where N_a, N_b are the nonces of A, B, and K_a, K_b are the public keys of A, B respectively. Messages encrypted by a party's public key can only be decrypted by the party. At Step (1), A initiates the protocol by sending a nonce and its identity (encrypted by B's public key) to B. Using its private key, B deciphers the message and gets A's identity. At Step (2), B sends A's and its nonces (encrypted by A's public key) back to A. Using its private key, A decodes the message and checks its nonce is returned. At Step (3), A returns B's nonce (encrypted by B's public key) back to B.

Here is the man-in-the-middle attack to the simplified protocol:

(1A) $A \to E$: $\{N_a, A\}_{K_e}$ (A wants to talk to E)
(1B) $E \to B$: $\{N_a, A\}_{K_b}$ (E wants to convince B that it is A)
(2B) $B \to E$: $\{N_a, N_b\}_{K_a}$ (B returns nonces encrypted by K_a)
(2A) $E \to A$: $\{N_a, N_b\}_{K_a}$ (E forwards the encrypted message to A)
(3A) $A \to E$: $\{N_b\}_{K_e}$ (A confirms it is talking to E)
(3B) $E \to B$: $\{N_b\}_{K_b}$ (E returns B's nonce back)

The NuSMV source code (http://www.iis.sinica.edu.tw/~bywang/courses/comp-logic/hw3-1.smv) contains a model for the Needham-Schroeder protocol.

When the attack was found, a fix was proposed to prevent the attack:

(1) $A \to B$: $\{N_a, A\}_{K_b}$
(2) $B \to A$: $\{N_a, N_b, B\}_{K_a}$
(3) $A \to B$: $\{N_b\}_{K_b}$

In Step (2) of the Needham-Schroeder-Lowe protocol, B sends its identity along with the nonces back to A.

For this homework, please turn in two NuSMV files.

(1) Please modify the NuSMV module `eve` to model the attacker and witness the man-in-the-middle attack.
(2) Please add the fix to your NuSMV source code and check if the fix prevents the attack.