Proverif Exercises

Deadline: May 10, 2023. 2359 hrs

1. Consider the following protocol.

$$\begin{array}{lll} 1. & A \rightarrow B: & \{\!\![\, \{\!\![\, \langle \mathsf{pk}_a, \{\!\![n]\!\!\}_{\mathsf{pk}_b} \rangle \,]\!\!\}_{\mathsf{pk}_b} \,]\!\!\}_{\mathsf{pk}_b} \\ 2. & B \rightarrow A: & \{\!\![\, \langle \mathsf{pk}_b, n \rangle \,]\!\!\}_{\mathsf{pk}_a} \end{array}$$

   A sends to be a fresh nonce *n*, buried under three levels of encryption using the public key of *B*. She also adds her identity (via her public key) embedded in the second level of encryption. *B* unlocks thrice to retrieve *n*, and sends it back to *A*, along with her own identity, encrypted in *A*'s public key.

   Assume that *U* and *V* are agents, whose secret keys are not known to the intruder. Assume *U* generates a fresh *z* and sends to *V*. *z* is leaked to the intruder by the following attack. *U*! means a message send by *U*, *V*! is a message send by *V*, ?*V* is a receive by *V*. pk_i is a public key whose secret key is known to the intruder.

$$\begin{array}{lll} U! & : & \{\!\![\, \{\!\![\, \langle \mathsf{pk}_u, \{\!\![z]\!\!\}_{\mathsf{pk}_v} \rangle \,]\!\!\}_{\mathsf{pk}_v} \,]\!\!\}_{\mathsf{pk}_v} \\ ?V & : & \{\!\![\, \{\!\![\, \langle \mathsf{pk}_i, \{\!\![\, \{\!\![\, \langle \mathsf{pk}_u, \{\!\![z]\!\!\}_{\mathsf{pk}_v} \rangle \,]\!\!\}_{\mathsf{pk}_v} \,]\!\!\}_{\mathsf{pk}_v} \rangle \,]\!\!\}_{\mathsf{pk}_v} \,]\!\!\}_{\mathsf{pk}_v} \\ V! & : & \{\!\![\, \langle \mathsf{pk}_v, \{\!\![\, \langle \mathsf{pk}_u, \{\!\![z]\!\!\}_{\mathsf{pk}_v} \rangle \,]\!\!\}_{\mathsf{pk}_v} \rangle \,]\!\!\}_{\mathsf{pk}_i} \\ ?V & : & \{\!\![\, \{\!\![\, \langle \mathsf{pk}_i, \{\!\![\, \langle \mathsf{pk}_u, \{\!\![z]\!\!\}_{\mathsf{pk}_v} \rangle \,]\!\!\}_{\mathsf{pk}_v} \rangle \,]\!\!\}_{\mathsf{pk}_v} \,]\!\!\}_{\mathsf{pk}_v} \\ V! & : & \{\!\![\, \langle \mathsf{pk}_v, \langle \mathsf{pk}_u, \{\!\![z]\!\!\}_{\mathsf{pk}_v} \rangle \rangle \,]\!\!\}_{\mathsf{pk}_i} \\ ?V & : & \{\!\![\, \{\!\![\, \langle \mathsf{pk}_i, \{\!\![z]\!\!\}_{\mathsf{pk}_v} \rangle \,]\!\!\}_{\mathsf{pk}_v} \,]\!\!\}_{\mathsf{pk}_v} \\ V! & : & \{\!\![\, \langle \mathsf{pk}_v, z \rangle \,]\!\!\}_{\mathsf{pk}_i} \end{array}$$

   At the end of this attack, the intruder knows *z*. Attached is the file `lockthrice.pv`, which has code partially filled in. Specifically, we have added the overall process and declared various events. Complete the description of the two roles, and add a query whose violation happens due to the above attack. The attack should at least contain the above pattern – it could contain a few other communications too. Submit the completed Proverif file and the PDF containing the graph of the attack trace.

2. In the file `rpc.pv`, we have outlined a Remote Procedure Call protocol. *A* sends to *B* a message *msg*, and *B* responds with *f*(*msg*), where *f* is a remote procedure (this means that *A* cannot use *f* in its own protocol – either in the messages or tests). The aim of this exercise is to complete the description of the *A* and *B* roles, in such a manner that the queries in the file give the expected results. Submit the completed Proverif file and four PDFs, each containing a graph of an attack trace violating each of the properties.