Ne twork Security Technology Spring, 2019
Tutorial 5, Week 6 (April 3) LIU Zhen
Due Date: April 10

Questions:

1. **Key Exchange** Consider the following protocol, where E is a symmetric key encryption scheme, and K is computed as $K = g^{ab}$.

$$\begin{array}{lcll} A & \rightarrow & B & : \text{ “I'm Alice”, } g^a \\ A & \leftarrow & B & : \text{ “Bob”, } g^b, E_K([g^a, g^b]_{\text{Bob}}) \\ A & \rightarrow & B & : \text{ “Alice”, } E_K([g^a, g^b]_{\text{Alice}}) \end{array}$$

   (a) What is the long-term secret of this scheme?

   (b) Does the protocol support forward secrecy?

2. **Authentication** Consider the following protocol, where E is a symmetric key encryption scheme and K is a long-term symmetric key shared between A and B.

$$\begin{array}{lcll} A & \rightarrow & B & : \text{ “Alice”, } R_1 \\ A & \leftarrow & B & : R_2, E_K(R_1) \\ A & \rightarrow & B & : E_K(R_2) \end{array}$$

   (a) Does the scheme support session key establishment? If not, modify the protocol so that it does.

   (b) Does your protocol proposed in (a) support Perfect Forward Secrecy? If not, modify it so it supports PFS without adding any new encryption, digital signature or additional message flows.