Homework 2

Problem 1 (34 points). One weakness of the “Wide-Mouth Frog” protocol is that it relies on Alice to generate the symmetric encryption key that Alice and Bob will then use to communicate. This is not always reasonable as Alice is only a user who may generate the key in an insecure manner. The best candidate for generating the key \( K \) is Trent, the trusted third party.

Describe the simplest way to modify the “Wide-Mouth Frog” protocol to enable Trent to generate the symmetric key \( K \), instead of Alice. Do not copy the Yahalom or any of the other authentication and key exchange protocols.

Problem 2, (33 points)
(a - 23 points) Remember the Needham Schroeder protocol. The protocol has a weakness when an old session key \( K \), shared by \( A \) and \( B \) is compromised. That is, assume the attacker \( M \) gets hold of an old session key \( K \). \( M \) can then launch a successful attack. All he has to do is to capture \( A \)’s message to \( B \) in step 5:

\[ E_B(K, A). \]

Then, using knowledge of the old key \( K \) and the above message, \( M \) can contact \( B \) (in the Needham Schroeder protocol) and pretend to be \( A \). Show how this can be done, through the sequence of steps of the attack.

(b - 10 points) Show how to use timestamps to prevent this attack.

Problem 3. (33 points)
In the “Public Key Authority Use (Needham-Schroeder with Public Keys)” slide, show how to modify the protocol to enable Alice and Bob to also establish a session key.

Hint: The modifications should occur in steps 6 and 7 of the protocol.