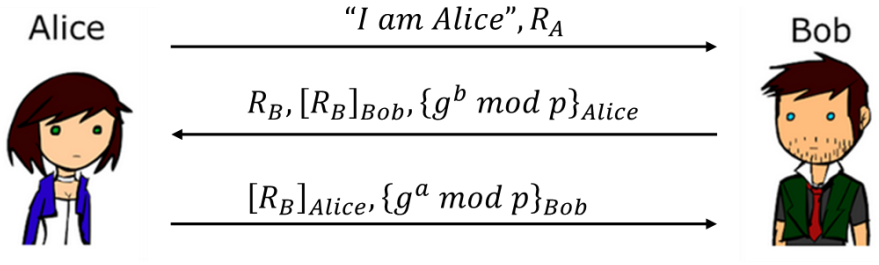
Assignment 4

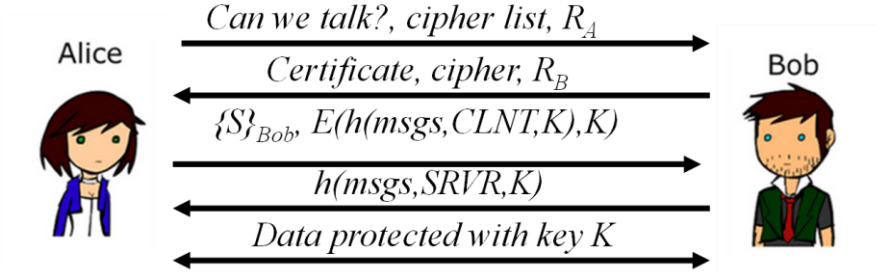
1. In the following protocol, Trudy can attack the protocol and will be able to decrypt one message from Alice. **Explain** how Trudy can do it.



2. Consider a man-in-the-middle attack on an SSL session between Alice and Bob.

a. At what point should this attack fail?
b. What mistake might Alice reasonably make that would allow this attack to succeed?

A simple SSL protocol is given below.



3. Consider the Kerberized login discussed in the book.

a. What is the TGT and what is its purpose?
b. Why is the TGT sent to Alice instead of being stored on the KDC?
c. Why is the TGT encrypted with KA when it is sent from the KDC to Alice's computer