Project Phase 1 – Due Tuesday, February 7

Review the system requirements from the project's "Basic Information" handout, and consider a situation in which a user Alice wishes to start a secure chat session with Bob. During the chat session, she will send at least one secure message to Bob, and will receive one secure reply from him. As you work on the following problems, think in particular about the second through fourth security requirements from that handout (the first requirement deals with efficiency rather than security, and we will deal with that later).

At this point in the class you are not expected to know much about how cryptographic protections work or what the requirements are for applying various security techniques. This does create a challenge in thinking through the design, but do the best you can — we will discuss design ideas and adjust as you learn more.

1. Draw a basic system model for the secure chat system that shows the different parties (Alice, Bob, and the chat hub). Label parts of the diagram where data might be stored or transmitted, and outline three basic operational steps:

   - Alice establishes a session with Bob.
   - Alice sends a message to Bob.
   - Bob sends a message to Alice.

   For each step, describe what information/data each participant must start the step with, and what confidentiality and integrity requirements exist for that data. Note that "data" means more than just a message that needs to be sent, and should include secrets or public information that is used to protect other data and to identify users. Also do your best to describe how much trust is placed in the chat hub (for example, is the hub trusted with secret information? is it trusted to identify chat participants?).

2. Consider security requirements two through four from the original handout, and for each one draw an attack tree for attacks against that security goal. Types of attacks to consider include compromising an end-user's system, compromising the chat hub, and intercepting or tampering with communication anywhere in the system.