EECS 190 - Honors Symposium

Perry Alexander, palexand@ku.edu

Fall 2011

The object of this project is to do some very simple protocol analysis and design.

Exercise 1 *Figure 1 represents a simple protocol where A and C are trying to communicate with B securely by establishing a shared secret key. A is being honest about its identity and succeeds. C is lying about its identity trying to pretend to be A. Considering the protocol in figure 1, answer the following questions:*

1. *What is going on where ??? appears in the figure?*
2. *At the end of the protocol, how do we know that A and B can communicate securely using No or N1? This is directly related to the previous question.*
3. *Why does C get stuck trying to establish a shared secret key? Why can't it pretend to be A?*

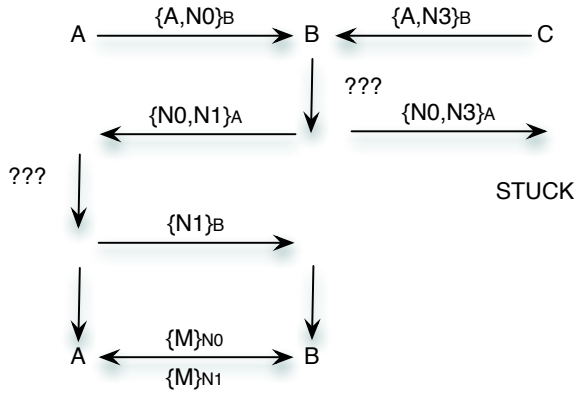

Figure 1: Protocol with A and C trying to establish secure communication with B.

Exercise 2 *Answer the following two questions about exchanging secure messages:*

1. *Assume A would like to send a secret message to B. A would like to know that only B can read the message and B would like to know that only A could have sent the message. How would you use encryption and signatures to accomplish this task?*
2. *What would you add to your message exchange to ensure that someone does not grab the message A sends, store it somewhere, and resend it later? (This is the tricky one.)*

Exercise 3 *There is no exercise 3. I hated the problem I gave you and I don't want you to do it after all.*