### Homework 3

1. (10 pts) Consider the following mutual authentication protocol. Give two different attacks Trudy can convince Bob she is Alice.



1. (10 pts) Design a secure two-message authentication protocol that provides mutual-authentication and establishes a session key K. Assume that Alice and Bob know each other’s public keys beforehand.
2. (10 pts) SSL and IPSec are both designed to provide security over the network.
3. What are the significant similarities between the two protocols?
4. What are the significant differences between the two protocols?
5. For SSL, what protocol does it use to establish security contexts (e.g., keys and algorithms) between two parties? How about IPSec?
6. What will a packet look like if you (IP address A) send a packet to another machine (IP address B) with AH at tunnel mode?
7. (10 pts) Consider the Kerberos interaction discussed in this chapter.
   1. Why is the ticket to Bob encrypted with KB?
   2. Why is “Alice” included in the (encrypted) ticket to Bob?
   3. In the REPLY message, why is the ticket to Bob encrypted with the key SA?
   4. Why is the ticket to Bob sent to Alice (who must then forward it to Bob) instead of being sent directly to Bob?
8. (10 pts) Consider the Kerberized login discussed in this chapter.
9. What is a TGT and what is its purpose?
10. Why is the TGT sent to Alice instead of being stored on the KDC?
11. Why is the TGT encrypted with KKDC?
12. Why is the TGT encrypted with KA when it is sent from the KDC to Alice’s computer?

Additional Questions:

5.33: (6 pts for part a) (2 bonus points for part b)

5.42: (10 pts)

(<http://www.cs.sjsu.edu/~stamp/infosec/files/>)

5.43: (12 pts)

5.48: (6 pts)

5.49: (8 pts)

10.1. (8 pts)