CS414, Fall 2005

Homework 9

Posted

There may be a pop-quiz on these homework questions during class on

You may work together on these homework questions. However, I strongly advise you to try to solve them yourself first, then check your answers with the solution set afterwards (at least for the first 8 questions). Please do not discuss the homework on the class discussion mailing list. which is posted on CMS).

1. p604 Exercise 15.1

2. p605 Exercise 15.4

3. p605 Exercise 15.11

4. p605 Exercise 15.12

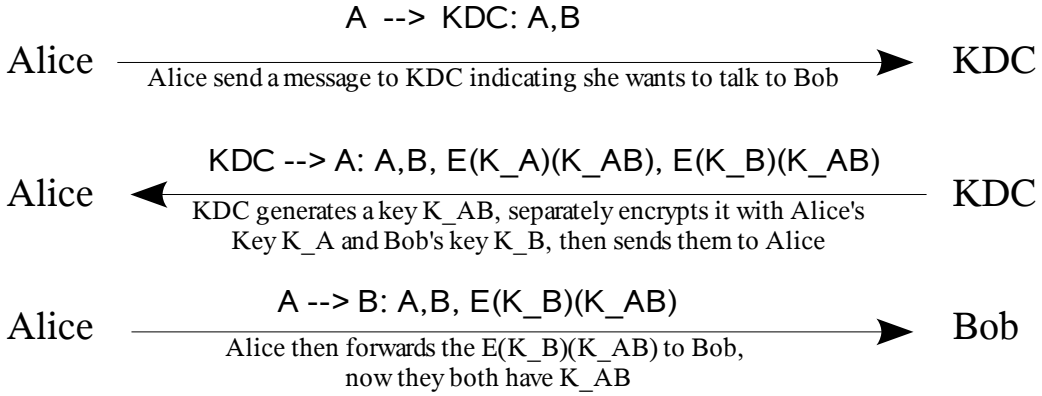
5. p605 Exercise 15.14

6. Discuss how the keyed hash function can be used to achieve secrecy.

7. A Key Distribution Center (KDC) has a database consisting of keys for all users. Any user registered with KDC can securely communicate with the KDC using his/her key. Imagine the following situation. Alice and Bob are registered users with KDC. Alice needs a session key to encrypt her communication with Bob. She asks the KDC to create such a key using the following protocol.

A --> KDC: A, B
KDC --> A: A, B, E(K_A)(K_AB), E(K_B)(K_AB)
A --> B: A, B, E(K_B)(K_AB)

(The protocol is explained in the following picture)




Is the above protocol secure? if not, outline a possible attack.

8. One mechanism for resisting replay attacks in password authentication is to use one-time passwords. A list of passwords is prepared, and once password[$N$] has been accepted, the server decrements $N$ and prompts for password[$N$-$1$] next time. At $N$=0 a new list is needed. Outline a mechanism by which the users and the server need only remember one master password *mp* and have available locally a way to compute password[$N$] = $f$ (*mp*, $N$). (Hint: make use of one-way hash functions)

9. What's the difference between a virus and a worm. How do they each reproduce?

10. The Secure Shell (SSH) provides a more secure remote login service comparing to Telnet. Any time a user uses SSH to log onto a remote machine, the first step is to have the client (user machine) authenticate the server (the remote machine) using RSA. Find out (by googling or other means) how this authentication is performed.