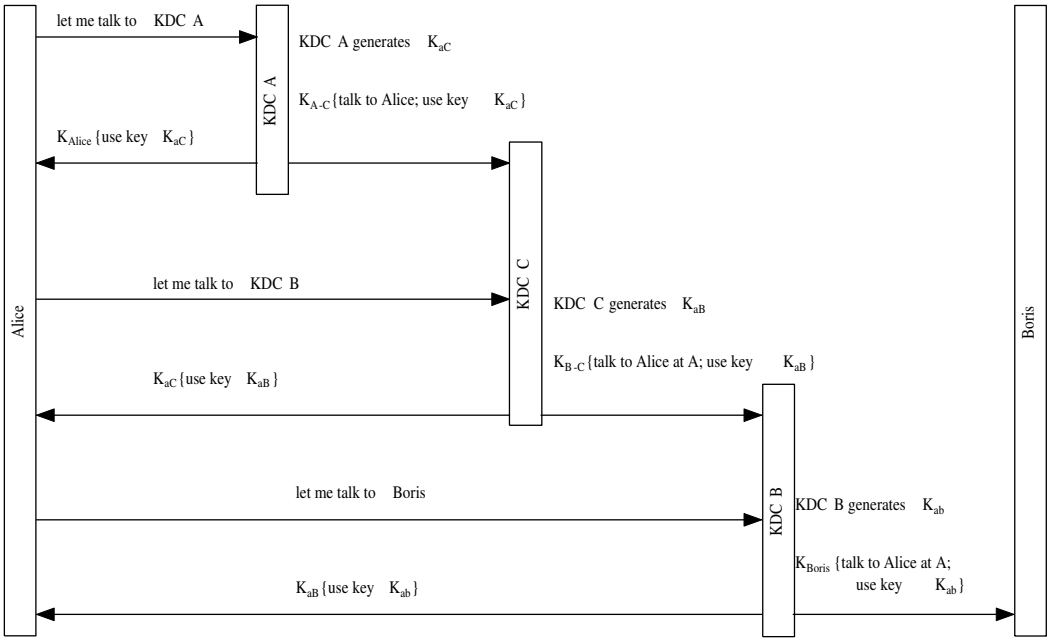
CSC474 - Information Systems Security: Homework2 Solutions

March 30, 2005

1. Problem 3 on page 236 (Multiple KDC Domains)



2. Problem 2 on page 255 (Eavesdropping)
   Let r be the no. of passwords in the list, q be the no. of passwords re-quested on each login, and s the no. of logins that have been eavesdropped on. Then the probability that the eavesdropper knows all q passwords for the next login is approximately $[1-(1-q/r)^s]^q$. For $q = 1$, the probability is roughly $1 - e^{-s/r}$. For values of s for which this probability is reasonably small, say $s < r/k$ for some reasonably large k, the probability for $q << k$ is about $(q/k)^q$, so using a larger q is advantageous. For example if $r = 100$ and $s = 10$, then the probability that the eavesdropper will know all the passwords is 0.10 for $q = 1$, but 0.01 for $q = 5$.

3. Problem 2 on page 288 (Mutual Authentication)
   Trudy cant impersonate Alice since Alice must prove knowledge of the secret before Bob will encrypt anything. However it should be possible for Trudy to impersonate Bob.

4. Problem 5 on page 288 (Three-way mutual authentication protocol)
   No. An eavesdropper can replay Alice's messages at any time. If Bob can't remember his current challenge, he won't know that the challenge response is to a previous challenge.

5. Problem 6 on page 289 (Modified mutual authentication protocol)
   No. Due to the possibility of a replay attack as mentioned above.

6. Problem 7 on page 289 (Timestamp based mutual authentication)
   Any timestamp older than 10min. is considered to have expired, and will thus be treated as invalid.

7. Problem 8 on page 289 (Two message authentication protocol)
   Alice picks a session key K and sends along a timestamp T. She encrypts K with Bob's public key and signs the entire message. Bob responds with the timestamp encrypted with K:
   Alice$\longrightarrow$ Bob : $[\{K\}_{Bob}, T]_{Alice}$
   Bob$\longrightarrow$Alice : $K\{T\}$
   Bob knows it's Alice from the signature and timestamp. Alice knows it's Bob because only he can decrypt K.

8. Problem 12 on page 289 (Fancy telephone wiretapping)
   Active Man-in-the-middle attack
   Alice$\rightarrow$Bob (but captured by X) : I'd like to talk to you. $g^{S_A} = 8389$
   X $\rightarrow$ Bob : I'd like to talk to you. $g^{S_X} = 5876$
   Bob$\rightarrow$ Alice (but captured by X) : So pleased to talk to you. $g^{S_B} = 9267$
   X$\rightarrow$Alice : So pleased to talk to you. $g^{S_X} = 5876$

   Shared key between Alice and X is $K_{AX} = 5876^{S_A} = 8389^{S_X}$
   Shared key between Bob and X is $K_{BX} = 9267^{S_X} = 5876^{S_B}$