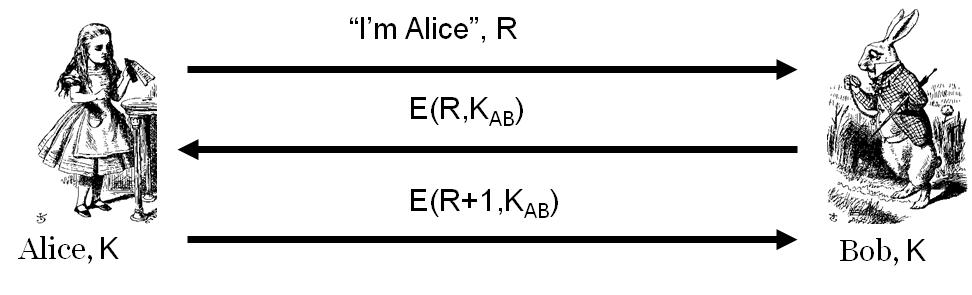
**Description for: CS 492 Homework Protocols – Authentication - Authorization**

Complete the problems below and submit this word document with the solution to the questions here.

Name(s):   
**100 possible points**

**Question 1 (20pts):** Design a secure mutual authentication protocol based on a shared symmetric key. We also want to establish a session key, and we want perfect forward secrecy. Solve for a protocol that can establish this in 2 to 3 messages

**Question 2 (10pts):** Consider the following mutual authentication protocol, where KAB is a shared symmetric key.



**Give an attack Trudy can use to convince Bob that she is Alice.**

**Question 3 (20pts):** Consider the following protocol, where CLNT and SRVR are constants and session key K = h(S, RA, RB)



1. **Does Alice authenticate Bob? Justify your answer**
2. **Does Bob authenticate Alice? Justify your answer**

**Question 4: Kerberos [10pts]**

1. Why can Alice not remain anonymous when requesting a TGT from the KDC?
2. Why can Alice remain anonymous in the sense of not needing to use her private key when requesting a ticket to Bob (what does she use instead and why is this sufficient)?
3. Why can Alice remain anonymous (not needing her private key) when she sends the “ticket to Bob” to Bob?

**Question 5: Describe what the confused deputy problem is and what types of authorization approach would be susceptible to it. [10pts]**

**Question 6: Authorization - MLS compartments [30 pts]**

* + Alice has the following clearances TopSecret, Secret{A}, Classified{B}
  + Bob has the following clearances TopSecret{A}, Secret{B}

Draw the **full tree** and indicate which files Alice and Bob each can read (don’t forget Unclassified)