Homework 2

Problem 1 (30 points). In the Wide Mouth Frog protocol, explain why at the end of the protocol, Alice believes that she is talking to Bob and sharing the key with him, and why Bob believes that he is talking to Alice and sharing the key with her.

Problem 2 (20 Points)
Alice can read and write to the file F, can read the file G, and can execute the file H. Bob can read F, can read and write to G, and cannot access H.
(a. 10 points) Write a set of access control lists for this situation. Which list is associated with which file?
(b. 10 points) Write a set of capability lists for this situation. With what is each list associated?

Problem 3 (30 points). Let object $O_1$ have classification $< \text{restricted}, \{\text{Denmark}\}>$. Let $O_2$ have classification $<\text{unclassified}, \{\text{Denmark}\}>$. Let $O_3$ have classification $<\text{secret}, \{\text{Denmark}\}>$. Let $O_4$ have classification $<\text{secret}, \{\text{Sweden}\}>$. Now, let subject Alice have clearance $<\text{confidential}, \{\text{Denmark}\}>$. Let subject Bob have clearance $<\text{top secret}, \{\text{Denmark, Sweden}\}>$.
Answer the following questions. Motivate your answer. A simple Yes or No is not sufficient. Assume the following order of the operations:
(a - 5 points) Can Alice read $O_1$?
(b - 5 points) Can Alice write to $O_2$ after reading from $O_1$?
(c - 5 points) Can Alice write to $O_3$?
(d - 5 points) Can Bob read from $O_3$?
(e - 5 points) Can Bob write to $O_4$?
(f - 5 points) Can Alice read from $O_3$?

Problem 4 (20 points). (a. 10 points). Explain why authentication systems should not accept short passwords. That is, show how an adversary could break a short password.
(b. 10 points). Assume an authentication system that splits the user password into halves, hashes each half separately, then stores or transfers the hashed halves for remote storage. Explain how in such a system, an attacker can infer information about the user password.