CSI3344 Distributed Systems

Workshop 10

Q1. Would it be safe to join message 3 and message 4 in the authentication protocol shown in the following figure into $K_{A,B}(R_B,R_A)$? Explain your answer.

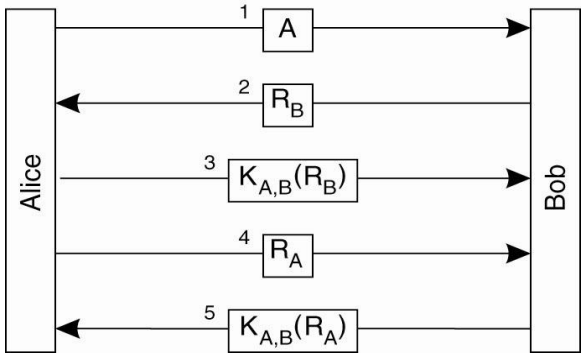

Figure 9-12. Authentication based on a shared secret key.

Q2. Why is it not necessary in the following figure for the KDC to know for sure it was talking to Alice when it receives a request for a secret key that Alice can share with Bob?

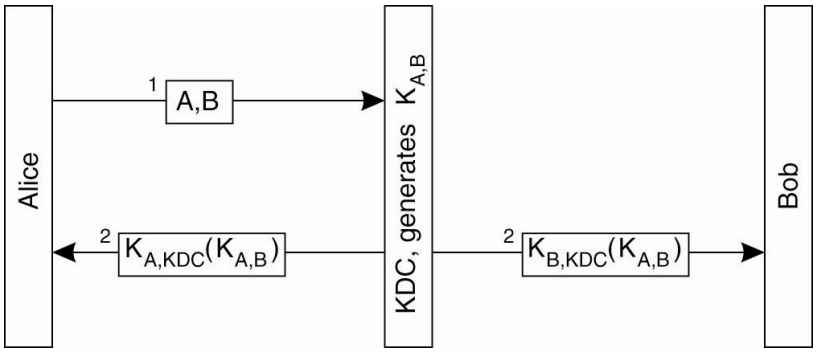

Figure 9-15. The principle of using a KDC.

END OF THE WORKSHOP