CSI3344 Distributed Systems

Workshop Solution 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.

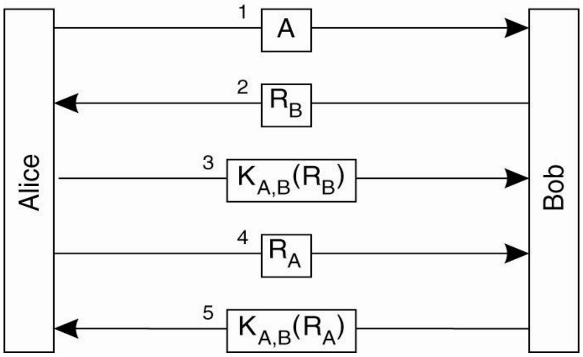

Figure 9-12. Authentication based on a shared secret key.

A: Yes, there is no reason why the challenge sent by Alice for Bob cannot be sent in the same message.

It should be safe to combine the two messages into one. Without possessing the shared key $K_{A,B}$, an attacker is unable to separate R_A and R_B, therefore the attacker could not pretend to be in the possession of the shared secret key to generate and return $K_{A,B}(R_A)$.

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?

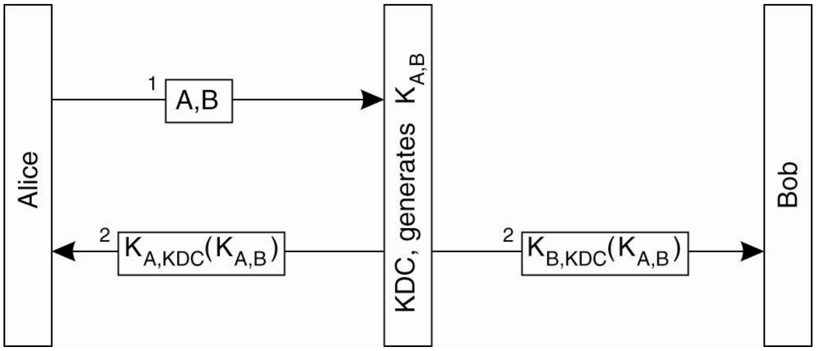

Figure 9-15. The principle of using a KDC.

A: Suppose a potential attacker, Chuck, had sent the message ‘‘I’m Alice and I want to talk to Bob’’.

After having received the communication request for a shared key between A (i.e., Alice) and B (i.e., Bob), the KDC returns $K_{A,B}$ encrypted with $K_{A, KDC}$. Because the key is encrypted with the shared secret key $K_{A, KDC}$, only Alice (besides the KDC) will be able to decrypt the key. Thus, a potential attacker will not be able to initiate a communication channel with Bob, which is why the KDC does not need to verify that it is indeed talking to Alice.

END OF THE WORKSHOP SOLUTION