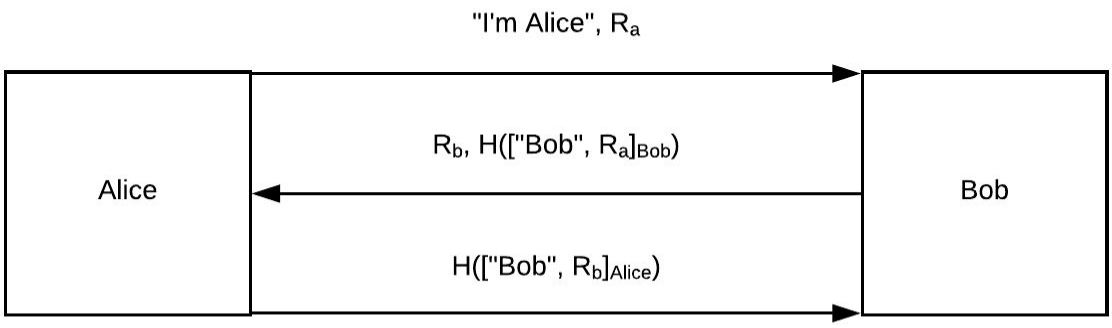
Arthur Levan

Dr. Coogan

CS355

Chapter 9

1.



6.

a. The primary advantage to using timestamps is that it prevents older messages from being reused in a replay attack.
b. The disadvantage is that the longer the connection exists, there will be larger packets being sent back in forth from the increasing timestamps.

7.

a. Alice does authenticate Bob. Bob sent a Certificate verifying his identity.
b. Bob does not authenticate Alice. Alice sent a message and a nonce in the clear, and encrypted a later message using Bob's public key, instead of her private key.

12. Yes it does. While Alice appears to send $\{S\}_{Bob}$, Bob does not use this in his next message to confirm the shared key and instead only sends $E(R_B, K)$.

18.

a. Yes, the Time and key are encrypted using Alice's private key which only she would have, and the overall message is encrypted with Bob's public key which only he can unencrypt.
b. Yes. Same reasoning as above, just with "Alice" included in the overall encryption.
c. Yes. See answer a.
d. No. The Timestamp is sent in the clear, while the Key is encrypted.
e. No. While the Timestamp is encrypted, the Key does not appear the in the message.

Chapter 10

6.

a. Removing the nonces has no effect on the protocol as they are not used in any of the later encryption.
b. This creates more work for Alice, but maintains the integrity and authenticity of the messages.
c. This weakens the overall exchange as it removes the encryption.

7.

11.

a. SSL is a simpler protocol, which allows for greater ease of understanding and use.
b. IPSec is more complex, which means that it is built into the OS, because of this it requires no changes to applications since it is all done in the network layer.

17.

a. Alice remains anonymous because she is issued a TGT when she firsts accesses the network, which contains her information, but the details are only known by the KDC.

b. Because TGTs expire, Alice will have to reestablish credentials with the KDC to get a new TGT.
c. Because Bob has yet to decrypt the “ticket to Bob,” he has no knowledge of Alice’s information as Kerberos maintains a statelessness feature.

27.

a. No.
b. No.
c. Yes
d. Yes
e. Yes
f. Yes