CptS/EE 455 Assignment #8

Instructor: Dingwen Tao

Due: 12/10/2020 at 11:59 pm

Deliverable: Complete the answers to the following questions and *submit to canvas before the due date*. If you have any questions regarding the assignment, please contact TA.

1. Suppose Alice wants to communicate with Bob using symmetric key cryptography using a session key KS. In Section 8.2, we learned how public-key cryptography can be used to distribute the session key from Alice to Bob. In this problem, we explore how the session key can be distributed—without public key cryptography—using a key distribution center (KDC). The KDC is a server that shares a unique secret symmetric key with each registered user. For Alice and Bob, denote these keys by $K_{A\text{-}KDC}$ and $K_{B\text{-}KDC}$. Design a scheme that uses the KDC to distribute KS to Alice and Bob. Your scheme should use three messages to distribute the session key: a message from Alice to the KDC; a message from the KDC to Alice; and finally, a message from Alice to Bob. The first message is $K_{A\text{-}KDC}$ (A, B). Using the notation, $K_{A\text{-}KDC}$, $K_{B\text{-}KDC}$, S, A, and B answer the following questions.
    A. What is the second message?
    B. What is the third message?

2. The OSPF routing protocol uses a MAC rather than digital signatures to provide message integrity. Why do you think a MAC was chosen over digital signatures?

3. A natural question is whether we can use a nonce and public key cryptography to solve the end-point authentication problem in Section 8.4. Consider the following natural protocol: (1) Alice sends the message "I am Alice" to Bob. (2) Bob chooses a nonce, R, and sends it to Alice. (3) Alice uses her private key to encrypt the nonce and sends the resulting value to Bob. (4) Bob applies Alice's public key to the received message. Thus, Bob computes R and authenticates Alice.
    A. Diagram this protocol, using the notation for public and private keys employed in the textbook.
    B. Suppose that certificates are not used. Describe how Trudy can become a "woman-in-the-middle" by intercepting Alice's messages and then pretending to be Alice to Bob.

4. Figure 1 shows the operations that Alice must perform with PGP to provide confidentiality, authentication, and integrity. Diagram the corresponding operations that Bob must perform on the package received from Alice.

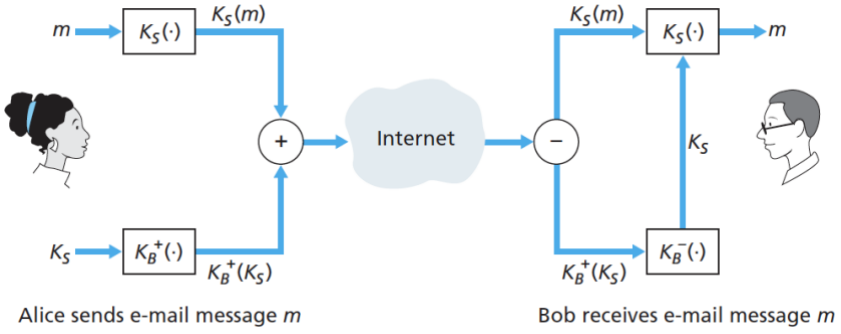

Figure 1: Alice used a symmetric session key, Ks, to send a secret

5. Suppose Alice wants to send an e-mail to Bob. Bob has a public-private key pair (K_B^+,K_B^-), and Alice has Bob's certificate. But Alice does not have a public, private key pair. Alice and Bob (and the entire world) share the same hash function H(•).
   A. In this situation, is it possible to design a scheme so that Bob can verify that Alice created the message? If so, show how with a block diagram for Alice and Bob.
   B. Is it possible to design a scheme that provides confidentiality for sending the message from Alice to Bob? If so, show how with a block diagram for Alice and Bob.