

CSCI 283 and CSCI 172 - Computer Security - Fall 2008
Quiz 5 Solutions

1. Consider

$$\text{Alice} \xrightarrow{\{k\}x} \text{Bob}$$

a. If Alice wants only Bob to determine k , what is x ?

Answer: x is Bob's public key. x can also be a key pre-shared between Alice and Bob that was not shared with anybody else.

b. If Alice wants Bob to know she sent k , what is x ?

Answer: x is Alice's private key, or a key pre-shared between Alice and Bob that was not shared with anybody else.

c. If Alice wants to send k to Bob such that:

(i) only Bob can see k

(ii) Bob knows Alice sent it

She sends $\{\{k\}x\}y$. What are x and y ?

Answer: One of x and y is Alice's private key, and the other is Bob's public key. Alternately, both x and y can be pre-shared keys that were not shared with anybody else.

Note: fewer points for providing pre-shared keys answers, because you end up assuming something (that Alice and Bob had the opportunity to pre-share keys) that is not stated in the question.

d. Describe an attack on the following protocol:

$$\begin{array}{ccc} & \text{BobPublicKey} & \\ \text{Alice} & \rightarrow & \text{server} \\ \\ & K_b & \\ \text{Alice} & \leftarrow & \text{server} \end{array}$$

where K_b is Bob's public key.

Answer: A common attack on the above protocol is a "man-in-the-middle" attack. An adversary capable of listening to, and changing, messages between the server and Alice sends Alice his own key instead of Bob's, and thereafter is able to read all messages sent by Alice to Bob, encrypted with the incorrect public key.