

CSCI 283 and CSCI 172 - Computer Security - Fall 2006
Quiz 9 Solutions

The following is a complete description of a model answer to this problem. While such detail would not be possible/required in a quiz, similar conceptual, though not verbal, detail would be expected in the test.

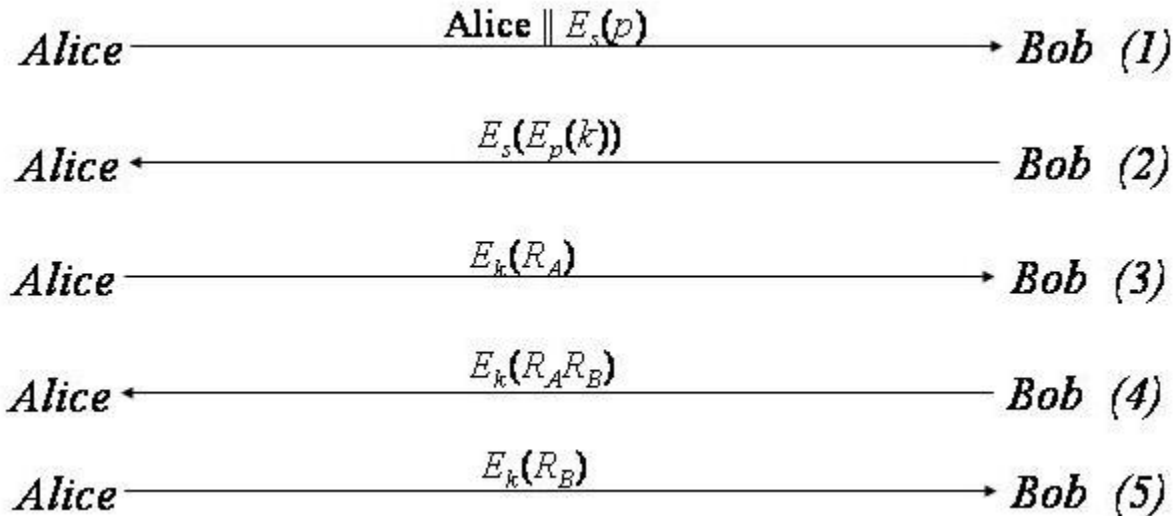


Figure 1: An Authentication Protocol

In the above protocol, you may assume that Alice and Bob previously share a secret s . Further, you may assume that p is Alice's public key, for which she possesses a private key.

Answer the following:

A. In the above protocol, at the end of which step is Bob convinced he is interacting with Alice? Why is he convinced at the end of the step you claim he is? Why is he not convinced earlier (you need to answer this for *each* of the earlier steps?)

Answer:

We examine the operation of the protocol for both cases: I. Alice communicating with Bob and II. Mallory communicating with Bob.

I. Alice communicating with Bob

Step 1: Alice sends $E_s(p)$. Bob decrypts this with s to obtain p .

Step 2: Bob sends $E_p(k)$ for randomly generated session key k . Alice decrypts this with the private key corresponding to p to obtain k .

Step 3: Alice sends $E_k(R_A)$ for randomly generated R_A . Bob decrypts with k to obtain R_A .

Step 4: Bob sends $E_k(R_A R_B)$ for randomly generated R_B . Alice decrypts with k and divides out by R_A to obtain R_B .

Step 5: Alice sends $E_k(R_B)$. Bob decrypts with k and checks that he has obtained R_B .

II. Mallory communicating with Bob

Step 1: Mallory, pretending to be Alice, sends some value $x \neq E_s(p)$. Bob decrypts this with s to obtain $D_s(x) = y \neq p$. Because Bob does not know p , he has no way of distinguishing between y obtained in this case, and the p obtained when it is Alice on the other side. Hence Bob does not know, at this step, whether it is Alice or Mallory on the other side.

Step 2: Bob sends $E_y(k)$ for randomly generated session key k . Mallory does not know s . Hence he is not able to obtain the key Bob thinks is Alice's public key, $y = D_s(x)$, or the corresponding private key. Hence he has no way of obtaining k . In this step, Bob receives no information, so he is not able to distinguish this outcome from that of Step 2 when it is Alice on the other side.

Step 3: Mallory sends R_M for randomly generated R_M . Even if he generates a value of R_A and encrypts with some key other than k , the effect will be that of sending a random number R_M . Bob decrypts with k to obtain $D_k(R_M)$. As Bob does not know the value of R_A , he is not able to distinguish this outcome from that of Step 3 when it is Alice on the other side. Hence he does not know, at this step, whether it is Alice or Mallory on the other side.

Step 4: Bob sends $E_k(D_k(R_M)R_B)$ for randomly generated R_B . If the encryption system is such that $E_k(D_k(R_M)R_B) = E_k(D_k(R_M)) \times E_k(R_B)$, Mallory can obtain $E_k(R_B)$. If it is not, he probably cannot do so. In this step, Bob receives no information, so he is not able to distinguish this outcome from that of Step 4 when it is Alice on the other side.

Step 5: For the particular encryption system, Mallory sends $E_k(R_B)$. Bob decrypts with k and checks that he has obtained R_B . He thinks he is talking to Alice. However, if the encryption system does not have the special property described above, Mallory is not able to find $E_k(R_B)$ and instead sends R'_M . Bob decrypts this with k and does not obtain R_B so he knows he is not talking to Alice. Thus, with the appropriate encryption system, Bob knows, at the end of Step 5, whether he is talking to Alice or not.

B. In the above protocol, at the end of which step is Alice convinced she is interacting with Alice? Why is she convinced at the end of the step you claim she is? Why is she not convinced earlier (you need to answer this for *each* of the earlier steps?)

Answer: We now examine the case III, with Alice on one side and Mallory on the other.

III. Alice communicating with Mallory

Step 1: Alice sends $E_s(p)$. Mallory does not have s and cannot obtain p . In this step, Alice receives no information, so she is not able to distinguish this outcome from that of Step 1 when it is Bob on the other side (Case I).

Step 2: Mallory sends randomly generated x , as he does not have p . Alice decrypts with her private key to obtain a number $y \neq k$. As she does not know k , she is unable to distinguish this outcome from that of Case I, Step 2, when Bob is on the other side. Hence she does not know, at this step, whether it is Bob or Mallory on the other side.

Step 3: Alice sends $E_y(R_A)$ for randomly generated R_A . Mallory cannot obtain R_A as he cannot determine y . Though he knows x , he does not know Alice's private key, nor the public key p . In this step, Alice receives no information, so she is not able to distinguish this outcome from that of Step 3 when it is Bob on the other side (Case I).

Step 4: Mallory sends randomly generated R_M . Alice decrypts this with k to obtain $D_k(R_M)$, which she divides by R_A to obtain $D_k(R_M)R_A^{-1}$. As she does not know R_B , she is unable to distinguish this outcome from that of Case I, Step 4, when Bob is on the other side. Hence she does not know, at this step, whether it is Bob or Mallory on the other side.

Step 5: Alice sends $E_k(D_k(R_M)R_A^{-1})$. In this step, Alice receives no information, so she is not able to distinguish this outcome from that of Step 5 when it is Bob on the other side (Case I).

Thus, Alice never knows through the protocol, whether she is talking to Bob or not. This is because this is an authentication protocol for Alice, who approaches Bob, and hence is required to prove to Bob who she claims she is. It is not an authentication protocol for Bob.