HW7 Sample Solutions

Answer to Problem 9.8.5

Two situations arise, the first in which Eve, the attacker, does not send an initial message to Bob (steps 1 and 2), and the second where she does. In both scenarios, assume that Eve knows the session key $k_{session}$, and has intercepted the message at step 5.

Begin with the first case. Eve replays the message to Bob. As Bob has not yet received a new message from Alice (steps 1 and 2), he rejects the message. But if Eve's message comes during Alice's execution of the protocol and after step 2, Bob opens the message and determines the random number $rand_3$. Because he kept track of the random number that he sent to Alice, he recognizes that this was not an attempt to begin a new session, but instead a replay of an older message (else it could not have been enciphered using the key he shares with Cathy, k_{Bob}). He therefore knows the message is legitimate but, since he has already seen the message with that random number in it, that it is a replay.

In the second case, Eve sends message 1 to Bob, who replies with message 2. Eve immediately sends message 5 to Bob. Bob opens the message, compares $rand_3$ with the nonce in the message he just sent Eve (masquerading as Alice), and notes it is different. So he rejects the message.

Answer to Problem 9.8.6

Given, $m = m_1 \times m_2 \bmod n_{\text{Bob}}$

Bob's Digital Signature on m_1 and m_2

$c_1 = m_1^{\text{dBob}} \bmod n_{\text{Bob}}$

$c_2 = m_2^{\text{dBob}} \bmod n_{\text{Bob}}$

Bob's Digital Signature on m

$c = m^{\text{dBob}} \bmod n_{\text{Bob}}$

Since Alice has c_1 and c_2, she can construct c from them as follows. (note n_{Bob} is publicly known)

$= [c_1 \times c_2] \bmod n_{\text{Bob}}$

$= [(m_1^{\text{dBob}} \bmod n_{\text{Bob}}) \times (m_2^{\text{dBob}} \bmod n_{\text{Bob}})] \bmod n_{\text{Bob}}$

$= (m_1^{\text{dBob}} \times m_2^{\text{dBob}}) \bmod n_{\text{Bob}}$

$= (m_1 \times m_2)^{\text{dBob}} \bmod n_{\text{Bob}}$

$= m^{\text{dBob}} \bmod n_{\text{Bob}}$

Thus, the forgery is possible.