**Sign then Encrypt Protocol**

***Assumptions & Skeletons:***

For this protocol, there were only two skeletons needed: one for the responder and one for the listener. We don’t need one for the initiator b/c it will always produce the same shape, a singular node. This doesn’t tell us anything because this is an email protocol. The initiator just sends the message, what we are looking for is if the responder gets the correct message or if it was altered by an intruder. This is why we have responder and listener skeletons. Both skeletons included (non-orig (privk a) (privk b)) because the assumption is that the private keys of the initiator (a) and the responder (b) cannot be attained by an intruder.

***Shapes:***

A picture containing diagram

Description automatically generatedChart, scatter chart

Description automatically generated

The first shape, PGP 1, for sign then encrypt has a dashed line going from the initiator to the responder. This signifies unequal messages, meaning the intruder was able to alter the message. I also know this, because for the variables b-0 and k-0 are there. To tell the full story, if you look at the PGP 3 shape, it has the same b-0 and k-0. Here, we know that the initiator is sending the message to a user with the name b-0 using the key b-0. But looking at our assumptions, the key b-0 is not non-originating. This means the intruder can get key b-0. The arrow in the shape is dashed. So, the intruder got ahold of key b-0, altered the message the initiator was sending to user b-0 and then sent it to user b-0.

**Encrypt then Sign Protocol**

***Assumptions and Skeletons:***

The assumptions and skeletons here are the same as the last protocol, but I will repeat for consistency. For this protocol, there were only two skeletons needed: one for the responder and one for the listener. We don’t need one for the initiator b/c it will always produce the same shape, a singular node. This doesn’t tell us anything because this is an email protocol. The initiator just sends the message, what we are looking for is if the responder gets the correct message or if it was altered by an intruder. This is why we have responder and listener skeletons. Both skeletons included (non-orig (privk a) (privk b)) because the assumption is that the private keys of the initiator (a) and the responder (b) cannot be attained by an intruder.

***Shapes:***

A picture containing diagram

Description automatically generatedChart, scatter chart

Description automatically generated

The shapes for this Encrypt the Sign protocol are exactly the same as the Sign and Encrypt protocol. Again, I will include the analysis for consistency. The first shape, SMIME 1, for encrypt then sign has a dashed line going from the initiator to the responder. This signifies unequal messages, meaning the intruder was able to alter the message. I also know this, because for the variables b-0 and k-0 are there. To tell the full story, if you look at the SMIME 3 shape, it has the same b-0 and k-0. Here, we know that the initiator is sending the message to a user with the name b-0 using the key b-0. But looking at our assumptions, the key b-0 is not non-originating. This means the intruder can get key b-0. The arrow in the shape is dashed. So, the intruder got ahold of key b-0, altered the message the initiator was sending to user b-0 and then sent it to user b-0.

Because the shapes formed are exactly the same there is no difference between the Sign and Encrypt and Encrypt then Sign protocols. So whatever order you chose does not affect the level of security you have against any potential intruders.

**Extra Credit:**

My solution to fix the Sign and Encrypt Protocol is to simply take the signed and encrypted portion and then encrypt it with the intended recipient’s (b) public key. Or in other words, “sign” it with their public key. This ensures that the only one who can see the message is the intended recipient. For my solution all assumptions, and skeletons were kept the same. The reason why my solution holds is because one of the assumptions was that the private key of b was non-orig, meaning that the intruder cannot get it. This means that the only one who can decrypt that “signature” is the intended recipient (b). The following shapes prove this:

Diagram

Description automatically generated with low confidenceChart, scatter chart

Description automatically generated

As you can see from the shapes, the lines between the initiator and responder nodes are solid, this means that the message sent by the initiator is the exact same as the one received by the responder. And we no longer have the issue of the unsecure b-0 key being used. The message was unable to be altered by the intruder.