Nick Pandelakis and Owen Barnett
CS 231
16 April 2021

Scenarios

1. Alice wants to send Bob a long message, and she doesn't want Eve to be able to read it. (I say "Eve" here because I want you to assume for this scenario that person-in-the-middle is impossible, and give an answer that is as simple as possible under that assumption.)
    a. Alice and Bob use Diffie-Hellman to agree on a key K. Using AES, Alice sends Bob S_k(M), and then Bob decrypts with S_k^{-1}(S_k(M)), which is equal to M.

2. Alice wants to send Bob a long message. She doesn't want Mal to be able to intercept, read, and modify the message without Bob detecting the change.
    a. Alice uses Bob's public key to encrypt the message C = E(P_B, K) where K is a secret key that only Alice knows. Bob then computes K = (S_B, C) to obtain this key. Alice then sends Bob S_k(M) and C = E(P_B,H(M)) to Bob. Bob can do S_k^{-1}(S_k(M)) to get the message and compute H(M) and check it equals K = (S_B, C) to make sure Mal didn't mess with the message. Note we don't have to encrypt the hash of the message since it should theoretically be pre-image resistant but it doesn't hurt to encrypt it.

3. Alice wants to send Bob a long message, she doesn't want Eve to be able to read it, and she wants Bob to have confidence that it was Alice who sent the message. (Again, don't worry about Mal and person-in-the-middle here.)
    a. Alice uses her private key and Bob's public key to encrypt the message C = E(P_B, E(S_A, K)) to send Bob an encryption key K. Bob then computes K = E(P_A, E(S_B, C)) to compute K. Alice then sends Bob the message S_K(M) to Bob. When Bob decrypts the message using S_K^{-1}S_K(M), if the message decrypts to something intelligible, Bob will be assured that the message came from Alice, since K was unencrypted using Alice's public key P_A.

4. Alice wants to send Bob a long message (in this case, it's a contract between AliceCom and BobCom). She doesn't want Eve to be able to read it. She wants Bob to have confidence that it was Alice who sent the message. She doesn't want Bob to be able to change the document and claim successfully in court that the changed version was the real version. And finally, Bob doesn't want Alice to be able to say in court that she never sent the contract in the first place.

a. Alice uses her private key and Bob’s public key to encrypt the message $C = E(P_B, E(S_A, K))$ to send Bob an encryption key K. Bob then computes $K = E(P_A, E(S_B, C))$ to compute K. Alice then sends Bob the messages $S_K(M)$ and $C = E(S_A, H(M))$ to Bob. Bob decrypts $M = S_L^{-1}S_K(M)$ and checks $H(M) = E(P_A, C)$. This allows Bob to claim in court that Alice sent the contract, since Alice’s public key decrypts C into the same hash of the document. This works because the hash function is highly input sensitive. Next, Bob sends back $C = E(S_B, H(M))$ to Alice, this allows Alice to also prove that Bob got the correct document and if it was changed by Bob she could prove it.

   We are assuming here that while logs of this conversation may exist. They are not verifiable. Alice and Bob are protected from the following scenarios.

   i. Alice wants Bob to have confidence that it was Alice who sent the message

      1. By encrypting the symmetric key K with her own Secret key S_A, Bob can be assured that a message came from Alice if $S_K^{-1}(S_K(M))$ unencrypts to something intelligible, since he computed K using Alice’s public key.

   ii. Alice doesn't want Bob to be able to change the document and claim successfully in court that the changed version was the real version.

      1. Because Alice is using a hash function which is input sensitive, any changes Bob makes to the contract will drastically change the Hash of that contract. Since Bob sent back an encryption of the Hash of the contract using his secret key, Alice can show in court that the contract received by Bob is the one she sent, which is different from the one Bob may be presenting.

   iii. Bob doesn't want Alice to be able to say in court that she never sent the contract in the first place.

      1. Because Bob has the hash of the contract encrypted with Alices’s secret key, he can prove Alice sent him the hash of the contract which should be enough to prove he sent the contract.