Eric Gassel and Eli Arbogast

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.)’

- Alice and Bob use Diffie Hellman to agree on a secret key.
- They then use a symmetric encryption algorithm. Their encryption function is $S_K(M)$, where K is the key used in the encryption function.
- Alice does $S_K(M) = C$ so that Eve cannot read C since she does not know K, and then sends C to Bob.
- Bob decrypts C by doing the following: $S_K^{-1}(C) = S_K^{-1}(S_K(M)) = M$

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.’

- Alice and Bob use Diffie Hellman to agree on a key
- They then use a symmetric encryption algorithm. Their encryption function is $S_K(M)$, where K is the key used in the encryption function.
- Alice does $S_K(M) = C$ so that Mal cannot read C since she does not know K.
- Alice then applies the cryptographic hash function SHA-256 to C to get D which is computed by: $D = H(C)$
- Alice sends Bob $C \| D$

- Bob checks $H(C) == D$ to confirm the integrity of the message. Had Mal changed C even slightly, $H(C_{ALTERED})$ would not equal D. Therefore, we know the message has not been modified.
- Bob decrypts C by doing the following: $S_K^{-1}(C) = S_K^{-1}(S_K(M)) = M$

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.)’

- Alice and Bob use Diffie Hellman to agree on a secret key.
- They then use a symmetric encryption algorithm. Their encryption function is $S_K(M)$, where K is the key used in the encryption function.
- Alice does $S_K(M) = C$ so that Eve cannot read C since she does not know K, and then sends C to Bob.
- Alice applies a cryptographic hash function (SHA-256). to C to obtain D by the following: $D = H(C)$
- Alice applies a public key encryption function E to D using her secret key S_A as shown by the following: $Sig = E(S_A,D)$.
- Alice sends $C || Sig$ to Bob
- Bob uses Alice’s public key P_A to check that $E(P_A, Sig) == H(C)$ to confirm that Alice sent the message. This works because only Alice knows her secret key S_A which was used to encrypt D.
- Bob decrypts C by doing the following: $S_K^{-1}(C) = S_K^{-1}(S_K(M)) = M$

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.’

- We believe that following the same protocol in 3 will lead to the desired results in 4
- First additional requirement of 4: Bob cannot change the message and prove in court that the changed message is the original message
    - Why it’s covered by the protocol in 3: Alice had subjected the encrypted message C to a one-way hash function to obtain D. Any changes to C (or to M from which C is derived) results in significant changes to D. But why can’t Bob claim that his D is the real one? Alice encrypts the original D using her private key, then sends that as a signature. Bob would have to know Alice’s private key to alter the signature.
- Second additional requirement of 4: Alice cannot prove in court that she didn’t send the message.
    - Why it’s covered by the protocol in 3: Alice had used a digital signature in 3. Since she had kept her private key private, no one could impersonate her.