Emma Roskopf

Scenarios:

1. Alice wants to send Bob a long message (M), and she doesn't want Eve to be able to read it. Assume for this scenario that PITM is impossible.

   Alice and Bob will use a Diffie-Hellman key exchange, because it is impossible for Eve to figure out the secret key if the numbers they use are large enough. Since it isn't possible for there to be a PITM, we don't have to worry about verifying Alice and Bob, Eve is just trying to figure out the message that is being sent. So Alice and Bob now have the shared secret key K. Alice is sending a long message, so she wants to block cipher it so it isn't vulnerable to attacks just on character frequency or something, so she creates her ciphertext message, C = (CBC, M). She then is going to use AES because they both have the same keys, so S = AES(K, C), where S is standing for Sent message. Bob receives S from Alice, and now can decrypt the ciphertext using AES, so M = AES_D(K, C) using the same block cipher. Bob now has the long message Alice wanted to send, and Eve couldn't break the secret key K or break the sent message S, so the transaction was secure and the communication was successful.

2. Alice wants to send Bob a long message. She doesn't want Mal to be able to modify the message without Bob detecting the change.

   Alice is trying to send the same message, but the Diffie-Hellman key exchange is vulnerable to the PITM attack so to keep the message safe from Mal, she is also going to instead use the Public Key Infrastructure to send Bob a hashed version of the message. So Alice takes her message M and hashes it into H(M), and then encodes this into ciphertext, C = E(S_A, H(M)), and sends this to Bob. Mal can see this message, but can't see the hash or the message. If they decide to change the message being sent along, the chances of it decrypting and dehashing into the same modified message that Alice will be sending seems remarkably low. So Mal will probably just pass this message on. Alice doesn't want her public/private key system to be broken, so she can't send the whole message through it. So Alice and Bob will use the Diffie Hellman key exchange to agree on the secret key K. Then Alice sends the message using the same block cipher as the previous question, and Bob can decode it with K. Mal could be in the middle of this, but if they edit Alice's message the message won't match up with H(M) that Alice sent through PKI. So Bob will know if Mal modifies the message.

3. Alice wants to send Bob a long message (in this case, it's a signed contract between AliceCom and BobCom), 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. Assume for this scenario that PITM is impossible.

   Alice and Bob will agree on a secret key K using Diffie-Hellman. Eve can't break this key because the numbers are too large and so this exchange is secure. Alice is now going to take the message, M, and create a ciphertext using her secret key, so C = E(S_A, M) and then using the key encodes it again so AES(K, C) and then sends this to Bob. Bob can now decrypt the AES with the shared key, and then uses Alice's public key, E(P_A, E(K, C)) = M. Bob now has the message M, and because it was encoded with Alice's private key and we're trusting that the private keys are actually private, Bob knows this is Alice. While Eve could decrypt using Alice's public key, she can't figure out E(K, C) because she doesn't have the secret key, so the message was transmitted safely.

4. Consider scenario #3 above. Suppose Bob sues Alice for breach of contract and presents as evidence: the digitally signed contract (C || Sig) and Alice's public key P_A. Suppose Alice says in court "C is not the contract I sent to Bob". (This is known as *repudiation* in cryptographic vocabulary.) Alice will now need to explain to the court what she believes happened that enabled Bob to end up with an erroneous contract. List at least three things Alice could claim happened. For each of Alice's claims, state briefly how plausible you would find the claim if you were the judge. (Assume that you, the judge, studied cryptography in college.)
   1) Alice could claim that Bob is just lying. She sent this contract to a different company, and it was a valid contract between AliceCom and CharlieCom. Bob was actually lurking during this exchange, used Alice's public key to decode the contract Alice sent to Charlie, and now is presenting this contract as evidence. So Alice is disputing here "C is not the contract I sent ***to Bob****"*

      This one would just be easy to solve, we just need to get Charlie to come in and see if this contract is the same. If it is, only one of them was properly negotiated with, and the other one only has a copy because they were eavesdropping.

   2) Alice could claim that her private key was leaked without her knowledge that it was compromised. So a PITM attack, and when Mal was in the

middle of the exchange, Mal could actually decrypt the contract with the secret key that they know from Diffie-Hellman, decrypt the message further with Alice's public key which is public information, edit it, encrypt it with Alice's stolen private key, and send it over to Bob who doesn't know the difference. Here, Alice is disputing "C is ***not the contract I sent*** to Bob"

This one is fairly convincing. Alice's private key could have been leaked, and she may not have known at all. If it was leaked, then Mal could have been in the middle of the exchange and messed with the contract when it was sent over.

3) Alice could claim a solar flare changed some of the bytes and made the contract different. She sent the correct contract over, conveniently at 11:35 a.m. EDT on October 28, 2021, and because of the solar flare the contract Bob received was different. Here, Alice is disputing "***C*** is not the contract I sent to Bob"

   Good try, but I am not convinced. A solar flare randomly changing bits probably would have led to a completely nonsensical result when Bob decrypted Alice's message, and then he would have told Alice and she would have sent over the contract again. It is very unlikely that a solar flare changed the data in such a way where it makes enough sense that Bob would accept this as a contract Alice would send, and now Alice accidentally violates part of this contract.

5. CA would have to have P_{CA}, S_{CA}, H, E, and a K that it would communicate with when sending certificates and information over to the client (assuming this is happening all online. To create the Sig_{CA} the CA would take the TBS part of the certificate, so "bob.com" and P_B and then hash it, so now they have H(TBS). Now they encode this with their public key, so $E(P_{CA}, H(TBS))$. The CA now has to get this certificate over to Bob, so it needs a key that Bob and the CA agreed to.
6. It's not enough for Alice to believe Bob, because Bob's certificate is now owned by whoever Bob has talked to in the past. So Alice is going to send a random number R when Alice and Bob start communicating. For Bob to prove himself, Alice wants to receive in return $E(S_B, H(K \| R))$ so that she knows that Bob has the key they agreed on (confirmation Mal isn't there in the middle) along with the S_B which matches with the P_B that Bob is claiming to be. Once Alice has this confirmation she is convinced.
7. If Mal was in between the CA and Bob, Mal now knows everything and has Bob's private key. Mal can now act as Bob. Or if Mal was actually posing as the CA, Mal

has everyone’s information, and one of the people they can pose as is Bob, and then use this to fool Alice.