Adela Dujsikova & Ethan Li

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.)

   First, Alice and Bob use Diffie-Hellman to agree on a shared key K. Then, they use K in a symmetric encryption algorithm to send the long message M: Alice sends $C = S_K(M)$ to Bob, and Bob can read it by $M' = S_K^{-1}(C)$.

   The message Alice sends is long, so we can't use asymmetric encryption (public-secret key pairs). And because integrity and authenticity of the message is not as important and person-in-the-middle is impossible, it is sufficient to use the Diffie-Hellman key exchange and encrypt the message symmetrically. Symmetric encryption allows for encrypting a long message and is secure to use when Mal is absent.

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.

   First, Alice and Bob agree on a key K for symmetric encryption using their public-private key pairs. Alice could send to Bob $E(P_B, random\_number)$, which Bob decrypts by doing $E(S_B, E(P_B, randon\_number)$ and could reply to her with $E(P_A, random\_number)$ to agree on the random_number to be their shared key K. Then, Alice encrypts (symmetrically with K) the message concatenated with H(M), such that $C = S_K(M||H(M))$, and sends this C to Bob. Bob can decrypt C and get the decrypted M' and H(M)' using K: $S_K^{-1}(C) = M'||H(M)'$, and ensure that H(M') == H(M)' (to prove that the message was not altered).

   The reason why Alice and Bob need to agree on a key K using asymmetric encryption and not Diffie-Hellman exchange is to ensure that Mal cannot intercept K or the message it encrypts. And because Alice cannot send the long message directly to Bob using asymmetric encryption, she sends the message symmetrically encrypted. To make sure that the message is not modified by Mal, the message is hashed to ensure the integrity of the message is preserved, and sent to Bob alone with the original message.

   The way we performed the exchange of keys and subsequent encryption should be secure enough to prevent Mal from being able to read and comprehend the message. He could still decide to make a random change to the message, therefore using hash helps Alice and Bob detect whether it has been manipulated. This way Bob knows whether Alice simply included some nonsense text in her message or whether it has been tampered with.

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.)

   First, Alice and Bob use Diffie-Hellman to agree on a shared key K. Then Alice concatenates her signature to the message and symmetrically encrypts it using K. The signature could be a simple sentence like "The message is from Alice" or even just her name "Alice" encrypted using public-secret key pairs. Therefore Alice sends to Bob: $C=S_K(M||E(S_A, Sig))$, where Sig = "The message is from Alice".

   It is safe to use Diffie-Hellman key exchange because there is no Mal or other man-in-the-middle, and Eve will only try to observe and not interfere. Symmetric encryption is used because it is better suited for longer messages, compared to using asymmetric encryption. There has to be a signature in the form of encryption with Alice's private key on the message, so that Bob can be sure the message is from her, however, the message itself is too long to be encrypted using (P, S). That's why a short phrase such as the ones mentioned above is used instead. Bob is sure Alice sent the message, because only she could have used her private key (assuming that the public/private key pairs are correct and secure), and he can easily decrypt the signature using her public key.

   Alternatively, the signature could be provided using the more conventional method, which is to hash the message, and then encrypt the resulting digest using Alice's private key. Therefore, the confidentiality, integrity and authenticity of the message would all be accomplished, however, technically the integrity aspect isn't required for this question, and we thought that hashing the message would make our solution not "as simple as possible given the goals of the scenario".

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.

   First, Alice and Bob agree on a shared key K using their public-secret key pairs (the same process we described in question 2). Alice encrypts the message, concatenated with a digital signature using her private key and the digest of the message. In other words, $C=S_K(M||E(S_A, H(M)))$. Bob can decrypt the message by doing $S_K^{-1}(C) = M'||E(S_A, H(M))'$ and decrypt Alice's digital signature by doing $E(P_A, E(S_A, H(M))')$, which yields H(M)'. Again, if H(M)' == H(M'), then Bob can know that the message is sent from Alice and has not been altered by a third party.

We used asymmetric encryption instead of Diffie-Hellman so that in case Mal was present, he couldn't interfere in the conversation. Symmetric encryption was used on the message because it is long and not suitable for (P, S). Using symmetric encryption also ensures that neither Eve nor Mal is able to read the message. For Bob to be sure that Alice sent the message, Alice's private key has to be used at some point. Since the message itself is too long to be encrypted by public-secret key pairs, we hashed the message first and then encrypted the digest using Alice's private key. Bob can be sure that the message came from her because Alice is the only person who knows her private key. The fact that Alice hashed the message and encrypted it with her private key also gives Bob a tool he can use to prove that Alice did send the contract. If Alice tries to claim that she never sent it, he can show that he can decrypt the digest using Alice's public key, and since Alice is the only one who could have encrypted it with her private key, there is no doubt that she sent the document. Lastly, this also shows the version of the contract Alice sent to Bob. If he changed the contract and claimed it was the original, Alice could ask him to hash it and compare it to the digest she concatenated to the message in which she sent the original to him. If the digests don't match, it is a proof that Bob changed it (there is only a marginal chance that Mal was the one who changed it, so it had to be Bob).