Scenarios

Ankit Sanghi, Eric Neidhart, Ginnie White

1. First, Alice and Bob used the Diffie-Hellman Key exchange to agree on a shared key K. Next, Alice uses that key K to encrypt the message M with AES and sends $S_K(M)$ to Bob. Bob then decrypts this message using the key K $S_K^{-1}(S_K(M)) = M$.
    a. If we're not worried about man-in-the-middle attacks, then we can use Diffie Hellman to safely make sure that both Alice and Bob have the same key, and that no one else knows that key. Then once they have the key, they can safely use AES.

2. We're not going to use Diffie-Hellman here because Mal is watching in the middle. We'll use RSA encryption using public and private keys instead. First, Alice comes up with a key K and encrypts it using Bob's public key. We end up with C = $E(P_B, M)$. Then she sends C to Bob, and since only Bob has his private key, Mal cannot decrypt it. Bob receives it and decrypts it using his private key to get $E(S_B, C) = E(S_B, E(P_B,K)) = K$. Then to verify to Alice that he has received the key, he encrypts K using Alice's public key and sends it to Alice. C here is $E(P_a, K)$. Alice receives this and decrypts it using her private key and sees the same K that she sent. Thus, a shared secret key K has been established between Alice and Bob. As the key is a short message, this was a valid method to use here. Alice then creates a hash of the message M to get H(M). Then Alice encrypts the message M with AES to get $S_K(M)$. She then concatenates $S_K(M)$ and H(M) and sends it to Bob. Bob then decrypts the message using K to get the original message M. Then he hashes M to get H(M) and checks to see if it matches the hash sent by Alice. If it does, then he knows the message is unmodified.

3. First, Alice and Bob go through the Diffie-Hellman key exchange to agree on a shared key K. We can use Diffie-Hellman here because there is no person watching in the middle. Next, Alice uses a cryptographic hash on her message H(M), which Alice then needs to use her private key on to create a digital signature $E(S_A, H(M))$. Alice then encrypts her original message M with AES using the shared key K $S_K(M)$. We then concatenate these two things together, and Alice sends $S_K(M) \,||\, E(S_A, H(M))$ to Bob. Once Bob has received the message, he first decrypts the message $S_K(M)$ using his key K to get M. He then hashes M to get H(M). Then he decrypts the digital signature $E(S_A, H(M))$ using Alice's public key to get her signed message. He then checks if this and H(M) match. If they do, then he knows for sure that the message was sent from Alice. If they don't, then he knows that someone has interfered with the message/is impersonating Alice.

4. We're assuming here that Mal is not an issue, but we do have to worry about Bob changing the message. First, Alice and Bob use the Diffie-Hellman Key exchange to agree on a shared key K, because in this scenario, we are acting as if there is no man in the middle. Then, Alice uses a cryptographic hash on her message H(M), which Alice then needs to use her private key on to create a digital signature $E(S_A, H(M))$. Alice then encrypts her original message M with AES using the shared key K $S_K(M)$. Finally, Alice sends $S_K(M) \,||\, E(S_A, H(M)) \,||\, H(M)$ to Bob. When Bob receives the message, he first

decrypts the message $S_K(M)$ using his key K to get M. He then hashes M to get H(M). Then he decrypts the digital signature $E(S_A, H(M))$ using Alice's public key to get her signed message. He then checks if this and H(M) match. If they do, then he knows for sure that the message was sent from Alice. If they don't, then he knows that someone has interfered with the message/is impersonating Alice. On Alice's side, she can ensure that Bob can't change the original message because she sent the hash of the original message to Bob in her payload. So if Bob changes the message, she can point to the hash to show that the hash of the modified contract does not match. To ensure that Alice can't say in court that she never sent the message in the first place, her signature is present in the payload, and since it can be decrypted using her public key, it must have been encrypted by her private key (which only Alice has). This proves that she sent the message.