Ben Aoki-Sherwood, Kenyon Nystrom, Avery Watts

1. Since we are assuming that a person-in-the-middle attack is impossible, Alice and Bob can safely use Diffie-Hellman to agree on a key to use with their symmetric encryption algorithm. They can then use this symmetric encryption algorithm to encrypt and decrypt their long message. Since it is a long message they will not use public key encryption.
    a. **Alice and Bob agree on a shared key K using Diffie-Hellman**
    b. **Alice sends Bob $S_K(M)$ and Bob gets the message by doing $S_K^{-1}(S_K(M)) = M$.**

2. Public key encryption ensures that a third party could not intercept the initial key and therefore secretly read and doctor messages between Alice and Bob. Also, given the ability of a person in the middle to potentially scramble messages without detection, a hash is necessary to guarantee the integrity of the message.
    a. **Alice decides on a key K to use for symmetric encryption and uses public key encryption to send Bob $C = E(S_A, K \,||\, H(K))$**
    b. **Bob receives the message and retrieves the key K by doing $E(P_A, C)$. He knows how long H(K) will be based on the hashing function, so he can separate that part out and then re-compute H(K) to check that the key he received was indeed the one Alice sent.**
    c. **Now having a safe key to use for symmetric encryption, Alice can send Bob $S_K(M \,||\, H(M))$, and Bob can receive the message by doing $S_K^{-1}(S_K(M \,||\, H(M)))$. Once again, he knows the length of the hash so he can separate out the hash digest and re-hash the message to make sure that Mal didn't tamper with it.**
3. Since there is no person in the middle, Bob and Alice can safely use Diffie-Hellman to exchange a key K to use with a MAC algorithm and with a symmetric encryption algorithm (we will assume that they can use the same key for both and be safe, since Eve cannot intercept the key). Alice can then use the MAC to create an authentication code for her message, combine this code with the message, use symmetric encryption to encrypt this, and send it to Bob. Bob can then decrypt and recalculate the MAC to verify that Alice sent the message (since we can assume that only Alice and Bob have access to the key K).
    a. **Alice and Bob can agree on a key K using Diffie-Hellman**
    b. **Alice can create an authentication code for her message using K by doing $C = MAC(K,M)$.**
    c. **Alice can encrypt the message and the code by doing $S_K(M \,||\, C)$ and then send this to Bob.**
    d. **Bob receives the encrypted message and code combination and can decrypt by applying the key again: $S_K^{-1}(S_K(M \,||\, C)) = M \,||\, C$.**

    e. **Since he knows how long the code C should be, he can separate the message and the code and recompute the code by doing C_2 = MAC(K,M), and check to see that C_2 == C so that he knows it was Alice that sent the message.**

4. We start with symmetric encryption to exchange a key. Then, we use digital signing using a cryptographic hash function to ensure the message cannot be modified by Alice or Bob without detection. Bob can use the digital signature and Alice's public key to verify that the message was sent from her, and thus if he keeps a record of the message he can use it as proof that Alice did in fact send the contract. If Alice keeps a record of her digital signature, Bob cannot duplicate it because he doesn't have Alice's secret key, so Bob cannot claim that any changed version is the real version she sent.
    a. **Alice and Bob agree on a shared key K using Diffie-Hellman.**
    b. **Alice creates a digital signature using her secret key and the hash digest of the message: Sig = $E(S_A, H(M))$.**
    c. **Alice concatenates her signature to the message and encrypts the concatenation using symmetric encryption, sending Bob S_K(M || Sig)**
    d. **Bob receives the encrypted message and decrypts it using the symmetric algorithm: $S_K^{-1}(S_K(M \| Sig)) = M \| Sig$**
    e. **Bob somehow separates the signature from the message and re-computes the hash D' = H(M). He can then decrypt the signature using Alice's public key and verify that the message was sent from Alice: he knows this if $E(P_A, Sig) = E(P_A, E(S_A,D)) = D == D'$**