Kaeden Berg and Kitty Tyree

1. Alice wants to send Bob a long message, and she doesn't want Eve to be able to read it.

   For this scenario, we would have Alice and Bob use Diffie Hellman to exchange keys, so they can encrypt and decrypt messages securely.
   Using Diffie Hellman Key exchange would be an effective way to exchange a message without Eve being able to read it because she could not feasibly compute the key K assuming that Alice and Bob are using large enough numbers in their computations.

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.

   For this scenario, we would have Alice and Bob doing asymmetric encryption with their public and private keys to exchange a secret key via the message M. So, Alice would compute $C = E(P_B, M_1)$ and in the message M_1, she would send a key K that would only be known to her and Bob. Bob would then decrypt C using his secret key S_B and would then have access to K. Using K, they would be able to use a cryptographic hash function to generate a message authentication code (MAC) for Alice to send a new message M_2 (the long message), which would allow Bob to double check the message's authenticity by re-hashing the message and comparing the hashes. Because Alice and Bob have exchanged K securely, Mal wouldn't be able to make a new hash for some modified message.

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.

   For this scenario, we would use Diffie Hellman to exchange a secret key K between Alice and Bob. Because we are assuming the exchange is done securely (as we don't have to worry about Mal in this scenario), Bob knows that any message that is encrypted using that key will be from Alice. We will use that key for a symmetric exchange algorithm, where Alice will compute $S_K(M) = C$ and send C, and Bob will decrypt $S_K^{-1}(C) = M$ to get the message. If the message he decrypts is comprehensible, then he will know that the message truly is from Alice (since we know she is the only one with their shared key K)

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.

Assuming that we are not trying to lie in court about sending the contract, we will use a combination of these tools to securely send the contract with signatures and a MAC. To make

sure Bob knows Alice sent the message, she can send a signature along with the message using her secret key. Alice would send along a private key using Asymmetric encryption that will be used to encrypt the contract using a Symmetric Encryption Algorithm, this key would be encrypted as such:

$C = E(P_{Bob}, E(S_{Alice}, M_1))$

Where M_1 contains the key K.

This way, only Bob can decrypt the signature, and because it was encrypted using Alice's private key, Bob knows Alice was the only one who could send it. Mal can't read it because she doesn't have Bob's private key, and couldn't possibly generate it without having Alice's private key. Alice will then encrypt the contract M_2 using the K she sent to Bob earlier, $S_K(M_2) = C$ and send C, and Bob will decrypt $S_K^{-1}(C) = M_2$ to get the contract. Finally, we have to ensure Bob doesn't change the contract.

One way to do this is to create a hash MAC for the contract, but with Alice's private key, and send this hash MAC along with the contract. This way, if Bob changes the contract, it will be different than the MAC, and Alice can show that in court. Bob can't generate a new MAC without Alice's private key, and if he tries to, we simply show that it is an invalid MAC that doesn't correspond with Alice's private key. The assumption is that Bob understands that Hash functions are input sensitive, so he knows that if he changes the document in any way, the hash function will be drastically different from the original document that Alice sent which she will surely be able to present in court.