Armira Nance
CS 338: Computer Security
Prof. Jeff Ondich

Cryptographic Scenarios

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

   Alice and Bob use Diffie-Hellman to agree on a shared secret key *K*. Alice then encrypts the message M using AES(K, M) and sends the ciphertext C to Bob. Upon receipt, Bob can decrypt the ciphertext using AES_D(K, C) to retrieve the message M. Since AITM is impossible here, Alice and Bob can securely use Diffie-Hellman. ANy adversary in the middle can't decipher the ciphertext without K.
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 creates a hash of her message: H(M), then she concatenates the hash with her message, producing M'. Alice and Bob (once again) use Diffie-Hellman to agree on a shared secret key K. Alice can use AES to encrypt M' with our key K to produce her ciphertext C. Alice sends her ciphertext C to Bob and he can decrypt it by using K to get M'. Lastly, he can extract the hash from M' along with the original message to see if the hash matches the message. This method is tamper-evident, because if the message is altered at all, it will no longer match its hash and Bob will be aware that it's not what was originally sent (especially if Alice sends the hash with the encrypted 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 AITM is impossible.

   Alice hashes her message and encrypts the hashed message with her private key to create a digital signature. Then, she concatenates her digital signature with the message to produce M'. Alice and Bob use Diffie-Hellman for a third time to agree on a shared key K, which they use to encrypt M' through AES. That gives us ciphertext C. Alice sends C to Bob and he decrypts it using K to get M'. He decrypts the signature using Alice's public key to get the hash and hashes the message he got from Alice to compare to the decrypted hash. The possibility for hash authentication alongside Alice's use of a digital signature encrypted with

her private key ensures that Alice and Bob have confidentiality and authenticity with their message exchange.

4. 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.)
    a. Alice say that Bob altered the original contract, which wouldn't be very plausible because if Bob had altered it, the hash would change and there would be proof of the alteration
    b. Alice could say her private key was stolen and used to forge her digital signature on a contract that was altered, which is more plausible, but would require Alice to prove that there was ample opportunity for someone to steal her key and that her key was vulnerable to attack.
    c. Alice could say her computer was hacked and someone switched out the actual contract with a fake, which could vary in plausibility depending on whether we're able to compare the hash of the "fake" with the version Alice signed.
5.
6. Bob now has the certificate Cert_B from the previous question. During a communication, Bob sends Alice Cert_B. Is that enough for Alice to believe she's talking to Bob? (Hint: no.) What could Alice and Bob do to convince Alice that Bob has the S_B that goes with the P_B in Cert_B?

    No, it's not enough. Alice and Bob could go through the process of encrypting a test message with the private key, then decrypting with the public key from the certificate. If they match, then that should be enough to assure Alice that she's communicating with Bob.
7. Finally, list at least two ways this certificate-based trust system could be subverted, allowing Mal to convince Alice that Mal is Bob.
    a. Mal could intercept communication and convince Alice that she's communicating with Bob by presenting a fraudulent certificate
    b. Mal could intercept communication and replace Bob's public key with another that could be used to decrypt messages sent from Alice.