Viktor Chekhovoi

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 PITM is impossible.
    a. Alice and Bob use Diffie-Hellman to agree on a shared secret key K.
    b. Alice encrypts the message with AES(K, M) and sends it to Bob.
    c. Bob decrypts the message with AES(K, C).
    d. Eve doesn't know K because Alice and Bob used Diffie-Hellman, so she can't decrypt the message.
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.
    a. Alice and Bob use Diffie-Hellman to agree on a shared secret key K.
    b. Alice encrypts the message with AES(K, M) and sends it to Bob.
    c. Alice also computes $C_h = E(P_B, H(M))$ and sends it to Bob.
    d. Bob decrypts the message with M = AES(K, C) and computes H(M). Then Bob decrypts the hash Alice sent him: $E(S_B, C_h)$. If it's equal to the hash he computed, Mal didn't modify the message.
    e. Because Diffie-Hellman is vulnerable to PITM attacks, Mal can obtain a secret key for communicating with Alice and another for communicating with Bob by intercepting their messages for Diffie-Hellman. As a result, he can tamper with the message Alice sent and replace it with his own message. However, because Alice also sent Bob an RSA-encrypted hash of her message and Mal can't decrypt that, Bob knows the real hash value. Therefore, if Mal modifies Alice's message, Bob will know.
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 PITM is impossible.
    a. Alice and Bob use Diffie-Hellman to agree on a shared secret key K.
    b. Alice computes the hash $H_A = H(M)$ and $Sig = E(S_A, H_A)$, then encrypts $C = AES(K, M||Sig)$ and sends it to Bob
    c. Bob decrypts the message and the encrypted hash with AES(K, C). He then decrypts $H_A = E(P_A, Sig)$. If H_A is equal to the hash of the message he received, he knows it was Alice who sent the message
    d. We know from the first scenario that Even won't be able to read the message. And since Bob can verify that the information in the signature was coherent (because it's the hash of the contract), he knows it could only be encrypted with Alice's private key. If somebody without that key encrypted it, Bob would get gibberish data.
4. Consider scenario #3 above. Suppose Bob sues Alice for breach of contract and presents as evidence: the digitally signed contract (C || Sig) and Alice's public key P_A. 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. Due to a person-in-the-middle attack, a third party was able to replace my signed and encrypted contract with a false contract and a false signature. Since Diffie-Hellman is

vulnerable to those kinds of attack, the person in the middle could have obtained a secret key for both Alice and Bob, then sent a false message to Bob with a fake contract. From a judge's perspective, this is plausible, since Alice and Bob presumed PITM is impossible, which is not true. Alice's explanation of how this attack could have been performed is also correct.

b. A third party impersonated Alice and send Bob a contract, while Alice wasn't a part of the exchange at all. It's unclear how Bob verified that the public key belongs to Alice, which is the only part of the exchange that was directly tied to Alice's identity. From a judge's perspective, this is possible, but unrealistic. Bob would probably verify Alice's public key by contacting a certificate authority, which would make this situation impossible. Moreover, it's unlikely Alice and Bob would not find out about the fake contact before the violation occurred, since from Alice's perspective, no contract existed.

c. Due to the primes used in the Diffie-Hellman exchange and RSA key generation being insufficiently big, an eavesdropper was able to figure out the secret key Alice and Bob agreed on, as well as Alice's private key from the first several packets of the exchange. The eavesdropper then sent Bob a fake certificate and tricked Bob into closing the connection. Judge's perspective: Alice is clearly lying, or the encryption was purposefully weak.

5. For this scenario, suppose the assumption that everybody has everybody else's correct public keys is no longer true. Instead, suppose we now have a certificate authority CA, and that everybody has the correct P_CA (i.e. the certificate authority's key). Suppose further that Bob sent his public key P_B to CA, and that CA then delivered to Bob this certificate:

   Cert_B = "bob.com" || P_B || Sig_CA

   In terms of P_CA, S_CA, H, E, etc., of what would CA consist? That is, show the formula CA would use to compute Sig_CA.

   a. First, CA computes the message M to be included in the certificate: "bob.com" || P_B
   b. The CA computes the hash of the message: $H_{CA} = H(M)$
   c. The CA computes the signature: Sig = $E(S_{CA}, H_{CA})$
   d. The CA concatenates all data together: Cert_B = "bob.com" || P_B || Sig_CA

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?

   a. First, Alice validates the certificate:

   $$Cert_B = TBS||Sig$$
   $$h = H(TBS)$$
   $$s = E(P_{CA}, Sig)$$

   If $h == s$, the certificate is valid.

   b. Alice then gives Bob a challenge to check if he really has the private key – she generates a random number, encrypts it with the public key in the certificate and sends it to Bob.
   c. Bob sends Alice the decrypted random number. If it matches the original, Alice confirmed Bob has the public key

7. Finally, list at least two ways this certificate-based trust system could be subverted, allowing Mal to convince Alice that Mal is Bob.
    1) Mal pretends to be Alice for Bob and Bob for Alice
        a. Mal gets the random number R from Alice and sends it to Bob
        b. Bob encrypts the number and sends it to Mal, who sends it to Alice.
        c. Alice successfully decrypts the random number and trusts Mal.
    2) Mal gets S_CA
        a. Mal forges a certificate that claims to belong to bob.com but has his public key.
        b. Mal sends the fake certificate to Alice.
        c. Alice has no way of telling Mal is Bob. However, it's very unlikely that Mal can get S_CA, although it does happen