Names: Ashok Khare, Lily Haas

SIMPLE COMMUNICATIONS SCENARIOS

1) To send Bob a long message without Eve being able to read it, Alice and Bob can first use Diffie-Hellman to obtain a shared secret key K. Then, Alice can encrypt the message by computing AES(K, M). When Bob receives the encrypted message, he can decrypt it by computing AES_D(K, C) to obtain the original message. Thus, Alice can send Bob her message without Eve being able to read it, since Eve doesn't intercept enough information during the Diffie-Hellman exchange to compute K, and thus is never able to decrypt the ciphertext Alice sends.

Alice		Bob	Eve
Knows K	Use Diffie-Hellman to agree on secret key K	Knows K	Doesn't know K
Has M	Alice sends message (M) as C = AES(K, M)	M = AES_D(K, C)	Can't decrypt

2) If Alice wanted to send Bob a long message while allowing him to detect modifications Mal made to the message, she could first use Diffie-Hellman with Bob to attempt to obtain a shared key K. However, assuming the worst case, Mal can take advantage of this to perform two Diffie-Hellman exchanges with Alice and Bob, obtaining a shared key K_A from the exchange with Alice and K_B from the exchange with Bob. After the Diffie-Hellman exchange, Alice can compute the hash of her message H(M) and encrypt that with her secret key to obtain her digital signature E(S_A, H(M)). Then, Alice can encrypt the message with K_A and concatenate that to her signature, obtaining AES(K_A, M) || E(S_A, H(M)). Then she can send that to Bob.

In this case, Mal could easily view the original message by performing AES_D(K_A, C). Mal could also obtain the hash of the original message by performing E(P_A, E(S_A, H(M)). Thus, Mal could easily modify the message and then encrypt it using K_B, as well as figure out the digest of the modified message. However, because Mal does not know S_A, they could not forge Alice's digital signature using the new digest.

Therefore, if Bob receives Mal's message and tries to decrypt the forged signature using P_A, it is very unlikely that he will end up with the same hash value as the one he gets when he hashes the changed message himself. This is because Mal cannot efficiently guess which hash would result in decrypting a signature created with S_A using P_A, and thus cannot ensure that the hash in the signature will match the hash generated by the modified message.

Alice		Mal		Bob
Has K_A	Diffie-Hellman	Has K_A and K_B	Diffie-Hellman	Has K_B
AES(K_A, M) || E(S_A, H(M))	Alice sends AES(K_A, M) || E(S_A, H(M))	Decrypts and modifies message but cannot forge digital signature without S_A	Mal sends modified message to Bob	Use AES_D(K_A, C) and E(P_A, E(S_A, H(M)) to check the integrity of the message, see that the messages do not match and terminate connection

3) To send Bob a long contract without Eve being able to read it, Alice and Bob can first use Diffie-Hellman to obtain a shared secret key K. Importantly, Eve can't intercept enough information during the exchange to be able to compute K herself. Then, Alice can compute the hash of the message H(M) and encrypt that digest using her secret key S_A. Then, Alice can concatenate E(S_A, H(M)) to the original message M, then encrypt the whole thing using the AES algorithm and K to send Bob AES(K, M || E(S_A, H(M))). Again, because Eve doesn't know K, she cannot decrypt the message and read it.

However, when Bob gets the message, he can compute AES_D(K, C) to obtain M and E(S_A, H(M)). Using Alice's public key P_A, Bob can compute E(P_A, E(S_A, H(M))) to obtain H(M), then hash M himself and check if the two hashes are equal. If they are, then Bob knows the digest must have been encrypted using Alice's secret key, which gives him confidence that she was really the one who sent the message.

Alice		Bob	Eve
Knows K	Use Diffie-Hellman to agree on secret key K	Knows K	Doesn't know K
AES(K, M || E(S_A, H(M)))	Alice sends AES(K, M || E(S_A, H(M)))	Check that both messages are the same, if so we're good	Cannot decrypt without K

QUESTIONS ABOUT BREAKING SECURITY

4) The first claim that Alice could make is that her private key has been compromised and Bob has used it to encrypt an altered version of the contract he and Alice had agreed on. The credibility of this relies on Alice and Bob’s knowledge of cryptography and how Alice claims her key has been stolen. If Alice can provide evidence she had no further exchanges with Bob after the contract she has was agreed upon, this would be credible.
Alice could also claim the contract exchange was subject to a Person in the Middle attack. She claims that Mal used Alice’s public key to pose as her and Bob did not ensure that it was really Alice sending the message by decrypting the signature with Alice’s public key. If this were the case, the contracts in the text and signature would not match because Mal would not have been able to change the signature and encrypt it without Alice’s secret key. The credibility of this claim would depend on how responsible Bob is as a business partner - if he is unreliable, then the claim is entirely possible, but if he reliably checks the legitimacy of the party sending the contract, then the claim is less plausible.
Lastly, Alice could claim that a corrupt certificate authority allowed someone to pose as her and negotiate a new contract with Bob, who trusted the certificate authority to do their job in vetting the connection. The believability of this is dependent on the reputation of the certificate authority and thus would need to be judged on a case by case basis.

5) To compute the signature Sig$_{CA}$, the certificate authority CA would first concatenate the items in the TBS, which in this case are “bob.com” and P_B. Then, the CA would hash the TBS by computing H(“bob.com” || P_B). Then, the CA would encrypt the digest using its secret key S_{CA}, computing E(S_{CA}, H(“bob.com” || P_B)) to get the final signature Sig$_{CA}$.

“bob.com”	TBS (to be signed)
P_B	
E(S_{CA}, H(“bob.com” || P_B))	Sig$_{CA}$ (Signature)

6) Bob sending Alice Cert$_B$ is not enough for Alice to trust that she is really talking to Bob. To increase Alice’s confidence, Bob can send Alice Cert$_B$ along with his part of a Diffie-Hellman exchange. When Alice receives Cert$_B$, she could send Bob a random number R. Then, Bob could encrypt R by computing E(S_B, H(K || R)), where K is whatever key Bob is using in the Diffie-Hellman exchange, and send that ciphertext to Alice. Alice can check it by computing E(P_B, E(S_B, H(K || R))). If the resulting digest is equal to the digest Alice gets when she hashes K || R, she knows that the message must have really been encrypted by Bob using S_B.

Mal can’t do anything about this - if they are just observing, then they can’t calculate K and thus can’t perform the AES encryption with Alice. If Mal instead used the classic person-in-the-middle strategy during Diffie-Helman and then passed on Alice’s challenge to Bob, then the K_B Bob uses to compute his response would not be the same as the K_A Mal has established with Alice. Therefore, when Mal passes on Bob’s response to Alice (Mal herself can’t respond because she doesn't know S_B), Alice will find that her digest resulting from hashing K_A || R is not the same as Bob's, which resulted from hashing K_B || R.

Alice		Bob
Knows K	Diffie-Hellman to agree on K and Bob sends Cert_B	Knows K
Knows R	Alice sends R	Knows R, encrypts a hash of K and R with his private key
Validates $E(P_B,E(S_B,H(K\|\|R)))) = H(K\|\|R)$	Bob sends $E(S_B, H(K\|\|R))$	
AES(K,M)	Alice sends AES(K,M)	

7) One way that Mal could subvert the certificate trust system to convince Alice that Mal is Bob is by falsely advertising their own public key as Bob's public key, and somehow tricking the CA into thinking that they are actually Bob to obtain a certificate in Bob's name. Then, Mal could use their certificate and public key to pose as Bob, and if Alice trusts the certificate authority and does not verify Bob's identity herself, she would not catch that she is actually talking to Mal.

In a simpler instance, Mal could intercept Bob's legitimate certificate when the CA sends the signed copy back to Bob. Then, Mal could claim that they are Bob by sending Bob's intercepted certificate to Alice. If Alice checks the certificate with the CA, she will find that it is indeed legitimate. Then, as long as Alice never checks that Mal (posing as Bob) actually has the real Bob's secret key, there is no evidence that Mal is not actually Bob.