Authors: Anders Shenholm, Riaz Kelly

Numbered bullet points are the plans

Lettered bullet points are the explanations of why the plans work

1. Alice and Bob use Diffie-Hellman key exchange to agree on a shared key K. Alice sends Bob $S_K(M)$ Bob can find $S_K^{-1}(S_K(M)) = M$.
    a. This plan will work because the Diffie–Hellman key exchange forces both Alice and Bob to create their own key and combine the two to eventually use K to encrypt and decrypt the message. Since Alice and Bob use very large integers to create their keys, Eve will not be able to crack the code and read their message with her minimal knowledge of the keys.
2. Alice generates H(M) and sends Bob M||H(M). Bob receives M'||H(M)'. Bob can check H(M'). If H(M') == H(M)', Bob can be sure that M'||H(M)' = M||H(M).
    a. This plan will work because Bob checks the hash of the message he receives against the hash he received. If Mal modified the message, Bob wouldn't receive the correct message, but would know this because the hashes wouldn't match.
3. Alice generates sig = $E(S_A, D)$. Additionally, Alice and Bob use Diffie-Hellman key exchange to agree on a shared key K. Alice sends Bob $S_K(M||sig)$. Bob receives $S_K(M'||sig')$ and determines $S_K^{-1}(S_K(M'||sig') = M'||sig'$. Bob then checks Alice's signature decrypted by her public key against the digest that results from H(M'). If D' = $E(P_A, sig')$, Bob can be sure that the message came from Alice.
    a. As previously explained, we know Eve will not be able to read the message because of the Diffie–Hellman procedure. We also know that Bob receives the correct message because Mal isn't involved and Eve can't decrypt it. To ensure that Bob knows it was Alice who sent the message, Bob, who can fully trust Alice's public key, decrypts the digital signature using Alice's public key against the digest of the message he received (which he knows is the correct message).
4. Alice generates sig = $E(S_A, D)$. Additionally, Alice and Bob use Diffie-Hellman key exchange to agree on a shared key K. Alice sends Bob $S_k(M||sig)$. Bob receives $S_K(M'||sig')$ and determines $S_K^{-1}(S_K(M'||sig') = M'||sig'$. Bob then checks Alice's signature decrypted by her public key against the digest that results from H(M'). If D' = $E(P_A, sig')$, Bob can be sure that the message came from Alice.
    a. As previously explained, we know Eve will not be able to read the message because of the Diffie–Hellman procedure. Also as explained in part three, Bob can be sure it was Alice who sent the message because of the digital signature. Since Alice sends a digest of the original message encrypted via her private key (her signature), if Bob changes the message he will be unable to generate an accurate signature for the message, so he would be detected. Therefore, Bob will not be able to change the message and claim the changed message to be the original message. Bob knows Alice won't be able to claim that she never sent the message because she sent her digital signature which was encrypted via her

private key. Since Alice’s private key is unique to her, she will not be able to claim she never sent the message.