Yasmeen Awad, Nacho Rodriguez-Cortes

1. Alice and Bob use Diffie-Hellman to agree on a shared secret key K. They then use symmetric encryption to encrypt the message in chunks (as large as the algorithm will allow) using the shared secret key K, using K to both encrypt and decrypt the ciphertext.

- Alice would use: $S_K(M)$ to encrypt her message into ciphertext.
- Bob would utilize: $S_K^{-1}(S_K(M)) = M$ to decrypt the message.

2. Alice and Bob should agree upon a shared secret key K.

- Alice should first send over $E(P_B, E(S_A, K))$, which represents the proposed shared key K encrypted with Alice's secret key, then encrypted with Bob's public key. When Bob receives this, he can use his secret key S_B and then Alice's public key P_A to twice-decrypt the message and get the shared key K.
- They should then use the shared key K for symmetric encryption.
- Alice should use a hash function H to create a digest D= H(M) and add this to the encrypted message when using symmetric encryption so that Bob can rehash after decrypting the message to make sure that it hasn't been altered by Mal.

3. Alice and Bob should use Diffie-Hellman to agree on a shared secret key K. Then Alice can use symmetric encryption to encrypt the message in chunks and Bob can decrypt them using the shared secret key K.

- Alice and Bob should use a cryptographic hash to create a digital signature, which ensures that Bob got the message from Alice, and nobody else (since Alice is the only one who knows her secret key). The digital signature will be executed as follows:
- Alice should send Bob a digest D=H(M) (appended to the end of the message), that has been encrypted with her secret key, $Sig = E(S_A , D)$. To check the signature, Bob will have to hash the message received with the signature and decrypt the signature using Alice's public key to check that it matches the hash he just created.

4. Alice and Bob should use Diffie-Hellman to agree on a shared secret key K. Then Alice can use symmetric encryption to encrypt the message in chunks, with her digital signature at the end.

- Since Alice's digital signature consists of the hash of the message, encrypted using her secret key, there is no way Bob or anyone else can modify the message without her knowing (because of the appended hash), and Bob can prove that Alice sent the message because the hash is encrypted using her secret key, which only Alice knows.
- Bob can decrypt the message using the shared key K, and can decrypt the digital signature using Alice's public key. Bob can then check that the decrypted digital signature matches the hash of the message.