1. **Steps:**

   (a) Alice and Bob use Diffie-Hellman to agree on a shared secrety key K.

   (b) Alice sends Bob $S_K(M)$.

   (c) Bob computes $S_K^{-1}(S_K(M)) = M$ to decrypt and find the plaintext.

   Analysis: The Diffie-Hellman exchange provides a way for Alice and Bob to decide upon a key without Eve knowing what that key is. We use the symmetric encryption algorithm to hide the contents of the message itself as it is transferred from Alice to Bob. Because the message is long, it would be impractical to use RSA to encrypt the entire message. This use of Diffie-Hellman with symmetric encryption forms the foundation for the rest of the scenarios, as it can always be used to hide the message, even if it does not guarantee who the message came from or that it was not tampered with.

2. **Steps:**

   (a) Alice and Bob use Diffie-Hellman to agree on a shared secret key K.

   (b) Alice finds $H(M)$.

   (c) Alice encrypts $H(M)$ as $C = E(P_B, H(M))$ where P_B is Bob's public key.

   (d) Alice sends Bob $S_K(M)$ and C.

   (e) Bob decrypts C with $E(S_B, C) = E(S_B, E(P_B, H(M))) = H(M)$.

   (f) Bob computes $S_K^{-1}(S_K(M)) = M$.

   (g) Bob computes $H_0(M)$. If $H(M) = H_0(M)$, then the message has not been tampered with. Otherwise, Mal has tampered with the message.

   Analysis: As in the first scenario, we apply Diffie-Hellman and symmetric encryption. If Mal, however, is in a position to intercept the message, they could hypothetically change its contents randomly even if they do not know what it says. Thus, we add a new security layer where Alice hashes the message, encrypts it using RSA, and then sends this extra information along with the message itself. The output of the hash function, or digest, is deterministic, so if Mal had intercepted the original message and made even a slight change, Bob would detect this change when he rehashes the message he receives and finds that the two hashes are different. Because the hash is always the same short length, we can efficiently apply RSA as an additional layer of protection so that only Bob can see the hash because only he knows his secret key.

3. **Steps:**

   (a) Alice and Bob use Diffie-Hellman to agree on a shared secret key K.

   (b) Alice finds $H(M)$.

   (c) Alice encrypts $H(M)$ as $C = E(S_A, H(M))$ where S_A is Alice's private key.

   (d) Alice sends Bob $S_K(M)$ and C.

   (e) Bob decrypts C with $E(P_A, C) = E(P_A, E(S_A, H(M))) = H(M)$.

   (f) Bob computes $S_K^{-1}(S_K(M)) = M$.

   (g) Bob computes $H_0(M)$. If $H_0(M) = H(M)$, then Alice sent the message. Otherwise, someone else sent it.

Analysis: We begin as in the previous scenarios. This time, Alice adds a digital signature to the message. As in the second scenario, Alice hashes the message she is sending. Instead of encrypting it using Bob's public key, she encrypts it using her own secret key. Bob has access to her public key, which will reverse this encryption. Thus, by comparing his own digest of the message to the unencrypted digest that Alice sent, he can prove that it originated with her. If applying Alice's public key doesn't produce an identical hash, then it can't have come from Alice.

4. **Steps:**

   (a) Alice and Bob use Diffie-Hellman to agree on a shared secret key K.

   (b) Alice finds $H(M)$.

   (c) Alice performs two encryptions. First she finds $C_1 = E(P_B, H(M))$. Then she finds $C_2 = E(S_A, E(P_B, H(M))) = E(S_A, C_1)$.

   (d) Alice sends Bob $S_K(M)$ and C_2.

   (e) Bob decrypts C_2 with $E(P_A, C_2) = E(P_A, E(S_A, C_1)) = C_1$. Then he decrypts C_1 with $E(S_B, C_1) = E(S_B, E(P_B, H(M))) = H(M)$.

   (f) Bob computes $S_K^{-1}(S_K(M)) = M$.

   (g) Bob computes $H_0(M)$. If $H_0(M) = H(M)$, then Alice sent the message. Otherwise, someone else sent it.

   Analysis: Between the third and fourth scenarios, Alice has added another layer of protection to the digest by encrypting it twice, first with Bob's public key, and then again using her own. That Alice's public key successfully decrypts the first layer of protection is enough proof that it came from Alice. Further, note that we must perform the encryption in this order. Suppose Alice had first encrypted with her secret key, encrypted it with George's public key, and then sent it to George. George could have applied his secret key to undo the first layer of protection and then encrypted it with Bob's public key and passed on the message to Bob. Thus, it is plausible that Alice never intended that the message would be sent to Bob, even though he is now in a position to decode it. Alice, then, could claim in court that this is how he came into possession of the message. Therefore, by applying Bob's public key before applying her own secret key, Alice not only ensures the message hasn't been tampered with, but also explicitly acknowledges who the intended receiver is, clarifying that Alice did in fact send the message to Bob. Finally, Bob cannot change the contents of the message without changing value of the digest, nor can he perform an encryption with Alice's secret key, so we can be assured that he cannot pass of an edited version as the real version.