Student name: Le Thi Thu Tra
Student ID: ITDSIU19058
Course: Fundamental Concepts of Data Security

FINAL EXAMINATION

Question 1

I. Explaining how the attack as shown in Figure 2 works

This attack involves 2 concurrent protocol runs:

- The 1st run (steps 1-3, 1-6, and 1-7): Alice establishes a valid session with Malice.
- The 2nd run (steps 2-3, 2-6, and 2-7): Malice impersonates Alice to form a bogus session with Bob.

Here is the process of how this attack works:

- **Step 1-3**: Alice begins to establish a normal session with Malice, sending him a nonce NA.
- **Step 2-3**: Malice impersonates Alice to try to establish a bogus session with Bob, sending the bonce NA from Alice to Bob.
- **Step 2-6**: Bob responds by picking a new nonce NB, and trying to return it to Alice together with NA. This communication is intercepted by Malice, but it can not be decrypted since it is encrypted with Alice's public key.
- **Step 1-6**: Malice tries to use Alice to execute the decryption for him by sending the message to Alice. This message is of the form expected by Alice in the first run of the protocol.
- **Step 1-7**: Alice decrypts the message to obtain NB, and encrypts it with Malice's public key, then she sends it to Malice.
- **Step 2-7**: Malice can then decode this message to obtain NB, and returns this to Bob.

As a result, Bob believes that he is sharing secrets NA, NB with Alice while actually sharing them with Malice.

II. Presenting a solution to address this attack

A solution to prevent the attack above:

Step 1: Alice → Bob: $[\{NA\}K_B, Alice]K_A$.

- Alice encrypts her nonce NA with Bob's public key K_B.
- Alice sends the message $[\{NA\}K_B, Alice]K_A$ which is signed by her public key K_A (Alice's signature) to Bob.

Step 2: Bob → Alice: $[\{NA, NB\}K_A]K_B$.

- Bob verifies the signature of Alice.
- If no errors when verifying, he uses his private key to decrypt the message and obtain Alice's nonce NA.
- Bob creates her own nonce NB randomly.
- Then, Bob encrypts the message, which includes both NA and NB, with Alice's public key K_A and sends it to Alice with his signature K_B.

Step 3: Alice → Bob: $[\{NB\}K_B]K_A$.

- Alice verifies the signature of Bob.
- If no errors when verifying, she decrypts the message to get NB.
- Then, Alice encrypts NB with Bob's public key K_B and sends it to Bob with her signature K_A.

In this solution, Alice can send her signature to Malice, and Malice can decrypt to retrieve the signature and re-encrypt it using Bob's public key. Malice also can impersonate Alice to establish a session with Bob by using Alice's signature. However, because in step 2, the message is signed by Bob, then Alice can detect an error when she tries to verify Malice's signature. Therefore, Malice can not forward Bob's response to Alice as he did in the attack.