Quiz 2

1. Describe the difference when we use secret key cryptography and public key cryptography for encryption and decryption.

   Secret key cryptography uses a single key for both encryption and decryption, i.e., the sender encrypts the plaintext with the key, and the receiver decrypts the ciphertext with the same key. In public key cryptography, each individual has two keys: a private key and a public key. The sender encrypts the plaintext using the public key of the receiver, and the receiver decrypts the ciphertext using his own private key.

2. How could Alice authenticate Bob by using secret key cryptography?

   Alice picks a random number, known as a challenge, and sends it to Bob. Bob encrypts the random number with the shared secret key, and sends back the ciphertext to Alice. Alice decrypts the ciphertext and compares the result with the original random number. If they are the same, Bob is authenticated.

3. Assume Alice wants to send a message to Bob. How to generate the digital signature for the message?

   Alice encrypts the message with her private key and the result is the digital signature. When Bob receives the message together with the digital signature, he decrypts the digital signature using Alice's public key and compare the result with the message itself to verify whether the message has been modified.