**2?a) Eve cannot do much. Diffie-Hellman is a public-key algorithm which is asymmetric cryptography. Because of the nature of asymmetric cryptography, she cannot do much to the conversation because asymmetric cryptography is great at providing authenticity. If she intercepted a message that was encrypted using a private key and decrypted it using the readily available corresponding public key, even if she altered the message and resent it to who was originally supposed to receive the message, the person who receives it would know if the message was intercepted because the receiver would have to decrypt the again encrypted message with their private key when they were expecting to decrypt the message using their public key because it was resent while encrypted using the public key because that’s all Eve had to resend the message. Also, if the message was altered, the receiver will know it was altered because the digital signature using a hash function will not match. Without any of the private keys known bye Eve, she can’t send messages under the false identity of Alice or Bob.**

**2?b) Eve could do a man-in-the-middle attack in which she impersonates both Alice and Bob. She can intercept the message from the sender, let’s say in this case Bob; decrypt it using Bob’s public key; tamper with the message; re-encrypt it using the receiver’s public key, in this case it’s Alice’s public key; and then resend it to who was meant to receive it, in this case Alice. Alice will then decrypt the tampered encrypted message using her private key. This only works if Eve can both trick Alice into believing she is Bob and trick Bob into believing she is Alice.**