**Question 3:**

Now that the secure channel has been established, further messages passed along the wire will be encrypted using symmetric ciphers for confidentiality and a message authentication code will be added for the purpose of integrity. One the session key has been successfully generated for Alice and Bob the due to the Discrete Logarithmic problem Eve will not be able to compute their private keys in a reasonable amount of time. This contributes to the security of the session. The session key will also go through the key derivation function (KDF) using a pseudo random function to use if the paradigm Extract-and-Expand, to distribute randomness of session key across multiple keys. These keys are used once for per each use and direction. The randomness from the secret key will be extracted using HMAC with a random salt using the Pseudo random function. The will each generate an array of keys that can then be used to encrypt future messages. Once a key has been used it is removed from the array. These keys will be indistinguishable from any group element.

**Question 4a:**

To break the Diffie Hellman key exchange as an active attacker, Eve will first intercept the value A from Alice. This value A doesn’t reach Bob. Eve will know the modulus and the base so will generate two secrets key of her own form (Zp)\*, ea and eb. She will perform the same calculation as Alice to get her own value Ea using the secret key ea. Eve will send her value Ea to Bob. Bob will then send his value B to Eve. Bob will generate his session key with Eves value Ea. Eve will then compute Eb using the secret key eb, she will send this to Alice. Alice will compute a session key with Eb . Eve knows Both A and B now and can compute the same session keys with Alice and Bob. Now Alice and Eve had a secure connection and Bob and Eve have a secure connection. Diffie Hellman is only secure against passive eavesdroppers.