16-124-836
Marcel Matti ZAUDER

8.6 Question 6

8.6.A What are the advantages of IKE key determination over the Diffie-Hellman key exchange algorithm.

An advantage of IKE would be that it prevents the use of clogging attacks and in order to counteract replay attacks nonces are used. Furthermore, by authenticating the exchanges Man-in-the-Middle attacks are made more difficult. Lastly, it is possible to negotiate a group and enable the exchange of DH public keys.