Assignment 4

Group – Sauls

Part 2:

2.1 First IKE_SA_INIT message that is sent: Name the types of IKE payloads carried in this message and indicate the purpose of each payload type.
The payload types are the Security Association, Key Exchange, and Nonce.
Nonces- These payloads are used as inputs to cryptographic functions.
Security Association – Used to negotiate attributes of a security association
Key Exchange – Used to exchange Diffie-Hellman public numbers as part of a Diffie-Hellman key exchange.
2.2 Second IKE_AUTH message (from the responder): Name all the cryptographic algorithms chosen in this message and indicate the purpose of each.
HMAC-MD5-96 is an algorithm used to help prevent any data from being tampered with.
HMAC-SHA-1-96 is an algorithm to help provide data origin authentication and integrity protection
ENCR_AES_CBC is an algorithm used for confidentiality
2.3 First ESP packet that is sent: Is it possible to find the number of encrypted bytes in this ESP packet excluding the ESP trailer and the ESP auth field that would be placed at the end of the packet? Explain your answer.
It would be very difficult to determine the exact number of bytes in any of the ESP packets due to how ESP greatly increasing the actual size of the data through the encryption algorithms used. As the algorithms like AES, and SHA will already expand the actual byte size making it nearly impossible to determine the actual amount of bytes in that specific packet.