4. a) Brute force attacks are countered by the key lifetime being only a few minutes in time. A brute force attack would have to reset every time the keys change since the brute force algorithm may have already looked over the new key. The key sizes are so large that a 5-10 minute brute force attack would not be enough time to find the key.

b) The sequence number in the AH or ESP headers ensures that replay attacks won’t happen. If an attacker sends a previously sent packet, the sequence number will be either behind the current sequence number or will be stored in the server briefly so it will know that the attack packet is a duplicate.

c) If the man in the middle attack is launched during the key exchange phase is mitigated by step 3 where the client and server authenticate who they are. If the certificate is not authentic, it will fail and the client will not continue communication.

d) Again, if the attacker spoofed IPs they still have to be authenticated in IPsec. So if a spoofed IP address comes in, it still has to be authenticated which a spoofed IP cannot do.

e) A TCP flood attack is mitigated by the firewalls in IPsec. Since VPNs use firewalls, the firewall can handle the TCP flood. The firewall is responsible for ensuring access control. It can also be mitigated because TCP flooding is usually done with IP address spoofing, which as discussed in d), can be stopped since IPs are authenticated.