Homework 3

1. Assume root server has Xbank’s certificate. Bob would like to securely communicate to Xbank’s server. Assume Bob has no trust established beforehand. (20 points)
2. What certificate/certificates does Bob need?
3. Show the names of issuer and owner (to whom this certificate is issued to) of each certificate/certificates
4. Why PGP certificates allows more than one signatures enclosed in one certificate? (10 points)
5. What is the different of DOS attack and Distributed DOS (DDOS) attack? (10 points)
6. What security property could be achieved after establishing TLS/SSL connection? (10 points)
7. If you as the client are using VPN to connect to a host V in a private network (e.g., the BSU campus network). The packet structure generated by client-side VPN is like this (only the IP address parts are shown): (20 points)

Src: 201.188.1.23 | Dst: 231.34.221.231 | Src: 192.168.0.31 | Dst: 10.31.331.59

1. For an intermediate router that transfers this packet in the middle of tunneling route, which source IP address and destination IP address are exposed?
2. For the host V inside the private network, what is the source IP address of the received packet?