In the name of beauty
The assignment #12 of the ComNet course

Q1)

a) At which layer is SSL implemented and why?

b) Why does sequence numbering prevent an intruder from re-ordering seg- ments? What happens if the sequence numbers are not encrypted by hash (i.e. only the data and the MAC key are included in hash calculations)?

Q2)

a) For what reason, is network-layer security said to provide blanket coverage and what does that mean anyway?

b) What is Security Policy Database (SPD) and what does it stand for?

Q3)

a) What problem can be caused when a duplicate key is used in WEP?

b) Since MK is a shared key between the client and the authentication server, how can we generate a shared key between the client and the access point?

Q4)
Assume that an attacker wants to perform a DoS (Denial of Service) attack by sending TCP ACK segments to an internal network. A possible solution is to configure the internal firewall to block (i.e. drop) all the incoming TCP ACK segments. What problem does this solution make and how to bypass it?