Tutorial – XIII (IPSec)

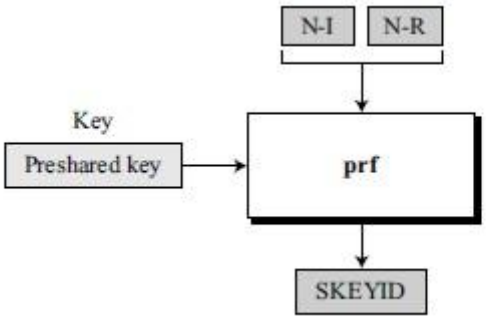
1. Discuss replay attack prevention using sequence numbers and a sliding receiver window in IPSec protocol. Assume the following scenario to answer

   (i) A host receives an authenticated packet with the sequence number 181. The replay window spans from 200 to 263. What will the host do with the packet? What is the window span after this event?

   (ii) A host receives an authenticated packet with the sequence number 208. The replay window spans from 200 to 263. What will the host do with the packet? What is the window span after this event?

   (iii)A host receives an authenticated packet with the sequence number 331. The replay window spans from 200 to 263. What will the host do with the packet? What is the window span after this event?

2. The diagram for calculation of SKEYID for the preshared-key method is shown below



   (i). Draw a similar diagram of SKEYID for the public-key method.
   (ii) Draw a similar diagram of SKEYID for the digital signature method.

   (iii) Draw a similar diagram for SKEYID_a, SKEYID_d, SKEYID_e and HASH-R

3. Draw a diagram and show actual ISAKMP packets that are exchanged between an initiator and a responder using the preshared-key method in the main mode. Use at least two proposal packets with at least two transform packets for each proposal.