CHAPTER 18

IPSec

(Solution to Odd-Numbered Problems)

Review Questions

1. IPSec operates in one of the two modes: the transport mode or tunnel mode.

a. In the transport mode, IPSec protects what is delivered from the transport layer to the network layer. In other words, the transport mode protects the network layer payload.

b. In the tunnel mode, IPSec protects the entire IP packet. It takes an IP packet, including the header, applies IPSec algorithm to the entire packet, and then adds a new IP header.

3. ESP is the more sophisticated protocol in IPSec. It adds both a header and a trailer to the IP payload. ESP provides source authentication, data integrity, and privacy.

5. SAD is a set of SAs that can be collected into a database. The database can be thought of as a two-dimensional table with each row defining a single SA.

7. The Internet Key Exchange (IKE) is a protocol designed to create Security Associations. When a peer needs to send an IP packet, it consults the Security Policy Database (SPD) to see if there is an SA for that type of traffic. If there is no SA, IKE is called to establish one. In other words, IKE creates SAs for IPSec.

9. The ISAKMP protocol is designed to carry messages for the IKE exchange.

Exercise

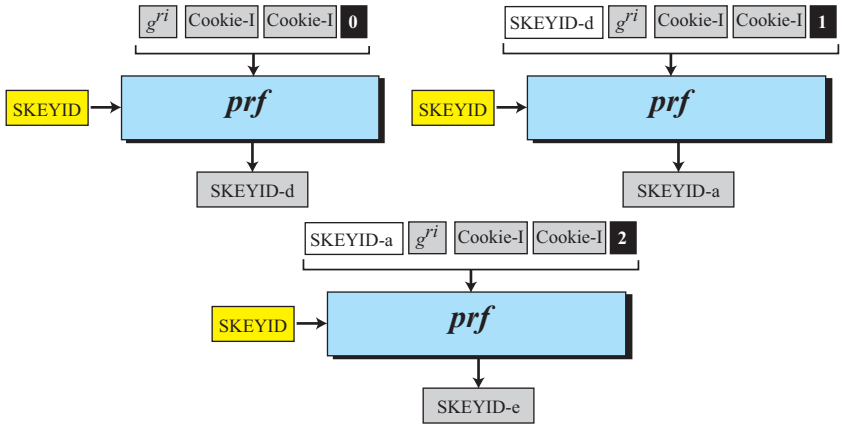
11. Since the sequence number of the packet (181) is out of the window (200 to 264), the packet is discarded. It is either duplicate or its arrival time has expired. The window span does not change.

13. The sequence number of the packet (331) is at the right of the window. Since the packet is authenticated, it is accepted and the window span will change as shown in Figure S18.13.

15. Figure S18.15 shows the diagram.

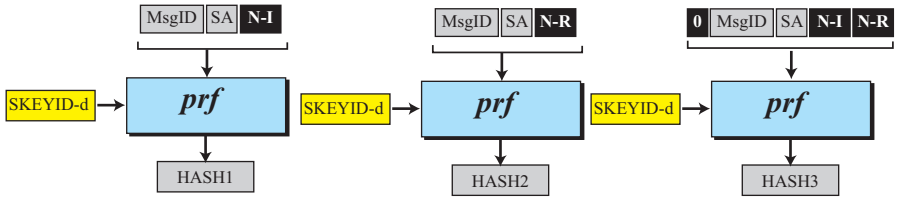
Figure S18.13 *Solution to Exercise 13*

Figure S18.15 *Solution to Exercise 15*



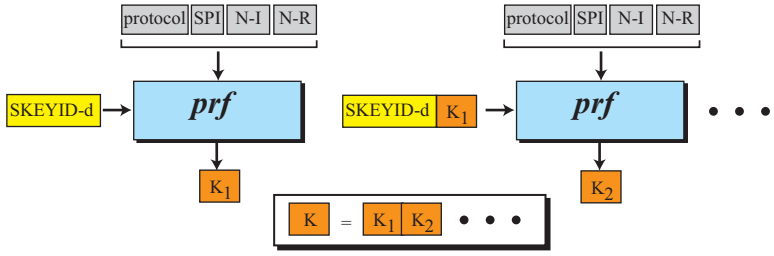
17. Figure S18.17 shows the diagram.

Figure S18.17 *Solution to Exercise 17*



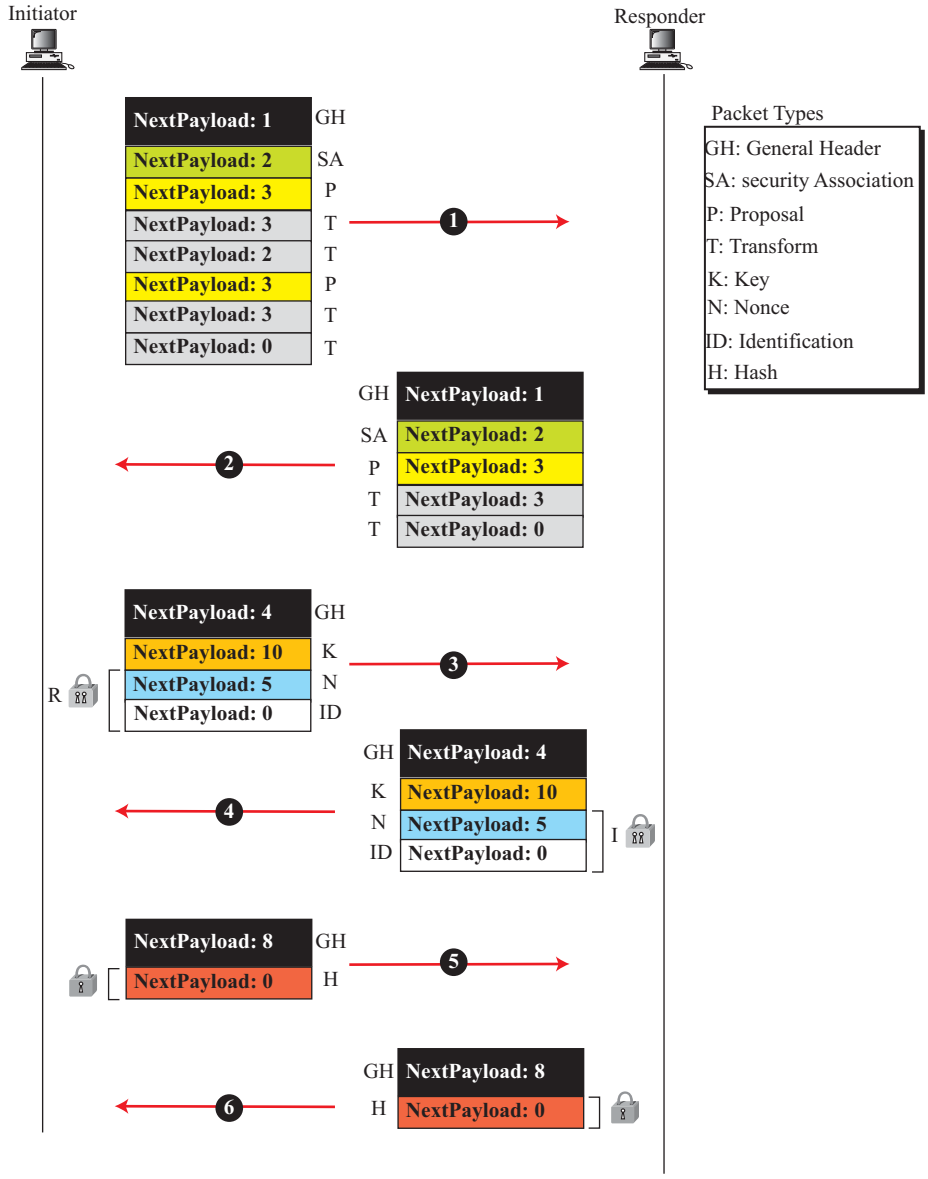
19. Figure S18.19 shows the diagram without using PSF. The one with PSF is similar. (see the solution to Exercise 18).

Figure S18.19 *Solution to Exercise 19*



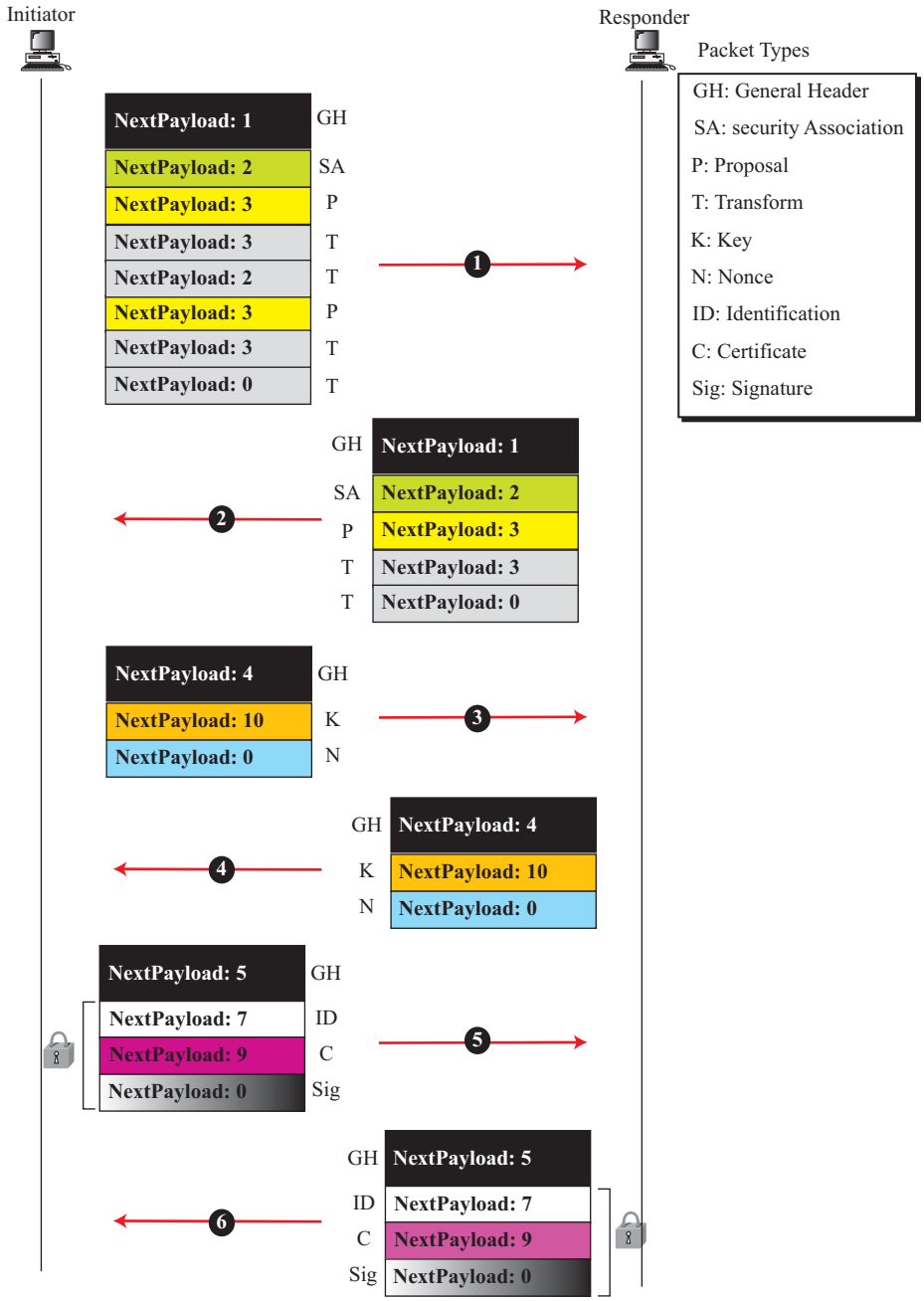
21. Figure S18.21 shows only the layout of the packets and next payload value. When a packet is encrypted, a padlock is inserted next to the packet.

Figure S18.21 *Solution to Exercise 21*



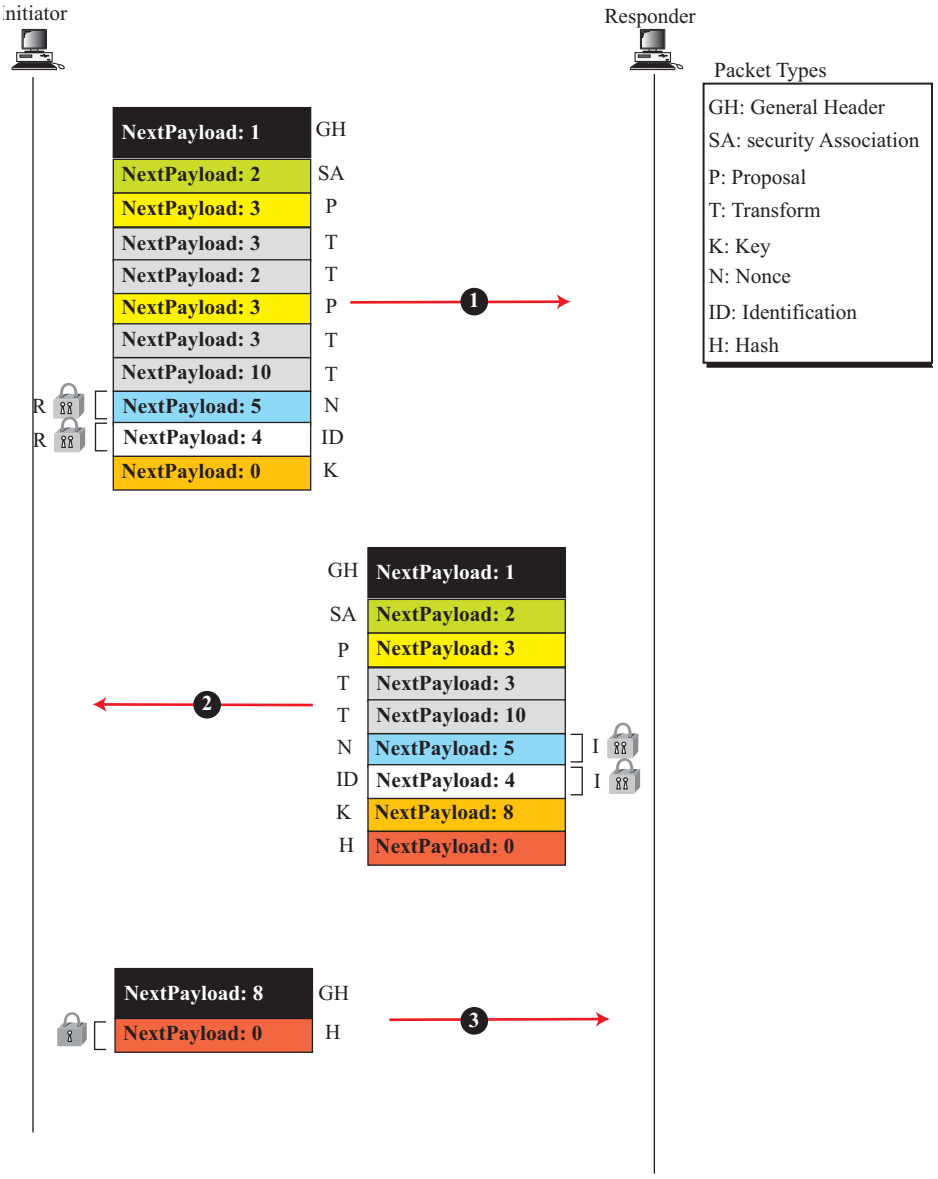
23. Figure S18.23 shows only the layout of the packets and next payload value. When a packet is encrypted, a padlock is inserted next to the packet.

Figure S18.23 *Solution to Exercise 23*



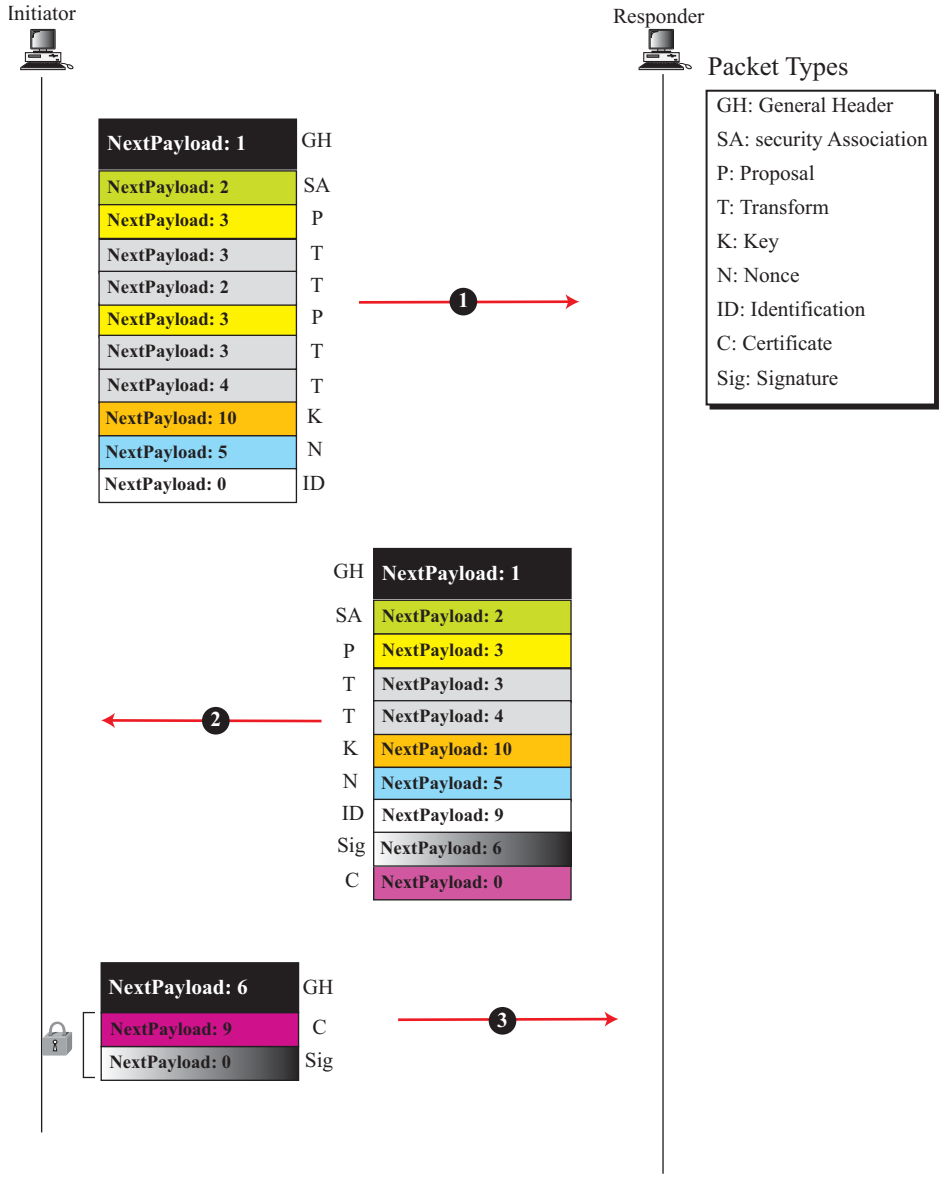
25. Figure S18.25 shows only the layout of the packets and next payload value. When a packet is encrypted, a padlock is inserted next to the packet. Compare this method with the corresponding method in the main mode.

Figure S18.25 *Solution to Exercise 25*



27. Figure S18.27 shows only the layout of the packets and next payload value. When a packet is encrypted, a padlock is inserted next to the packet. Compare this method with the corresponding method in the main mode.

Figure S18.27 *Solution to Exercise 27*



29.

a. The security compromise is that the ID's of the initiator and the responder are not encrypted in the aggressive mode.

b. The gain is that only three messages are sent instead of six.

31.

a. The security compromise is that the hash created by the responder is not encrypted in the aggressive mode.

b. The gain is that only three messages are sent instead of six.

33. SKEYID is calculated differently in different method, but provision is made in each method to protect it from the intrusion.

a. In the preshared secret-key method, SKEYID is calculated from the preshared secret key method which is supposed to be secured from intrusion.

b. In the public-key method, SKEYID is calculated from N-I and N-R, which are secretly exchanged using the public keys of two parties.

c. In the digital signature, SKEYID is calculated from the hashed values of N-R and N-R, which are secured if the hash function is a secured one.

35. All methods in the main mode protect the exchanges of ID's, some in the third or fourth messages and some in the fifth and sixth messages.

37. The exchange of N-I and N-R in the third and fourth messages protects these messages from being replayed. The inclusion of these values again in the encrypted hash or signature in the fifth and sixth messages glues the whole session together and protects the session against partial replay.

39. The exchange of encrypted N-I and N-R in the first and second messages protects these messages from being replayed. The inclusion of these values again in the encrypted hash or signature in the third message glues the whole session together and protects the session against partial replay.