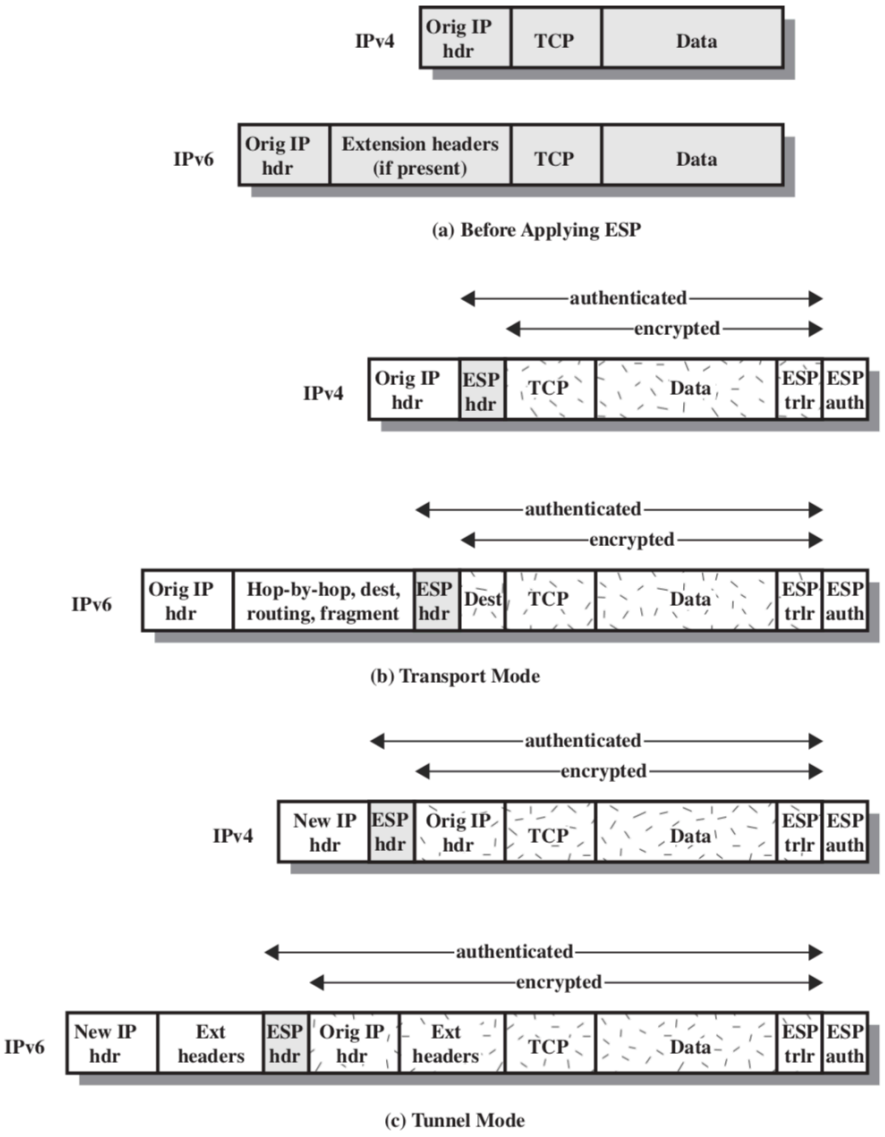
Auto-Evaluation Questions
(IPSec and VPNs)

1. Following the literature used in your study, explain in what consist the following examples of application scenarios for using IPsec:
    a. Secure branch office connectivity over the Internet
    b. Secure remote access over the Internet
    c. Extranet and intranet connectivity with partners

2. What security services are provided by IPsec to protect IP traffic between an origin and a destination? Hint: use X.800 terminology to express the security services provided.
3. What parameters identify and are managed in an IPSec Security Association (SA) and how SA parameters are indexed in IP packets' processing and what parameters characterize the nature and control in a particular SA?
4. What is the difference between using IPSec in transport mode and in tunnel mode? In those modes, what mode protects an entire IP packet and what mode protects only the payload?
5. What is a replay attack in IPSec and how the attack can be conducted and why and how possible replay attacks are protected in IPSec?
6. Why does ESP include a padding field and why padding can provide a way to protect partial traffic flow confidentiality?
7. What are the basic approaches to bundling SAs in SA Bundling strategies, namely when using:
    a. IPSec Transport adjacency
    b. IPSec Iterated Tunneling
8. What are the roles of the Oakley key determination protocol, IKE and ISAKMP in the IPsec stack?
9. Put the letters a, b, c, …. f as entries in table, discussing the protection provided in each cell of the table, from the following set of properties:
    a. Authentication of IP payload, Selective Authentication of IP Header fields and Authentication of IPV6 Extension Headers
    b. Encryption (confidentiality) of entire inner IP packets and Authentication of inner packets
    c. Authentication of entire inner IP packet (inner header plus IP payload) plus selected portions of outer IP header and plus Authentication of outer IPV6 extension headers
    d. Encrypts IP payload and any IPv6 extension headers following the ESP header. Authenticates IP payload but not IP header.
    e. Encrypts for confidentiality of entire inner IP packet.
    f. Encrypts IP payload and any IPv6 extension headers following the ESP header.

	Use of Transport Mode SA	Use of Tunnel Mode SA
AH Sub-protocol		
ESP Sub-Protocol (Encryption Only)		
ESP-AE Sub-Protocol (Authentication and Encryption)		

10. The following figure summarizes the encapsulation for ESP (with authentication and encryption) in transport and tunneling modes. Draw a similar figure for the case of AH.



11. List and summarize he major security services provided by AH and ESP, respectively, from the analysis in filling the table of question 9. Use the following security services and map them in AH and ESP, when IP packets are processed in a destination

    a. access control
    b. connectionless integrity
    c. data origin authentication
    d. detection and discarding of replayed packets
    e. confidentiality
    f. limited traffic flow confidentiality

12. A) In discussing AH processing, it was mentioned that not all of the fields in an IP header are included in MAC calculation. In each case, justify your decision for each field to be included or not in MAC protection and verification.

    B) Considering immutability, mutability with possible prediction or mutability without prediction of IP packets' fields, answer the following questions:

    a. For each of the fields in the IPv4 header, indicate whether the field is immutable, mutable but predictable, or mutable (zeroed prior to ICV calculation).

    b. Do the same for the IPv6 header.

    c. Do the same for the IPv6 extension headers.

13. Suppose that in a certain instant of IPSec processing in a receiver endpoint, the current replay window spans from 120 to 530.

    a. If the next incoming authenticated packet has sequence number 105, what will the receiver do with the packet, and what will be the parameters of the window after that?

    b. If instead the next incoming authenticated packet has sequence number 440, what will the receiver do with the packet, and what will be the parameters of the window after that?

    c. If instead the next incoming authenticated packet has sequence number 540, what will the receiver do with the packet, and what will be the parameters of the window after that?

14. When tunnel mode is used, a new outer IP header is constructed. For both IPv4 and IPv6, indicate the relationship of each outer IP header field and each extension header in the outer packet to the corresponding field or extension header of the inner IP packet. That is, indicate which outer values are derived from inner values and which are constructed independently of the inner values. To answer this question use the following table to fill the 2nd and 3rd columns filling in the following way:

    Column 2: "constructed", "never copied", "copied or configured"

    Column 3: "no change", "decrement"

    For each one of your choice in each cell, try to relate a complementary reference (1) (2) … (6) … according to the following references:

    (1) The IP version in the encapsulating header can be different from the value in the inner header.
    (2) The TTL in the inner header is decremented by the encapsulator prior to forwarding and by the decapsulator if it forwards the packet.
    (3) SRC and DEST addresses depend on the SA, which is used to determine the dest address, which in turn determines which src address (net interface) is used to forward the packet.
    (4) Configuration determines whether to copy from the inner header (IPv4 only), clear or set the DF.
    (5) If Inner Hdr is IPv4, copy the TOS. If Inner Hdr is IPv6, map the Class to TOS.
    (6) If Inner Hdr is IPv6, copy the Class. If Inner Hdr IPv4, map the TOS to Class.

IPv4 Header Fields	Outer Header at Encapsulator	Inner Header at Decapsulator
version	4 (1)	
header length		
TOS		no change
total length		
ID		
Flags	constructed, DF (4)	
Fragment offset		no change
TTL		
protocol	AH, ESP, routing header	
checksum		
source address		
destination address		
options		

IPv6 Header Fields	Outer Header at Encapsulator	Inner Header at Decapsulator
version	6 (1)	
class	copied or configured (6)	
flow id		
length		
next header	AH, ESP, routing header	
hop count	constructed (2)	
source address		no change
dest address	constructed (3)	
extension headers		

15. End-to-end authentication and encryption are desired between two hosts. Draw figures similar to those in question 10, to represent each of the following encapsulations:
    a. Transport adjacency with encryption applied before authentication.
    b. A transport SA bundled inside a tunnel SA with encryption applied before authentication
    c. A transport SA bundled inside a tunnel SA with authentication applied before encryption.
16. The IPsec architecture document states that when two transport mode SAs are bundled to allow both AH and ESP protocols on the same end-to-end flow, only one ordering of security protocols seems appropriate: performing the ESP protocol before performing the AH protocol. Why is this approach recommended rather than authentication before encryption?

    Hint: analyze the order that facilitates rapid detection and rejection of replayed or bogus packets by the receiver, prior to decrypting the packet, because this can reduce the impact

of potential DoS attacks. Analyze also in terms of the possibility to allow for parallel processing of packets at the receiver, i.e., decryption and authentication verification can take place in parallel

17. For the IKE key exchange, indicate which parameters in each message go in ISAKMP payload types.
18. Where does IPsec reside in the IPV4 or IPV6 protocol stack architecture?

    - - -

19. The establishment of SAs in IPSec is supported with a full-duplex or half-duplex vision? Explain.
20. Discuss if IPSec as a solution could be used to protect IP routing protocols, explaining why or why not in the Internet current operation (as you can analyze). See this question in the context of protection provided by specific secure routing protocols (ex., Secure BGP).
21. To support a VPN with IPSec, providing a way to remote access to an internal corporate network mapped in IPV4 private addressing, (ex., 10.0.0.0/24), to access different hosts (resources) mapped in this addressing space what would be the IPSec mode choice ?
22. Discuss the advantages and drawbacks or dangers for a company to support IPSec in transport mode giving remote access to specific hosts (or resources) inside the organization intranet. How and why IPSec in tunneling mode can avoid your mentioned drawbacks?
23. In IPSec management (IPsec endpoints), two data-management structures (as management databases) are used: the SAD – Security Association Database and SPD – Security Policy Database.
    a. What is the role and purpose of SAD ?
    b. What is the role and purpose of SPD
    c. Why is it interesting that SAD and SPD are manages as different “databases” ?
24. Why and how an IPSec endpoint “knows” to index the correct entries in the SAD database when processing IPSec packets arriving from different origins?
25. Why and how an IPSec endpoint “knows” to process correctly the rules expressed in the SPD database when processing IPSec packets arriving from different origins?
26. Give an example (using a diagram) where two hosts (H1, H2) installed in two branches of corporation intranets exchange IPsec packets using two transport SAs in a end-to-end intranetworking environment, protected by a SA bundle in tunnel mode in the public internetworking environment.
27. Repeat question 26, but now the Hosts H1 and H2 will use an adjacency bundle, with the routers (or firewlls) using an adjacent tunneling.
28. In the IKE protocol, which is the authentication and key-establishment method (including security association shared secrets)?
29. What kind of digital signatures are standardized for use in IPSec and what IPSec sup-protocols use those digital signatures?
30. Summarize possible advantages in using ECC-based digital signatures in the IPSec IKE agreement?
31. Secure VPNs can be supported with other forms of encapsulation, with IPSec encapsulated in other protocols such as SSH or TLS. Try to summarize advantages and possible drawbacks in using Secure VPNs supported by SSH or TLS, compared with Secure VPNs supported in IPSec tunneling with ESP and/or AH.