#1: What are “application-level security implementations”? What are “protocol-level security implementations”?

- **Application-level security implementations**: security implementation for each particular network application type (e.g., PGP for emails, SSL (https) for web, and Kerberos for C/S network applications).

- **Protocol-level security implementations**: security implementation for each particular network protocol layer, except for network layers above layer 4 (e.g., layer-1, layer-2, layer-3 (IPsec), and layer-4).

#2: What are the four security functions IPSec perform?

1. encryption
2. data integrity
3. authentication
4. key-exchange (using ISAKMP (Internet Security Association and Key Management Protocol)).

#3: What are the primary advantages in using “protocol-level security implementations”? Mention at least three.

- Even if network applications (email, web, and any other) do not apply security, a particular protocol layer can secure their payload. This will make managing security tools (to be installed at a host computer) easier (you do not have to apply patches to different security tools, each time a path is available).

- Especially using the IPsec R-R mode, network administrators do not have to install (many) security tools at each host computer he/she manages.

- Especially using the IPsec R-R tunnel mode, traffic analysis can be easier to prevent (from attackers outside of a network domain).
#4: What are the four security issues “data integrity” in IPSec provides protection for?

- No missing (unauthorized deletion of) payload (any deletion of the transmitted payload by attackers can be detected).
- No duplication (including any unauthorized addition to) payload (any addition by attackers can be detected).
- No modification (including any unauthorized replacement of) payload (any modification of the transmitted payload by attackers can be detected).
- The ordered deliveries of the transmitted payload (receivers can reorder the messages they receive).

#5: What does “Tunnel” in “IPsec Tunnel Mode” mean?

In network protocol suite, “tunneling” means any deviation from the (expected, standard) protocol layer organization.

For example, for the OSI seven-layer model, while a network-layer protocol should be used below a transport-layer protocol, if another transport-layer protocol is used below the first transport-layer protocol, it is called “layer4 tunneling”.

For another example, if another sequence of the seven layers is applied (after the first sequence), such as (#7 → #6 → #5 → #4 → #3 → #2 → #1) followed by another (#7 → #6 → #5 → #4 → #3 → #2 → #1), it is also considered as a “tunneling”.

#6: What are the nine different IPSec configurations (for the final exam)?

<table>
<thead>
<tr>
<th>Mode</th>
<th>Sub-Mode</th>
<th>Functions</th>
</tr>
</thead>
<tbody>
<tr>
<td>IPSec Tunnel Mode</td>
<td>R-R (Router-to-Router) Tunnel</td>
<td>AH (Authentication Only)</td>
</tr>
<tr>
<td>IPSec Transport Mode</td>
<td>R-H (Router-to-Host) Tunnel</td>
<td>ESP (Encryption Only)</td>
</tr>
<tr>
<td></td>
<td>H-H (Host-to-Host)</td>
<td>AH × ESP</td>
</tr>
</tbody>
</table>

#7: What security threats “IPSec Transport-Mode AH” prevent?

#8: “IPSec AH mode” uses “secret hash key”. What is it for?
#9: If anything in TCP payload field has been modified (unauthorized modification) after the TCP packet was transmitted, does “IPSec Transport-Mode AH” detect such unauthorized modifications? If no, explain why not. If yes, explain how.

#10: Is it possible for MIM attackers to change the destination IP address of IP packets that are protected by “IPSec Transport-Mode AH” so that the attackers modify the receiver IP address in IP packets to redirect IP packets to other host computers in the Internet? If no, explain why not. If yes, explain how.

#11: Is it possible for masquerading attackers to transmit IP packets using a spoofed (bogus) IP address to a receiver (without a receiver detecting the spoofed sender IP address) If no, explain why not. If yes, explain how.