1. What are “services” and “modes” in the context of IPSec?

Services are AH and ESP. Modes are transport and tunnel.

2. What is SAD and SPD? How are they used in IPSec?

Security association data base and security policy data base. SPD enables IPSec to determine if IPSec needs to be used to send a IP packet, and if so, the appropriate mode and services to be used. To send an IPSec packet to a destination a security association must exist with the destination. This is stored in the SAD.

3. What are some important features of the Oakley Key Determination Protocol?

Oakley is an extension of Diffie-Helman. One of the most important features is the use of cookies to thwart replay attacks.

4. What are the two of the poor design choices in the WEP protocol?

Small IV, CRC for integrity (especially bad since it used in conjunction with a stream cipher)

5. How does TKIP address the limitations of WEP?

By simply using the shared key to generate per-packet keys. As every packet is encrypted with a different sequence of bits irrespective of the choice of the IV, the issues with WEP are avoided.

6. What is the 802.1X protocol? Who are the participants in 802.1X?

A MAC layer security protocol involving clients, access points and radius server. Clients authenticate themselves to the radius server before a shared secret is established between the client and the AP.