Web Security

1. What protocols comprise SSL?
2. What is the difference between an SSL connection and an SSL session?
3. What services are provided by the SSL Record Protocol?
4. What steps are involved in the SSL Record Protocol transmission?
5. What is a dual signature and what is its purpose?
6. Consider the following threats to Web security and describe how each is countered by a particular feature of SSL.

    a. Brute-Force Cryptanalytic Attack: An exhaustive search of the key space for a conventional encryption algorithm.
    b. Replay Attack: Earlier SSL handshake messages are replayed.
    c. Man-in-the-Middle Attack: An attacker interposes during key exchange, acting as the client to the server and as the server to the client.
    d. Password Sniffing: Passwords in HTTP or other application traffic are eavesdropped.
    e. IP Spoofing: Uses forged IP addresses to fool a host into accepting bogus data.
    f. IP Hijacking: An active, authenticated connection between two hosts is disrupted and the attacker takes the place of one of the hosts.