Problems

17.1 In SSL and TLS, why is there a separate Change Cipher Spec Protocol, rather than including a change_cipher_spec message in the Handshake Protocol?

17.2 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. Known Plaintext Dictionary Attack: Many messages will contain predictable plaintext, such as the HTTP GET command. An attacker constructs a dictionary containing every possible encryption of the known-plaintext message. When an encrypted message is intercepted, the attacker takes the portion containing the encrypted known plaintext and looks up the ciphertext in the dictionary. The ciphertext should match against an entry that was encrypted with the same
secret key. If there are several matches, each of these can be tried against the full
ciphertext to determine the right one. This attack is especially effective against
small key sizes (e.g., 40-bit keys).

c. Replay Attack: Earlier SSL handshake messages are replayed.
d. 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.
e. Password Sniffing: Passwords in HTTP or other application traffic are eavesdropped.
f. IP Spooing: Uses forged IP addresses to fool a host into accepting bogus data.
g. IP Hijacking: An active, authenticated connection between two hosts is disrupted
   and the attacker takes the place of one of the hosts.
h. SYN Flooding: An attacker sends TCP SYN messages to request a connection but
   does not respond to the final message to establish the connection fully. The attacked
   TCP module typically leaves the "half-open connection" around for a few minutes.
   Repeated SYN messages can clog the TCP module.

17.3 Based on what you have learned in this chapter, is it possible in SSL for the receiver
to reorder SSL record blocks that arrive out of order? If so, explain how it can be
done. If not, why not?