Sample Questions on Security

1) Suppose that an intruder has an encrypted message as well as the decrypted version of that message. Can the intruder mount a ciphertext-only attack, a known-plaintext attack, or a chosen-plaintext attack?

2) Using the monoalphabetic cipher in Figure 8.3 of the textbook, encode the message "This is an easy problem". Decode the message "rmij'u uamu xyj".

3) Using RSA, choose p = 3 and q = 11, and encode the word "hello". Apply the decryption algorithm to the encrypted version to recover the original plaintext message.

4) What is the purpose of a nonce in an authentication protocol?

5) The Internet BGP routing protocol uses a MAC rather than public key encryption to sign BGP messages. Why do you think a MAC is chosen over public key encryption?

6) In what way does a MAC provide a better message integrity check than a checksum such as the Internet checksum?

7) Consider Figure 8.8 from the text (the one which shows that two messages can have the same checksum). Compute a third message different from the two messages that has the same checksum as the two messages in that figure.