Network Security - Sample Questions

1) Suppose that an intruder has an encrypted message as well as the decrypted version of that message. Can the intruder launch a ciphertext-only attack, a known-plaintext attack, or a chosen-plaintext attack?
2) 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.
3) What is the purpose of a nonce in an authentication protocol?
4) 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?
5) In which way does a MAC provide a better message integrity check than a checksum such as the Internet checksum?