Network Security - Answers

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?

Answer: In this case, a known plaintext attack is performed. If, somehow, the message encrypted by the sender was chosen by the attacker, then this would be 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.

Answer: We are given p = 3 and q =11.We thus have n = 33 and q =11. Choose e = 9 (9 is a good value to choose, since the resulting calculations are less likely to run into numerical stability problems than other choices for e, since 3 and (p - 1) * (q - 1) = 20 have no common factors.

Choose d =9 also so that e * d = 81 and thus e*d - 1= 80 is exactly divisible by 20. We can now perform the RSA encryption and decryption using n = 33, e = 9 and d = 9.

Letter	m	m^e	Ciphertext: m^e mod 33
h	8	134217728	29
e	5	1953125	20
l	12	5159780352	12
l	12	5159780352	12
o	15	38443359375	3

ciphertext	c^d	m = c^d mod n	Letter
29	14507145975869	8	h
20	512000000000	5	e
12	5159780352	12	l
12	5159780352	12	l
3	19683	15	o

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

Answer: A nonce is used to ensure that the person being authenticated is "live." Nonces thus are used to combat playback attacks.

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?

Answer: Signing messages using public key encryption is computationally expensive. MACs are much more computationally efficient. Hence BGP resorts to using MAC.

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

Answer: One requirement of a MAC is that given a message M, it is very difficult to find another message M' that has the same message digest and, as a corollary, that given a MAC it is difficult to find a message M'' that has that given MAC value. We have "message integrity" in the sense that we have reasonable confidence that given a message M and its signed MAC that the message was not altered since the MAC was computed and signed. This is not true of the Internet checksum, where we have seen that it is easy to find two messages with the same Internet checksum.