CEG 4750/6750 (Information Security)
Homework # 5

Student Name: Brandon Walker

Wright UID: U00998563

[✓ Undergraduate]/Graduate:_______________

Question 1 (10 points).

In class we learned a fundamental set of cryptography systems. For the duration of these questions presume you have access to a small, but trusted source of information (i.e., a public website).

Discuss how you would apply them to the following situations:
1. Someone who has never communicated with you in the past needs to send you a secret message over an insecure channel. How can he create it so that only you can read it?

You could send them a copy of your public key, and then they could encrypt it using your public key, and then only someone with your private key could read it, which should be only you.

2. You need to receive orders over an insecure channel from your boss. How can you make sure his message's integrity has been preserved?

He could sign it with his private key, and you would know that no one else has changed it if the signature still contains an accurate hash.

Question 2 (10 points) What is the difference between a message authentication code and a one-way hash function?

a one way hash function takes in no external input other than the information to be "hashed" a message authentication code takes in a private key while hashing the information, so the one-way hash function proves integrity, while the message authentication code proves integrity and authentication.

Question 3 (10 points). List possible ways to distribute secret keys to two communicating parties.

use public keys first to encrypt the secret keys, so that the secret keys can't be read
use symmetric encryption to create a secure channel to then distribute secret keys

Question 4 (10 points). List four general categories of schemes for the distribution of public keys.

Public Announcement
Public Directory
Public-key Authority
Public Key Certificates

Question 5 (10 points). What is a public key certificate?

A public key certificate is a digital document used to prove the validity of a public key, the certificate contains information about the owner and the signature of an entity that has verified the certificates contents.

Question 6 (15 points) Consider a Diffie-Hellman scheme with a common prime q=11, and a primitive root g=2.

(1) Show that 2 is a primitive root of 11.

(2^1 mod 11, 2^2 mod 11, 2^3 mod 11, 2^4 mod 11, 2^5 mod 11, 2^6 mod 11, 2^7 mod 11, 2^8 mod 11, 2^9 mod 11, 2^10 mod 11) == (1, 2, 3, 4, 5, 6, 7, 8, 9, 10)

(2) If user A has public key Ya=9, what is A’s private key Xa?

9 = 2^Xa mod 11 2^8 mod 11 = 9 therefore Xa = 8

(3) If user B has public key Yb=3, what is the shared secret key K, shared with A?

K = 3^8 mod 11 = 19683 mod 11 = 9 = K

Question 7 (20 points, graduate students only) (1) Consider the Davies and Price hash code scheme described in Section 11.4 and assume that DES is used as the encryption algorithm:

$$H_i = E_{M_i}[H_{i-1}] \oplus H_{i-1}$$

And recall the complementarity property of DES: If Y = $DES_K(X)$, then Y’ = $DES_{K'}(X')$. Use this property to show how a message consisting of blocks M_1, M_2, …, M_N can be altered without altering its hash code.

We can alter each block of Mi such that they are the complement of their original value, that way when they are xor’ed in the hashing, they will end up at the same value.

(2) Show that a similar attack will succeed against the scheme proposed in [MEYE88]:

$$H^{i} = E^{H_{i-1}}[M^{i}] \oplus M^{i}$$