CIS4367.01 **Brandon Thompson**
Prof. Elibol Due Date: 1/27/20

Homework 4

PROBLEM 1:

Briefly summarize what you know about the field of cryptography.

SOLUTION:

The purpose of cryptography is to prevent unwanted people from from gaining access to information that should be private, or changing information without the owners knowledge.

In the early days all cryptographic algorithms relied on the alphabet, by transposing the letters in a certain patter or swapping the location of letters many times. These can easily be broken by frequency analysis.

Later came rotor machines that sped up the encryption process during WWII by using rotors to create a faster, more secure method of encryption that could not be broken using frequency analysis.

Current cryptographic algorithms rely on prime factorization for security because multiplying numbers is much easier than finding the correct factors from a very large number.

PROBLEM 2:

List seven questions or things you don't know about cryptography. For each question you list, indicate why it might be important to know the answer.

SOLUTION:

1. How does the encryption process actually happen?
   It would be important to know the steps and an in depth example for debugging purposes or ensuring proper functionality.

2. How does one go about attacking a ciphertext?
   Knowing how to break into things is important in understanding how to secure things.

3. What are some mathematical algorithms used in encryption?
   Understanding the current standards, and why they are used is important for implementing encryption in a system.

4. How does one stop an attacker from changing a message and just generating a new hash?
   This is important because an attacker could change all of your messages and hashed and the recipient would never know.

5. How does elliptic curve cryptography work?
   Elliptic curve cryptography is being implemented in more and more things recently.

6. Why does changing a key size make things more difficult to break into?
   The correlation between key size and computation speed is important to find a balance between the two.

7. How will common cryptographic algorithms hold up to quantum computing in the next few years.
   Quantum computing is starting to become more prevalent, and boasts much better processing power than current systems. Will quantum computers force new algorithms to be developed.

PROBLEM 3:

Describe situations in your life when you might need to use encryption or secret codes. How important would it be to have enough understating of the subject of cryptography to assess the strength of the code used?

SOLUTION:

If i needed to store private information on a public server I would like to know what algorithms are strong enough to secure my data. How to verify that nobody has modified my data. How to securely send data to someone else.

With the proper understanding of cryptographic codes, I could ensure that my data is secure and it has not been tampered with.

PROBLEM 4:

Prepare a one paragraph objective summary of the main ideas in this chapter.

SOLUTION:

Symmetric encryption uses a single key (secret key) to encrypt or decrypt, and requires both the sender and receiver to share the same key. Asymmetric encryption uses two keys (public / private key) to encrypt and decrypt information. MAC algorithms and hash functions are used to verify the validity of data by sending the message along with a hash value. If the message is altered en route, the receiver will know because the hash will not be the same. The combination of encryption and MAC algorithms provides very good security.