ISEC 400 Homework 11 Name: Megan Leonard

Answer the following questions based on your reading of the textbooks, any supplemental material, and the instructor’s presentation this week. If you use an external source (i.e. a web page, the required textbook, or an additional book) to help you answer the questions then be sure to cite that source. Hint: you should probably always be citing a source.

## Questions

1. **[5 points]** What are the differences between symmetric and asymmetric cryptography? How are both used in secure communications?

Symmetric uses a single key to encipher and decipher the given message meaning you have to give someone the key to be able to decrypt it. Asymmetric uses two keys, one private and one public, so that the public key can be used to encrypt while the private key is used to decrypt. Both of them are a means of encryption and decryption of communication.

1. **[8 points]** For each of the following cryptographic algorithms, describe what they do your own words and state where they are commonly used in application security. Identify them as either hashing, key exchange, symmetric encryption, or asymmetric encryption.
   1. AES: Block cipher used by the US government, symmetric encryption.
   2. RSA: Algorithm using two keys, asymmetric encryption.
   3. Triple DES: Block cipher encryption repeats three times, 3 keys, symmetric encryption.
   4. MD5: Message digest algorithm 128-bit, hashing.
   5. SHA256: Function using 32-bit, hashing.
   6. PKI: Public key interface, asymmetric encryption.
   7. RC4: Rivest Cipher 4 stream cipher, asymmetric encryption.
   8. Diffie-Hellman: Public channel between two parties, key exchange.
2. **[12 points]** Find three different up-voted incorrect answers about implementing cryptography on [Stack Overflow](https://stackoverflow.com/) or another programming-related site. Provide a link, a summary of the wrong answer, a rationale as to why it is wrong, and a replacement answer of your own based on cryptography best practices in Application Security.

<https://crypto.stackexchange.com/questions/6448/bad-crackable-encryption-example>

Finding examples of incorrect answers is difficult so the link I provided is the question of bad encryption examples. The first answer talks about the Caesar Cipher and how it is easy to break as it has a limit of possible combinations. The best way to handle this is to add other encryption methods to this such as hashing or Feistel ciphers.

<https://www.crypteron.com/blog/the-real-problem-with-encryption/>

This second link has a list of mistakes that are made with encryption, and we are looking at mistake number five which is when you are trying to implement a cipher, but you do not do it correctly like using random numbers or using AES with the wrong bit size. The best fix for this is to look at the different types of encryptions and compare them to the data you wish to encrypt. You look at the bit size and the different possible ciphers and encryptions that fit with the size.

<https://resources.infosecinstitute.com/topic/cryptography-errors/>

This final link covers different cryptography errors and we are looking at insufficient randomness where the use of random can lead to predictable code as if the seed is not determined it will be set as 1. The best way for this would be to use srand or srandom which will take the outcome and use that as the seed for the rand function to make it more randomized and harder to guess.

1. **[5 points]** In approximately 300 to 400 of prose (i.e. sentences, not bullet lists) using APA style citations if needed, summarize and interact with the content that was covered this week in class. In your summary, you should highlight the major topics, theories, practices, and knowledge that were covered. Your summary should also interact with the material through personal observations, reflections, and applications to the field of study. In particular, highlight what surprised, enlightened, or otherwise engaged you. Make sure to include at least one thing that you’re still confused about. In other words, you should think and write critically not just about what was presented but also what you have learned through the session. Ask at least one question that your instructor can answer in the returned assignment or class discussion.

This week we looked more into cryptography which is a topic I have gone over a lot. We start by looking at ciphers and how they have two main types of byte and block methods with three primary operations of substitution, transposition, and exclusive. There is also encryption that is symmetric or asymmetric based on the keys they use. I have looked at a lot of cryptography but not as many ciphers as I have in this lesson. Ciphers are quite fun to work with and learn about. My question this week is do you have a favorite cipher?