**CIS3360: Security in Computing**

**Homework 5**

1. **( 15 points) Knowledge-based Question:**
   1. What are the differences between public/symmetric key cryptography? The advantage and disadvantage of each?
   2. For English alphabet based texts regardless of upper or lower case (i.e., assuming each letter has only 26 possible value), if the length of the key using Vigenere Cipher is 4, how many possible encryption keys exist? (hint: we all know that Caesar cipher has 26 possible encryption keys)
   3. What is the usage of a cryptographic hash function? Can two documents have the same hash value?
2. **(10 points) Determine whether a statement is True or False. If a statement is false, you must explain why.**
   1. Digital signature of a message m is H(m), where H() represent a cryptographic hash function such as MD5 or SHA-1.
   2. Cesar cipher is a kind of substitution cipher, while Vigenere cipher is a kind of transposition cipher.
3. **(20 points)** Cipher Generation:
   1. What are the substitutions for the (decimal) numbers 12, 7, and 2 using the S-box shown in the textbook as Figure 8.3.
   2. What is the encryption of the following string “THELAZYFOX” using the Caesar cipher with a key of “3
   3. What is the Hill cipher key matrix **K** that can realize the following permutation:

π: (1,2,3,4,5) 🡪 (3,5,1,4,2)

1. **(10 points)** Birthday Attack: Suppose in our class we have 25 students, what is the probability that we have two students having the same day as their birthday?
2. **(20 points)** Binary to IP Address calculation

Convert 10000100.10101010.11110000.10000011 back to a decimal IP address. What is the domain name for this IP address? Show all math back to decimal to get full credit.

1. **(25 points)** Euclid’s GCD Algorithm: Show the steps of applying the Euclid GCD algorithm to compute the following GCDs. You can show the steps by providing the similar computation table shown in the book.
2. GCD(412,200)
3. GCD(510,412)