Homework #7 Chapters 8-9 (11 points total)
Due: Wednesday, April 10th, 2019 in class

1. Using the simple hash algorithm discussed in class, find the encrypted forms of the following passwords (you can find slides from class on Canvas):
   a. hashes
   b. java
   c. html5

2. The pin number for a bank account is 4 digits, each 0–9.
   a. How many different pins are possible?
   b. If you can enter a 4-digit pin in 2 seconds (on average), about how long would it take you to try all possible passcodes?

3. A virus attacks a single user’s computer and within one hour embeds itself in 15 email attachment files sent out to other users. By the end of the hour, 20% of these have been opened and have infected their host machines. If this process continues, how many machines will be infected at the end of 6 hours? Can you find a formula for the number of machines infected after n hours? (2 points)
4. A certain individual has a Hilton account, a RitzCarlton account, and a Marriott International account. The following email message is sent to this individual. Point out clues (plural) that should alert this individual that he/she is a victim of a phishing attack.

We here at Marriott appreciate your loyalty as a customer. We want to make things more easy for you when you travel, so we have partnered with Hilton and Ritz-Carlton to create a unified rewards program. Now when you stay at any of these fine brand hotels, you will earn award points that can apply to a future stay at any of the three hotels. For you we will quick set this up, just click on the link below to get started: www.Mariott.com

5. Your friend tells you that a Caesar Cipher is more secure when you use larger numbers for the key (like 100 or 100000). Do you believe them? Why, or why not?

6. The centurion who was supposed to inform you of the secret key s was killed en route, but you have received the message ohwwf zwypun in a Caesar cipher. Find the value of s and decode the message.

7. In class, we encrypted (M Q) with the block cipher algorithm to obtain (U L). Take the result of this encryption, and then show the steps to get back to the original text. The inverse of X is:

\[
X' = \begin{bmatrix} 23 & 5 \\ 2 & 23 \end{bmatrix}
\]
8. You receive a message that was encoded using a block encoding scheme with the encoding matrix below. The decoding matrix is also shown. (2 points; 1 point each)

\[ X = \begin{bmatrix} 3 & 2 \\ 7 & 5 \end{bmatrix} \quad X' = \begin{bmatrix} 5 & 24 \\ 19 & 3 \end{bmatrix} \]

a. Encode the plaintext message CSCI.

b. Decode the ciphertext message MXOSHI.

9. Bob and Alice both have their own public key and a private key. Bob wants to send Alice a message that only she can read and which she will know was written by him. How could he encrypt the message? How could Alice decrypt it?