Homework #7 Chapters 8 & 9 (18 points total)
Due: Friday, November 8th, 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): (2 points)
   
   a. hash
   
   b. privacy
   
   c. m3tadat

2. The password for a bank account is 8 characters, 7 of which are letters (A-Z, a-z) and 1 is a single digit (0-9). (2 points)
   
   a. How many different passwords are possible?
   
   b. If you write a program that can test 5,000 passwords per second, about how many hours would it take you to try every possible password?

3. Compare and contrast DES, AES, and RSA. Which of these are still used today? (2 pts)

4. List 4 different ways to detect phishing. (2 points)

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? (1 point)
6. The centurion who was supposed to inform you of the secret key, S, was killed en route, but you have received the message "ngrruckkt" in a Caesar cipher. Find the value of S and decode the message. (2 points)

7. What is a DDoS attack? What kind of malware is used? (1 point)

8. You receive a message that was encoded using a block encoding scheme with the encoding matrix below. The decoding matrix is also shown. (4 points) (2 points 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? (2 points)