Homework Chapter 8 (11 points total)  
Due: Friday, Nov 10th, in class

1. Using the hash function described in Section 8.2.1, find the encrypted forms of the following passwords:
   a. fido
   b. blank
   c. ti34pper

2. The default passcode on a cell phone is usually 4 digits, each 0–9.
   a. How many different passcodes are possible?
   b. If you can enter a 4-digit passcode in one second, 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 50 email attachment files sent out to other users. By the end of the hour, 10% 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 5 hours? Can you find a formula for the number of machines infected after n hours?

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 that should alert this individual that he or she is the 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. A messenger tells you that the secret key for today for the Caesar cipher is \( s=26 \). Should you trust the messenger? Why, or why not?

6. The centurion who was supposed to inform you of \( s \) was killed en route, but you have received the message MXX SMGX UE PUHUPQP in a Caesar cipher. Find the value of \( s \) and decode the message.

7. In problem Q8.19 in class, we encrypted \((M Q)\). Take the result of this encryption, and then show the steps to get back to the original block. 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.

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

a. Encode the plaintext message GO.

b. Decode the ciphertext message MXOSHI.