Name: _____

Homework #13: Privacy and Security (10 points)
Due to Gradescope by 11:45 PM on Thursday, November 11th
You need to submit a pdf to Gradescope; failure to assign questions to pages will result in a 10% deduction on your grade

Homework Goal: Practice various types of encryption and decryption; understand the importance of security and different algorithms

<u>Simple Password "Hash"</u>
(1) Replace each letter with its number (a → 1, etc.), leave digits alone
(2) Reverse the string of digits
(3) Add up the digits
(4) Find the remainder of: step 3 result / 10
(5) Multiply the result of step 4 by the number of digits in step 2
(6) Exchange each digit with its character

A	B	C	D	E	F	G	H	I	J	K	L	M
1	2	3	4	5	6	7	8	9	10	11	12	13
N	O	P	Q	R	S	T	U	V	W	X	Y	Z
14	15	16	17	18	19	20	21	22	23	24	25	26

1. Using the simple hash algorithm above, find the encrypted forms of the following passwords. (1 point)

    a. abc1234

    b. password

    c. ilove101

2. The password for a Zoom account is 4 characters long, consisting of letters (A-Z, a-z), digits (0-9), and these four symbols: ! @ # $
   The characters can occur in any order and repeats are allowed. (1 point)
   a. How many different passwords are possible?

   b. If you write a program that can test 4,000 passwords per second, about how many **hours** would it take you to try every possible password?

3. Consider the encryption algorithms we've talked about in class. (1 point)
   a. Which algorithm(s) are symmetric encryption algorithm(s)?

   b. Which algorithm(s) are asymmetric encryption algorithm(s)?

4. Given the following sample email, what are two clues that indicate this might be a phishing email? (0.5 points)

   ```
   Dear customer:
   We write to inform you that you account will soon expire. In
   order to keep it up to date, please go this link and enter your
   password: http://zoorn.us
   Sincerly,
   Your Zoom Team
   ```

5. Your friend tells you that a Caesar Cipher is more secure when you use larger numbers for the key (like 500 or 50,000). Do you believe them? Why or why not? (1 point)

6. My cat, Bones, encoded a message for me using a Meow-sar Cipher (Caesar Cipher for cats): "LKKJ SK ZATG". Unfortunately, she is unable to tell me the shift (how I even got the message from her, I'll never know). Determine the shift and decode the message from Bones (by hand, not through an online site). (1 point)

7. What is a Trojan? Explain an example of a real Trojan . (1 point)

8. Your dad has taken to sending you block-encoded messages to help you prepare for your upcoming CS exam. Today's dad joke (almost worse than your instructor's CS jokes) has arrived in your inbox, and it reads "I can sum up 2021 in one word… CEWQ" To determine his punchline, decrypt the message "CEWQ". Show your work. (2 points)

$$X = \begin{bmatrix} 3 & 2 \\ 7 & 5 \end{bmatrix} \qquad X' = \begin{bmatrix} 5 & 24 \\ 19 & 3 \end{bmatrix}$$

9. Bob and Alice both have their own public key and private key. Alice wants to send Bob a message that he will know was sent from her. With what key should Alice encrypt the message? Would this way of encryption prevent a third party from being able to read Alice's message? (1.5 points)