Cryptography
Spring 2022
Practice Exam 2
March 30, 2022
Time Limit: 50 Minutes

Name (Print): _____

Section _____

This exam contains 2 pages (including this cover page) and 2 problems. Check to see if any pages are missing. Enter all requested information on the top of this page and sign the Honor Code pledge at the bottom of this page.

You are required to show your work on each problem on this exam. The following rules apply:

- **Organize your work** in a reasonably neat and coherent way. Clearly label your work and circle your answer. Work scattered all over the page without a clear ordering will receive very little credit.
- This is an open notes exam, but you may not copy code from any online source.
- Ask for scratch paper if you need more space. Clearly label any work completed on scratch paper.

Problem	Points	Score
1	20	
2	15	
Total:	35	

Do not write in the table to the right.

Honor Code Pledge: By signing below, you are verifying that you have completed this examination in accordance with the ethical standards expected at NCSSM.

Signature: _____

1. (a) (10 points) Write a function in Python which
    1. accepts no arguments;
    2. uses a while loop to prompt the user for a single number in each loop, and stops looping once the user types "stop";
    3. returns the average of all numbers typed by the user.

   (b) (10 points) Suppose you want to encrypt a message by reversing the order of all characters in the message. As an example, "I LOVE MATHEMATICS" would be encrypted as "SCITAMEHTAM EVOL I". Write a function in Python which
    1. accepts a plaintext message (string);
    2. reverses the order of all characters in the message;
    3. prints the encrypted message

2. (a) (5 points) Suppose you want to encrypt an integer message using a multiplicative cipher with modulus of n where n is larger than the integer message. How many valid multiplicative keys are there?

   (b) (5 points) Explain how we know that 25 has a multiplicative inverse modulo 109, and then find the multiplicative inverse of 25 modulo 109 without using a calculator or computer. You must show all work.

   (c) (5 points) Explain how multiplicative inverses are used to decrypt integer messages in the multiplicative cipher, and then decrypt the integer 69 which was encrypted by multiplying a plaintext integer by 25 modulo 109. You must show all work.