**Cryptography**
**Spring 2022**
**Practice Exam 1**
**February 23, 2022**
**Time Limit: 50 Minutes**

**Name (Print):** _____

Section _____

---

This exam contains 2 pages (including this cover page) and 3 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 | 30 | |
| 2 | 10 | |
| 3 | 15 | |
| Total: | 55 | |

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 accepts integers $a$, $b$, and $n$ as inputs and returns the sum of all the (distinct) multiples of $a$ or $b$ which are less that $n$.

   (b) (10 points) Write a function in Python which prompts the user for an integer $k$ as an input and returns a list of all distinct prime factors of $k$.

   (c) (10 points) (Bonus) Let $n$ be a positive integer. The Collatz sequence is defined recursively by the following rules:

$$A_0 = n$$
$$A_{i+1} = \begin{cases} \frac{A_i}{2} & \text{if } A_i \text{ is even} \\ 3A_i + 1 & \text{if } A_i \text{ is odd} \end{cases}$$

   Using the rule above and starting with 13, we generate the following sequence:

$$13, 40, 20, 10, 5, 16, 8, 4, 2, 1$$

   It can be seen that this sequence (starting at 13 and finishing at 1) contains 10 terms. The Collatz Conjecture states that all Collatz sequences terminate at 1 in finitely many steps.

   Which starting number, under one million, produces the longest Collatz sequence?

2. Write a short response outlining the strengths and weaknesses of each of the following encryption schemes.

   (a) (5 points) Additive Caesar Cipher

   (b) (5 points) One-Time Pad

3. Determine whether the following statements are true or false, in general. If a statement is true, show why. If a statement is false, explain why or provide a counterexample.

   (a) (5 points) $(x + y)^2 \equiv x^2 + y^2 \mod 2$

   (b) (5 points) If $x + z \equiv y + z \mod n$, then $x \equiv y \mod n$

   (c) (5 points) The last digit of $7^{20222023}$ is 1.