CSCI474 - Course Project Proposal

Thomas Applegate
Colorado School of Mines
Golden, CO, USA
tapplegate@mines.edu

Kaelyn Boutin
Colorado School of Mines
Golden, CO, USA
kvboutin@mines.edu

Gabrielle Hadi
Colorado School of Mines
Golden, CO, USA
ghadi@mines.edu

Addison Hart
Colorado School of Mines
Golden, CO, USA
addisonhart@mines.edu

Et Griffin
Colorado School of Mines
Golden, CO, USA
egriffin@mines.edu

Isabelle Neckel
Colorado School of Mines
Golden, CO, USA
ineckel@mines.edu

***Abstract*—The National Institute of Standards and Technology, NIST, defines fifteen separate tests for the randomness and unpredictability of random numbers. True Random, Deskewed True Random and Pseudorandom are the three classes of random numbers that are going to be compared using the tests outlined by NIST. We plan to use a Python implementation that will provide us the P-values to compare and contrast to determine the random numbers that are closest to being truly random. The generation of the random numbers will also be considered when discussing the choice in relation to cryptography.**

***Index Terms*—random numbers, pseudorandomness, NIST, python**

I. Introduction

Introduction here.

II. Methods

To test the randomness of various algorithms, we will use the NIST randomness tests as implemented in Python [1]. The tests require a binary string of indeterminate length as the input. Each of the fifteen tests will output the P-value, as well as the result of whether the P-value means that the data can be considered truly random or not. For each of the algorithms that we test, we will use many samples of equal length to compare their randomness to each other.

III. Expected Results

Expected Results here.

IV. Conclusion

Conclusion here.

References

[1] S. Ang. “Randomness testsuite.” (), [Online]. Available: https://github.com/stevenang/randomness_testsuite (visited on 03/14/2024).