Quiz. 5

(Deadline April 4, 2024)

Problem 1

In this homework, you need to download the Random Number Generator Test Suite from the US National Institute of Standards and Technology (NIST) to ensure that the random numbers you choose are truly unpredictable and secure.

a) Write a Python/C++ program to generate **1M bytes** of cryptographically secure random numbers.

b) Run the NIST SP 800-22 statistical test on your **1M bytes** of binary cryptographically secure random numbers and analyze the test results to identify any deviations from the expected statistical properties of random numbers.

c) Extra credit: Find out a non-cryptographically secure random number generator, such as random(), to demonstrate its lack of safety. Then, propose modifications to enhance its security to generate cryptographically secure random numbers that meet the highest standards of security and reliability.

Hint:
https://csrc.nist.gov/Projects/Random-Bit-Generation/Documentation-and-Software
https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-22r1a.pdf

What to turn in:

a) The file you need to upload is structured as follows:

- <student_id>.zip
  - <student_id>.pdf
  - RNG.py or RNG.cpp
  - random.bin
  - finalAnalysisReport.txt (testing result in ./experiments/AlgorithmTesting)
  - (Any libraries if needed)

b) The <student_id>.pdf file should contain instructions on how to run your code, the screenshots of the result of program, and the solution to the provided problems.