CIS313, Cryptography
Module 2 Lab – Random Numbers

In this second module, we will explore randomness. The objective of this lab is to utilize automated tools to test numbers for randomness and generate random numbers. Be sure to answer all the questions.

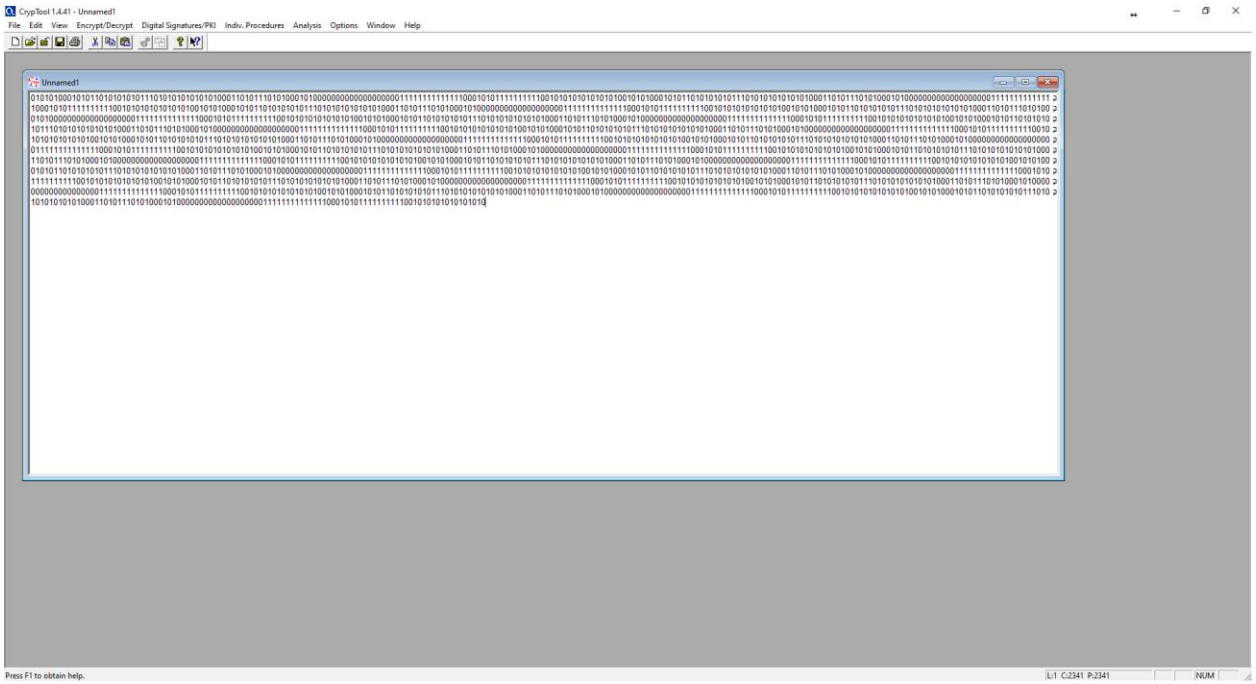
You will be required to submit the following graded items as part of this lab:

- Answer all questions listed in **BOLD**
- Provide screenshots when asked

Lab 1 – Generating and Testing Random Numbers

To complete this lab, you will be using the Cryptool 1 application. This application is available on the Cybersecurity desktop at workspace.bellevue.edu. See the instructions provided with this assignment to access the Cybersecurity Desktop.

1. Open the Cryptool 1 program and select **File | New**. In the window created type a long series of 0s and 1s. Use any technique you want, type randomly, use copy and paste, have your cat walk across the keyboard. Try to make it as random as possible. Your screen should look something like the below.



2. Select one of the tests for randomness from Analysis | Analyze Randomness. For help answering the question see the following sources:

Wikipedia Article and Statistical Randomness

Runs Test for Detecting Non-Randomness (YouTube)

Frequency Test NIST

What is the name of the test?

The test I read about is the frequency test.

What does it test for to determine the level of randomness?

The frequency test tests the randomness of a sequence of 0s and 1s to see what the proportion is between the two.

3. Run the selected test from Cryptool.

What was the results?

I'm not sure if I did it right but it says the maximal test value is 3.841000, the test result is 2374.680576, and that the frequency test failed.

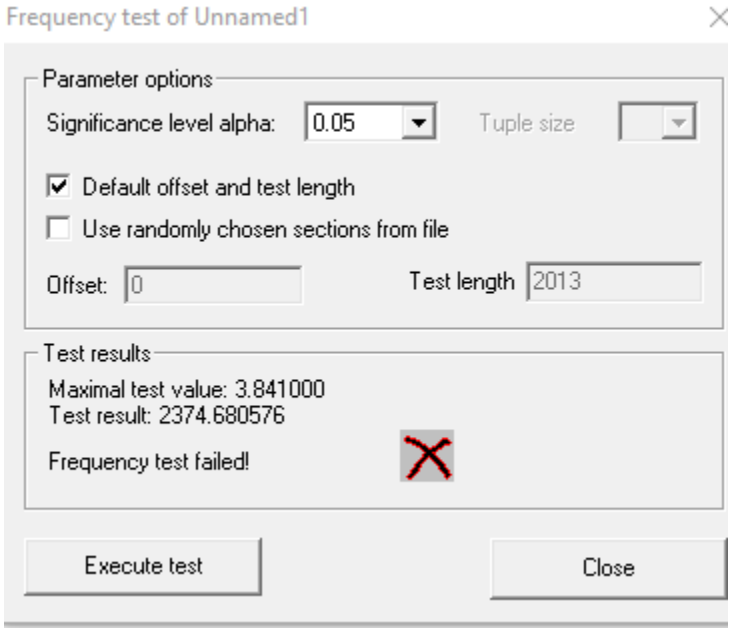
What do the results tell you about your "random" number?

My random number wasn't very random.

How good are humans at generating randomness?

Humans are not very good at generating randomness.

Paste a screen shot of your test results.



4. Select **Indiv. Procedures | Tools | Generate Random Numbers** from the Cryptool menu. Your screen should provide these options.
5. Select the X^2 (mod N) random number generator and either use the default seed value in the Parameters field or set your own. Click the Generate output button.
6. Leave that window on the screen and repeat step #4 and 5 (above) again making sure to use the same seed value.

What is interesting about that seed value?

The two generated outputs are the same.

7. Change the seed value and generate another random number.

What is different about this random number from the earlier sets?

This one has different numbers, symbols, and letters.

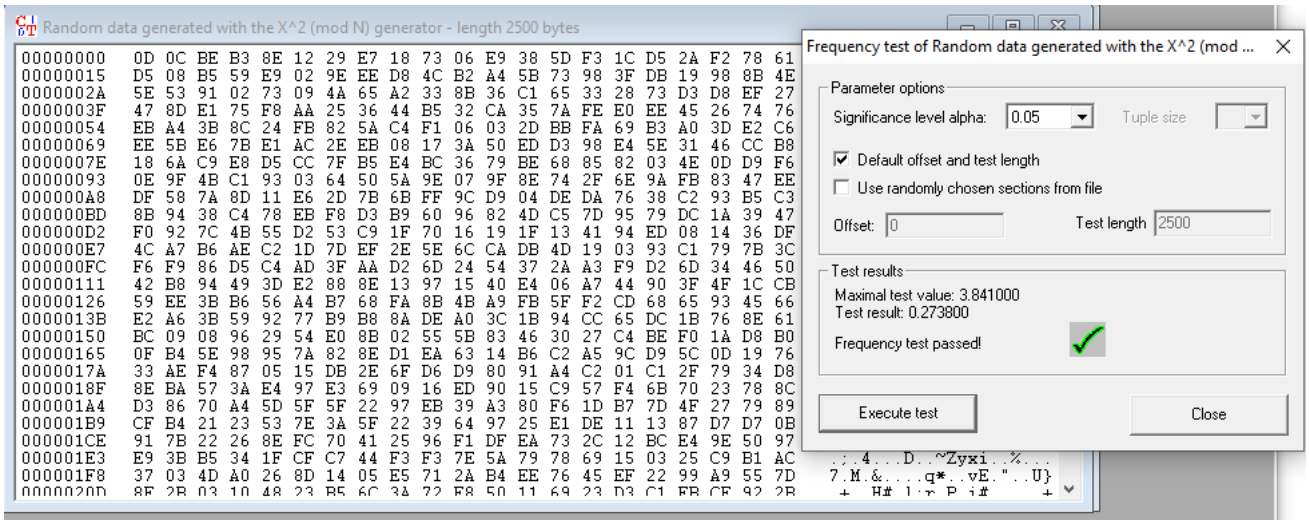
What does this tell you about choosing a seed value, and randomness, when using this generator function?

By choosing the seed value you are adjusting the output that is being generated to be different.

Research random seed values. What is important about a seed value used for cryptographically strong PRNG?

Random seed values are important for a strong PRNG so that the series of values created are unpredictable.

Paste a screen shot of your results below:



8. 15. Close the windows with the random numbers you have generated. Select **Indiv. Procedures | Tools | Generate Random Numbers** from the Cryptool menu again and select the X^2 (mod N) random number generator and use the default parameters. Click the Generate output button.
9. Run a poker test (**Analysis | Analyze Randomness**)

What is the result?

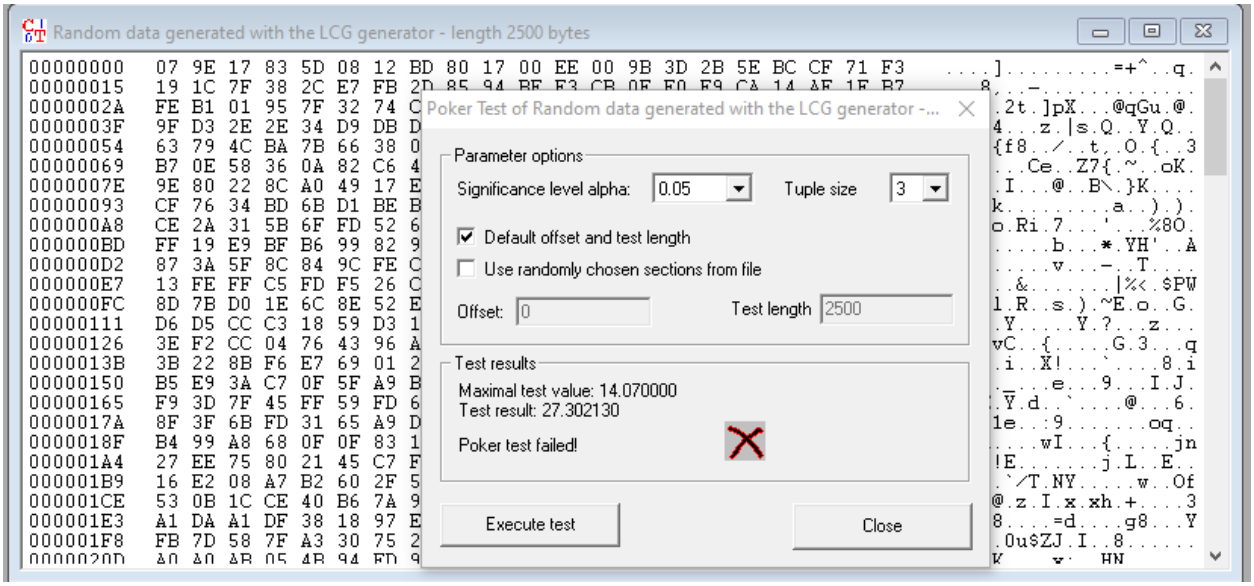
The result is a maximal test value of 14.070000, a test result of 3.966997, and it passed.

10. Now generate a random number (Select **Indiv. Procedures | Tools | Generate Random Numbers**) using the Linear Congruence Generator (LCG). Run a poker test on this number.

What is the result?

The result is a maximal test value of 14.070000, a test result of 27.302130, and it failed.

Paste a screenshot below that shows your results?



What does the test you just ran tell you about the quality of random numbers generated by some LCGs, specifically in relation to cryptography?

This test tells me that when generating numbers with LCG they are more predictable.

Why is the quality of random numbers important to cryptography? Think about what randomness is used for in cryptography.

The quality of random numbers is important so that exploits can't be used and the numbers can't be guessed in order to keep everything secure and protected.