Network Security PA4

Name: Kshitij Ramesh Tadkase
Roll: 18075029
Dept: CSE (B.Tech)

Github Link: https://github.com/KRT2305/NetSec-PA4

Pseudo Random Number Generator(PRNG) refers to an algorithm that uses mathematical formulas to produce sequences of random numbers. PRNGs generate a sequence of numbers approximating the properties of random numbers. A PRNG starts from an arbitrary starting state using a seed state. Many numbers are generated in a short time and can also be reproduced later, if the starting point in the sequence is known. Hence, the numbers are deterministic and efficient.

Characteristics of PRNG:

- Efficient: PRNG can produce many numbers in a short time and is advantageous for applications that need many numbers
- Deterministic: A given sequence of numbers can be reproduced at a later date if the starting point in the sequence is known.Determinism is handy if you need to replay the same sequence of numbers again at a later stage.
- Periodic: PRNGs are periodic, which means that the sequence will eventually repeat itself. While periodicity is hardly ever a desirable characteristic, modern PRNGs have a period that is so long that it can be ignored for most practical purposes

Results:

1. For Python's Random Function:

```
Please select a method for generating random numbers:
 1. Python's Random Function
 2. Linear Congruential Generator
      (or type 3 to quit)

Selection > 1
How many observations should we perform?
Selection > 20
Successfully stored %d random numbers in file named:
'py_random_output.txt'. 20

TEST SUITE FOR:  PYTHON BUILT-IN RAND
=====================================
---------CHI-SQ_TEST-----------
Significance Level: 0.8
Chi Sq: 17.0
Crit Value: 10118.8246
Result is: FAIL TO REJECT null hypothesis
```

```
.....................................
Significance Level: 0.9
Chi Sq: 17.0
Crit Value: 10181.6616
Result is: FAIL TO REJECT null hypothesis
.....................................
Significance Level: 0.95
Chi Sq: 17.0
Crit Value: 10233.7489
Result is: FAIL TO REJECT null hypothesis
.....................................

---------KS_TEST-----------
D+ VALUE =0
D- VALUE=0.6314006161858726
D VALUE (max): 0.6314006161858726



Alpha Level is: 0.1
D_statistic is: 0.6314006161858726
Critical value is: 0.122
Result is: REJECT null hypothesis
.............................
Alpha Level is: 0.05
D_statistic is: 0.6314006161858726
Critical value is: 0.136
Result is: REJECT null hypothesis
.............................
Alpha Level is: 0.01
D_statistic is: 0.6314006161858726
Critical value is: 0.16299999999999998
Result is: REJECT null hypothesis
.............................
Kolmogorov-Smirnov Test Result for D-Value: 0.6314006161858726
```

2. For Linear Congruential Generator:

```
Please select a method for generating random numbers:
 1. Python's Random Function
 2. Linear Congruential Generator
      (or type 3 to quit)

Selection > 2
How many observations should we perform?
Selection > 20
Successfully stored 20 random numbers in file named: 'lgc_output.txt'.
```

```
TEST SUITE FOR:  LINEAR CONGRUENTIAL GENERATOR
=======================================
---------CHI-SQ_TEST-----------
Significance Level: 0.8
Chi Sq: 12.0
Crit Value: 10118.8246
Result is: FAIL TO REJECT null hypothesis
.....................................
Significance Level: 0.9
Chi Sq: 12.0
Crit Value: 10181.6616
Result is: FAIL TO REJECT null hypothesis
.....................................
Significance Level: 0.95
Chi Sq: 12.0
Crit Value: 10233.7489
Result is: FAIL TO REJECT null hypothesis
.....................................

---------KS_TEST-----------
D+ VALUE =0
D- VALUE=0.7446466064453126
D VALUE (max): 0.7446466064453126



Alpha Level is: 0.1
D_statistic is: 0.7446466064453126
Critical value is: 0.122
Result is: REJECT null hypothesis
.............................
Alpha Level is: 0.05
D_statistic is: 0.7446466064453126
Critical value is: 0.136
Result is: REJECT null hypothesis
.............................
Alpha Level is: 0.01
D_statistic is: 0.7446466064453126
Critical value is: 0.16299999999999998
Result is: REJECT null hypothesis
.............................
Kolmogorov-Smirnov Test Result for D-Value: 0.7446466064453126
```