LAB Assignment #1 for ECE 525

Description: Compute NIST and Inter-chip HD on the bitstring data provided.

1) Install the NIST statistical tools SP 800-22rev1a (2010) on your laptop or on the UNM server. Download from

`https://csrc.nist.gov/projects/random-bit-generation/documentation-and-software`

Unzip the file, under linux type

`unzip sts-2_1_2.zip`

And then change directory to

`sts-2.1.2/sts-2.1.2/`

And then compile

`make`

The executable is generated in the current directory and is called *assess*.

2) Run NIST statistical tests on bitstring data posted for lab1. Include the contents of the *final_analysis_report.txt* file in your report and a 1 paragraph explanation of your findings.

Running *assess*: You need to type in the components of the following that are **bolded**

cd lab1

cp -r *path_to_NIST_install*/experiments .

***path_to_NIST_install*/assess 5093**

```
          G E N E R A T O R    S E L E C T I O N
          _________________________________________

    [0] Input File                 [1] Linear Congruential
    [2] Quadratic Congruential I   [3] Quadratic Congruential II
    [4] Cubic Congruential         [5] XOR
    [6] Modular Exponentiation     [7] Blum-Blum-Shub
    [8] Micali-Schnorr             [9] G Using SHA-1

Enter Choice: 0

            User Prescribed Input File: path_to_bitstrings/
SHDBitstrings_optKEK_TVN_0.52_WID_1.20_Margin_03_Mod_24_NumSeeds_0010_MeanS_OMR_4
_OTM_1.txt

              S T A T I S T I C A L   T E S T S
              _________________________________

[01] Frequency                       [02] Block Frequency
[03] Cumulative Sums                 [04] Runs
[05] Longest Run of Ones             [06] Rank
[07] Discrete Fourier Transform      [08] Nonperiodic Template Matchings
[09] Overlapping Template Matchings  [10] Universal Statistical
[11] Approximate Entropy             [12] Random Excursions
```

```
[13] Random Excursions Variant       [14] Serial
[15] Linear Complexity

         INSTRUCTIONS
            Enter 0 if you DO NOT want to apply all of the
            statistical tests to each sequence and 1 if you DO.

   Enter Choice: 0

         INSTRUCTIONS
            Enter a 0 or 1 to indicate whether or not the numbered statis-
tical
            test should be applied to each sequence.

      123456789111111
               012345

      111110100000010

        P a r a m e t e r   A d j u s t m e n t s
        ----------------------------------------
    [1] Block Frequency Test - block length(M):         128
    [2] Serial Test - block length(m):                  16

   Select Test (0 to continue): 0

   How many bitstreams? 500

   Input File Format:
    [0] ASCII - A sequence of ASCII 0's and 1's
    [1] Binary - Each byte in data file contains 8 bits of data

   Select input mode: 0


     Statistical Testing In Progress.........

     Statistical Testing Complete!!!!!!!!!!!!
```

The results are written to *experiments/AlgorithmTesting/finalAnalysisReport.txt*

The instructions are included in the documentation at
`https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-22r1a.pdf`
Section 5 *User's Guide* gives additional information on *assess*.

3) Compute the individual Inter-chip HDs using the same bitstring data in a programming language of your choice (C is best but perl/python also works well). Plot the distribution as a histogram. You should have 500*499/2 = 124,750 individual HDs tabulated in your histogram.

4) Compute the mean and standard deviation of the histogram data. Compare to the value predicted from a binomial distribution.

5) Turn in a lab report of your findings.

See PUF1.pdf for additional information on the NIST tools and result file format.