NIST-Test PRG220 AES128 (PTG.3) IBB, 14.04.2014

```
################################################################

              THE NIST STATISTICAL TEST SUITE

################################################################


---------------------------------------------------------------
  1.  FREQUENCY TEST
---------------------------------------------------------------

Computational information:
(a) The nth partial sum = -1380
(b) S_n/n               = -0.001380

p_value = 0.167587, SUCCESS

---------------------------------------------------------------
  2.  BLOCK FREQUENCY TEST
---------------------------------------------------------------

Computational information:
(a) Chi^2           = 124874.000000
(b) # of substrings = 125000
(c) block length    = 8

p_value = 0.598997, SUCCESS

---------------------------------------------------------------
  3.  CUMULATIVE SUMS TEST
---------------------------------------------------------------

Cumulative sums forward test:

Computational information:
(a) The maximum partial sum =

p_value = 0.301404, SUCCESS


Cumulative sums reverse test:

Computational information:
(a) The maximum partial sum =

p_value = 0.066014, SUCCESS

---------------------------------------------------------------
  4.  RUNS TEST
---------------------------------------------------------------

Computational information:
(a) Pi                         = 0.499310
(b) V_n_obs (Total # of runs) = 500067
(c) V_n_obs - 2 n pi (1-pi)
     --------------------- = 0.096099
      2 sqrt(2n) pi (1-pi)

p_value = 0.891897, SUCCESS
```

```
------------------------------------------------------------
  5.  LONGEST RUNS OF ONES TEST
------------------------------------------------------------

Computational information:
(a) N (# of substrings)  = 100
(b) M (Substring Length) = 10000
(c) Chi^2                = 2.449555


Frequency
-------------------------------------------------
<=10     11     12     13     14     15    >=16
-------------------------------------------------
  11     23     26     14     11      7       8

p_value = 0.874070, SUCCESS

------------------------------------------------------------
  6.  RANK TEST
------------------------------------------------------------

Computational information:
(a) Probability P_32 = 0.288788
(b)             P_31 = 0.577576
(c)             P_30 = 0.133636
(d) Frequency   F_32 = 287
(e)             F_31 = 551
(f)             F_30 = 138
(g) # of matrices    = 976
(h) Chi^2            = 0.820142
(i) NOTE: 576 BITS WERE DISCARDED.

p_value = 0.663603, SUCCESS

------------------------------------------------------------
  7.  DFT TEST
------------------------------------------------------------

Computational information:
(a) Percentile = 95.019800
(b) N_l        = 475099.000000
(c) N_o        = 475000.000000
(d) d          = 0.642397

p_value = 0.520616, SUCCESS

------------------------------------------------------------
  8.  NONOVERLAPPING TEMPLATES TEST
------------------------------------------------------------

Computational information:
LAMBDA = 122.061523
M = 125000, N = 8, m = 10, n = 1000000

Template   W_1  W_2  W_3  W_4  W_5  W_6  W_7  W_8
-------------------------------------------------
1100100100 111  103  111  113  137  107  135  119

chi2_value = 10.992433
p_value = 0.202128, SUCCESS

------------------------------------------------------------
  9.  OVERLAPPING TEMPLATE OF ALL ONES TEST
------------------------------------------------------------

Computational information:
(a) n (sequence_length)      = 1000000
```

```
(b) m (block length of 1s)   = 10
(c) M (length of substring)  = 1032
(d) N (number of substrings) = 968
(e) lambda [(M-m+1)/2^m]     = 0.999023
(f) eta                      = 0.499512

Frequency:
-----------------------------------------------
0    1    2    3    4    >=5    Chi^2
-----------------------------------------------
596  149   87   66   22   48    6.6981

p_value = 0.244078, SUCCESS

------------------------------------------------------------
 10.  UNIVERSAL TEST
------------------------------------------------------------

Computational information:
(a) L         = 7
(b) Q         = 1280
(c) K         = 141577
(d) sum       = 877468.273027
(e) sigma     = 0.002768
(f) variance  = 3.125000
(g) exp_value = 6.196251
(h) phi       = 6.197817
(i) WARNING:  1 bits were discarded.

p_value = 0.571661, SUCCESS

------------------------------------------------------------
 11.  APPROXIMATE ENTROPY TEST
------------------------------------------------------------

Computational information:
(a) m (block length)    = 5
(b) n (sequence length) = 1000000
(c) Chi^2               = 32.591256
(d) Phi(m)              = -3.465721
(e) Phi(m+1)            = -4.158852
(f) ApEn                = 0.693131
(g) Log(2)              = 0.693147

p_value = 0.437707, SUCCESS

------------------------------------------------------------
 12.  RANDOM EXCURSIONS TEST
------------------------------------------------------------

Computational information:
(a) Number Of Cycles (J) = 1474
(b) Sequence Length (n)  = 1000000
(c) Rejection Constraint = 500.000000

x = -4 chi^2 =  7.589109 p_value = 0.180382, SUCCESS
x = -3 chi^2 =  7.313574 p_value = 0.198344, SUCCESS
x = -2 chi^2 =  5.668560 p_value = 0.339816, SUCCESS
x = -1 chi^2 =  1.550882 p_value = 0.907124, SUCCESS
x =  1 chi^2 =  1.549525 p_value = 0.907285, SUCCESS
x =  2 chi^2 = 10.506893 p_value = 0.062082, SUCCESS
x =  3 chi^2 =  7.351186 p_value = 0.195805, SUCCESS
x =  4 chi^2 =  3.901069 p_value = 0.563746, SUCCESS

------------------------------------------------------------
 13.  RANDOM EXCURSIONS VARIANT TEST
------------------------------------------------------------
```

```
Computational information:
(a) Number Of Cycles (J) = 1474
(b) Sequence Length (n)  = 1000000

(x = -9) Total visits = 1514; p-value = 0.858190
 SUCCESS
(x = -8) Total visits = 1509; p-value = 0.867810
 SUCCESS
(x = -7) Total visits = 1468; p-value = 0.975549
 SUCCESS
(x = -6) Total visits = 1361; p-value = 0.530327
 SUCCESS
(x = -5) Total visits = 1317; p-value = 0.335115
 SUCCESS
(x = -4) Total visits = 1372; p-value = 0.477675
 SUCCESS
(x = -3) Total visits = 1467; p-value = 0.954022
 SUCCESS
(x = -2) Total visits = 1547; p-value = 0.437605
 SUCCESS
(x = -1) Total visits = 1541; p-value = 0.217207
 SUCCESS
(x =  1) Total visits = 1438; p-value = 0.507306
 SUCCESS
(x =  2) Total visits = 1501; p-value = 0.774033
 SUCCESS
(x =  3) Total visits = 1570; p-value = 0.429108
 SUCCESS
(x =  4) Total visits = 1554; p-value = 0.577596
 SUCCESS
(x =  5) Total visits = 1555; p-value = 0.618992
 SUCCESS
(x =  6) Total visits = 1592; p-value = 0.512292
 SUCCESS
(x =  7) Total visits = 1542; p-value = 0.728325
 SUCCESS
(x =  8) Total visits = 1475; p-value = 0.996206
 SUCCESS
(x =  9) Total visits = 1512; p-value = 0.865211
 SUCCESS

------------------------------------------------------------
 14.  SERIAL TEST
------------------------------------------------------------

Computational information:
(a) Block length    (m) = 5
(b) Sequence length (n) = 1000000
(c) Psi_m               = 29.811648
(d) Psi_m-1             = 15.490208
(e) Psi_m-2             = 8.552096
(f) Del_1               = 14.321440
(g) Del_2               = 7.383328

p_value1 = 0.574781, SUCCESS

p_value2 = 0.495895, SUCCESS

------------------------------------------------------------
 15.  LEMPEL-ZIV COMPRESSION TEST
------------------------------------------------------------

Computational information:
(a) W (# of words) = 69588

p_value = 0.490589, SUCCESS
```