Diehard-Test PRG310 AES128 (PTG.3) IBB, 14.04.2014

```
BIRTHDAY SPACINGS TEST, M= 512 N=2**24 LAMBDA=  2.0000
          taes1.rnd       using bits  1 to 24 p-value=  .732352
          taes1.rnd       using bits  2 to 25 p-value=  .441727
          taes1.rnd       using bits  3 to 26 p-value=  .007405
          taes1.rnd       using bits  4 to 27 p-value=  .813373
          taes1.rnd       using bits  5 to 28 p-value=  .115171
          taes1.rnd       using bits  6 to 29 p-value=  .393101
          taes1.rnd       using bits  7 to 30 p-value=  .847603
          taes1.rnd       using bits  8 to 31 p-value=  .099781
          taes1.rnd       using bits  9 to 32 p-value=  .105542
   The 9 p-values were
        .732352   .441727   .007405   .813373   .115171
        .393101   .847603   .099781   .105542
  A KSTEST for the 9 p-values yields  .745850
-------------------------------------------------------------------------------
          OPERM5 test for file taes1.rnd
 chisquare for 99 degrees of freedom= 82.328; p-value= .112956
          OPERM5 test for file taes1.rnd
 chisquare for 99 degrees of freedom= 87.796; p-value= .217431
-------------------------------------------------------------------------------
    Binary rank test for taes1.rnd
         Rank test for 31x31 binary matrices:
        rows from leftmost 31 bits of each 32-bit integer
      rank   observed  expected (o-e)^2/e  sum
        28       182     211.4  4.093405    4.093
        29      5195    5134.0   .724531    4.818
        30     23143   23103.0   .069093    4.887
        31     11480   11551.5   .442863    5.330
  chisquare= 5.330 for 3 d. of f.; p-value= .861307
    Binary rank test for taes1.rnd
         Rank test for 32x32 binary matrices:
        rows from leftmost 32 bits of each 32-bit integer
      rank   observed  expected (o-e)^2/e  sum
        29       181     211.4  4.376428    4.376
        30      4976    5134.0  4.863107    9.240
        31     23310   23103.0  1.853850   11.093
        32     11533   11551.5   .029706   11.123
  chisquare=11.123 for 3 d. of f.; p-value= .989348
-------------------------------------------------------------------------------
 b-rank test for bits  1 to  8 p=1-exp(-SUM/2)= .59320
 b-rank test for bits  2 to  9 p=1-exp(-SUM/2)= .47113
 b-rank test for bits  3 to 10 p=1-exp(-SUM/2)= .72991
 b-rank test for bits  4 to 11 p=1-exp(-SUM/2)= .88404
 b-rank test for bits  5 to 12 p=1-exp(-SUM/2)= .33460
 b-rank test for bits  6 to 13 p=1-exp(-SUM/2)= .80056
 b-rank test for bits  7 to 14 p=1-exp(-SUM/2)= .20357
 b-rank test for bits  8 to 15 p=1-exp(-SUM/2)= .37389
 b-rank test for bits  9 to 16 p=1-exp(-SUM/2)= .09358
 b-rank test for bits 10 to 17 p=1-exp(-SUM/2)= .58868
 b-rank test for bits 11 to 18 p=1-exp(-SUM/2)= .81523
 b-rank test for bits 12 to 19 p=1-exp(-SUM/2)= .06497
 b-rank test for bits 13 to 20 p=1-exp(-SUM/2)= .96420
 b-rank test for bits 14 to 21 p=1-exp(-SUM/2)= .89280
 b-rank test for bits 15 to 22 p=1-exp(-SUM/2)= .66964
 b-rank test for bits 16 to 23 p=1-exp(-SUM/2)= .10005
 b-rank test for bits 17 to 24 p=1-exp(-SUM/2)= .14185
 b-rank test for bits 18 to 25 p=1-exp(-SUM/2)= .09615
 b-rank test for bits 19 to 26 p=1-exp(-SUM/2)= .28939
 b-rank test for bits 20 to 27 p=1-exp(-SUM/2)= .24190
 b-rank test for bits 21 to 28 p=1-exp(-SUM/2)= .52847
 b-rank test for bits 22 to 29 p=1-exp(-SUM/2)= .05579
 b-rank test for bits 23 to 30 p=1-exp(-SUM/2)= .07577
 b-rank test for bits 24 to 31 p=1-exp(-SUM/2)= .29206
 b-rank test for bits 25 to 32 p=1-exp(-SUM/2)= .11641
   TEST SUMMARY, 25 tests on 100,000 random 6x8 matrices
```

```
 These should be 25 uniform [0,1] random variables:
     .593202     .471134     .729906     .884040     .334596
     .800559     .203569     .373894     .093583     .588676
     .815229     .064973     .964198     .892796     .669644
     .100046     .141854     .096155     .289389     .241901
     .528472     .055787     .075773     .292065     .116414
   brank test summary for taes1.rnd
       The KS test for those 25 supposed UNI's yields
                  KS p-value= .818483
-------------------------------------------------------------------------------
  No. missing words should average  141909. with sigma=428.
 tst no  1:  141638 missing words,    -.63 sigmas from mean, p-value= .26306
 tst no  2:  142090 missing words,     .42 sigmas from mean, p-value= .66354
 tst no  3:  141015 missing words,   -2.09 sigmas from mean, p-value= .01833
 tst no  4:  141842 missing words,    -.16 sigmas from mean, p-value= .43750
 tst no  5:  142419 missing words,    1.19 sigmas from mean, p-value= .88314
 tst no  6:  142015 missing words,     .25 sigmas from mean, p-value= .59751
 tst no  7:  141789 missing words,    -.28 sigmas from mean, p-value= .38930
 tst no  8:  140759 missing words,   -2.69 sigmas from mean, p-value= .00360
 tst no  9:  142490 missing words,    1.36 sigmas from mean, p-value= .91256
 tst no 10:  142206 missing words,     .69 sigmas from mean, p-value= .75589
 tst no 11:  141568 missing words,    -.80 sigmas from mean, p-value= .21258
 tst no 12:  142039 missing words,     .30 sigmas from mean, p-value= .61904
 tst no 13:  141570 missing words,    -.79 sigmas from mean, p-value= .21394
 tst no 14:  142047 missing words,     .32 sigmas from mean, p-value= .62615
 tst no 15:  141908 missing words,     .00 sigmas from mean, p-value= .49876
 tst no 16:  141764 missing words,    -.34 sigmas from mean, p-value= .36710
 tst no 17:  142882 missing words,    2.27 sigmas from mean, p-value= .98847
 tst no 18:  141855 missing words,    -.13 sigmas from mean, p-value= .44950
 tst no 19:  142074 missing words,     .38 sigmas from mean, p-value= .64979
 tst no 20:  142441 missing words,    1.24 sigmas from mean, p-value= .89292
-------------------------------------------------------------------------------
    OPSO for taes1.rnd       using bits 23 to 32        142173   .909  .8184
    OPSO for taes1.rnd       using bits 22 to 31        142079   .585  .7208
    OPSO for taes1.rnd       using bits 21 to 30        142030   .416  .6613
    OPSO for taes1.rnd       using bits 20 to 29        141508 -1.384  .0832
    OPSO for taes1.rnd       using bits 19 to 28        142202  1.009  .8436
    OPSO for taes1.rnd       using bits 18 to 27        141711  -.684  .2470
    OPSO for taes1.rnd       using bits 17 to 26        141839  -.243  .4042
    OPSO for taes1.rnd       using bits 16 to 25        142195   .985  .8377
    OPSO for taes1.rnd       using bits 15 to 24        142089   .620  .7322
    OPSO for taes1.rnd       using bits 14 to 23        141953   .151  .5599
    OPSO for taes1.rnd       using bits 13 to 22        141896  -.046  .4817
    OPSO for taes1.rnd       using bits 12 to 21        142025   .399  .6550
    OPSO for taes1.rnd       using bits 11 to 20        142556  2.230  .9871
    OPSO for taes1.rnd       using bits 10 to 19        142273  1.254  .8951
    OPSO for taes1.rnd       using bits  9 to 18        142148   .823  .7947
    OPSO for taes1.rnd       using bits  8 to 17        141988   .271  .6069
    OPSO for taes1.rnd       using bits  7 to 16        141625  -.980  .1634
    OPSO for taes1.rnd       using bits  6 to 15        141991   .282  .6109
    OPSO for taes1.rnd       using bits  5 to 14        141637  -.939  .1738
    OPSO for taes1.rnd       using bits  4 to 13        141847  -.215  .4149
    OPSO for taes1.rnd       using bits  3 to 12        141785  -.429  .3341
    OPSO for taes1.rnd       using bits  2 to 11        141618 -1.005  .1575
    OPSO for taes1.rnd       using bits  1 to 10        142334  1.464  .9285
    OQSO for taes1.rnd       using bits 28 to 32        141964   .185  .5735
    OQSO for taes1.rnd       using bits 27 to 31        141851  -.198  .4216
    OQSO for taes1.rnd       using bits 26 to 30        141728  -.615  .2694
    OQSO for taes1.rnd       using bits 25 to 29        142172   .890  .8134
    OQSO for taes1.rnd       using bits 24 to 28        142112   .687  .7540
    OQSO for taes1.rnd       using bits 23 to 27        141637  -.923  .1780
    OQSO for taes1.rnd       using bits 22 to 26        141288 -2.106  .0176
    OQSO for taes1.rnd       using bits 21 to 25        141950   .138  .5548
    OQSO for taes1.rnd       using bits 20 to 24        141726  -.621  .2672
    OQSO for taes1.rnd       using bits 19 to 23        141336 -1.943  .0260
    OQSO for taes1.rnd       using bits 18 to 22        142073   .555  .7105
    OQSO for taes1.rnd       using bits 17 to 21        141995   .290  .6142
    OQSO for taes1.rnd       using bits 16 to 20        142113   .690  .7550
```

```
   OQSO for taes1.rnd       using bits 15 to 19        142264  1.202  .8854
   OQSO for taes1.rnd       using bits 14 to 18        141396 -1.740  .0409
   OQSO for taes1.rnd       using bits 13 to 17        142231  1.090  .8622
   OQSO for taes1.rnd       using bits 12 to 16        141595 -1.066  .1433
   OQSO for taes1.rnd       using bits 11 to 15        142023   .385  .6500
   OQSO for taes1.rnd       using bits 10 to 14        141869  -.137  .4456
   OQSO for taes1.rnd       using bits  9 to 13        141393 -1.750  .0400
   OQSO for taes1.rnd       using bits  8 to 12        141715  -.659  .2550
   OQSO for taes1.rnd       using bits  7 to 11        142095   .629  .7355
   OQSO for taes1.rnd       using bits  6 to 10        142183   .928  .8232
   OQSO for taes1.rnd       using bits  5 to  9        142139   .779  .7819
   OQSO for taes1.rnd       using bits  4 to  8        142521  2.073  .9809
   OQSO for taes1.rnd       using bits  3 to  7        142058   .504  .6929
   OQSO for taes1.rnd       using bits  2 to  6        142170   .884  .8116
   OQSO for taes1.rnd       using bits  1 to  5        141528 -1.293  .0981
    DNA for taes1.rnd       using bits 31 to 32        141696  -.629  .2646
    DNA for taes1.rnd       using bits 30 to 31        142456  1.613  .9466
    DNA for taes1.rnd       using bits 29 to 30        141860  -.146  .4422
    DNA for taes1.rnd       using bits 28 to 29        141974   .191  .5756
    DNA for taes1.rnd       using bits 27 to 28        141865  -.131  .4480
    DNA for taes1.rnd       using bits 26 to 27        142322  1.217  .8883
    DNA for taes1.rnd       using bits 25 to 26        141962   .155  .5617
    DNA for taes1.rnd       using bits 24 to 25        142037   .377  .6468
    DNA for taes1.rnd       using bits 23 to 24        142083   .512  .6958
    DNA for taes1.rnd       using bits 22 to 23        141344 -1.668  .0477
    DNA for taes1.rnd       using bits 21 to 22        141931   .064  .5255
    DNA for taes1.rnd       using bits 20 to 21        142380  1.388  .9175
    DNA for taes1.rnd       using bits 19 to 20        142453  1.604  .9456
    DNA for taes1.rnd       using bits 18 to 19        141856  -.157  .4375
    DNA for taes1.rnd       using bits 17 to 18        141809  -.296  .3836
    DNA for taes1.rnd       using bits 16 to 17        141554 -1.048  .1473
    DNA for taes1.rnd       using bits 15 to 16        141420 -1.443  .0744
    DNA for taes1.rnd       using bits 14 to 15        142068   .468  .6801
    DNA for taes1.rnd       using bits 13 to 14        141835  -.219  .4132
    DNA for taes1.rnd       using bits 12 to 13        142075   .489  .6875
    DNA for taes1.rnd       using bits 11 to 12        142291  1.126  .8699
    DNA for taes1.rnd       using bits 10 to 11        141750  -.470  .3192
    DNA for taes1.rnd       using bits  9 to 10        142368  1.353  .9120
    DNA for taes1.rnd       using bits  8 to  9        141975   .194  .5768
    DNA for taes1.rnd       using bits  7 to  8        141785  -.367  .3569
    DNA for taes1.rnd       using bits  6 to  7        142324  1.223  .8894
    DNA for taes1.rnd       using bits  5 to  6        142163   .748  .7729
    DNA for taes1.rnd       using bits  4 to  5        142049   .412  .6598
    DNA for taes1.rnd       using bits  3 to  4        141963   .158  .5629
    DNA for taes1.rnd       using bits  2 to  3        142546  1.878  .9698
    DNA for taes1.rnd       using bits  1 to  2        142264  1.046  .8523
------------------------------------------------------------------------------
  Test results for taes1.rnd
 Chi-square with 5^5-5^4=2500 d.of f. for sample size:2560000
                              chisquare  equiv normal  p-value
  Results fo COUNT-THE-1's in successive bytes:
 byte stream for taes1.rnd        2513.53       .191      .575848
 byte stream for taes1.rnd        2464.21      -.506      .306384
------------------------------------------------------------------------------
 Chi-square with 5^5-5^4=2500 d.of f. for sample size: 256000
                     chisquare  equiv normal  p value
  Results for COUNT-THE-1's in specified bytes:
           bits  1 to  8  2467.04      -.466      .320578
           bits  2 to  9  2530.13       .426      .664966
           bits  3 to 10  2553.18       .752      .774018
           bits  4 to 11  2523.19       .328      .628536
           bits  5 to 12  2570.18       .992      .839510
           bits  6 to 13  2427.26     -1.029      .151800
           bits  7 to 14  2577.83      1.101      .864475
           bits  8 to 15  2620.05      1.698      .955225
           bits  9 to 16  2539.34       .556      .711024
           bits 10 to 17  2396.09     -1.470      .070841
           bits 11 to 18  2455.37      -.631      .263964
```

```
          bits 12 to 19  2362.88     -1.939      .026245
          bits 13 to 20  2504.03       .057      .522705
          bits 14 to 21  2390.50     -1.549      .060744
          bits 15 to 22  2490.66      -.132      .447471
          bits 16 to 23  2520.55       .291      .614344
          bits 17 to 24  2544.72       .632      .736450
          bits 18 to 25  2453.22      -.662      .254126
          bits 19 to 26  2548.36       .684      .753005
          bits 20 to 27  2488.50      -.163      .435389
          bits 21 to 28  2377.67     -1.730      .041808
          bits 22 to 29  2443.96      -.792      .214044
          bits 23 to 30  2566.17       .936      .825321
          bits 24 to 31  2664.64      2.328      .990055
          bits 25 to 32  2661.52      2.284      .988823
------------------------------------------------------------------------------
          CDPARK: result of ten tests on file taes1.rnd
           Of 12,000 tries, the average no. of successes
                should be 3523 with sigma=21.9
           Successes: 3479    z-score: -2.009 p-value: .022262
           Successes: 3522    z-score:  -.046 p-value: .481790
           Successes: 3543    z-score:   .913 p-value: .819442
           Successes: 3536    z-score:   .594 p-value: .723613
           Successes: 3514    z-score:  -.411 p-value: .340551
           Successes: 3500    z-score: -1.050 p-value: .146807
           Successes: 3552    z-score:  1.324 p-value: .907282
           Successes: 3515    z-score:  -.365 p-value: .357445
           Successes: 3548    z-score:  1.142 p-value: .873180
           Successes: 3561    z-score:  1.735 p-value: .958644

          square size   avg. no.  parked   sample sigma
            100.           3527.000       24.343
           KSTEST for the above 10: p=  .343710
------------------------------------------------------------------------------
              This is the MINIMUM DISTANCE test
             for random integers in the file taes1.rnd
    Sample no.    d^2     avg     equiv uni
          5     .1721    .6354     .158840
         10    2.8389   1.1258     .942341
         15     .0721   1.1329     .069883
         20    1.0535    .9666     .653126
         25    1.3439    .9925     .740918
         30     .3471    .9033     .294494
         35     .4523    .8802     .365267
         40    1.6034    .8820     .800404
         45    1.1710    .8738     .691764
         50     .7622    .8550     .535159
         55    2.0705    .8654     .875185
         60    2.5056    .8581     .919399
         65    1.9319    .8579     .856534
         70    1.7826    .8595     .833303
         75     .6230    .8634     .465330
         80     .5124    .8626     .402460
         85     .6409    .8471     .474884
         90     .5578    .8219     .429149
         95     .0179    .8518     .017849
        100     .3911    .8592     .325007
    MINIMUM DISTANCE TEST for taes1.rnd
         Result of KS test on 20 transformed mindist^2's:
                              p-value= .524249
------------------------------------------------------------------------------
              The 3DSPHERES test for file taes1.rnd
 sample no:  1     r^3=  52.831     p-value= .82813
 sample no:  2     r^3=  12.849     p-value= .34838
 sample no:  3     r^3=   3.516     p-value= .11058
 sample no:  4     r^3=  43.259     p-value= .76354
 sample no:  5     r^3=  19.434     p-value= .47681
 sample no:  6     r^3=  13.230     p-value= .35660
 sample no:  7     r^3=  39.815     p-value= .73477
```

```
 sample no:  8     r^3=  47.744     p-value= .79637
 sample no:  9     r^3=  11.126     p-value= .30985
 sample no: 10     r^3=  60.781     p-value= .86814
 sample no: 11     r^3=    .069     p-value= .00229
 sample no: 12     r^3=   6.201     p-value= .18673
 sample no: 13     r^3=  26.505     p-value= .58666
 sample no: 14     r^3=   5.578     p-value= .16968
 sample no: 15     r^3=  44.841     p-value= .77569
 sample no: 16     r^3=  20.799     p-value= .50008
 sample no: 17     r^3=  40.731     p-value= .74274
 sample no: 18     r^3=  31.489     p-value= .64994
 sample no: 19     r^3=  39.710     p-value= .73384
 sample no: 20     r^3=  41.537     p-value= .74957
       3DSPHERES test for file taes1.rnd           p-value= .571827
------------------------------------------------------------------------------
           RESULTS OF SQUEEZE TEST FOR taes1.rnd
         Table of standardized frequency counts
     ( (obs-exp)/sqrt(exp) )^2
        for j taking values <=6,7,8,...,47,>=48:
    -.8     1.3     -.6      .5     -.8      .6
     .0    -1.6      .7    -2.9     1.1      .2
   -1.2      .9     -.1     -.5     1.9      .3
    -.6     -.9     -.1    -1.1     -.7      .8
    -.6     1.3      .9     1.2     1.0      .6
     .0     1.0      .2      .8     -.2     -.1
    1.0     -.7      .1      .4      .9     1.0
   -1.1
          Chi-square with 42 degrees of freedom: 38.757
             z-score=  -.354  p-value= .385665
_____________________________________________________
------------------------------------------------------------------------------
               Test no.  1      p-value  .407500
               Test no.  2      p-value  .896252
               Test no.  3      p-value  .243365
               Test no.  4      p-value  .181625
               Test no.  5      p-value  .430341
               Test no.  6      p-value  .585691
               Test no.  7      p-value  .963620
               Test no.  8      p-value  .351454
               Test no.  9      p-value  .484607
               Test no. 10      p-value  .560133
  Results of the OSUM test for taes1.rnd
       KSTEST on the above 10 p-values:  .294647
------------------------------------------------------------------------------
          The RUNS test for file taes1.rnd
    Up and down runs in a sample of 10000
_____________________________________________
                Run test for taes1.rnd      :
      runs up; ks test for 10 p's: .515991
    runs down; ks test for 10 p's: .530047
                Run test for taes1.rnd      :
      runs up; ks test for 10 p's: .919836
    runs down; ks test for 10 p's: .104965
------------------------------------------------------------------------------
               Results of craps test for taes1.rnd
 No. of wins:  Observed Expected
                              98223    98585.86
Chisq=  29.25 for 20 degrees of freedom, p=  .91705
             Throws Observed Expected  Chisq     Sum
           SUMMARY  FOR taes1.rnd
               p-value for no. of wins: .052303
               p-value for throws/game: .917048
 Test completed.  File taes1.rnd
::::::::::::::::::::::::::::::::::::::::::::::::::::::::::::::::::::::::::::::
```