Diehard-Test PRG610 AES128 (PTG.3) IBB, 18.02.2015

```
BIRTHDAY SPACINGS TEST, M= 512 N=2**24 LAMBDA=  2.0000
           prg610_1.rnd    using bits  1 to 24 p-value=  .789798
           prg610_1.rnd    using bits  2 to 25 p-value=  .337132
           prg610_1.rnd    using bits  3 to 26 p-value=  .430563
           prg610_1.rnd    using bits  4 to 27 p-value=  .501090
           prg610_1.rnd    using bits  5 to 28 p-value=  .619900
           prg610_1.rnd    using bits  6 to 29 p-value=  .800086
           prg610_1.rnd    using bits  7 to 30 p-value=  .372001
           prg610_1.rnd    using bits  8 to 31 p-value=  .018392
           prg610_1.rnd    using bits  9 to 32 p-value=  .954537
   The 9 p-values were
        .789798   .337132   .430563   .501090   .619900
        .800086   .372001   .018392   .954537
  A KSTEST for the 9 p-values yields  .114516
-------------------------------------------------------------------------------
           OPERM5 test for file prg610_1.rnd
 chisquare for 99 degrees of freedom=108.439; p-value= .757386
           OPERM5 test for file prg610_1.rnd
 chisquare for 99 degrees of freedom=108.083; p-value= .749880
-------------------------------------------------------------------------------
    Binary rank test for prg610_1.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       206     211.4   .138848     .139
        29      5201    5134.0   .874098    1.013
        30     23038   23103.0   .183140    1.196
        31     11555   11551.5   .001046    1.197
  chisquare= 1.197 for 3 d. of f.; p-value= .383256
    Binary rank test for prg610_1.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       234     211.4  2.412028    2.412
        30      5099    5134.0   .238745    2.651
        31     23166   23103.0   .171540    2.822
        32     11501   11551.5   .220985    3.043
  chisquare= 3.043 for 3 d. of f.; p-value= .655538
-------------------------------------------------------------------------------
 b-rank test for bits  1 to  8 p=1-exp(-SUM/2)= .21790
 b-rank test for bits  2 to  9 p=1-exp(-SUM/2)= .09771
 b-rank test for bits  3 to 10 p=1-exp(-SUM/2)= .82327
 b-rank test for bits  4 to 11 p=1-exp(-SUM/2)= .43745
 b-rank test for bits  5 to 12 p=1-exp(-SUM/2)= .81658
 b-rank test for bits  6 to 13 p=1-exp(-SUM/2)= .76641
 b-rank test for bits  7 to 14 p=1-exp(-SUM/2)= .21211
 b-rank test for bits  8 to 15 p=1-exp(-SUM/2)= .30866
 b-rank test for bits  9 to 16 p=1-exp(-SUM/2)= .01882
 b-rank test for bits 10 to 17 p=1-exp(-SUM/2)= .43885
 b-rank test for bits 11 to 18 p=1-exp(-SUM/2)= .93367
 b-rank test for bits 12 to 19 p=1-exp(-SUM/2)= .45908
 b-rank test for bits 13 to 20 p=1-exp(-SUM/2)= .45408
 b-rank test for bits 14 to 21 p=1-exp(-SUM/2)= .58841
 b-rank test for bits 15 to 22 p=1-exp(-SUM/2)= .06114
 b-rank test for bits 16 to 23 p=1-exp(-SUM/2)= .23707
 b-rank test for bits 17 to 24 p=1-exp(-SUM/2)= .27429
 b-rank test for bits 18 to 25 p=1-exp(-SUM/2)= .61453
 b-rank test for bits 19 to 26 p=1-exp(-SUM/2)= .30922
 b-rank test for bits 20 to 27 p=1-exp(-SUM/2)= .39616
 b-rank test for bits 21 to 28 p=1-exp(-SUM/2)= .45784
 b-rank test for bits 22 to 29 p=1-exp(-SUM/2)= .96128
 b-rank test for bits 23 to 30 p=1-exp(-SUM/2)= .78924
 b-rank test for bits 24 to 31 p=1-exp(-SUM/2)= .10953
 b-rank test for bits 25 to 32 p=1-exp(-SUM/2)= .53559
   TEST SUMMARY, 25 tests on 100,000 random 6x8 matrices
```

```
 These should be 25 uniform [0,1] random variables:
     .217904     .097707     .823272     .437455     .816577
     .766405     .212113     .308661     .018816     .438853
     .933674     .459080     .454078     .588410     .061136
     .237073     .274285     .614532     .309221     .396157
     .457843     .961276     .789241     .109526     .535591
   brank test summary for prg610_1.rnd
       The KS test for those 25 supposed UNI's yields
                  KS p-value= .318262
--------------------------------------------------------------------------------
  No. missing words should average  141909. with sigma=428.
 tst no  1:  141736 missing words,    -.40 sigmas from mean, p-value= .34275
 tst no  2:  141495 missing words,    -.97 sigmas from mean, p-value= .16651
 tst no  3:  142016 missing words,     .25 sigmas from mean, p-value= .59841
 tst no  4:  142352 missing words,    1.03 sigmas from mean, p-value= .84950
 tst no  5:  141901 missing words,    -.02 sigmas from mean, p-value= .49224
 tst no  6:  141544 missing words,    -.85 sigmas from mean, p-value= .19667
 tst no  7:  142221 missing words,     .73 sigmas from mean, p-value= .76676
 tst no  8:  142356 missing words,    1.04 sigmas from mean, p-value= .85167
 tst no  9:  142030 missing words,     .28 sigmas from mean, p-value= .61101
 tst no 10:  141916 missing words,     .02 sigmas from mean, p-value= .50622
 tst no 11:  142242 missing words,     .78 sigmas from mean, p-value= .78150
 tst no 12:  142446 missing words,    1.25 sigmas from mean, p-value= .89506
 tst no 13:  140620 missing words,   -3.01 sigmas from mean, p-value= .00130
 tst no 14:  142024 missing words,     .27 sigmas from mean, p-value= .60562
 tst no 15:  142237 missing words,     .77 sigmas from mean, p-value= .77804
 tst no 16:  141923 missing words,     .03 sigmas from mean, p-value= .51274
 tst no 17:  141941 missing words,     .07 sigmas from mean, p-value= .52949
 tst no 18:  141756 missing words,    -.36 sigmas from mean, p-value= .36008
 tst no 19:  141630 missing words,    -.65 sigmas from mean, p-value= .25700
 tst no 20:  142105 missing words,     .46 sigmas from mean, p-value= .67623
--------------------------------------------------------------------------------
    OPSO for prg610_1.rnd    using bits 23 to 32        141990   .278  .6096
    OPSO for prg610_1.rnd    using bits 22 to 31        141587 -1.111  .1332
    OPSO for prg610_1.rnd    using bits 21 to 30        141607 -1.043  .1486
    OPSO for prg610_1.rnd    using bits 20 to 29        141823  -.298  .3830
    OPSO for prg610_1.rnd    using bits 19 to 28        141846  -.218  .4136
    OPSO for prg610_1.rnd    using bits 18 to 27        141175 -2.532  .0057
    OPSO for prg610_1.rnd    using bits 17 to 26        141963   .185  .5734
    OPSO for prg610_1.rnd    using bits 16 to 25        141680  -.791  .2145
    OPSO for prg610_1.rnd    using bits 15 to 24        141800  -.377  .3531
    OPSO for prg610_1.rnd    using bits 14 to 23        141975   .226  .5896
    OPSO for prg610_1.rnd    using bits 13 to 22        141919   .033  .5133
    OPSO for prg610_1.rnd    using bits 12 to 21        141776  -.460  .3228
    OPSO for prg610_1.rnd    using bits 11 to 20        141783  -.436  .3316
    OPSO for prg610_1.rnd    using bits 10 to 19        141534 -1.294  .0978
    OPSO for prg610_1.rnd    using bits  9 to 18        141384 -1.811  .0350
    OPSO for prg610_1.rnd    using bits  8 to 17        142082   .595  .7242
    OPSO for prg610_1.rnd    using bits  7 to 16        141971   .213  .5842
    OPSO for prg610_1.rnd    using bits  6 to 15        141597 -1.077  .1407
    OPSO for prg610_1.rnd    using bits  5 to 14        142150   .830  .7967
    OPSO for prg610_1.rnd    using bits  4 to 13        142175   .916  .8202
    OPSO for prg610_1.rnd    using bits  3 to 12        142223  1.082  .8603
    OPSO for prg610_1.rnd    using bits  2 to 11        141374 -1.846  .0324
    OPSO for prg610_1.rnd    using bits  1 to 10        141621  -.994  .1601
    OQSO for prg610_1.rnd    using bits 28 to 32        141974   .219  .5868
    OQSO for prg610_1.rnd    using bits 27 to 31        141708  -.682  .2475
    OQSO for prg610_1.rnd    using bits 26 to 30        141690  -.743  .2286
    OQSO for prg610_1.rnd    using bits 25 to 29        141871  -.130  .4483
    OQSO for prg610_1.rnd    using bits 24 to 28        141930   .070  .5279
    OQSO for prg610_1.rnd    using bits 23 to 27        141536 -1.266  .1028
    OQSO for prg610_1.rnd    using bits 22 to 26        142380  1.595  .9447
    OQSO for prg610_1.rnd    using bits 21 to 25        141520 -1.320  .0935
    OQSO for prg610_1.rnd    using bits 20 to 24        141460 -1.523  .0639
    OQSO for prg610_1.rnd    using bits 19 to 23        141915   .019  .5077
    OQSO for prg610_1.rnd    using bits 18 to 22        142182   .924  .8223
    OQSO for prg610_1.rnd    using bits 17 to 21        142309  1.355  .9123
    OQSO for prg610_1.rnd    using bits 16 to 20        141844  -.221  .4124
```

```
   OQSO for prg610_1.rnd    using bits 15 to 19        142003   .318  .6246
   OQSO for prg610_1.rnd    using bits 14 to 18        141892  -.059  .4766
   OQSO for prg610_1.rnd    using bits 13 to 17        141655  -.862  .1943
   OQSO for prg610_1.rnd    using bits 12 to 16        142082   .585  .7208
   OQSO for prg610_1.rnd    using bits 11 to 15        141879  -.103  .4591
   OQSO for prg610_1.rnd    using bits 10 to 14        141735  -.591  .2773
   OQSO for prg610_1.rnd    using bits  9 to 13        141836  -.249  .4018
   OQSO for prg610_1.rnd    using bits  8 to 12        141843  -.225  .4111
   OQSO for prg610_1.rnd    using bits  7 to 11        141387 -1.771  .0383
   OQSO for prg610_1.rnd    using bits  6 to 10        141754  -.527  .2993
   OQSO for prg610_1.rnd    using bits  5 to  9        141697  -.720  .2358
   OQSO for prg610_1.rnd    using bits  4 to  8        141634  -.933  .1753
   OQSO for prg610_1.rnd    using bits  3 to  7        142519  2.067  .9806
   OQSO for prg610_1.rnd    using bits  2 to  6        141676  -.791  .2145
   OQSO for prg610_1.rnd    using bits  1 to  5        142201   .989  .8386
    DNA for prg610_1.rnd    using bits 31 to 32        141668  -.712  .2383
    DNA for prg610_1.rnd    using bits 30 to 31        141519 -1.151  .1248
    DNA for prg610_1.rnd    using bits 29 to 30        141954   .132  .5524
    DNA for prg610_1.rnd    using bits 28 to 29        142007   .288  .6134
    DNA for prg610_1.rnd    using bits 27 to 28        141755  -.455  .3245
    DNA for prg610_1.rnd    using bits 26 to 27        141957   .141  .5559
    DNA for prg610_1.rnd    using bits 25 to 26        141769  -.414  .3395
    DNA for prg610_1.rnd    using bits 24 to 25        141838  -.210  .4167
    DNA for prg610_1.rnd    using bits 23 to 24        141831  -.231  .4086
    DNA for prg610_1.rnd    using bits 22 to 23        141798  -.328  .3713
    DNA for prg610_1.rnd    using bits 21 to 22        142182   .804  .7894
    DNA for prg610_1.rnd    using bits 20 to 21        141498 -1.213  .1125
    DNA for prg610_1.rnd    using bits 19 to 20        141905  -.013  .4949
    DNA for prg610_1.rnd    using bits 18 to 19        142067   .465  .6791
    DNA for prg610_1.rnd    using bits 17 to 18        142203   .866  .8068
    DNA for prg610_1.rnd    using bits 16 to 17        141356 -1.632  .0513
    DNA for prg610_1.rnd    using bits 15 to 16        142144   .692  .7556
    DNA for prg610_1.rnd    using bits 14 to 15        141809  -.296  .3836
    DNA for prg610_1.rnd    using bits 13 to 14        141834  -.222  .4121
    DNA for prg610_1.rnd    using bits 12 to 13        141838  -.210  .4167
    DNA for prg610_1.rnd    using bits 11 to 12        142160   .739  .7702
    DNA for prg610_1.rnd    using bits 10 to 11        141986   .226  .5895
    DNA for prg610_1.rnd    using bits  9 to 10        142465  1.639  .9494
    DNA for prg610_1.rnd    using bits  8 to  9        141494 -1.225  .1103
    DNA for prg610_1.rnd    using bits  7 to  8        141578  -.977  .1642
    DNA for prg610_1.rnd    using bits  6 to  7        142285  1.108  .8661
    DNA for prg610_1.rnd    using bits  5 to  6        141841  -.202  .4201
    DNA for prg610_1.rnd    using bits  4 to  5        142084   .515  .6968
    DNA for prg610_1.rnd    using bits  3 to  4        142078   .498  .6906
    DNA for prg610_1.rnd    using bits  2 to  3        141976   .197  .5780
    DNA for prg610_1.rnd    using bits  1 to  2        141862  -.140  .4445
------------------------------------------------------------------------------
  Test results for prg610_1.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 prg610_1.rnd     2565.60       .928      .823210
 byte stream for prg610_1.rnd     2538.78       .548      .708299
------------------------------------------------------------------------------
 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  2387.33     -1.593      .055538
          bits  2 to  9  2468.73      -.442      .329184
          bits  3 to 10  2595.23      1.347      .910975
          bits  4 to 11  2509.42       .133      .552985
          bits  5 to 12  2631.26      1.856      .968293
          bits  6 to 13  2499.30      -.010      .496076
          bits  7 to 14  2524.11       .341      .633459
          bits  8 to 15  2674.69      2.470      .993252
          bits  9 to 16  2557.52       .813      .792006
          bits 10 to 17  2449.14      -.719      .235980
          bits 11 to 18  2497.81      -.031      .487668
```

```
          bits 12 to 19  2588.20      1.247      .893874
          bits 13 to 20  2648.46      2.100      .982118
          bits 14 to 21  2502.84       .040      .516006
          bits 15 to 22  2673.46      2.453      .992919
          bits 16 to 23  2426.49     -1.040      .149275
          bits 17 to 24  2558.41       .826      .795607
          bits 18 to 25  2511.87       .168      .566636
          bits 19 to 26  2532.27       .456      .675914
          bits 20 to 27  2471.21      -.407      .341968
          bits 21 to 28  2393.70     -1.503      .066386
          bits 22 to 29  2479.41      -.291      .385478
          bits 23 to 30  2527.86       .394      .653205
          bits 24 to 31  2484.78      -.215      .414813
          bits 25 to 32  2505.58       .079      .531451
------------------------------------------------------------------------------
          CDPARK: result of ten tests on file prg610_1.rnd
           Of 12,000 tries, the average no. of successes
                should be 3523 with sigma=21.9
           Successes: 3507    z-score:  -.731 p-value: .232514
           Successes: 3519    z-score:  -.183 p-value: .427537
           Successes: 3546    z-score:  1.050 p-value: .853193
           Successes: 3516    z-score:  -.320 p-value: .374623
           Successes: 3524    z-score:   .046 p-value: .518210
           Successes: 3548    z-score:  1.142 p-value: .873180
           Successes: 3539    z-score:   .731 p-value: .767486
           Successes: 3527    z-score:   .183 p-value: .572463
           Successes: 3517    z-score:  -.274 p-value: .392053
           Successes: 3516    z-score:  -.320 p-value: .374623

          square size   avg. no.  parked   sample sigma
            100.           3525.900       13.221
           KSTEST for the above 10: p=  .484124
------------------------------------------------------------------------------
              This is the MINIMUM DISTANCE test
             for random integers in the file prg610_1.rnd
    Sample no.    d^2     avg     equiv uni
          5     .6922    .6689     .501274
         10    1.9020   1.0877     .852148
         15     .3343   1.4596     .285378
         20    1.4020   1.7599     .755619
         25    2.0414   1.6346     .871477
         30     .0343   1.6773     .033919
         35     .5739   1.5833     .438283
         40     .2072   1.5812     .187967
         45     .7880   1.5183     .547032
         50     .1928   1.4700     .176181
         55     .3982   1.4033     .329825
         60     .4667   1.3457     .374391
         65     .7136   1.2807     .511858
         70     .5073   1.2396     .399419
         75    1.4984   1.2662     .778186
         80     .0749   1.2227     .072525
         85     .1941   1.1764     .177227
         90     .6805   1.1693     .495386
         95     .1516   1.1631     .141304
        100    1.9769   1.1566     .862872
    MINIMUM DISTANCE TEST for prg610_1.rnd
         Result of KS test on 20 transformed mindist^2's:
                              p-value= .820567
------------------------------------------------------------------------------
              The 3DSPHERES test for file prg610_1.rnd
 sample no:  1     r^3=  27.294     p-value= .59740
 sample no:  2     r^3=  99.560     p-value= .96380
 sample no:  3     r^3=  21.667     p-value= .51433
 sample no:  4     r^3=   7.373     p-value= .21788
 sample no:  5     r^3=  17.415     p-value= .44038
 sample no:  6     r^3=  57.122     p-value= .85104
 sample no:  7     r^3=   4.503     p-value= .13939
```

```
 sample no:  8     r^3=   4.540     p-value= .14044
 sample no:  9     r^3= 102.213     p-value= .96686
 sample no: 10     r^3=   4.869     p-value= .14980
 sample no: 11     r^3=    .573     p-value= .01891
 sample no: 12     r^3=  92.582     p-value= .95432
 sample no: 13     r^3=  21.780     p-value= .51615
 sample no: 14     r^3=   3.747     p-value= .11743
 sample no: 15     r^3=  27.844     p-value= .60471
 sample no: 16     r^3=  55.075     p-value= .84052
 sample no: 17     r^3=  19.592     p-value= .47955
 sample no: 18     r^3=  38.296     p-value= .72099
 sample no: 19     r^3=  24.078     p-value= .55184
 sample no: 20     r^3=  47.386     p-value= .79393
       3DSPHERES test for file prg610_1.rnd         p-value= .239248
------------------------------------------------------------------------------
           RESULTS OF SQUEEZE TEST FOR prg610_1.rnd
         Table of standardized frequency counts
     ( (obs-exp)/sqrt(exp) )^2
        for j taking values <=6,7,8,...,47,>=48:
     -.1    -2.0     -.1     -.7     1.3      .9
      .7     3.1      .6     1.2     2.4     1.6
     -.4      .2     -.9    -2.1     -.5     -.5
    -1.2     1.0      .2      .9    -2.7     -.1
    -1.0      .2      .9     2.3      .5     -.7
     -.3     -.7     -.5     -.3     2.3      .4
     1.0    -1.3     1.3     1.0     -.6      .0
     1.8
           Chi-square with 42 degrees of freedom: 66.879
              z-score=  2.714  p-value= .991315
_____________________________________________________________
------------------------------------------------------------------------------
                Test no.  1      p-value  .685008
                Test no.  2      p-value  .989362
                Test no.  3      p-value  .100701
                Test no.  4      p-value  .197879
                Test no.  5      p-value  .952224
                Test no.  6      p-value  .086146
                Test no.  7      p-value  .801825
                Test no.  8      p-value  .636309
                Test no.  9      p-value  .219971
                Test no. 10      p-value  .373953
   Results of the OSUM test for prg610_1.rnd
        KSTEST on the above 10 p-values:  .282125
------------------------------------------------------------------------------
           The RUNS test for file prg610_1.rnd
     Up and down runs in a sample of 10000
_____________________________________________
                 Run test for prg610_1.rnd   :
       runs up; ks test for 10 p's: .979780
     runs down; ks test for 10 p's: .060795
                 Run test for prg610_1.rnd   :
       runs up; ks test for 10 p's: .764511
     runs down; ks test for 10 p's: .095280
------------------------------------------------------------------------------
                Results of craps test for prg610_1.rnd
  No. of wins:  Observed Expected
                               98502    98585.86
 Chisq=  17.70 for 20 degrees of freedom, p=  .39260
                Throws Observed Expected  Chisq     Sum
            SUMMARY  FOR prg610_1.rnd
                p-value for no. of wins: .353805
                p-value for throws/game: .392598
  Test completed.  File prg610_1.rnd
::::::::::::::::::::::::::::::::::::::::::::::::::::::::::::::::::::::::::::::
```