```
Basic statistical test of bit sequences
=======================================
Date/Time: 05.10.2016,12:49 hour

file: aes_p85.rnd  size:    10240000 Bytes

Test of null-hypothesis:
------------------------
Bit stream ist a stream of truly randomly
drawn number 0,1 with same probability p = 0.5

Non-overlapping byte count:

00      39820  39967  39879  39740  39963  39878  39707  40271
08      39779  39526  40253  40310  40125  40131  40156  40207
10      39958  39833  40087  39881  40132  40411  39809  39846
18      40004  40064  40257  40122  39781  39770  39920  39627
20      40138  39798  39886  39963  39998  39794  39517  39928
28      40100  40006  40107  40096  39918  39913  39953  40214
30      40129  39760  39806  39820  39929  39914  40132  40122
38      39992  39778  39706  39875  40001  40264  39931  40063
40      40068  40246  40021  40285  39871  39995  39770  39820
48      39976  39792  40134  39742  39925  40030  39810  39997
50      39860  40053  39643  39943  39750  40148  40344  40099
58      39949  40209  39839  39875  39925  40286  40052  39982
60      40015  40109  40027  40212  40110  39933  39852  40078
68      39511  40261  39935  40039  39831  40118  40125  39907
70      39950  40119  39860  39985  40234  40121  40151  40191
78      40311  39944  40242  40000  40297  40207  40238  40297
80      40130  40323  40393  39829  39890  39993  39892  40248
88      39962  39538  39823  40049  39542  40209  39682  39655
90      40061  40060  39880  40164  39905  39967  40134  39904
98      40201  40051  40321  40108  40096  40015  40112  40202
a0      39922  39975  40152  40074  40275  39901  39945  39974
a8      40047  39681  39728  40223  40002  39763  40038  40068
b0      39963  40296  39919  39862  39953  40275  40049  39971
b8      40156  39874  40199  39628  40375  39723  40033  40292
c0      40152  39893  39894  40172  39738  40044  39770  40296
c8      40088  40001  40123  39884  40055  40003  40014  40068
d0      39614  39989  40131  39816  39994  39811  39771  40060
d8      39975  39945  39767  40291  40076  39856  40088  40060
e0      40151  39664  40258  40319  39932  40004  40090  39818
e8      40176  40326  40095  39932  40332  39840  40057  40253
f0      39608  39826  40179  39662  40062  40069  40185  40027
f8      39890  40544  40100  39787  39788  39728  40194  39576

Evaluation of count of   10240000 Bytes =    81920000 Bits:

  Theoretical average of byte-frequencies: 40000
  '68' = 39511 (minimum)    'f9' = 40544 (maximum)

  Theoretical interval I of byte-frequencies:
  I = (39609 to 40391) (for 95 % of 256 frequency)

Test 1:
  The theoretical permissible number of the 5% outliers (average 13)
  from the interval I is between 6 and 20

  The real number of the outliers from interval I:
  smaller: 7  greater: 3  summary: 10

Test 2:
```

```
  Evaluation of byte-frequencies
  Chi-square non-overlapping:
  Theoretical maximum chi-square = 293.25
  Chi-square value               = 237.44

  Chi-square overlapping:
  Theoretical maximum chi-square = 155.40
  Chi-square value               = 132.14

Test 3:
  r = 0.50009418 (relative frequency of bit 1 in the bit stream)

  For a truly random sequence, the probability for r to have values in the
  complement of the open interval (0.49990582 , 0.50009418) is w = 0.08823992.
  If w is very small (e.g., w < 0.05), the null-hypothesis is rejected.
  If more sequences can be tested, the probability w has to be >= 0.05
  for about 95% of the tested bit sequences.

Test 4:
  Frequencies of overlapping 2-tuples:
  tuples 00:   20472824     tuples 01:   20479463
  tuples 10:   20479463     tuples 11:   20488250

  Check size: Chi-square of 2-bit patterns minus chi square of 1-bit patterns
  Theoretical maximum chi-square = 5.99
  Chi-square value               = 2.96

Test 5:
  Frequencies of 2-tuples on even places:
  tuples 00:   10234965     tuples 01:   10240863
  tuples 10:   10241494     tuples 11:   10242678

  Theoretical maximum chi-square = 7.81
  Chi-square value               = 3.47

Test 6:
  Frequencies of 2-tuples on odd places:
  tuples 00:   10237859     tuples 01:   10238600
  tuples 10:   10237969     tuples 11:   10245572

  Theoretical maximum chi-square = 7.81
  Chi-square value               = 4.07

Result of statistical analysis of file aes_p85.rnd:
================================================
The tests: 1 2 3 4 5 6  were fulfilled!

The null-hypothesis is accepted!
```

```
#################################################################
               THE NIST STATISTICAL TEST SUITE
#################################################################

---------------------------------------------------------------
  1.  FREQUENCY TEST
---------------------------------------------------------------
Computational information:
(a) The nth partial sum = 1400
(b) S_n/n               = 0.001400

p_value = 0.161513, SUCCESS

---------------------------------------------------------------
  2.  BLOCK FREQUENCY TEST
---------------------------------------------------------------
Computational information:
(a) Chi^2           = 124652.000000
(b) # of substrings = 125000
(c) block length    = 8

p_value = 0.756571, SUCCESS

---------------------------------------------------------------
  3.  CUMULATIVE SUMS TEST
---------------------------------------------------------------
Cumulative sums forward test:

Computational information:
(a) The maximum partial sum =

p_value = 0.269814, SUCCESS

Cumulative sums reverse test:

Computational information:
(a) The maximum partial sum =

p_value = 0.117784, SUCCESS

---------------------------------------------------------------
  4.  RUNS TEST
---------------------------------------------------------------
Computational information:
(a) Pi                         = 0.500700
(b) V_n_obs (Total # of runs) = 500495
(c) V_n_obs - 2 n pi (1-pi)
     ---------------------- = 0.701423
      2 sqrt(2n) pi (1-pi)

p_value = 0.321216, SUCCESS

---------------------------------------------------------------
  5.  LONGEST RUNS OF ONES TEST
---------------------------------------------------------------
Computational information:
(a) N (# of substrings)  = 100
(b) M (Substring Length) = 10000
(c) Chi^2                = 4.112291

Frequency
-------------------------------------------------
<=10     11     12     13     14     15    >=16
-------------------------------------------------
   8     23     30     18     13      4       4

p_value = 0.661483, 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 = 272
(e)             F_31 = 580
(f)             F_30 = 124
(g) # of matrices    = 976
(h) Chi^2            = 1.132059
(i) NOTE: 576 BITS WERE DISCARDED.

p_value = 0.567775, SUCCESS

------------------------------------------------------------
  7.  DFT TEST
------------------------------------------------------------
Computational information:
(a) Percentile = 95.024800
(b) N_l        = 475124.000000
(c) N_o        = 475000.000000
(d) d          = 0.804618

p_value = 0.421040, 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 126  133  119  130  115  112  115  131
chi2_value =  4.076739
p_value = 0.850134, 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
-----------------------------------------------
598  146   89   62   32   41    3.0192

p_value = 0.697025, SUCCESS

------------------------------------------------------------
 10.  UNIVERSAL TEST
------------------------------------------------------------
Computational information:
(a) L         = 7
(b) Q         = 1280
(c) K         = 141577
(d) sum       = 877641.604957
(e) sigma     = 0.002768
```

```
(f) variance  = 3.125000
(g) exp_value = 6.196251
(h) phi       = 6.199041
(i) WARNING:  1 bits were discarded.

p_value = 0.313531, SUCCESS

------------------------------------------------------------
 11.  APPROXIMATE ENTROPY TEST
------------------------------------------------------------
Computational information:
(a) m (block length)    = 5
(b) n (sequence length) = 1000000
(c) Chi^2               = 26.292179
(d) Phi(m)              = -3.465716
(e) Phi(m+1)            = -4.158850
(f) ApEn                = 0.693134
(g) Log(2)              = 0.693147

p_value = 0.750539, SUCCESS
------------------------------------------------------------
 12.  RANDOM EXCURSIONS TEST
------------------------------------------------------------
Computational information:
(a) Number Of Cycles (J) = 0691
(b) Sequence Length (n)  = 1000000
(c) Rejection Constraint = 500.000000

x = -4 chi^2 =  4.251865 p_value = 0.513752, SUCCESS
x = -3 chi^2 =  4.701177 p_value = 0.453426, SUCCESS
x = -2 chi^2 =  2.127155 p_value = 0.831286, SUCCESS
x = -1 chi^2 =  2.736614 p_value = 0.740513, SUCCESS
x =  1 chi^2 =  2.065123 p_value = 0.840063, SUCCESS
x =  2 chi^2 =  2.865538 p_value = 0.720707, SUCCESS
x =  3 chi^2 =  3.000588 p_value = 0.699895, SUCCESS
x =  4 chi^2 =  4.164839 p_value = 0.525936, SUCCESS

------------------------------------------------------------
 13.  RANDOM EXCURSIONS VARIANT TEST
------------------------------------------------------------
Computational information:
(a) Number Of Cycles (J) = 691
(b) Sequence Length (n)  = 1000000

(x = -9) Total visits =  467; p-value = 0.143905
 SUCCESS
(x = -8) Total visits =  463; p-value = 0.113293
 SUCCESS
(x = -7) Total visits =  502; p-value = 0.158523
 SUCCESS
(x = -6) Total visits =  551; p-value = 0.256176
 SUCCESS
(x = -5) Total visits =  568; p-value = 0.270078
 SUCCESS
(x = -4) Total visits =  589; p-value = 0.299715
 SUCCESS
(x = -3) Total visits =  614; p-value = 0.354290
 SUCCESS
(x = -2) Total visits =  630; p-value = 0.343455
 SUCCESS
(x = -1) Total visits =  663; p-value = 0.451336
 SUCCESS
(x =  1) Total visits =  664; p-value = 0.467661
 SUCCESS
(x =  2) Total visits =  613; p-value = 0.225750
 SUCCESS
(x =  3) Total visits =  598; p-value = 0.263235
 SUCCESS
(x =  4) Total visits =  632; p-value = 0.548600
```

```
 SUCCESS
(x =  5) Total visits =  684; p-value = 0.949953
 SUCCESS
(x =  6) Total visits =  698; p-value = 0.954725
 SUCCESS
(x =  7) Total visits =  674; p-value = 0.899075
 SUCCESS
(x =  8) Total visits =  679; p-value = 0.933577
 SUCCESS
(x =  9) Total visits =  688; p-value = 0.984385
 SUCCESS

---------------------------------------------------------------
 14.  SERIAL TEST
---------------------------------------------------------------
Computational information:
(a) Block length    (m) = 5
(b) Sequence length (n) = 1000000
(c) Psi_m               = 39.782976
(d) Psi_m-1             = 21.038400
(e) Psi_m-2             = 9.706848
(f) Del_1               = 18.744576
(g) Del_2               = 7.413024

p_value1 = 0.282131, SUCCESS
p_value2 = 0.492795, SUCCESS

---------------------------------------------------------------
 15.  LEMPEL-ZIV COMPRESSION TEST
---------------------------------------------------------------
Computational information:
(a) W (# of words) = 69595

p_value = 0.786509, SUCCESS
```

```
############################################################
                    Diehard Test-Suite
############################################################

BIRTHDAY SPACINGS TEST, M= 512 N=2**24 LAMBDA=  2.0000
          aes_p85.rnd    using bits  1 to 24 p-value=  .184818
          aes_p85.rnd    using bits  2 to 25 p-value=  .373843
          aes_p85.rnd    using bits  3 to 26 p-value=  .990343
          aes_p85.rnd    using bits  4 to 27 p-value=  .156810
          aes_p85.rnd    using bits  5 to 28 p-value=  .319564
          aes_p85.rnd    using bits  6 to 29 p-value=  .312137
          aes_p85.rnd    using bits  7 to 30 p-value=  .972692
          aes_p85.rnd    using bits  8 to 31 p-value=  .394578
          aes_p85.rnd    using bits  9 to 32 p-value=  .881670
   The 9 p-values were
        .184818   .373843   .990343   .156810   .319564
        .312137   .972692   .394578   .881670
  A KSTEST for the 9 p-values yields  .692794
------------------------------------------------------------------------------
          OPERM5 test for file aes_p85.rnd
 chisquare for 99 degrees of freedom= 94.099; p-value= .379498
          OPERM5 test for file aes_p85.rnd
 chisquare for 99 degrees of freedom=111.040; p-value= .807993
------------------------------------------------------------------------------
    Binary rank test for aes_p85.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       198     211.4   .851598     .852
        29      5095    5134.0   .296415    1.148
        30     23101   23103.0   .000181    1.148
        31     11606   11551.5   .256900    1.405
  chisquare= 1.405 for 3 d. of f.; p-value= .413596
    Binary rank test for aes_p85.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       215     211.4   .060688     .061
        30      5219    5134.0  1.406942    1.468
        31     23082   23103.0   .019174    1.487
        32     11484   11551.5   .394714    1.882
  chisquare= 1.882 for 3 d. of f.; p-value= .487723
------------------------------------------------------------------------------
 b-rank test for bits  1 to  8 p=1-exp(-SUM/2)= .53742
 b-rank test for bits  2 to  9 p=1-exp(-SUM/2)= .74779
 b-rank test for bits  3 to 10 p=1-exp(-SUM/2)= .39070
 b-rank test for bits  4 to 11 p=1-exp(-SUM/2)= .40859
 b-rank test for bits  5 to 12 p=1-exp(-SUM/2)= .26705
 b-rank test for bits  6 to 13 p=1-exp(-SUM/2)= .19311
 b-rank test for bits  7 to 14 p=1-exp(-SUM/2)= .38039
 b-rank test for bits  8 to 15 p=1-exp(-SUM/2)= .88026
 b-rank test for bits  9 to 16 p=1-exp(-SUM/2)= .55631
 b-rank test for bits 10 to 17 p=1-exp(-SUM/2)= .26774
 b-rank test for bits 11 to 18 p=1-exp(-SUM/2)= .10458
 b-rank test for bits 12 to 19 p=1-exp(-SUM/2)= .56117
 b-rank test for bits 13 to 20 p=1-exp(-SUM/2)= .22391
 b-rank test for bits 14 to 21 p=1-exp(-SUM/2)= .19092
 b-rank test for bits 15 to 22 p=1-exp(-SUM/2)= .33642
 b-rank test for bits 16 to 23 p=1-exp(-SUM/2)= .49980
 b-rank test for bits 17 to 24 p=1-exp(-SUM/2)= .15279
 b-rank test for bits 18 to 25 p=1-exp(-SUM/2)= .03556
 b-rank test for bits 19 to 26 p=1-exp(-SUM/2)= .14043
 b-rank test for bits 20 to 27 p=1-exp(-SUM/2)= .34797
 b-rank test for bits 21 to 28 p=1-exp(-SUM/2)= .15434
 b-rank test for bits 22 to 29 p=1-exp(-SUM/2)= .66075
 b-rank test for bits 23 to 30 p=1-exp(-SUM/2)= .83671
 b-rank test for bits 24 to 31 p=1-exp(-SUM/2)= .95981
```

```
 b-rank test for bits 25 to 32 p=1-exp(-SUM/2)= .17717
   TEST SUMMARY, 25 tests on 100,000 random 6x8 matrices
 These should be 25 uniform [0,1] random variables:
     .537418     .747789     .390702     .408587     .267045
     .193109     .380392     .880263     .556308     .267742
     .104579     .561172     .223910     .190916     .336415
     .499795     .152793     .035564     .140427     .347968
     .154344     .660747     .836714     .959808     .177175
   brank test summary for aes_p85.rnd
       The KS test for those 25 supposed UNI's yields
                  KS p-value= .893964
------------------------------------------------------------------------------
  No. missing words should average  141909. with sigma=428.
 tst no  1:  141825 missing words,    -.20 sigmas from mean, p-value= .42190
 tst no  2:  141269 missing words,   -1.50 sigmas from mean, p-value= .06731
 tst no  3:  142013 missing words,     .24 sigmas from mean, p-value= .59570
 tst no  4:  141967 missing words,     .13 sigmas from mean, p-value= .55359
 tst no  5:  141662 missing words,    -.58 sigmas from mean, p-value= .28168
 tst no  6:  141137 missing words,   -1.80 sigmas from mean, p-value= .03558
 tst no  7:  141266 missing words,   -1.50 sigmas from mean, p-value= .06641
 tst no  8:  142058 missing words,     .35 sigmas from mean, p-value= .63584
 tst no  9:  141998 missing words,     .21 sigmas from mean, p-value= .58206
 tst no 10:  141222 missing words,   -1.61 sigmas from mean, p-value= .05415
 tst no 11:  141779 missing words,    -.30 sigmas from mean, p-value= .38037
 tst no 12:  142546 missing words,    1.49 sigmas from mean, p-value= .93157
 tst no 13:  142432 missing words,    1.22 sigmas from mean, p-value= .88899
 tst no 14:  141403 missing words,   -1.18 sigmas from mean, p-value= .11840
 tst no 15:  142285 missing words,     .88 sigmas from mean, p-value= .80996
 tst no 16:  141865 missing words,    -.10 sigmas from mean, p-value= .45876
 tst no 17:  142303 missing words,     .92 sigmas from mean, p-value= .82116
 tst no 18:  141982 missing words,     .17 sigmas from mean, p-value= .56741
 tst no 19:  142244 missing words,     .78 sigmas from mean, p-value= .78288
 tst no 20:  141527 missing words,    -.89 sigmas from mean, p-value= .18585
------------------------------------------------------------------------------
    OPSO for aes_p85.rnd    using bits 23 to 32        142170   .899  .8156
    OPSO for aes_p85.rnd    using bits 22 to 31        141910   .002  .5009
    OPSO for aes_p85.rnd    using bits 21 to 30        141577 -1.146  .1259
    OPSO for aes_p85.rnd    using bits 20 to 29        142040   .451  .6739
    OPSO for aes_p85.rnd    using bits 19 to 28        142112   .699  .7577
    OPSO for aes_p85.rnd    using bits 18 to 27        141951   .144  .5571
    OPSO for aes_p85.rnd    using bits 17 to 26        141577 -1.146  .1259
    OPSO for aes_p85.rnd    using bits 16 to 25        142442  1.837  .9669
    OPSO for aes_p85.rnd    using bits 15 to 24        141852  -.198  .4216
    OPSO for aes_p85.rnd    using bits 14 to 23        141826  -.287  .3869
    OPSO for aes_p85.rnd    using bits 13 to 22        141924   .051  .5202
    OPSO for aes_p85.rnd    using bits 12 to 21        141883  -.091  .4638
    OPSO for aes_p85.rnd    using bits 11 to 20        141741  -.580  .2808
    OPSO for aes_p85.rnd    using bits 10 to 19        142000   .313  .6227
    OPSO for aes_p85.rnd    using bits  9 to 18        141674  -.811  .2085
    OPSO for aes_p85.rnd    using bits  8 to 17        141874  -.122  .4515
    OPSO for aes_p85.rnd    using bits  7 to 16        141788  -.418  .3378
    OPSO for aes_p85.rnd    using bits  6 to 15        141779  -.449  .3266
    OPSO for aes_p85.rnd    using bits  5 to 14        141864  -.156  .4379
    OPSO for aes_p85.rnd    using bits  4 to 13        142248  1.168  .8786
    OPSO for aes_p85.rnd    using bits  3 to 12        141555 -1.222  .1109
    OPSO for aes_p85.rnd    using bits  2 to 11        141751  -.546  .2925
    OPSO for aes_p85.rnd    using bits  1 to 10        142088   .616  .7311
    OQSO for aes_p85.rnd    using bits 28 to 32        142066   .531  .7023
    OQSO for aes_p85.rnd    using bits 27 to 31        142179   .914  .8197
    OQSO for aes_p85.rnd    using bits 26 to 30        141849  -.205  .4190
    OQSO for aes_p85.rnd    using bits 25 to 29        141973   .216  .5854
    OQSO for aes_p85.rnd    using bits 24 to 28        141900  -.032  .4874
    OQSO for aes_p85.rnd    using bits 23 to 27        141906  -.011  .4955
    OQSO for aes_p85.rnd    using bits 22 to 26        142109   .677  .7508
    OQSO for aes_p85.rnd    using bits 21 to 25        141854  -.188  .4256
    OQSO for aes_p85.rnd    using bits 20 to 24        142058   .504  .6929
    OQSO for aes_p85.rnd    using bits 19 to 23        141872  -.127  .4497
    OQSO for aes_p85.rnd    using bits 18 to 22        141614 -1.001  .1584
    OQSO for aes_p85.rnd    using bits 17 to 21        141700  -.710  .2390
```

```
   OQSO for aes_p85.rnd    using bits 16 to 20        142103   .657  .7443
   OQSO for aes_p85.rnd    using bits 15 to 19        141389 -1.764  .0389
   OQSO for aes_p85.rnd    using bits 14 to 18        141766  -.486  .3135
   OQSO for aes_p85.rnd    using bits 13 to 17        141870  -.133  .4470
   OQSO for aes_p85.rnd    using bits 12 to 16        141804  -.357  .3605
   OQSO for aes_p85.rnd    using bits 11 to 15        142086   .599  .7254
   OQSO for aes_p85.rnd    using bits 10 to 14        141989   .270  .6064
   OQSO for aes_p85.rnd    using bits  9 to 13        141965   .189  .5748
   OQSO for aes_p85.rnd    using bits  8 to 12        141784  -.425  .3355
   OQSO for aes_p85.rnd    using bits  7 to 11        141835  -.252  .4005
   OQSO for aes_p85.rnd    using bits  6 to 10        141845  -.218  .4137
   OQSO for aes_p85.rnd    using bits  5 to  9        142167   .873  .8088
   OQSO for aes_p85.rnd    using bits  4 to  8        141370 -1.828  .0338
   OQSO for aes_p85.rnd    using bits  3 to  7        141723  -.632  .2638
   OQSO for aes_p85.rnd    using bits  2 to  6        141970   .206  .5815
   OQSO for aes_p85.rnd    using bits  1 to  5        142328  1.419  .9221
    DNA for aes_p85.rnd    using bits 31 to 32        141884  -.075  .4702
    DNA for aes_p85.rnd    using bits 30 to 31        141336 -1.691  .0454
    DNA for aes_p85.rnd    using bits 29 to 30        142810  2.657  .9961
    DNA for aes_p85.rnd    using bits 28 to 29        142398  1.442  .9253
    DNA for aes_p85.rnd    using bits 27 to 28        141844  -.193  .4236
    DNA for aes_p85.rnd    using bits 26 to 27        141279 -1.859  .0315
    DNA for aes_p85.rnd    using bits 25 to 26        141914   .014  .5055
    DNA for aes_p85.rnd    using bits 24 to 25        141542 -1.084  .1393
    DNA for aes_p85.rnd    using bits 23 to 24        141817  -.272  .3927
    DNA for aes_p85.rnd    using bits 22 to 23        141656  -.747  .2274
    DNA for aes_p85.rnd    using bits 21 to 22        141717  -.567  .2852
    DNA for aes_p85.rnd    using bits 20 to 21        142302  1.158  .8766
    DNA for aes_p85.rnd    using bits 19 to 20        141351 -1.647  .0498
    DNA for aes_p85.rnd    using bits 18 to 19        141647  -.774  .2195
    DNA for aes_p85.rnd    using bits 17 to 18        141609  -.886  .1878
    DNA for aes_p85.rnd    using bits 16 to 17        141853  -.166  .4340
    DNA for aes_p85.rnd    using bits 15 to 16        141962   .155  .5617
    DNA for aes_p85.rnd    using bits 14 to 15        141588  -.948  .1716
    DNA for aes_p85.rnd    using bits 13 to 14        142202   .863  .8060
    DNA for aes_p85.rnd    using bits 12 to 13        141911   .005  .5020
    DNA for aes_p85.rnd    using bits 11 to 12        142636  2.144  .9840
    DNA for aes_p85.rnd    using bits 10 to 11        141444 -1.373  .0849
    DNA for aes_p85.rnd    using bits  9 to 10        141545 -1.075  .1413
    DNA for aes_p85.rnd    using bits  8 to  9        141855  -.160  .4363
    DNA for aes_p85.rnd    using bits  7 to  8        141643  -.786  .2160
    DNA for aes_p85.rnd    using bits  6 to  7        142060   .444  .6716
    DNA for aes_p85.rnd    using bits  5 to  6        141595  -.927  .1769
    DNA for aes_p85.rnd    using bits  4 to  5        141867  -.125  .4503
    DNA for aes_p85.rnd    using bits  3 to  4        141126 -2.311  .0104
    DNA for aes_p85.rnd    using bits  2 to  3        142106   .580  .7191
    DNA for aes_p85.rnd    using bits  1 to  2        141434 -1.402  .0804
------------------------------------------------------------------------------
  Test results for aes_p85.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 aes_p85.rnd     2614.81      1.624      .947779
 byte stream for aes_p85.rnd     2543.88       .621      .732571
------------------------------------------------------------------------------
 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  2519.78       .280      .610145
           bits  2 to  9  2565.42       .925      .822575
           bits  3 to 10  2357.25     -2.019      .021758
           bits  4 to 11  2453.48      -.658      .255292
           bits  5 to 12  2481.45      -.262      .396545
           bits  6 to 13  2519.35       .274      .607842
           bits  7 to 14  2438.80      -.866      .193378
           bits  8 to 15  2512.22       .173      .568613
           bits  9 to 16  2442.54      -.813      .208213
           bits 10 to 17  2604.06      1.472      .929439
           bits 11 to 18  2491.03      -.127      .449550
```

```
          bits 12 to 19  2454.65      -.641      .260647
          bits 13 to 20  2505.45       .077      .530711
          bits 14 to 21  2386.66     -1.603      .054488
          bits 15 to 22  2550.87       .719      .764037
          bits 16 to 23  2435.61      -.911      .181242
          bits 17 to 24  2598.83      1.398      .918889
          bits 18 to 25  2555.48       .785      .783667
          bits 19 to 26  2558.18       .823      .794700
          bits 20 to 27  2466.75      -.470      .319083
          bits 21 to 28  2527.19       .385      .649699
          bits 22 to 29  2470.55      -.417      .338521
          bits 23 to 30  2471.09      -.409      .341308
          bits 24 to 31  2594.29      1.333      .908801
          bits 25 to 32  2507.21       .102      .540621
------------------------------------------------------------------------------
          CDPARK: result of ten tests on file aes_p85.rnd
           Of 12,000 tries, the average no. of successes
                should be 3523 with sigma=21.9
           Successes: 3523    z-score:   .000 p-value: .500000
           Successes: 3522    z-score:  -.046 p-value: .481790
           Successes: 3490    z-score: -1.507 p-value: .065925
           Successes: 3545    z-score:  1.005 p-value: .842447
           Successes: 3523    z-score:   .000 p-value: .500000
           Successes: 3484    z-score: -1.781 p-value: .037471
           Successes: 3522    z-score:  -.046 p-value: .481790
           Successes: 3540    z-score:   .776 p-value: .781201
           Successes: 3527    z-score:   .183 p-value: .572463
           Successes: 3504    z-score:  -.868 p-value: .192812

          square size   avg. no.  parked   sample sigma
            100.           3518.000       18.740
           KSTEST for the above 10: p=  .392174
------------------------------------------------------------------------------
              This is the MINIMUM DISTANCE test
             for random integers in the file aes_p85.rnd
    Sample no.    d^2     avg     equiv uni
           5    1.3759    .8709     .749126
          10    2.8634   1.2424     .943742
          15     .2300   1.2511     .206360
          20    1.0727   1.1668     .659771
          25    1.3207   1.1495     .734819
          30     .5914   1.2764     .448107
          35    2.2441   1.3055     .895169
          40     .1178   1.2519     .111625
          45     .2053   1.1609     .186470
          50     .3002   1.0706     .260437
          55    4.1528   1.0877     .984604
          60     .1136   1.0509     .107890
          65     .6448   1.0278     .476938
          70     .3175   1.0046     .273167
          75     .1823    .9871     .167452
          80     .0251    .9983     .024875
          85    1.4869    .9957     .775607
          90     .2717    .9982     .238950
          95     .8655   1.0213     .580967
         100     .3532   1.0149     .298833
    MINIMUM DISTANCE TEST for aes_p85.rnd
         Result of KS test on 20 transformed mindist^2's:
                                  p-value= .050270
------------------------------------------------------------------------------
              The 3DSPHERES test for file aes_p85.rnd
 sample no:  1     r^3=  45.841     p-value= .78304
 sample no:  2     r^3=   2.621     p-value= .08367
 sample no:  3     r^3=  33.526     p-value= .67292
 sample no:  4     r^3=  96.547     p-value= .95997
 sample no:  5     r^3=  22.471     p-value= .52718
 sample no:  6     r^3=   2.401     p-value= .07692
 sample no:  7     r^3=  19.159     p-value= .47199
 sample no:  8     r^3=   4.665     p-value= .14402
```

```
 sample no:  9     r^3=   5.509     p-value= .16777
 sample no: 10     r^3=  38.158     p-value= .71971
 sample no: 11     r^3=  14.856     p-value= .39054
 sample no: 12     r^3=   7.159     p-value= .21228
 sample no: 13     r^3=  69.861     p-value= .90258
 sample no: 14     r^3=  47.515     p-value= .79481
 sample no: 15     r^3=   9.272     p-value= .26587
 sample no: 16     r^3=  19.433     p-value= .47679
 sample no: 17     r^3=  17.556     p-value= .44300
 sample no: 18     r^3=  22.286     p-value= .52425
 sample no: 19     r^3=  51.953     p-value= .82303
 sample no: 20     r^3=   8.499     p-value= .24671
       3DSPHERES test for file aes_p85.rnd        p-value= .016734
------------------------------------------------------------------------------
            RESULTS OF SQUEEZE TEST FOR aes_p85.rnd
          Table of standardized frequency counts
     ( (obs-exp)/sqrt(exp) )^2
        for j taking values <=6,7,8,...,47,>=48:
     -.8      .5     -.6     -.4      .5     1.8
     -.5     1.1     1.4      .6     -.6    -1.2
     2.1     -.8     1.3    -1.3      .2     -.6
    -1.5    -1.2     1.2     -.8     -.4     1.9
    -1.9     1.0     1.7      .1     -.1     1.8
    -1.2     2.4      .6     -.6    -2.3     -.5
     1.0    -1.0      .5    -1.3      .9      .0
     -.1
           Chi-square with 42 degrees of freedom: 56.726
              z-score=  1.607  p-value= .935923
_____________________________________________________________
------------------------------------------------------------------------------
                Test no.  1      p-value  .117384
                Test no.  2      p-value  .053421
                Test no.  3      p-value  .104882
                Test no.  4      p-value  .098179
                Test no.  5      p-value  .432743
                Test no.  6      p-value  .697157
                Test no.  7      p-value  .089164
                Test no.  8      p-value  .322160
                Test no.  9      p-value  .556744
                Test no. 10      p-value  .343511
   Results of the OSUM test for aes_p85.rnd
        KSTEST on the above 10 p-values:  .979502
------------------------------------------------------------------------------
           The RUNS test for file aes_p85.rnd
     Up and down runs in a sample of 10000
_____________________________________________
                 Run test for aes_p85.rnd   :
       runs up; ks test for 10 p's: .181678
     runs down; ks test for 10 p's: .226470
                 Run test for aes_p85.rnd   :
       runs up; ks test for 10 p's: .438905
     runs down; ks test for 10 p's: .718690
------------------------------------------------------------------------------
                Results of craps test for aes_p85.rnd
  No. of wins:  Observed Expected
                              98929    98585.86
 Chisq=  27.89 for 20 degrees of freedom, p=  .88800
               Throws Observed Expected  Chisq     Sum
             SUMMARY  FOR aes_p85.rnd
                 p-value for no. of wins: .937574
                 p-value for throws/game: .888003
  Test completed.  File aes_p85.rnd
::::::::::::::::::::::::::::::::::::::::::::::::::::::::::::::::::::::::::::::
```