```
Basic statistical test of bit sequences
=======================================
Date/Time: 05.10.2016,14:50 hour

file:  aes_m20.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      39630  40061  39965  39997  40034  39802  39781  40265
08      40067  40018  39716  40255  40364  40323  39866  39990
10      40241  39746  40280  40005  40405  40150  39618  39797
18      40131  39979  39823  40381  39801  40027  39970  39912
20      40148  39727  39822  40186  39978  39755  40084  40082
28      39731  40056  40195  39876  40258  40040  40099  40049
30      40157  40341  39877  40209  39768  40058  40029  39881
38      40119  40088  40030  40395  40007  40197  39924  40124
40      39970  39847  40126  40401  39685  40081  39830  39934
48      39989  40393  39906  40364  39600  39897  39863  40249
50      40211  39806  39611  39875  40246  40061  39945  40004
58      39878  40275  39615  40008  40162  40139  40022  40205
60      40072  40021  39905  40033  39627  40130  40292  40244
68      40026  39701  40326  39864  39840  39863  40249  40227
70      40110  39866  39762  39954  39799  39914  40088  40063
78      40008  39981  40069  39697  39853  39913  39850  39828
80      40139  39807  39912  40080  39989  39800  39725  39906
88      40126  39727  39626  39915  39782  40103  40048  40457
90      39840  40238  39961  39882  39908  39772  40223  40389
98      40133  40055  40381  39737  40192  39476  40077  39862
a0      39888  39846  40076  39781  39879  39557  40345  40065
a8      39851  40099  39964  40327  40070  40040  40470  40130
b0      39779  40096  39961  40077  40021  39843  39971  39940
b8      39700  39771  40015  39972  39935  39929  40014  40048
c0      40027  40073  40214  40192  39846  39741  40171  39754
c8      39682  40130  39867  40246  40119  40270  40020  39892
d0      40295  40189  40029  39989  39757  40023  39981  39933
d8      40412  39876  40041  40163  39708  39882  40144  40028
e0      39967  39849  40164  39941  39906  39963  39870  39972
e8      40301  39797  40045  40215  39970  39693  39533  39800
f0      40147  39890  39961  40228  40390  40029  39835  39983
f8      39675  40037  39544  40465  39939  40211  40126  40069

Evaluation of count of   10240000 Bytes =    81920000 Bits:

  Theoretical average of byte-frequencies: 40000
  '9d' = 39476 (minimum)    'ae' = 40470 (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: 5  greater: 8  summary: 13

Test 2:
```

```
  Evaluation of byte-frequencies
  Chi-square non-overlapping:
  Theoretical maximum chi-square = 293.25
  Chi-square value               = 257.22

  Chi-square overlapping:
  Theoretical maximum chi-square = 155.40
  Chi-square value               = 129.96

Test 3:
  r = 0.50003904 (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 (0.49996096 , 0.50003904) is w = 0.47974133.
  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:   20477313     tuples 01:   20479492
  tuples 10:   20479491     tuples 11:   20483704

  Check size: Chi-square of 2-bit patterns minus chi square of 1-bit patterns
  Theoretical maximum chi-square = 5.99
  Chi-square value               = 0.55

Test 5:
  Frequencies of 2-tuples on even places:
  tuples 00:   10241113     tuples 01:   10236263
  tuples 10:   10238315     tuples 11:   10244309

  Theoretical maximum chi-square = 7.81
  Chi-square value               = 3.58

Test 6:
  Frequencies of 2-tuples on odd places:
  tuples 00:   10236200     tuples 01:   10243229
  tuples 10:   10241176     tuples 11:   10239395

  Theoretical maximum chi-square = 7.81
  Chi-square value               = 2.60

Result of statistical analysis of file  aes_m20.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 = -46
(b) S_n/n               = -0.000046

p_value = 0.963310, SUCCESS

----------------------------------------------------------------
  2.  BLOCK FREQUENCY TEST
----------------------------------------------------------------
Computational information:
(a) Chi^2           = 124674.500000
(b) # of substrings = 125000
(c) block length    = 8

p_value = 0.742229, SUCCESS

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

Computational information:
(a) The maximum partial sum =

p_value = 0.965807, SUCCESS

Cumulative sums reverse test:

Computational information:
(a) The maximum partial sum =

p_value = 0.956723, SUCCESS

----------------------------------------------------------------
  4.  RUNS TEST
----------------------------------------------------------------
Computational information:
(a) Pi                         = 0.499977
(b) V_n_obs (Total # of runs) = 500781
(c) V_n_obs - 2 n pi (1-pi)
     ---------------------- = 1.104502
      2 sqrt(2n) pi (1-pi)

p_value = 0.118287, SUCCESS

----------------------------------------------------------------
  5.  LONGEST RUNS OF ONES TEST
----------------------------------------------------------------
Computational information:
(a) N (# of substrings)  = 100
(b) M (Substring Length) = 10000
(c) Chi^2                = 9.372986

Frequency
-------------------------------------------------
<=10     11     12     13     14     15    >=16
-------------------------------------------------
  11     29     17     18      9      5      11

p_value = 0.153663, 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 = 296
(e)             F_31 = 553
(f)             F_30 = 127
(g) # of matrices    = 976
(h) Chi^2            = 1.003414
(i) NOTE: 576 BITS WERE DISCARDED.

p_value = 0.605496, SUCCESS

------------------------------------------------------------
  7.  DFT TEST
------------------------------------------------------------
Computational information:
(a) Percentile = 95.007400
(b) N_l        = 475037.000000
(c) N_o        = 475000.000000
(d) d          = 0.240088

p_value = 0.810262, 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 105  115  123  130  112  113  134  121

chi2_value =  6.108746
p_value = 0.635052, 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
-----------------------------------------------
611  140   85   43   39   50    5.6024

p_value = 0.346851, SUCCESS

------------------------------------------------------------
 10.  UNIVERSAL TEST
------------------------------------------------------------
Computational information:
(a) L         = 7
(b) Q         = 1280
(c) K         = 141577
(d) sum       = 877768.269411
(e) sigma     = 0.002768
```

```
(f) variance  = 3.125000
(g) exp_value = 6.196251
(h) phi       = 6.199936
(i) WARNING:  1 bits were discarded.

p_value = 0.183186, SUCCESS

---------------------------------------------------------------
 11.  APPROXIMATE ENTROPY TEST
---------------------------------------------------------------
Computational information:
(a) m (block length)    = 5
(b) n (sequence length) = 1000000
(c) Chi^2               = 30.019959
(d) Phi(m)              = -3.465720
(e) Phi(m+1)            = -4.158852
(f) ApEn                = 0.693132
(g) Log(2)              = 0.693147

p_value = 0.567067, SUCCESS

---------------------------------------------------------------
 12.  RANDOM EXCURSIONS TEST
---------------------------------------------------------------
Computational information:
(a) Number Of Cycles (J) = 1971
(b) Sequence Length (n)  = 1000000
(c) Rejection Constraint = 500.000000

x = -4 chi^2 =  6.038786 p_value = 0.302463, SUCCESS
x = -3 chi^2 =  7.239557 p_value = 0.203425, SUCCESS
x = -2 chi^2 =  1.899562 p_value = 0.862861, SUCCESS
x = -1 chi^2 =  8.759513 p_value = 0.119049, SUCCESS
x =  1 chi^2 =  4.858955 p_value = 0.433335, SUCCESS
x =  2 chi^2 = 11.551616 p_value = 0.041476, SUCCESS
x =  3 chi^2 =  5.187100 p_value = 0.393476, SUCCESS
x =  4 chi^2 =  7.956473 p_value = 0.158651, SUCCESS

---------------------------------------------------------------
 13.  RANDOM EXCURSIONS VARIANT TEST
---------------------------------------------------------------
Computational information:
(a) Number Of Cycles (J) = 1971
(b) Sequence Length (n)  = 1000000

(x = -9) Total visits = 1716; p-value = 0.324600
 SUCCESS
(x = -8) Total visits = 1796; p-value = 0.471727
 SUCCESS
(x = -7) Total visits = 1857; p-value = 0.614551
 SUCCESS
(x = -6) Total visits = 1955; p-value = 0.938754
 SUCCESS
(x = -5) Total visits = 1993; p-value = 0.907018
 SUCCESS
(x = -4) Total visits = 1971; p-value = 1.000000
 SUCCESS
(x = -3) Total visits = 2004; p-value = 0.814166
 SUCCESS
(x = -2) Total visits = 1974; p-value = 0.977992
 SUCCESS
(x = -1) Total visits = 1902; p-value = 0.271776
 SUCCESS
(x =  1) Total visits = 2043; p-value = 0.251479
 SUCCESS
(x =  2) Total visits = 2009; p-value = 0.726764
 SUCCESS
(x =  3) Total visits = 2010; p-value = 0.781171
 SUCCESS
```

```
(x =  4) Total visits = 2068; p-value = 0.559264
 SUCCESS
(x =  5) Total visits = 2100; p-value = 0.493424
 SUCCESS
(x =  6) Total visits = 2132; p-value = 0.439426
 SUCCESS
(x =  7) Total visits = 2083; p-value = 0.620775
 SUCCESS
(x =  8) Total visits = 2069; p-value = 0.686937
 SUCCESS
(x =  9) Total visits = 2104; p-value = 0.607413
 SUCCESS

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

Computational information:
(a) Block length    (m) = 5
(b) Sequence length (n) = 1000000
(c) Psi_m               = 31.831808
(d) Psi_m-1             = 15.324224
(e) Psi_m-2             = 6.194176
(f) Del_1               = 16.507584
(g) Del_2               = 7.377536

p_value1 = 0.418131, SUCCESS
p_value2 = 0.496500, SUCCESS

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

Computational information:
(a) W (# of words) = 69576

p_value = 0.076962, SUCCESS
```

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

BIRTHDAY SPACINGS TEST, M= 512 N=2**24 LAMBDA=  2.0000
           aes_m20.rnd     using bits  1 to 24 p-value=  .845584
           aes_m20.rnd     using bits  2 to 25 p-value=  .920963
           aes_m20.rnd     using bits  3 to 26 p-value=  .493935
           aes_m20.rnd     using bits  4 to 27 p-value=  .187911
           aes_m20.rnd     using bits  5 to 28 p-value=  .123604
           aes_m20.rnd     using bits  6 to 29 p-value=  .958876
           aes_m20.rnd     using bits  7 to 30 p-value=  .866952
           aes_m20.rnd     using bits  8 to 31 p-value=  .633801
           aes_m20.rnd     using bits  9 to 32 p-value=  .874244
   The 9 p-values were
        .845584   .920963   .493935   .187911   .123604
        .958876   .866952   .633801   .874244
  A KSTEST for the 9 p-values yields  .894053
------------------------------------------------------------------------------
           OPERM5 test for file aes_m20.rnd
 chisquare for 99 degrees of freedom= 96.333; p-value= .442805
           OPERM5 test for file aes_m20.rnd
 chisquare for 99 degrees of freedom= 87.692; p-value= .215063
------------------------------------------------------------------------------
    Binary rank test for aes_m20.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       200     211.4   .616651     .617
        29      5154    5134.0   .077832     .694
        30     23086   23103.0   .012578     .707
        31     11560   11551.5   .006219     .713
  chisquare=  .713 for 3 d. of f.; p-value= .329103
    Binary rank test for aes_m20.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       221     211.4   .434279     .434
        30      5221    5134.0  1.473939    1.908
        31     23042   23103.0   .161309    2.070
        32     11516   11551.5   .109248    2.179
  chisquare= 2.179 for 3 d. of f.; p-value= .533822
------------------------------------------------------------------------------
 b-rank test for bits  1 to  8 p=1-exp(-SUM/2)= .88909
 b-rank test for bits  2 to  9 p=1-exp(-SUM/2)= .74950
 b-rank test for bits  3 to 10 p=1-exp(-SUM/2)= .88463
 b-rank test for bits  4 to 11 p=1-exp(-SUM/2)= .58049
 b-rank test for bits  5 to 12 p=1-exp(-SUM/2)= .19404
 b-rank test for bits  6 to 13 p=1-exp(-SUM/2)= .31219
 b-rank test for bits  7 to 14 p=1-exp(-SUM/2)= .60232
 b-rank test for bits  8 to 15 p=1-exp(-SUM/2)= .17110
 b-rank test for bits  9 to 16 p=1-exp(-SUM/2)= .52613
 b-rank test for bits 10 to 17 p=1-exp(-SUM/2)= .84371
 b-rank test for bits 11 to 18 p=1-exp(-SUM/2)= .61291
 b-rank test for bits 12 to 19 p=1-exp(-SUM/2)= .85753
 b-rank test for bits 13 to 20 p=1-exp(-SUM/2)= .94537
 b-rank test for bits 14 to 21 p=1-exp(-SUM/2)= .14827
 b-rank test for bits 15 to 22 p=1-exp(-SUM/2)= .97174
 b-rank test for bits 16 to 23 p=1-exp(-SUM/2)= .45829
 b-rank test for bits 17 to 24 p=1-exp(-SUM/2)= .86116
 b-rank test for bits 18 to 25 p=1-exp(-SUM/2)= .11578
 b-rank test for bits 19 to 26 p=1-exp(-SUM/2)= .74119
 b-rank test for bits 20 to 27 p=1-exp(-SUM/2)= .39538
 b-rank test for bits 21 to 28 p=1-exp(-SUM/2)= .77150
 b-rank test for bits 22 to 29 p=1-exp(-SUM/2)= .01353
 b-rank test for bits 23 to 30 p=1-exp(-SUM/2)= .78747
 b-rank test for bits 24 to 31 p=1-exp(-SUM/2)= .20470
 b-rank test for bits 25 to 32 p=1-exp(-SUM/2)= .85194
   TEST SUMMARY, 25 tests on 100,000 random 6x8 matrices
```

```
 These should be 25 uniform [0,1] random variables:
     .889093     .749497     .884631     .580485     .194042
     .312193     .602324     .171095     .526130     .843708
     .612908     .857530     .945369     .148273     .971736
     .458291     .861162     .115784     .741185     .395384
     .771499     .013533     .787470     .204696     .851936
   brank test summary for aes_m20.rnd
       The KS test for those 25 supposed UNI's yields
                  KS p-value= .782564
-------------------------------------------------------------------------------
  No. missing words should average  141909. with sigma=428.
 tst no  1:  142366 missing words,    1.07 sigmas from mean, p-value= .85701
 tst no  2:  141950 missing words,     .10 sigmas from mean, p-value= .53785
 tst no  3:  141531 missing words,    -.88 sigmas from mean, p-value= .18836
 tst no  4:  142143 missing words,     .55 sigmas from mean, p-value= .70745
 tst no  5:  141528 missing words,    -.89 sigmas from mean, p-value= .18648
 tst no  6:  141168 missing words,   -1.73 sigmas from mean, p-value= .04163
 tst no  7:  142630 missing words,    1.68 sigmas from mean, p-value= .95389
 tst no  8:  142351 missing words,    1.03 sigmas from mean, p-value= .84895
 tst no  9:  141777 missing words,    -.31 sigmas from mean, p-value= .37859
 tst no 10:  141804 missing words,    -.25 sigmas from mean, p-value= .40280
 tst no 11:  142130 missing words,     .52 sigmas from mean, p-value= .69693
 tst no 12:  142271 missing words,     .85 sigmas from mean, p-value= .80095
 tst no 13:  141937 missing words,     .06 sigmas from mean, p-value= .52578
 tst no 14:  142994 missing words,    2.53 sigmas from mean, p-value= .99437
 tst no 15:  142272 missing words,     .85 sigmas from mean, p-value= .80160
 tst no 16:  142728 missing words,    1.91 sigmas from mean, p-value= .97211
 tst no 17:  141956 missing words,     .11 sigmas from mean, p-value= .54342
 tst no 18:  141996 missing words,     .20 sigmas from mean, p-value= .58024
 tst no 19:  141783 missing words,    -.30 sigmas from mean, p-value= .38394
 tst no 20:  142421 missing words,    1.20 sigmas from mean, p-value= .88405
-------------------------------------------------------------------------------
    OPSO for aes_m20.rnd     using bits 23 to 32        142537  2.164  .9848
    OPSO for aes_m20.rnd     using bits 22 to 31        142086   .609  .7288
    OPSO for aes_m20.rnd     using bits 21 to 30        142130   .761  .7767
    OPSO for aes_m20.rnd     using bits 20 to 29        141713  -.677  .2492
    OPSO for aes_m20.rnd     using bits 19 to 28        141758  -.522  .3009
    OPSO for aes_m20.rnd     using bits 18 to 27        142117   .716  .7630
    OPSO for aes_m20.rnd     using bits 17 to 26        141940   .106  .5421
    OPSO for aes_m20.rnd     using bits 16 to 25        142389  1.654  .9509
    OPSO for aes_m20.rnd     using bits 15 to 24        141839  -.243  .4042
    OPSO for aes_m20.rnd     using bits 14 to 23        141698  -.729  .2331
    OPSO for aes_m20.rnd     using bits 13 to 22        142224  1.085  .8611
    OPSO for aes_m20.rnd     using bits 12 to 21        142044   .464  .6788
    OPSO for aes_m20.rnd     using bits 11 to 20        142403  1.702  .9557
    OPSO for aes_m20.rnd     using bits 10 to 19        141637  -.939  .1738
    OPSO for aes_m20.rnd     using bits  9 to 18        141795  -.394  .3467
    OPSO for aes_m20.rnd     using bits  8 to 17        142084   .602  .7265
    OPSO for aes_m20.rnd     using bits  7 to 16        142159   .861  .8054
    OPSO for aes_m20.rnd     using bits  6 to 15        142311  1.385  .9170
    OPSO for aes_m20.rnd     using bits  5 to 14        142204  1.016  .8452
    OPSO for aes_m20.rnd     using bits  4 to 13        141710  -.687  .2459
    OPSO for aes_m20.rnd     using bits  3 to 12        142051   .489  .6874
    OPSO for aes_m20.rnd     using bits  2 to 11        141531 -1.305  .0960
    OPSO for aes_m20.rnd     using bits  1 to 10        141502 -1.405  .0801
    OQSO for aes_m20.rnd     using bits 28 to 32        141894  -.052  .4793
    OQSO for aes_m20.rnd     using bits 27 to 31        142516  2.057  .9801
    OQSO for aes_m20.rnd     using bits 26 to 30        141853  -.191  .4243
    OQSO for aes_m20.rnd     using bits 25 to 29        141731  -.605  .2728
    OQSO for aes_m20.rnd     using bits 24 to 28        141529 -1.289  .0987
    OQSO for aes_m20.rnd     using bits 23 to 27        142061   .514  .6964
    OQSO for aes_m20.rnd     using bits 22 to 26        141753  -.530  .2981
    OQSO for aes_m20.rnd     using bits 21 to 25        141660  -.845  .1990
    OQSO for aes_m20.rnd     using bits 20 to 24        141762  -.499  .3087
    OQSO for aes_m20.rnd     using bits 19 to 23        142175   .901  .8161
    OQSO for aes_m20.rnd     using bits 18 to 22        142561  2.209  .9864
    OQSO for aes_m20.rnd     using bits 17 to 21        141832  -.262  .3966
    OQSO for aes_m20.rnd     using bits 16 to 20        142129   .745  .7718
    OQSO for aes_m20.rnd     using bits 15 to 19        141998   .301  .6181
```

```
   OQSO for aes_m20.rnd     using bits 14 to 18        141967   .195  .5775
   OQSO for aes_m20.rnd     using bits 13 to 17        142324  1.406  .9201
   OQSO for aes_m20.rnd     using bits 12 to 16        141846  -.215  .4150
   OQSO for aes_m20.rnd     using bits 11 to 15        141933   .080  .5320
   OQSO for aes_m20.rnd     using bits 10 to 14        141891  -.062  .4752
   OQSO for aes_m20.rnd     using bits  9 to 13        142182   .924  .8223
   OQSO for aes_m20.rnd     using bits  8 to 12        142053   .487  .6869
   OQSO for aes_m20.rnd     using bits  7 to 11        141680  -.777  .2185
   OQSO for aes_m20.rnd     using bits  6 to 10        141914   .016  .5063
   OQSO for aes_m20.rnd     using bits  5 to  9        141954   .151  .5602
   OQSO for aes_m20.rnd     using bits  4 to  8        141842  -.228  .4097
   OQSO for aes_m20.rnd     using bits  3 to  7        141706  -.689  .2453
   OQSO for aes_m20.rnd     using bits  2 to  6        141899  -.035  .4860
   OQSO for aes_m20.rnd     using bits  1 to  5        141711  -.672  .2507
    DNA for aes_m20.rnd     using bits 31 to 32        142412  1.483  .9309
    DNA for aes_m20.rnd     using bits 30 to 31        142261  1.037  .8502
    DNA for aes_m20.rnd     using bits 29 to 30        142206   .875  .8093
    DNA for aes_m20.rnd     using bits 28 to 29        141701  -.615  .2694
    DNA for aes_m20.rnd     using bits 27 to 28        142047   .406  .6577
    DNA for aes_m20.rnd     using bits 26 to 27        141724  -.547  .2923
    DNA for aes_m20.rnd     using bits 25 to 26        142069   .471  .6812
    DNA for aes_m20.rnd     using bits 24 to 25        142462  1.630  .9485
    DNA for aes_m20.rnd     using bits 23 to 24        142192   .834  .7978
    DNA for aes_m20.rnd     using bits 22 to 23        141944   .102  .5407
    DNA for aes_m20.rnd     using bits 21 to 22        142139   .677  .7510
    DNA for aes_m20.rnd     using bits 20 to 21        141974   .191  .5756
    DNA for aes_m20.rnd     using bits 19 to 20        142177   .790  .7851
    DNA for aes_m20.rnd     using bits 18 to 19        142093   .542  .7060
    DNA for aes_m20.rnd     using bits 17 to 18        141975   .194  .5768
    DNA for aes_m20.rnd     using bits 16 to 17        141741  -.497  .3098
    DNA for aes_m20.rnd     using bits 15 to 16        141297 -1.806  .0354
    DNA for aes_m20.rnd     using bits 14 to 15        141791  -.349  .3635
    DNA for aes_m20.rnd     using bits 13 to 14        141707  -.597  .2753
    DNA for aes_m20.rnd     using bits 12 to 13        141849  -.178  .4294
    DNA for aes_m20.rnd     using bits 11 to 12        142151   .713  .7620
    DNA for aes_m20.rnd     using bits 10 to 11        142203   .866  .8068
    DNA for aes_m20.rnd     using bits  9 to 10        142275  1.079  .8596
    DNA for aes_m20.rnd     using bits  8 to  9        141596  -.924  .1777
    DNA for aes_m20.rnd     using bits  7 to  8        142257  1.026  .8475
    DNA for aes_m20.rnd     using bits  6 to  7        141912   .008  .5031
    DNA for aes_m20.rnd     using bits  5 to  6        142049   .412  .6598
    DNA for aes_m20.rnd     using bits  4 to  5        141596  -.924  .1777
    DNA for aes_m20.rnd     using bits  3 to  4        142054   .427  .6652
    DNA for aes_m20.rnd     using bits  2 to  3        141437 -1.393  .0818
    DNA for aes_m20.rnd     using bits  1 to  2        142057   .436  .6684
------------------------------------------------------------------------------
   Test results for aes_m20.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_m20.rnd      2467.39      -.461      .322319
 byte stream for aes_m20.rnd      2502.02       .029      .511377
------------------------------------------------------------------------------
 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  2468.18      -.450      .326368
           bits  2 to  9  2437.22      -.888      .187325
           bits  3 to 10  2549.39       .698      .757554
           bits  4 to 11  2547.72       .675      .750121
           bits  5 to 12  2502.55       .036      .514365
           bits  6 to 13  2521.94       .310      .621800
           bits  7 to 14  2589.03      1.259      .895995
           bits  8 to 15  2323.86     -2.491      .006369
           bits  9 to 16  2434.36      -.928      .176612
           bits 10 to 17  2412.12     -1.243      .106972
           bits 11 to 18  2505.85       .083      .532941
           bits 12 to 19  2624.17      1.756      .960452
           bits 13 to 20  2570.16       .992      .839450
```

```
          bits 14 to 21  2465.54      -.487      .313025
          bits 15 to 22  2481.26      -.265      .395499
          bits 16 to 23  2664.50      2.326      .990001
          bits 17 to 24  2464.61      -.501      .308353
          bits 18 to 25  2479.44      -.291      .385592
          bits 19 to 26  2501.98       .028      .511190
          bits 20 to 27  2488.50      -.163      .435381
          bits 21 to 28  2554.03       .764      .777599
          bits 22 to 29  2488.17      -.167      .433540
          bits 23 to 30  2533.76       .477      .683459
          bits 24 to 31  2598.50      1.393      .918189
          bits 25 to 32  2699.45      2.821      .997604
------------------------------------------------------------------------------
          CDPARK: result of ten tests on file aes_m20.rnd
           Of 12,000 tries, the average no. of successes
                should be 3523 with sigma=21.9
           Successes: 3529    z-score:   .274 p-value: .607947
           Successes: 3528    z-score:   .228 p-value: .590298
           Successes: 3517    z-score:  -.274 p-value: .392053
           Successes: 3523    z-score:   .000 p-value: .500000
           Successes: 3495    z-score: -1.279 p-value: .100530
           Successes: 3475    z-score: -2.192 p-value: .014198
           Successes: 3544    z-score:   .959 p-value: .831196
           Successes: 3523    z-score:   .000 p-value: .500000
           Successes: 3524    z-score:   .046 p-value: .518210
           Successes: 3540    z-score:   .776 p-value: .781201

          square size   avg. no.  parked   sample sigma
            100.           3519.800       19.513
           KSTEST for the above 10: p=  .369809
------------------------------------------------------------------------------
              This is the MINIMUM DISTANCE test
             for random integers in the file aes_m20.rnd
    Sample no.    d^2     avg     equiv uni
          5    1.3470   1.2854     .741731
         10     .8570   1.1619     .577411
         15    2.8812   1.1463     .944738
         20     .0745   1.0384     .072122
         25     .1464   1.1532     .136820
         30     .2825   1.1678     .247202
         35    1.9932   1.1061     .865099
         40    1.5223   1.1136     .783452
         45    1.4143   1.1266     .758619
         50     .0314   1.1164     .031066
         55     .3162   1.0598     .272214
         60     .6691   1.0828     .489537
         65    1.8205   1.0579     .839532
         70     .1042   1.0240     .099444
         75    3.3312   1.0651     .964843
         80     .2005   1.0585     .182494
         85    1.2975   1.0530     .728566
         90     .2095   1.0132     .189877
         95     .1286   1.0098     .121224
        100     .0869    .9809     .083599
    MINIMUM DISTANCE TEST for aes_m20.rnd
         Result of KS test on 20 transformed mindist^2's:
                                  p-value= .099319
------------------------------------------------------------------------------
              The 3DSPHERES test for file aes_m20.rnd
 sample no:  1     r^3=   5.074     p-value= .15562
 sample no:  2     r^3=  10.341     p-value= .29156
 sample no:  3     r^3=  15.324     p-value= .39998
 sample no:  4     r^3=  13.190     p-value= .35576
 sample no:  5     r^3=  71.970     p-value= .90919
 sample no:  6     r^3=  28.122     p-value= .60835
 sample no:  7     r^3=   7.443     p-value= .21971
 sample no:  8     r^3=  47.007     p-value= .79131
 sample no:  9     r^3=  93.403     p-value= .95555
 sample no: 10     r^3=   2.898     p-value= .09208
```

```
 sample no: 11     r^3=  23.370     p-value= .54114
 sample no: 12     r^3= 103.652     p-value= .96841
 sample no: 13     r^3=  39.065     p-value= .72806
 sample no: 14     r^3=   6.389     p-value= .19183
 sample no: 15     r^3=  16.635     p-value= .42563
 sample no: 16     r^3=   4.197     p-value= .13057
 sample no: 17     r^3=  86.851     p-value= .94470
 sample no: 18     r^3=  16.905     p-value= .43078
 sample no: 19     r^3=  48.634     p-value= .80233
 sample no: 20     r^3=  31.041     p-value= .64466
       3DSPHERES test for file aes_m20.rnd          p-value= .135926
------------------------------------------------------------------------------
            RESULTS OF SQUEEZE TEST FOR aes_m20.rnd
          Table of standardized frequency counts
     ( (obs-exp)/sqrt(exp) )^2
        for j taking values <=6,7,8,...,47,>=48:
     -.1     -.3      .6     -.1     -.4    -1.3
    -1.3     -.2    -1.3     -.5     1.3     -.6
     -.4      .4      .9     1.1      .5      .0
      .4     -.1    -1.1    -1.1      .4     -.6
    -1.4     2.4     1.0     -.2     1.3      .4
    -2.1    -2.2      .1      .3     -.5    -1.7
     -.9    -1.0      .9     -.7     -.6    -1.0
    -1.1
           Chi-square with 42 degrees of freedom: 42.214
              z-score=   .023  p-value= .538242
_____________________________________________________________________
------------------------------------------------------------------------------
                Test no.  1      p-value  .148317
                Test no.  2      p-value  .544192
                Test no.  3      p-value  .789787
                Test no.  4      p-value  .445670
                Test no.  5      p-value  .101957
                Test no.  6      p-value  .933215
                Test no.  7      p-value  .090458
                Test no.  8      p-value  .571810
                Test no.  9      p-value  .826102
                Test no. 10      p-value  .688721
   Results of the OSUM test for aes_m20.rnd
        KSTEST on the above 10 p-values:  .056732
------------------------------------------------------------------------------
           The RUNS test for file aes_m20.rnd
     Up and down runs in a sample of 10000
_____________________________________________
                 Run test for aes_m20.rnd    :
       runs up; ks test for 10 p's: .744289
     runs down; ks test for 10 p's: .264294
                 Run test for aes_m20.rnd    :
       runs up; ks test for 10 p's: .465256
     runs down; ks test for 10 p's: .588151
------------------------------------------------------------------------------
                Results of craps test for aes_m20.rnd
  No. of wins:  Observed Expected
                               98556    98585.86
 Chisq=  16.53 for 20 degrees of freedom, p=  .31703
               Throws Observed Expected  Chisq     Sum
             SUMMARY  FOR aes_m20.rnd
                 p-value for no. of wins: .446880
                 p-value for throws/game: .317025
  Test completed.  File aes_m20.rnd
::::::::::::::::::::::::::::::::::::::::::::::::::::::::::::::::::::::::::::::
```