

```

BIRTHDAY SPACINGS TEST, M= 512 N=2**24 LAMBDA= 2.0000
  aes.rnd      using bits 1 to 24 p-value= .579693
  aes.rnd      using bits 2 to 25 p-value= .402942
  aes.rnd      using bits 3 to 26 p-value= .949239
  aes.rnd      using bits 4 to 27 p-value= .695333
  aes.rnd      using bits 5 to 28 p-value= .061102
  aes.rnd      using bits 6 to 29 p-value= .335062
  aes.rnd      using bits 7 to 30 p-value= .982575
  aes.rnd      using bits 8 to 31 p-value= .363990
  aes.rnd      using bits 9 to 32 p-value= .123880

```

```

The 9 p-values were
.579693 .402942 .949239 .695333 .061102
.335062 .982575 .363990 .123880

```

```

A KSTEST for the 9 p-values yields .147596

```

```

-----
OPERM5 test for file aes.rnd
chisquare for 99 degrees of freedom= 93.936; p-value= .374923
OPERM5 test for file aes.rnd
chisquare for 99 degrees of freedom= 92.596; p-value= .338015

```

```

-----
Binary rank test for aes.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	201	211.4	.513367	.513
29	5216	5134.0	1.309370	1.823
30	23079	23103.0	.025029	1.848
31	11504	11551.5	.195521	2.043

```

chisquare= 2.043 for 3 d. of f.; p-value= .512969

```

```

Binary rank test for aes.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	199	211.4	.729394	.729
30	5088	5134.0	.412337	1.142
31	23207	23103.0	.467741	1.609
32	11506	11551.5	.179411	1.789

```

chisquare= 1.789 for 3 d. of f.; p-value= .473175

```

```

-----
b-rank test for bits 1 to 8 p=1-exp(-SUM/2)= .26210
b-rank test for bits 2 to 9 p=1-exp(-SUM/2)= .73663
b-rank test for bits 3 to 10 p=1-exp(-SUM/2)= .92043
b-rank test for bits 4 to 11 p=1-exp(-SUM/2)= .94981
b-rank test for bits 5 to 12 p=1-exp(-SUM/2)= .00181
b-rank test for bits 6 to 13 p=1-exp(-SUM/2)= .70773
b-rank test for bits 7 to 14 p=1-exp(-SUM/2)= .00615
b-rank test for bits 8 to 15 p=1-exp(-SUM/2)= .19925
b-rank test for bits 9 to 16 p=1-exp(-SUM/2)= .02540
b-rank test for bits 10 to 17 p=1-exp(-SUM/2)= .55925
b-rank test for bits 11 to 18 p=1-exp(-SUM/2)= .56977
b-rank test for bits 12 to 19 p=1-exp(-SUM/2)= .71466
b-rank test for bits 13 to 20 p=1-exp(-SUM/2)= .54520
b-rank test for bits 14 to 21 p=1-exp(-SUM/2)= .46945
b-rank test for bits 15 to 22 p=1-exp(-SUM/2)= .16413
b-rank test for bits 16 to 23 p=1-exp(-SUM/2)= .66986
b-rank test for bits 17 to 24 p=1-exp(-SUM/2)= .04968
b-rank test for bits 18 to 25 p=1-exp(-SUM/2)= .48229
b-rank test for bits 19 to 26 p=1-exp(-SUM/2)= .18963
b-rank test for bits 20 to 27 p=1-exp(-SUM/2)= .15529
b-rank test for bits 21 to 28 p=1-exp(-SUM/2)= .70383
b-rank test for bits 22 to 29 p=1-exp(-SUM/2)= .02225
b-rank test for bits 23 to 30 p=1-exp(-SUM/2)= .60106
b-rank test for bits 24 to 31 p=1-exp(-SUM/2)= .79797
b-rank test for bits 25 to 32 p=1-exp(-SUM/2)= .72037

```

TEST SUMMARY, 25 tests on 100,000 random 6x8 matrices
 These should be 25 uniform [0,1] random variables:

.262100	.736634	.920426	.949806	.001810
.707729	.006146	.199249	.025400	.559249
.569767	.714664	.545196	.469447	.164133
.669857	.049676	.482288	.189630	.155290
.703828	.022254	.601063	.797974	.720366

brank test summary for aes.rnd

The KS test for those 25 supposed UNI's yields

KS p-value= .831689

No. missing words should average 141909. with sigma=428.

tst no 1:	142074 missing words,	.38 sigmas from mean,	p-value= .64979
tst no 2:	141664 missing words,	-.57 sigmas from mean,	p-value= .28326
tst no 3:	141553 missing words,	-.83 sigmas from mean,	p-value= .20255
tst no 4:	141954 missing words,	.10 sigmas from mean,	p-value= .54156
tst no 5:	142357 missing words,	1.05 sigmas from mean,	p-value= .85221
tst no 6:	141779 missing words,	-.30 sigmas from mean,	p-value= .38037
tst no 7:	141893 missing words,	-.04 sigmas from mean,	p-value= .48478
tst no 8:	141719 missing words,	-.44 sigmas from mean,	p-value= .32827
tst no 9:	142121 missing words,	.49 sigmas from mean,	p-value= .68954
tst no 10:	142358 missing words,	1.05 sigmas from mean,	p-value= .85275
tst no 11:	141593 missing words,	-.74 sigmas from mean,	p-value= .22993
tst no 12:	141542 missing words,	-.86 sigmas from mean,	p-value= .19538
tst no 13:	142491 missing words,	1.36 sigmas from mean,	p-value= .91293
tst no 14:	141731 missing words,	-.42 sigmas from mean,	p-value= .33847
tst no 15:	141588 missing words,	-.75 sigmas from mean,	p-value= .22640
tst no 16:	142026 missing words,	.27 sigmas from mean,	p-value= .60742
tst no 17:	141096 missing words,	-1.90 sigmas from mean,	p-value= .02870
tst no 18:	141518 missing words,	-.91 sigmas from mean,	p-value= .18027
tst no 19:	142322 missing words,	.96 sigmas from mean,	p-value= .83252
tst no 20:	141683 missing words,	-.53 sigmas from mean,	p-value= .29847

OPSO for aes.rnd	using bits 23 to 32	142123	.737	.7694
OPSO for aes.rnd	using bits 22 to 31	142126	.747	.7725
OPSO for aes.rnd	using bits 21 to 30	142134	.775	.7808
OPSO for aes.rnd	using bits 20 to 29	141392	-1.784	.0372
OPSO for aes.rnd	using bits 19 to 28	141964	.189	.5748
OPSO for aes.rnd	using bits 18 to 27	142040	.451	.6739
OPSO for aes.rnd	using bits 17 to 26	141855	-.187	.4257
OPSO for aes.rnd	using bits 16 to 25	141541	-1.270	.1020
OPSO for aes.rnd	using bits 15 to 24	141739	-.587	.2785
OPSO for aes.rnd	using bits 14 to 23	142125	.744	.7715
OPSO for aes.rnd	using bits 13 to 22	141937	.095	.5380
OPSO for aes.rnd	using bits 12 to 21	142131	.764	.7777
OPSO for aes.rnd	using bits 11 to 20	141791	-.408	.3416
OPSO for aes.rnd	using bits 10 to 19	142237	1.130	.8707
OPSO for aes.rnd	using bits 9 to 18	141465	-1.532	.0627
OPSO for aes.rnd	using bits 8 to 17	141421	-1.684	.0461
OPSO for aes.rnd	using bits 7 to 16	142061	.523	.6995
OPSO for aes.rnd	using bits 6 to 15	141889	-.070	.4721
OPSO for aes.rnd	using bits 5 to 14	141498	-1.418	.0780
OPSO for aes.rnd	using bits 4 to 13	141805	-.360	.3595
OPSO for aes.rnd	using bits 3 to 12	141903	-.022	.4913
OPSO for aes.rnd	using bits 2 to 11	142524	2.120	.9830
OPSO for aes.rnd	using bits 1 to 10	141810	-.343	.3660
OQSO for aes.rnd	using bits 28 to 32	141947	.128	.5508
OQSO for aes.rnd	using bits 27 to 31	141868	-.140	.4443
OQSO for aes.rnd	using bits 26 to 30	141909	-.001	.4996
OQSO for aes.rnd	using bits 25 to 29	142089	.609	.7288
OQSO for aes.rnd	using bits 24 to 28	141928	.063	.5252
OQSO for aes.rnd	using bits 23 to 27	142177	.907	.8179
OQSO for aes.rnd	using bits 22 to 26	141942	.111	.5441
OQSO for aes.rnd	using bits 21 to 25	142036	.429	.6662
OQSO for aes.rnd	using bits 20 to 24	142000	.307	.6207
OQSO for aes.rnd	using bits 19 to 23	142045	.460	.6772
OQSO for aes.rnd	using bits 18 to 22	141293	-2.089	.0183
OQSO for aes.rnd	using bits 17 to 21	141488	-1.428	.0766

QQSO for aes.rnd	using bits 16 to 20	141894	-.052	.4793
QQSO for aes.rnd	using bits 15 to 19	142337	1.450	.9264
QQSO for aes.rnd	using bits 14 to 18	141501	-1.384	.0832
QQSO for aes.rnd	using bits 13 to 17	141799	-.374	.3542
QQSO for aes.rnd	using bits 12 to 16	141963	.182	.5722
QQSO for aes.rnd	using bits 11 to 15	141715	-.659	.2550
QQSO for aes.rnd	using bits 10 to 14	141936	.090	.5360
QQSO for aes.rnd	using bits 9 to 13	141985	.257	.6012
QQSO for aes.rnd	using bits 8 to 12	141795	-.388	.3492
QQSO for aes.rnd	using bits 7 to 11	141802	-.364	.3580
QQSO for aes.rnd	using bits 6 to 10	142271	1.226	.8899
QQSO for aes.rnd	using bits 5 to 9	141488	-1.428	.0766
QQSO for aes.rnd	using bits 4 to 8	142387	1.619	.9473
QQSO for aes.rnd	using bits 3 to 7	142339	1.457	.9274
QQSO for aes.rnd	using bits 2 to 6	141748	-.547	.2922
QQSO for aes.rnd	using bits 1 to 5	142134	.762	.7769
DNA for aes.rnd	using bits 31 to 32	141790	-.352	.3624
DNA for aes.rnd	using bits 30 to 31	141580	-.971	.1657
DNA for aes.rnd	using bits 29 to 30	142045	.400	.6555
DNA for aes.rnd	using bits 28 to 29	142032	.362	.6413
DNA for aes.rnd	using bits 27 to 28	141962	.155	.5617
DNA for aes.rnd	using bits 26 to 27	141847	-.184	.4271
DNA for aes.rnd	using bits 25 to 26	142172	.775	.7808
DNA for aes.rnd	using bits 24 to 25	141508	-1.184	.1182
DNA for aes.rnd	using bits 23 to 24	142148	.704	.7593
DNA for aes.rnd	using bits 22 to 23	142196	.846	.8011
DNA for aes.rnd	using bits 21 to 22	141625	-.839	.2008
DNA for aes.rnd	using bits 20 to 21	141604	-.901	.1839
DNA for aes.rnd	using bits 19 to 20	141369	-1.594	.0555
DNA for aes.rnd	using bits 18 to 19	142055	.430	.6663
DNA for aes.rnd	using bits 17 to 18	141532	-1.113	.1328
DNA for aes.rnd	using bits 16 to 17	141549	-1.063	.1439
DNA for aes.rnd	using bits 15 to 16	141964	.161	.5641
DNA for aes.rnd	using bits 14 to 15	141774	-.399	.3449
DNA for aes.rnd	using bits 13 to 14	142361	1.332	.9086
DNA for aes.rnd	using bits 12 to 13	141895	-.042	.4831
DNA for aes.rnd	using bits 11 to 12	142227	.937	.8256
DNA for aes.rnd	using bits 10 to 11	141639	-.797	.2126
DNA for aes.rnd	using bits 9 to 10	142277	1.085	.8609
DNA for aes.rnd	using bits 8 to 9	142060	.444	.6716
DNA for aes.rnd	using bits 7 to 8	142200	.857	.8044
DNA for aes.rnd	using bits 6 to 7	141621	-.851	.1975
DNA for aes.rnd	using bits 5 to 6	141904	-.016	.4937
DNA for aes.rnd	using bits 4 to 5	141751	-.467	.3202
DNA for aes.rnd	using bits 3 to 4	141992	.244	.5963
DNA for aes.rnd	using bits 2 to 3	141877	-.095	.4620
DNA for aes.rnd	using bits 1 to 2	141859	-.148	.4410

Test results for aes.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.rnd	2535.85	.507	.693903
byte stream for aes.rnd	2491.52	-.120	.452274

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	2575.17	1.063	.856132
bits 2 to 9	2504.10	.058	.523097
bits 3 to 10	2445.76	-.767	.221503
bits 4 to 11	2492.36	-.108	.456979
bits 5 to 12	2547.35	.670	.748461
bits 6 to 13	2585.28	1.206	.886108
bits 7 to 14	2452.35	-.674	.250194
bits 8 to 15	2443.52	-.799	.212212
bits 9 to 16	2563.62	.900	.815848
bits 10 to 17	2533.07	.468	.680011

bits 11 to 18	2591.04	1.287	.901033
bits 12 to 19	2446.93	-.751	.226472
bits 13 to 20	2459.73	-.569	.284520
bits 14 to 21	2413.16	-1.228	.109705
bits 15 to 22	2483.09	-.239	.405491
bits 16 to 23	2478.16	-.309	.378732
bits 17 to 24	2262.15	-3.364	.000384
bits 18 to 25	2436.33	-.900	.183942
bits 19 to 26	2514.90	.211	.583423
bits 20 to 27	2485.33	-.207	.417811
bits 21 to 28	2609.30	1.546	.938915
bits 22 to 29	2394.06	-1.498	.067033
bits 23 to 30	2452.29	-.675	.249905
bits 24 to 31	2433.92	-.934	.175028
bits 25 to 32	2477.75	-.315	.376496

CDPARK: result of ten tests on file aes.rnd

Of 12,000 tries, the average no. of successes
should be 3523 with sigma=21.9

Successes: 3531	z-score: .365	p-value: .642555
Successes: 3552	z-score: 1.324	p-value: .907282
Successes: 3489	z-score: -1.553	p-value: .060270
Successes: 3517	z-score: -.274	p-value: .392053
Successes: 3526	z-score: .137	p-value: .554479
Successes: 3505	z-score: -.822	p-value: .205562
Successes: 3531	z-score: .365	p-value: .642555
Successes: 3581	z-score: 2.648	p-value: .995956
Successes: 3542	z-score: .868	p-value: .807188
Successes: 3524	z-score: .046	p-value: .518210

square size	avg. no. parked	sample sigma
100.	3529.800	23.999

KSTEST for the above 10: p= .350737

This is the MINIMUM DISTANCE test
for random integers in the file aes.rnd

Sample no.	d^2	avg	equiv uni
5	1.8629	1.0853	.846219
10	3.2153	1.0034	.960501
15	.6326	.9636	.470495
20	.6416	.8321	.475251
25	.3080	.7880	.266210
30	.0951	.7864	.091195
35	.7415	.7903	.525370
40	.5398	.8055	.418716
45	.3405	.8034	.289772
50	.6121	.7736	.459458
55	1.8345	.7979	.841768
60	2.3579	.7803	.906491
65	.0896	.7720	.086104
70	1.3878	.8280	.752118
75	.8295	.7982	.565565
80	.1902	.7724	.173960
85	.7393	.7803	.524340
90	.2206	.7859	.198813
95	.6176	.7758	.462422
100	.3191	.7710	.274368

MINIMUM DISTANCE TEST for aes.rnd

Result of KS test on 20 transformed mindist^2's:
p-value= .920520

The 3DSPHERES test for file aes.rnd

sample no: 1	r^3= 48.326	p-value= .80029
sample no: 2	r^3= 42.780	p-value= .75974
sample no: 3	r^3= 53.377	p-value= .83123
sample no: 4	r^3= 26.284	p-value= .58361
sample no: 5	r^3= 1.359	p-value= .04430
sample no: 6	r^3= 39.470	p-value= .73171

```

sample no: 7      r^3= 8.545      p-value= .24787
sample no: 8      r^3= 4.939      p-value= .15180
sample no: 9      r^3= 2.721      p-value= .08671
sample no: 10     r^3= 15.507     p-value= .40363
sample no: 11     r^3= 5.117      p-value= .15683
sample no: 12     r^3= .412       p-value= .01364
sample no: 13     r^3= 13.448     p-value= .36127
sample no: 14     r^3= 24.208     p-value= .55377
sample no: 15     r^3= 41.973     p-value= .75318
sample no: 16     r^3= 15.265     p-value= .39881
sample no: 17     r^3= 9.587      p-value= .27353
sample no: 18     r^3= 23.736     p-value= .54671
sample no: 19     r^3= 27.957     p-value= .60619
sample no: 20     r^3= 23.204     p-value= .53859

```

3DSPHERES test for file aes.rnd p-value= .478649

RESULTS OF SQUEEZE TEST FOR aes.rnd
Table of standardized frequency counts
((obs-exp)/sqrt(exp))^2

for j taking values <=6,7,8,...,47,>=48:

-.8	.1	2.0	-.3	.4	1.7
.4	-.9	-.6	1.1	-.2	-.2
-1.4	-1.4	2.2	.3	-.5	1.1
-.9	-.8	-.4	.1	2.1	.1
-1.6	.1	.4	1.6	-1.6	.0
-.1	-.2	.2	-.4	.3	.2
1.4	1.1	.1	-.1	-.6	-1.0
-1.1					

Chi-square with 42 degrees of freedom: 40.889
z-score= -.121 p-value= .480230

Test no. 1	p-value	.143713
Test no. 2	p-value	.169891
Test no. 3	p-value	.517660
Test no. 4	p-value	.490167
Test no. 5	p-value	.558415
Test no. 6	p-value	.588005
Test no. 7	p-value	.250006
Test no. 8	p-value	.631206
Test no. 9	p-value	.617305
Test no. 10	p-value	.793520

Results of the OSUM test for aes.rnd
KSTEST on the above 10 p-values: .520024

The RUNS test for file aes.rnd
Up and down runs in a sample of 10000

```

Run test for aes.rnd      :
runs up; ks test for 10 p's: .939894
runs down; ks test for 10 p's: .252441
Run test for aes.rnd      :
runs up; ks test for 10 p's: .640263
runs down; ks test for 10 p's: .893134

```

Results of craps test for aes.rnd

No. of wins:	Observed	Expected		
	98932	98585.86		

Chisq= 8.81 for 20 degrees of freedom, p= .01496

Throws	Observed	Expected	Chisq	Sum

SUMMARY FOR aes.rnd
p-value for no. of wins: .939206
p-value for throws/game: .014958

Test completed. File aes.rnd

::