

BIRTHDAY SPACINGS TEST, M= 512 N=2\*\*24 LAMBDA= 2.0000

aes_1.dat	using bits	1 to 24	p-value=	.391835
aes_1.dat	using bits	2 to 25	p-value=	.430808
aes_1.dat	using bits	3 to 26	p-value=	.647158
aes_1.dat	using bits	4 to 27	p-value=	.751409
aes_1.dat	using bits	5 to 28	p-value=	.332968
aes_1.dat	using bits	6 to 29	p-value=	.046950
aes_1.dat	using bits	7 to 30	p-value=	.290668
aes_1.dat	using bits	8 to 31	p-value=	.940532
aes_1.dat	using bits	9 to 32	p-value=	.569729

The 9 p-values were  
 .391835 .430808 .647158 .751409 .332968  
 .046950 .290668 .940532 .569729  
 A KSTEST for the 9 p-values yields .043370

---

OPERM5 test for file aes\_1.dat  
 chisquare for 99 degrees of freedom= 75.551; p-value= .038258  
 OPERM5 test for file aes\_1.dat  
 chisquare for 99 degrees of freedom= 69.043; p-value= .009595

---

Binary rank test for aes\_1.dat  
 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	172	211.4	7.349326	7.349
29	5192	5134.0	.655007	8.004
30	23028	23103.0	.243779	8.248
31	11608	11551.5	.276110	8.524

chisquare= 8.524 for 3 d. of f.; p-value= .965419

Binary rank test for aes\_1.dat  
 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	252	211.4	7.789769	7.790
30	5157	5134.0	.102947	7.893
31	23050	23103.0	.121801	8.015
32	11541	11551.5	.009589	8.024

chisquare= 8.024 for 3 d. of f.; p-value= .956792

---

b-rank test for bits 1 to 8 p=1-exp(-SUM/2)= .05414  
 b-rank test for bits 2 to 9 p=1-exp(-SUM/2)= .64158  
 b-rank test for bits 3 to 10 p=1-exp(-SUM/2)= .16014  
 b-rank test for bits 4 to 11 p=1-exp(-SUM/2)= .99717  
 b-rank test for bits 5 to 12 p=1-exp(-SUM/2)= .82128  
 b-rank test for bits 6 to 13 p=1-exp(-SUM/2)= .51305  
 b-rank test for bits 7 to 14 p=1-exp(-SUM/2)= .19219  
 b-rank test for bits 8 to 15 p=1-exp(-SUM/2)= .93230  
 b-rank test for bits 9 to 16 p=1-exp(-SUM/2)= .14529  
 b-rank test for bits 10 to 17 p=1-exp(-SUM/2)= .60174  
 b-rank test for bits 11 to 18 p=1-exp(-SUM/2)= .12093  
 b-rank test for bits 12 to 19 p=1-exp(-SUM/2)= .83358  
 b-rank test for bits 13 to 20 p=1-exp(-SUM/2)= .94933  
 b-rank test for bits 14 to 21 p=1-exp(-SUM/2)= .04003  
 b-rank test for bits 15 to 22 p=1-exp(-SUM/2)= .73263  
 b-rank test for bits 16 to 23 p=1-exp(-SUM/2)= .54176  
 b-rank test for bits 17 to 24 p=1-exp(-SUM/2)= .87555  
 b-rank test for bits 18 to 25 p=1-exp(-SUM/2)= .09449  
 b-rank test for bits 19 to 26 p=1-exp(-SUM/2)= .86063  
 b-rank test for bits 20 to 27 p=1-exp(-SUM/2)= .49616  
 b-rank test for bits 21 to 28 p=1-exp(-SUM/2)= .01175  
 b-rank test for bits 22 to 29 p=1-exp(-SUM/2)= .54347  
 b-rank test for bits 23 to 30 p=1-exp(-SUM/2)= .51844  
 b-rank test for bits 24 to 31 p=1-exp(-SUM/2)= .42886  
 b-rank test for bits 25 to 32 p=1-exp(-SUM/2)= .41052

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

.054141	.641577	.160136	.997167	.821282
.513052	.192191	.932305	.145286	.601743
.120930	.833583	.949330	.040027	.732632
.541761	.875554	.094488	.860629	.496163
.011754	.543466	.518443	.428856	.410516

brank test summary for aes\_1.dat

The KS test for those 25 supposed UNI's yields  
 KS p-value= .274724

---

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

tst no 1:	142272 missing words,	.85 sigmas from mean,	p-value= .80160
tst no 2:	142307 missing words,	.93 sigmas from mean,	p-value= .82359
tst no 3:	141916 missing words,	.02 sigmas from mean,	p-value= .50622
tst no 4:	142003 missing words,	.22 sigmas from mean,	p-value= .58662
tst no 5:	142231 missing words,	.75 sigmas from mean,	p-value= .77385
tst no 6:	142155 missing words,	.57 sigmas from mean,	p-value= .71702
tst no 7:	141657 missing words,	-.59 sigmas from mean,	p-value= .27775
tst no 8:	141912 missing words,	.01 sigmas from mean,	p-value= .50249
tst no 9:	141603 missing words,	-.72 sigmas from mean,	p-value= .23708
tst no 10:	141836 missing words,	-.17 sigmas from mean,	p-value= .43198
tst no 11:	141846 missing words,	-.15 sigmas from mean,	p-value= .44119
tst no 12:	142163 missing words,	.59 sigmas from mean,	p-value= .72331
tst no 13:	142173 missing words,	.62 sigmas from mean,	p-value= .73107
tst no 14:	141452 missing words,	-1.07 sigmas from mean,	p-value= .14264
tst no 15:	141940 missing words,	.07 sigmas from mean,	p-value= .52857
tst no 16:	141554 missing words,	-.83 sigmas from mean,	p-value= .20321
tst no 17:	141365 missing words,	-1.27 sigmas from mean,	p-value= .10172
tst no 18:	142033 missing words,	.29 sigmas from mean,	p-value= .61369
tst no 19:	142090 missing words,	.42 sigmas from mean,	p-value= .66354
tst no 20:	142508 missing words,	1.40 sigmas from mean,	p-value= .91906

---

OPSO for aes_1.dat	using bits 23 to 32	141987	.268	.6056
OPSO for aes_1.dat	using bits 22 to 31	142182	.940	.8265
OPSO for aes_1.dat	using bits 21 to 30	142203	1.013	.8444
OPSO for aes_1.dat	using bits 20 to 29	142136	.782	.7828
OPSO for aes_1.dat	using bits 19 to 28	142035	.433	.6676
OPSO for aes_1.dat	using bits 18 to 27	142293	1.323	.9071
OPSO for aes_1.dat	using bits 17 to 26	142288	1.306	.9042
OPSO for aes_1.dat	using bits 16 to 25	142064	.533	.7031
OPSO for aes_1.dat	using bits 15 to 24	142023	.392	.6525
OPSO for aes_1.dat	using bits 14 to 23	141739	-.587	.2785
OPSO for aes_1.dat	using bits 13 to 22	142058	.513	.6959
OPSO for aes_1.dat	using bits 12 to 21	141867	-.146	.4420
OPSO for aes_1.dat	using bits 11 to 20	142315	1.399	.9191
OPSO for aes_1.dat	using bits 10 to 19	142222	1.078	.8595
OPSO for aes_1.dat	using bits 9 to 18	141971	.213	.5842
OPSO for aes_1.dat	using bits 8 to 17	142339	1.482	.9308
OPSO for aes_1.dat	using bits 7 to 16	142145	.813	.7918
OPSO for aes_1.dat	using bits 6 to 15	142034	.430	.6664
OPSO for aes_1.dat	using bits 5 to 14	142013	.357	.6396
OPSO for aes_1.dat	using bits 4 to 13	142125	.744	.7715
OPSO for aes_1.dat	using bits 3 to 12	142328	1.444	.9256
OPSO for aes_1.dat	using bits 2 to 11	142295	1.330	.9082
OPSO for aes_1.dat	using bits 1 to 10	142174	.913	.8193
QOSO for aes_1.dat	using bits 28 to 32	142738	2.809	.9975
QOSO for aes_1.dat	using bits 27 to 31	141548	-1.225	.1103
QOSO for aes_1.dat	using bits 26 to 30	141866	-.147	.4416
QOSO for aes_1.dat	using bits 25 to 29	142286	1.277	.8992
QOSO for aes_1.dat	using bits 24 to 28	141686	-.757	.2245
QOSO for aes_1.dat	using bits 23 to 27	141708	-.682	.2475
QOSO for aes_1.dat	using bits 22 to 26	141748	-.547	.2922
QOSO for aes_1.dat	using bits 21 to 25	142063	.521	.6988

QOSO for aes_1.dat	using bits 20 to 24	141721	-.638	.2616
QOSO for aes_1.dat	using bits 19 to 23	142062	.518	.6976
QOSO for aes_1.dat	using bits 18 to 22	142392	1.636	.9491
QOSO for aes_1.dat	using bits 17 to 21	141846	-.215	.4150
QOSO for aes_1.dat	using bits 16 to 20	142444	1.812	.9650
QOSO for aes_1.dat	using bits 15 to 19	142505	2.019	.9783
QOSO for aes_1.dat	using bits 14 to 18	142026	.395	.6538
QOSO for aes_1.dat	using bits 13 to 17	142181	.921	.8215
QOSO for aes_1.dat	using bits 12 to 16	141503	-1.377	.0842
QOSO for aes_1.dat	using bits 11 to 15	141961	.175	.5695
QOSO for aes_1.dat	using bits 10 to 14	142585	2.290	.9890
QOSO for aes_1.dat	using bits 9 to 13	142025	.392	.6525
QOSO for aes_1.dat	using bits 8 to 12	142171	.887	.8125
QOSO for aes_1.dat	using bits 7 to 11	141804	-.357	.3605
QOSO for aes_1.dat	using bits 6 to 10	142422	1.738	.9589
QOSO for aes_1.dat	using bits 5 to 9	142011	.345	.6348
QOSO for aes_1.dat	using bits 4 to 8	142046	.463	.6784
QOSO for aes_1.dat	using bits 3 to 7	141366	-1.842	.0328
QOSO for aes_1.dat	using bits 2 to 6	141676	-.791	.2145
QOSO for aes_1.dat	using bits 1 to 5	141974	.219	.5868
DNA for aes_1.dat	using bits 31 to 32	142220	.916	.8203
DNA for aes_1.dat	using bits 30 to 31	142421	1.509	.9344
DNA for aes_1.dat	using bits 29 to 30	141263	-1.907	.0283
DNA for aes_1.dat	using bits 28 to 29	141797	-.331	.3702
DNA for aes_1.dat	using bits 27 to 28	141470	-1.296	.0975
DNA for aes_1.dat	using bits 26 to 27	141778	-.387	.3492
DNA for aes_1.dat	using bits 25 to 26	141779	-.384	.3503
DNA for aes_1.dat	using bits 24 to 25	141713	-.579	.2812
DNA for aes_1.dat	using bits 23 to 24	141784	-.370	.3558
DNA for aes_1.dat	using bits 22 to 23	141797	-.331	.3702
DNA for aes_1.dat	using bits 21 to 22	142237	.967	.8331
DNA for aes_1.dat	using bits 20 to 21	142282	1.099	.8642
DNA for aes_1.dat	using bits 19 to 20	141857	-.154	.4387
DNA for aes_1.dat	using bits 18 to 19	141608	-.889	.1870
DNA for aes_1.dat	using bits 17 to 18	141542	-1.084	.1393
DNA for aes_1.dat	using bits 16 to 17	142057	.436	.6684
DNA for aes_1.dat	using bits 15 to 16	141345	-1.665	.0480
DNA for aes_1.dat	using bits 14 to 15	142349	1.297	.9027
DNA for aes_1.dat	using bits 13 to 14	141674	-.694	.2438
DNA for aes_1.dat	using bits 12 to 13	141885	-.072	.4714
DNA for aes_1.dat	using bits 11 to 12	141929	.058	.5231
DNA for aes_1.dat	using bits 10 to 11	141885	-.072	.4714
DNA for aes_1.dat	using bits 9 to 10	141906	-.010	.4961
DNA for aes_1.dat	using bits 8 to 9	141825	-.249	.4018
DNA for aes_1.dat	using bits 7 to 8	142137	.672	.7491
DNA for aes_1.dat	using bits 6 to 7	142114	.604	.7270
DNA for aes_1.dat	using bits 5 to 6	141804	-.311	.3780
DNA for aes_1.dat	using bits 4 to 5	141511	-1.175	.1200
DNA for aes_1.dat	using bits 3 to 4	142136	.669	.7481
DNA for aes_1.dat	using bits 2 to 3	142772	2.545	.9945
DNA for aes_1.dat	using bits 1 to 2	142748	2.474	.9933

-----  
Test results for aes\_1.dat

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_1.dat	2394.99	-1.485	.068769
byte stream for aes_1.dat	2626.09	1.783	.962725

-----  
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	2470.25	-.421	.336965
bits 2 to 9	2488.47	-.163	.435251

bits 3 to 10	2515.83	.224	.588555
bits 4 to 11	2568.45	.968	.833474
bits 5 to 12	2528.65	.405	.657323
bits 6 to 13	2584.53	1.195	.884053
bits 7 to 14	2372.68	-1.801	.035886
bits 8 to 15	2481.25	-.265	.395464
bits 9 to 16	2436.19	-.902	.183409
bits 10 to 17	2652.51	2.157	.984487
bits 11 to 18	2487.37	-.179	.429116
bits 12 to 19	2595.28	1.347	.911083
bits 13 to 20	2372.00	-1.810	.035130
bits 14 to 21	2495.96	-.057	.477227
bits 15 to 22	2553.64	.759	.775952
bits 16 to 23	2501.70	.024	.509591
bits 17 to 24	2501.91	.027	.510783
bits 18 to 25	2733.69	3.305	.999525
bits 19 to 26	2600.41	1.420	.922193
bits 20 to 27	2496.24	-.053	.478769
bits 21 to 28	2617.65	1.664	.951919
bits 22 to 29	2545.73	.647	.741098
bits 23 to 30	2421.91	-1.104	.134712
bits 24 to 31	2510.76	.152	.560489
bits 25 to 32	2419.19	-1.143	.126567

-----

CDPARK: result of ten tests on file aes\_1.dat  
 Of 12,000 tries, the average no. of successes  
 should be 3523 with sigma=21.9

Successes: 3532	z-score: .411	p-value: .659449
Successes: 3499	z-score: -1.096	p-value: .136563
Successes: 3537	z-score: .639	p-value: .738676
Successes: 3506	z-score: -.776	p-value: .218799
Successes: 3509	z-score: -.639	p-value: .261324
Successes: 3530	z-score: .320	p-value: .625377
Successes: 3529	z-score: .274	p-value: .607947
Successes: 3488	z-score: -1.598	p-value: .055002
Successes: 3513	z-score: -.457	p-value: .323972
Successes: 3503	z-score: -.913	p-value: .180558

square size	avg. no. parked	sample sigma
100.	3514.600	15.609

KSTEST for the above 10: p= .714774

-----

This is the MINIMUM DISTANCE test  
 for random integers in the file aes\_1.dat

Sample no.	d^2	avg	equiv uni
5	.8186	.6540	.560764
10	1.1887	1.0536	.697199
15	.6670	.9922	.488493
20	1.2036	1.0004	.701685
25	4.9353	1.1507	.992987
30	.6867	1.1276	.498523
35	2.4700	1.0877	.916458
40	1.3609	1.0519	.745314
45	.1717	1.0670	.158485
50	.9396	1.0940	.611068
55	1.7558	1.1033	.828747
60	1.7036	1.1106	.819517
65	.6255	1.0612	.466683
70	1.4132	1.0638	.758347
75	1.7178	1.0470	.822087
80	.2860	1.0290	.249839
85	.4964	1.0135	.392784
90	.1473	.9758	.137564
95	.2816	.9895	.246476

100 1.0306 .9823 .645033  
 MINIMUM DISTANCE TEST for aes\_1.dat  
 Result of KS test on 20 transformed mindist^2's:  
 p-value= .035629

The 3DSPHERES test for file aes\_1.dat

sample no:	r^3=	p-value=
1	52.626	.82695
2	94.824	.95761
3	5.211	.15945
4	21.173	.50626
5	38.803	.72567
6	57.672	.85374
7	19.713	.48165
8	48.502	.80145
9	13.260	.35724
10	4.802	.14791
11	26.201	.58246
12	58.521	.85782
13	7.386	.21823
14	43.913	.76864
15	51.583	.82083
16	41.354	.74804
17	17.829	.44804
18	41.181	.74658
19	16.276	.41873
20	26.066	.58058

3DSPHERES test for file aes\_1.dat p-value= .856367

RESULTS OF SQUEEZE TEST FOR aes\_1.dat  
 Table of standardized frequency counts  
 ( (obs-exp)/sqrt(exp) )^2

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

.6	1.3	.8	1.2	.4	1.0
-2.7	-1.9	-.6	1.0	-.5	.3
.4	.7	-.6	-.6	.0	-.2
1.5	.4	-.7	-.5	1.8	.5
-.5	.6	-1.6	-1.4	-.5	.8
-1.7	1.2	-.5	-.4	-1.2	-.8
.5	1.1	.1	-1.8	-.6	-1.0
2.7					

Chi-square with 42 degrees of freedom: 52.191  
 z-score= 1.112 p-value= .865458

Test no. 1	p-value .130688
Test no. 2	p-value .064423
Test no. 3	p-value .678106
Test no. 4	p-value .400353
Test no. 5	p-value .378323
Test no. 6	p-value .233532
Test no. 7	p-value .456413
Test no. 8	p-value .832616
Test no. 9	p-value .672351
Test no. 10	p-value .386014

Results of the OSUM test for aes\_1.dat  
 KSTEST on the above 10 p-values: .408013

The RUNS test for file aes\_1.dat  
 Up and down runs in a sample of 10000

Run test for aes_1.dat	:
runs up; ks test for 10 p's:	.015223
runs down; ks test for 10 p's:	.258154
Run test for aes_1.dat	:

runs up; ks test for 10 p's: .754840  
runs down; ks test for 10 p's: .583505

---

Results of craps test for aes\_1.dat

No. of wins: Observed Expected

98989 98585.86

Chisq= 24.62 for 20 degrees of freedom, p= .78353

Throws Observed Expected Chisq Sum

SUMMARY FOR aes\_1.dat

p-value for no. of wins: .964312

p-value for throws/game: .783531

Test completed. File aes\_1.dat

.....  
: