Statistischer-Basistest PRG600 AES128 (PTG.3) IBB, 30.06.2014

Basic statistical test of bit sequences
==========
Date/Time: 16.06.2014, 9:21 hour

file: random1.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	39819	40070	39931	40100	40248	39843	40075	39950
08	39916	39915	39970	39937	39722	40546	39790	39871
10	39839	40139	39945	39835	40173	40204	40367	39899
18	40293	39985	39871	39967	39783	39840	40137	40025
20	39944	40265	39958	39588	39893	39942	40031	40047
28	39881	40414	39840	39932	40113	40215	40050	39968
30	40156	40093	40228	40205	40042	39947	40131	40129
38	40156	39826	40204	40017	39999	39956	40160	40012
40	40249	40003	40105	39963	39865	39894	39941	39773
48	39969	39812	39955	40162	39993	39930	40055	40009
50	39914	40032	39946	39902	39883	40069	40433	39965
58	40055	39874	39829	39405	40201	39961	39414	40396
60	39843	40257	40275	40252	40153	40205	40118	39949
68	39979	40260	39746	39826	39902	39811	40261	40192
70	39758	40027	40109	39867	40158	39951	39801	39961
78	39802	39982	40065	39991	39747	40278	39914	39997
80	40405	40365	40129	39990	40413	39774	39837	40064
88	40076	40209	40125	40100	39973	39708	39867	39875
90	40018	39695	39963	39922	39810	40138	40193	40031
98	39903	40121	40117	39993	39934	40099	40058	39622
a0	40040	40026	40126	39930	39627	39659	39577	40081
a8	39939	39880	40033	40040	39413	39924	40202	40059
b0	40137	39937	39758	40055	39906	39927	40344	40105
b8	39866	39796	40410	39943	39780	40099	40058	39796
c0	40319	40001	39720	39731	40015	40186	40088	39799
c8	39795	40329	39955	40421	39968	40170	40169	40119
d0	39846	39936	40080	39925	40048	39958	40256	39824
d8	40089	40211	39758	40211	39916	39704	40475	39964
e0	39678	40418	40486	39874	39896	39862	40124	39869
e8	40013	40000	39912	40078	39976	40168	39843	39959
f0	39634	39887	40243	39975	40173	39975	39689	39785
f8	40116	39923	40143	39623	40144	40070	39719	40018

Evaluation of count of 10240000 Bytes = 81920000 Bits:

  Theoretical average of byte-frequencies: 40000
  '5b' = 39405 (minimum) '0d' = 40546 (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: 11 summary: 16

Test 2:
  Evaluation of byte-frequencies
  Chi-square non-overlapping:

```
  Theoretical maximum chi-square = 293.25
  Chi-square value               = 239.44

  Chi-square overlapping:
  Theoretical maximum chi-square = 155.40
  Chi-square value               = 131.88

Test 3:
  r = 0.49994299 (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 (0.49994299 , 0.50005698) is w = 0.30231348.
  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:   20485629     tuples 01:   20479043
  tuples 10:   20479042     tuples 11:   20476286

  Check size: Chi-square of 2-bit patterns minus chi square of 1-bit patterns
  Theoretical maximum chi-square = 5.99
  Chi-square value               = 1.24

Test 5:
  Frequencies of 2-tuples on even places:
  tuples 00:   10241603     tuples 01:   10240567
  tuples 10:   10240898     tuples 11:   10236932

  Theoretical maximum chi-square = 7.81
  Chi-square value               = 1.28

Test 6:
  Frequencies of 2-tuples on odd places:
  tuples 00:   10244026     tuples 01:   10238476
  tuples 10:   10238144     tuples 11:   10239354

  Theoretical maximum chi-square = 7.81
  Chi-square value               = 2.19

Result of statistical analysis of file datxor34.rnd:
================================================
The tests: 1 2 3 4 5 6  were fulfilled!

The null-hypothesis is accepted!
```