Statistischer-Basistest PRG220 AES128 (PTG.3) IBB, 14.04.2014

Basic statistical test of bit sequences
==========
Date/Time: 14.04.2014,12:48 hour

file: aes.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	39734	40131	39573	40088	39676	40048	39951	40024
08	40258	40204	39996	40133	40129	40034	39841	40008
10	39985	39808	39738	40068	39874	40058	40038	40252
18	39766	40161	40079	39839	40002	40034	40028	40240
20	39780	40073	40310	40231	39949	40038	39680	39987
28	40079	40442	39817	40148	40161	39785	39734	39733
30	40135	40241	40471	40242	39405	39930	40206	39762
38	40293	39763	40444	39977	40168	39974	40215	40017
40	40191	39755	39815	40108	39791	40027	40150	39891
48	39925	39587	40208	39713	40280	39867	39943	40172
50	40269	39966	39995	40031	40269	39985	39402	39584
58	40205	39970	39950	40191	40251	40079	40228	39618
60	39846	39665	39927	40288	39873	40063	39632	40179
68	39960	39800	39979	39912	40374	40133	39856	39717
70	40347	40123	39962	40083	39880	40209	39762	40044
78	39859	39849	40227	39756	40433	40010	40083	39943
80	39731	40181	40038	40022	39998	39836	40034	40085
88	39767	40111	40041	39717	39742	39876	39802	39978
90	40063	40053	40065	39955	40160	39810	40211	40082
98	39627	40213	40086	40300	40136	39849	40178	39865
a0	40262	40043	40195	40238	40090	40295	40232	39946
a8	40075	40001	40154	40030	40045	40164	39666	40075
b0	39828	39707	39670	39982	39541	40079	40303	40226
b8	39918	39785	39990	40205	39579	39983	40237	40406
c0	40053	39807	40521	40029	40378	39890	39922	40121
c8	39729	40201	39902	40032	40194	39965	39912	39693
d0	39774	39853	40275	39912	40411	40053	39785	40016
d8	40395	40016	40339	39775	39571	40060	40010	39914
e0	39880	40180	40410	40035	39923	40047	39842	39664
e8	40289	39723	39941	39961	40100	40009	39844	40247
f0	40232	40169	39803	39702	39778	39923	39863	40037
f8	40177	39871	40172	39565	39829	39759	39730	40047

Evaluation of count of 10240000 Bytes = 81920000 Bits:

Theoretical average of byte-frequencies: 40000
'56' = 39402 (minimum) 'c2' = 40521 (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: 9 greater: 9 summary: 18

Test 2:
Evaluation of byte-frequencies

```
  Chi-square non-overlapping:
  Theoretical maximum chi-square = 293.25
  Chi-square value               = 285.26

  Chi-square overlapping:
  Theoretical maximum chi-square = 155.40
  Chi-square value               = 118.77

Test 3:
  r = 0.49996275 (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 (0.49996275 , 0.50003725) is w = 0.50008905.
  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:   20481801     tuples 01:   20481251
  tuples 10:   20481250     tuples 11:   20475698

  Check size: Chi-square of 2-bit patterns minus chi square of 1-bit patterns
  Theoretical maximum chi-square = 5.99
  Chi-square value               = 0.76

Test 5:
  Frequencies of 2-tuples on even places:
  tuples 00:   10241616     tuples 01:   10237489
  tuples 10:   10242330     tuples 11:   10238565

  Theoretical maximum chi-square = 7.81
  Chi-square value               = 1.60

Test 6:
  Frequencies of 2-tuples on odd places:
  tuples 00:   10240185     tuples 01:   10243762
  tuples 10:   10238920     tuples 11:   10237133

  Theoretical maximum chi-square = 7.81
  Chi-square value               = 2.30

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

The null-hypothesis is accepted!
```