Basic statistical test of bit sequences
==========
Date/Time: 2.08.2002,18:41 hour

file: aes_1.dat size: 10000000 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	39024	39087	39365	39053	38847	38725	39105	38833
08	39004	38269	39335	39276	38940	38973	38982	39188
10	39231	39013	39106	39169	38914	38970	39129	39066
18	39262	38833	39033	39202	39333	38993	39048	39055
20	39444	39097	39369	39054	39024	38551	39121	39070
28	39133	38693	38977	38968	38797	39015	38901	39535
30	38916	39300	38871	39003	39019	38648	39209	39087
38	39018	38904	38978	39360	39242	39056	38836	39060
40	38960	39218	38928	38898	39438	38624	38990	38866
48	38764	39021	39135	38950	39169	39290	39025	38838
50	39000	39160	38967	39118	38934	38801	39149	39188
58	39244	38613	39255	39162	39213	39338	39015	38902
60	39057	39141	39112	38949	38950	39049	38791	39198
68	39293	39041	39455	38674	39318	39126	39178	38824
70	38923	39131	39090	39071	39085	38993	39378	39033
78	39034	38912	39241	39022	39195	38740	38633	39087
80	38800	39070	39089	39009	39164	39234	39028	39120
88	39425	39192	39325	38946	39029	39032	38941	39063
90	38851	39297	39071	39016	39033	39015	39133	38592
98	39109	38784	39184	38682	38832	39512	39014	39304
a0	39293	38978	39023	38974	38977	39005	39323	39113
a8	38849	39046	39428	39028	39115	39205	39016	39343
b0	38935	38872	39286	39044	39040	38803	39326	38933
b8	38827	39134	39142	39069	39138	39499	38867	38878
c0	39080	39329	38909	39159	38815	38975	39155	38982
c8	39156	39366	39216	38786	39267	39145	38955	39110
d0	38749	39108	39192	39008	38983	39026	39054	38889
d8	38967	38892	38799	39083	38930	39057	38878	39151
e0	39065	39113	39098	39008	39039	39288	39176	38980
e8	39351	39017	39276	39277	39003	39074	39643	38961
f0	39260	39238	39007	39099	38890	39389	39078	39166
f8	39308	38890	39230	39361	39163	38992	39433	39035

Evaluation of count of   10000000 Bytes =   80000000 Bits:

  Theoretical average of byte-frequencies: 39062
  '09' = 38269 (minimum)   'ee' = 39643 (maximum)

  Theoretical interval I of byte-frequencies:
  I = (38676 to 39449) (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: 8 greater: 5 summary: 13

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

```
  Theoretical maximum chi-square = 293.25
  Chi-square value               = 242.40

  Chi-square overlapping:
  Theoretical maximum chi-square = 155.40
  Chi-square value               = 124.62

Test 3:
  r = 0.50005263 (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 (0.49994737 , 0.50005263) is w = 0.34645373.
  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:   19996381     tuples 01:   19999410
  tuples 10:   19999409     tuples 11:   20004800

  Check size: Chi-square of 2-bit patterns minus chi square of 1-bit patterns
  Theoretical maximum chi-square = 5.99
  Chi-square value               = 0.96

Test 5:
  Frequencies of 2-tuples on even places:
  tuples 00:    9998634     tuples 01:    9992919
  tuples 10:   10005603     tuples 11:   10002844

  Theoretical maximum chi-square = 7.81
  Chi-square value               = 9.15

Test 6:
  Frequencies of 2-tuples on odd places:
  tuples 00:    9997747     tuples 01:   10006491
  tuples 10:    9993806     tuples 11:   10001956

  Theoretical maximum chi-square = 7.81
  Chi-square value               = 8.94

Result of statistical analysis of file    aes_1.dat:
================================================
The tests: 1 2 3 4  were fulfilled!
```