NESSIE Document NES/DOC/KUL/WP3/013/1
The Statistical Evaluation of the NESSIE Submission RC6 *†

Jorge Nakahara Jr

Katholieke Universiteit Leuven,
B-3001 Leuven-Heverlee,
Belgium
jorge.nakahara@esat.kuleuven.ac.be

22 October 2001

Abstract

The purpose of this document is to give a statistical evaluation of the NESSIE submission RC6. For this evaluation, we follow the recommendations of the NESSIE statistical evaluation process for blockcipher submissions as described in [Sch01a].

1 Overview

The NESSIE submission RC6 is a fully parameterized family of encryption algorithms. A version of RC6 is more accurately specified as RC6-w/r/b, where the word size is w bits, encryption consists of a non-negative number of r rounds, and b denotes the length of the encryption key in bytes. For a 128-bit block size, w = 32 and r = 20 are recommended values and RC6 is a shorthand to refer to such versions. The key length can vary between 0 and 256 bytes, though the most useful values mght be versions with 16-, 24- and 32-byte keys (128, 192 or 256 bits). RC6 was designed by Ronald L. Rivest, Matthew J. B.Robshaw, Ray Sidney, and Yiqun L. Yin.

The plaintext is stored in four w-bit registers (A, B, C, D), and B and D are added, modulo 2^w with two subkeys. In a cipher round the B and D registers are individually input into a quadratic function $f(X) = (X * (2X + 1)) \lll lgw$. The A and C registers are combined by exclusive-or and left-rotation by the output of $f(B)$ and $f(C)$ and subsequently combined with the round subkeys. The last operation in a round is left rotation of the register (A, B, C, D) into (B, C, D, A).

In this document only the cipher version with 128 bit key size will be evaluated.

This document is organized as follows: The next two sections present the statistical evaluation of the full round version of RC6 as well as the statistical evaluation of reduced round versions of the cipher. In the two remaining sections we give the results of the NESSIE streamcipher tests applied to RC6 in OFB mode and in counter mode [Sch01b], respectively.

In order to get a reasonable statistical evaluation, all NESSIE tests were repeated several times, and all tests were started with their default input parameters.

*The work described in this paper has been supported by the Commission of the European Communities through the IST program under contract IST-1999-12324.

†The information in this document is provided as is, and no warranty is given or implied that the information is fit for any particular purpose. The user thereof uses the information at its sole risk and liability.

2 Statistical evaluation of the NESSIE blockcipher RC6 with full rounds

The NESSIE evaluation tools for blockciphers consist of the dependence test and the linear factors test. For a detailed introduction to the dependence test and linear factors test, please refer to the documents [Bol90, Dic91].

2.1 The Dependence Test

The dependence test evaluates the dependence matrix and the distance matrix of the cipher. Furthermore, the degree of completeness, the degree of avalanche effect and the degree of strict avalanche criterion of the cipher are computed. A cryptographic function is complete if each output bit depends on each input bit. For a function to exhibit the avalanche effect, an average of one half of the output bits should change whenever a single input bit is complemented. A function satisfies the strict avalanche criterion if each output bit changes with a probability of one half whenever a single input bit is complemented. The exact definitions of the degree of completeness, the avalanche effect and the strict avalanche criterion can be found in document [Ser00].

```
DEPENDENCE TEST for
NESSIE submission blockcipher rc6 with 128 bit key and 128 bit block



Number of inputs:     10000

Average number of output bits changed: 64.000608

Degree of completeness               : 1.000000
Degree of avalanche effect           : 0.999269
Degree of strict avalanche criterion : 0.991951



ANALYSIS OF THE DISTANCE MATRIX


Average fractions of inputs yielding distance j if one bit is complemented,
and the expected fractions for a random function

 j            0        1        2        3        4        5        6        7
exp.   0.000000 0.000000 0.000000 0.000000 0.000000 0.000000 0.000000 0.000000
av.    0.000000 0.000000 0.000000 0.000000 0.000000 0.000000 0.000000 0.000000

 j            8        9       10       11       12       13       14       15
exp.   0.000000 0.000000 0.000000 0.000000 0.000000 0.000000 0.000000 0.000000
av.    0.000000 0.000000 0.000000 0.000000 0.000000 0.000000 0.000000 0.000000

 j           16       17       18       19       20       21       22       23
exp.   0.000000 0.000000 0.000000 0.000000 0.000000 0.000000 0.000000 0.000000
av.    0.000000 0.000000 0.000000 0.000000 0.000000 0.000000 0.000000 0.000000

 j           24       25       26       27       28       29       30       31
exp.   0.000000 0.000000 0.000000 0.000000 0.000000 0.000000 0.000000 0.000000
av.    0.000000 0.000000 0.000000 0.000000 0.000000 0.000000 0.000001 0.000000
```

j	32	33	34	35	36	37	38	39
exp.	0.000000	0.000000	0.000000	0.000000	0.000000	0.000001	0.000001	0.000003
av.	0.000000	0.000000	0.000000	0.000000	0.000001	0.000000	0.000003	0.000001

j	40	41	42	43	44	45	46	47
exp.	0.000007	0.000016	0.000033	0.000067	0.000129	0.000240	0.000433	0.000756
av.	0.000008	0.000014	0.000030	0.000069	0.000119	0.000227	0.000427	0.000715

j	48	49	50	51	52	53	54	55
exp.	0.001276	0.002082	0.003290	0.005032	0.007452	0.010685	0.014841	0.019967
av.	0.001282	0.002066	0.003280	0.005042	0.007495	0.010549	0.014668	0.020036

j	56	57	58	59	60	61	62	63
exp.	0.026029	0.032879	0.040248	0.047752	0.054915	0.061216	0.066153	0.069303
av.	0.025970	0.033423	0.040334	0.047782	0.055188	0.061086	0.066182	0.069250

j	64	65	66	67	68	69	70	71
exp.	0.070386	0.069303	0.066153	0.061216	0.054915	0.047752	0.040248	0.032879
av.	0.070095	0.069160	0.065763	0.061625	0.054778	0.047655	0.040308	0.032855

j	72	73	74	75	76	77	78	79
exp.	0.026029	0.019967	0.014841	0.010685	0.007452	0.005032	0.003290	0.002082
av.	0.026075	0.020138	0.014572	0.010645	0.007655	0.005042	0.003205	0.002175

j	80	81	82	83	84	85	86	87
exp.	0.001276	0.000756	0.000433	0.000240	0.000129	0.000067	0.000033	0.000016
av.	0.001298	0.000782	0.000426	0.000234	0.000134	0.000068	0.000040	0.000015

j	88	89	90	91	92	93	94	95
exp.	0.000007	0.000003	0.000001	0.000001	0.000000	0.000000	0.000000	0.000000
av.	0.000005	0.000002	0.000002	0.000001	0.000000	0.000000	0.000000	0.000000

j	96	97	98	99	100	101	102	103
exp.	0.000000	0.000000	0.000000	0.000000	0.000000	0.000000	0.000000	0.000000
av.	0.000000	0.000000	0.000000	0.000000	0.000000	0.000000	0.000000	0.000000

j	104	105	106	107	108	109	110	111
exp.	0.000000	0.000000	0.000000	0.000000	0.000000	0.000000	0.000000	0.000000
av.	0.000000	0.000000	0.000000	0.000000	0.000000	0.000000	0.000000	0.000000

j	112	113	114	115	116	117	118	119
exp.	0.000000	0.000000	0.000000	0.000000	0.000000	0.000000	0.000000	0.000000
av.	0.000000	0.000000	0.000000	0.000000	0.000000	0.000000	0.000000	0.000000

j	120	121	122	123	124	125	126	127
exp.	0.000000	0.000000	0.000000	0.000000	0.000000	0.000000	0.000000	0.000000
av.	0.000000	0.000000	0.000000	0.000000	0.000000	0.000000	0.000000	0.000000

j	128
exp.	0.000000
av.	0.000000

Application of the Chi-square test to the rows of the distance matrix

(% levels of significance)

row	%	row	%	row	%	row	%	row	%
1	87.7	2	75.3	3	36.4	4	57.2	5	68.6
6	78.0	7	18.9	8	72.0	9	99.3	10	62.4
11	90.8	12	34.2	13	67.4	14	4.8	15	65.5
16	27.2	17	22.9	18	28.2	19	74.4	20	90.1
21	94.9	22	93.2	23	40.6	24	55.7	25	33.8
26	4.7	27	81.3	28	6.5	29	93.2	30	26.0
31	25.6	32	56.2	33	45.7	34	8.6	35	20.2
36	76.5	37	21.5	38	15.5	39	98.7	40	58.5
41	82.6	42	79.9	43	37.8	44	25.0	45	55.9
46	86.6	47	92.6	48	74.7	49	44.3	50	76.6
51	17.0	52	49.1	53	97.0	54	12.0	55	51.9
56	53.9	57	26.1	58	86.6	59	33.5	60	89.8
61	65.5	62	82.2	63	1.9	64	25.9	65	5.3
66	45.7	67	89.1	68	77.9	69	32.1	70	24.9
71	76.5	72	36.2	73	83.6	74	51.7	75	26.7
76	7.7	77	3.4	78	37.7	79	46.5	80	95.6
81	20.6	82	60.7	83	43.4	84	56.5	85	69.2
86	82.1	87	10.0	88	89.7	89	40.2	90	27.4
91	2.9	92	3.7	93	59.1	94	92.2	95	48.3
96	41.6	97	70.3	98	37.8	99	7.7	100	8.8
101	25.0	102	19.3	103	91.2	104	5.2	105	74.3
106	24.9	107	36.5	108	36.8	109	47.1	110	21.7
111	54.9	112	96.3	113	16.4	114	31.6	115	89.7
116	30.7	117	46.1	118	81.0	119	41.6	120	48.3
121	10.1	122	99.3	123	10.1	124	21.0	125	41.7
126	14.4	127	65.5	128	8.5				

ANALYSIS OF THE DEPENDENCE MATRIX

Row average of the dependence matrix

i		i		i		i	
1	0.500624	2	0.500073	3	0.500183	4	0.499871
5	0.499803	6	0.500077	7	0.500522	8	0.499559
9	0.500473	10	0.500357	11	0.501060	12	0.500296
13	0.499141	14	0.499738	15	0.499780	16	0.500077
17	0.499987	18	0.499427	19	0.500184	20	0.499811
21	0.500153	22	0.500111	23	0.499799	24	0.499965
25	0.500209	26	0.499463	27	0.500437	28	0.499423
29	0.499623	30	0.500909	31	0.499598	32	0.499823
33	0.499679	34	0.500722	35	0.499596	36	0.499884
37	0.500093	38	0.499920	39	0.499833	40	0.500072
41	0.500298	42	0.499828	43	0.499807	44	0.500289
45	0.499639	46	0.499520	47	0.499566	48	0.500084
49	0.499936	50	0.499581	51	0.499473	52	0.499046
53	0.500420	54	0.499276	55	0.500458	56	0.500277
57	0.498939	58	0.500169	59	0.499627	60	0.499667
61	0.500788	62	0.500909	63	0.500143	64	0.500205
65	0.499838	66	0.499780	67	0.499423	68	0.499780
69	0.500596	70	0.500530	71	0.499983	72	0.499743
73	0.500457	74	0.500023	75	0.500559	76	0.500273

77	0.500677	78	0.500420	79	0.500073	80	0.499486
81	0.499867	82	0.500088	83	0.500878	84	0.500148
85	0.500155	86	0.499931	87	0.499983	88	0.500002
89	0.499468	90	0.500598	91	0.498772	92	0.499496
93	0.500411	94	0.499843	95	0.500363	96	0.500881
97	0.500579	98	0.499869	99	0.500270	100	0.500034
101	0.499578	102	0.500439	103	0.500699	104	0.500166
105	0.500124	106	0.500048	107	0.499744	108	0.499463
109	0.499759	110	0.499757	111	0.499845	112	0.500367
113	0.499547	114	0.499745	115	0.499730	116	0.499681
117	0.499643	118	0.500645	119	0.499924	120	0.499538
121	0.500392	122	0.499539	123	0.498962	124	0.500856
125	0.500977	126	0.499694	127	0.499884	128	0.500286

Column average of the dep. matrix

i		i		i		i	
1	0.500680	2	0.498831	3	0.500420	4	0.500123
5	0.499741	6	0.499726	7	0.499378	8	0.499805
9	0.500264	10	0.499559	11	0.500337	12	0.500568
13	0.499870	14	0.499896	15	0.500154	16	0.499796
17	0.499687	18	0.500132	19	0.499630	20	0.499638
21	0.499474	22	0.499801	23	0.500477	24	0.499941
25	0.499974	26	0.500139	27	0.500609	28	0.500276
29	0.500362	30	0.500445	31	0.499101	32	0.499757
33	0.500729	34	0.499920	35	0.500781	36	0.500705
37	0.500291	38	0.499895	39	0.500270	40	0.500373
41	0.499721	42	0.500701	43	0.499699	44	0.500054
45	0.499363	46	0.501063	47	0.499496	48	0.499742
49	0.500472	50	0.500717	51	0.499863	52	0.500560
53	0.499987	54	0.499814	55	0.499726	56	0.499314
57	0.499936	58	0.499725	59	0.500107	60	0.499601
61	0.499763	62	0.499852	63	0.499583	64	0.500129
65	0.500334	66	0.500171	67	0.499994	68	0.499819
69	0.500571	70	0.499986	71	0.499719	72	0.500517
73	0.499566	74	0.499517	75	0.500489	76	0.499932
77	0.500115	78	0.499698	79	0.500134	80	0.499971
81	0.499361	82	0.500172	83	0.500098	84	0.500250
85	0.500251	86	0.499498	87	0.499501	88	0.499951
89	0.499887	90	0.499650	91	0.499707	92	0.500255
93	0.500654	94	0.499623	95	0.500074	96	0.500903
97	0.499756	98	0.500045	99	0.500118	100	0.500090
101	0.500135	102	0.500370	103	0.500361	104	0.500902
105	0.500181	106	0.500480	107	0.499984	108	0.500736
109	0.499888	110	0.500298	111	0.499940	112	0.500341
113	0.499261	114	0.499929	115	0.499974	116	0.499680
117	0.499435	118	0.499615	119	0.500336	120	0.499633
121	0.500266	122	0.500094	123	0.499020	124	0.499606
125	0.499803	126	0.500303	127	0.499527	128	0.499588

2.2 The Linear Factors Test

The linear factors test is used to find out whether there are any linear combinations of output bits which, for all keys and plaintexts, are independent of one or more key or plaintext bits. Such a linear combination is called a linear factor. It is practically impossible to check a potential linear factor for all keys and plaintexts. Therefore, we only consider for a sufficiently large number of pairs of random keys and random plaintexts [Dic91]. For the full round version of the cipher, no linear factors were found.

3 Statistical evaluation of the NESSIE blockcipher RC6 with reduced rounds

The blockcipher RC6 with 128 bit key is a cipher with 20 rounds plus pre- and post-whitening. For the reduced round tests of the cipher, we always perform the pre- and post-whitening ("+0.5"). As in document [Ser00], we examined

(1) the average number of output bits changed when changing one input bit

(2) the degree of completeness d_c

(3) the degree of avalanche effect d_a

(4) the degree of strict avalanche criterion d_{sa}

for the cipher with the full number of rounds down to just the last round. Table 1 shows the results of these tests.

♯rounds	(1)	(2) = d_c	(3) = d_a	(4) = d_{sa}
$20 + 0.5$	64.000608	1.000000	0.999269	0.991951
$19 + 0.5$	64.004094	1.000000	0.999334	0.992022
$18 + 0.5$	63.991391	1.000000	0.999296	0.991975
$17 + 0.5$	63.999673	1.000000	0.999233	0.992055
$16 + 0.5$	64.000473	1.000000	0.999332	0.992095
$15 + 0.5$	63.998055	1.000000	0.999280	0.992061
$14 + 0.5$	64.000656	1.000000	0.999356	0.992036
$13 + 0.5$	63.995730	1.000000	0.999249	0.991960
$12 + 0.5$	63.988077	1.000000	0.999288	0.992087
$11 + 0.5$	64.003752	1.000000	0.999292	0.992021
$10 + 0.5$	64.004796	1.000000	0.999247	0.991948
$9 + 0.5$	64.002852	1.000000	0.999237	0.992009
$8 + 0.5$	64.003945	1.000000	0.999327	0.992037
$7 + 0.5$	64.000458	1.000000	0.999357	0.992060
$6 + 0.5$	63.997502	1.000000	0.999300	0.991980
$5 + 0.5$	63.994611	1.000000	0.999273	0.992041
$4 + 0.5$	63.923282	1.000000	0.998479	0.991661
$3 + 0.5$	60.301572	1.000000	0.942141	0.937845
$2 + 0.5$	41.784901	0.875000	0.652889	0.651275
$1 + 0.5$	14.334177	0.417847	0.223972	0.213940
0.5	1.934266	0.086853	0.030223	0.010645

Table 1: Dependence test of the reduced round versions of RC6

The values (1)-(4) remain stable until the number of rounds becomes less than $4 + 0.5$.
We state that the blockcipher RC6

- is complete after $4 + 0.5$ rounds.
- has a degree of strict avalanche criterion greater than 0.98 after $4 + 0.5$ rounds.
- reveals no linear factors after $3 + 0.5$ rounds

4 Evaluation of the NESSIE blockcipher RC6 in OFB mode

4.1 The Frequency Test

The frequency test splits up the bit sequence into subsequent, disjoint m-tuples of bits. m is called the blocksize of the test. The frequencies of the occurrences of these m-tuples are counted and evaluated statistically. This test is performed for various values of m.

```
Frequency Test for
NESSIE submission RC6 in OFB mode

Number of bits generated and ignored before starting to test: 0
Number of bits used for testing: 10000000
Block size: 1
sequencelength= 10000000 blocksize= 1
block: 0  count: 4997535
block: 1  count: 5002465
chisquare = 2.430490  nu= 1
Percentage Level of Acceptance:  11.90
```

We conclude, that the test results do not indicate a deviation from random behaviour.

```
Frequency Test for
NESSIE submission RC6 in OFB mode

Number of bits generated and ignored before starting to test: 0
Number of bits used for testing: 10000000
Block size: 2
sequencelength= 10000000 blocksize= 2
block: 0  count: 1250351
block: 1  count: 1248991
block: 2  count: 1250232
block: 3  count: 1250426
chisquare = 1.101266  nu= 3
Percentage Level of Acceptance:  77.68
```

The test result does not indicate a deviation from random behaviour.

```
Frequency Test for
NESSIE submission RC6 in OFB mode

Number of bits generated and ignored before starting to test: 0
Number of bits used for testing: 10000000
Block size: 3
sequencelength= 10000000 blocksize= 3
block: 0  count: 416697
block: 1  count: 416711
block: 2  count: 417672
block: 3  count: 417460
```

```
block: 4  count: 416442
block: 5  count: 415364
block: 6  count: 415986
block: 7  count: 417001
chisquare = 9.517105  nu= 7
Percentage Level of Acceptance:  21.76
```

The test result does not indicate a deviation from random behaviour.

```
Frequency Test for
NESSIE submission RC6 in OFB mode

Number of bits generated and ignored before starting to test: 0
Number of bits used for testing: 10000000
Block size: 4
sequencelength= 10000000 blocksize= 4
block: 0  count: 156419
block: 1  count: 156302
block: 2  count: 156379
block: 3  count: 156144
block: 4  count: 156825
block: 5  count: 155671
block: 6  count: 156378
block: 7  count: 156306
block: 8  count: 155981
block: 9  count: 156518
block: 10  count: 156495
block: 11  count: 156573
block: 12  count: 156034
block: 13  count: 155938
block: 14  count: 155892
block: 15  count: 156145
chisquare = 8.552038  nu= 15
Percentage Level of Acceptance:  89.98
```

The test result does not indicate a deviation from random behaviour.

```
Frequency Test for
NESSIE submission RC6 in OFB mode

Number of bits generated and ignored before starting to test: 0
Number of bits used for testing: 10000000
Block size: 5
sequencelength= 10000000 blocksize= 5
chisquare = 26.722656  nu= 31
Percentage Level of Acceptance:  68.60
```

The test result does not indicate a deviation from random behaviour.

```
Frequency Test for
NESSIE submission RC6 in OFB mode

Number of bits generated and ignored before starting to test: 0
Number of bits used for testing: 10000000
Block size: 6
```

```
sequencelength= 10000000 blocksize= 6
chisquare = 69.127648  nu= 63
Percentage Level of Acceptance:  27.82
```

The test result does not indicate a deviation from random behaviour.

```
Frequency Test for
NESSIE submission RC6 in OFB mode

Number of bits generated and ignored before starting to test: 0
Number of bits used for testing: 10000000
Block size: 7
sequencelength= 10000000 blocksize= 7
chisquare = 154.343958  nu= 127
Percentage Level of Acceptance:  4.98
```

The test result does not indicate a deviation from random behaviour.

```
Frequency Test for
NESSIE submission RC6 in OFB mode

Number of bits generated and ignored before starting to test: 0
Number of bits used for testing: 10000000
Block size: 8
sequencelength= 10000000 blocksize= 8
chisquare = 265.099878  nu= 255
Percentage Level of Acceptance:  31.89
```

The test result does not indicate a deviation from random behaviour.

```
Frequency Test for
NESSIE submission RC6 in OFB mode

Number of bits generated and ignored before starting to test: 0
Number of bits used for testing: 10000000
Block size: 12
sequencelength= 10000000 blocksize= 12
chisquare = 4215.473515  nu= 4095
Percentage Level of Acceptance:  9.25
```

The test result does not indicate a deviation from random behaviour.

```
Frequency Test for
NESSIE submission RC6 in OFB mode

Number of bits generated and ignored before starting to test: 0
Number of bits used for testing: 10000000
Block size: 16
sequencelength= 10000000 blocksize= 16
chisquare = 65638.290944  nu= 65535
Percentage Level of Acceptance:  38.71
```

The test result does not indicate a deviation from random behaviour.

4.2 The Collision Test

The collision test splits up the bit sequence into subsequent, disjoint m-tuples of bits. The test evaluates statistically how often such m-tuples occur more than once.

```
Collision Test for
NESSIE submission RC6 in OFB mode

Number of bits generated and ignored before starting to test: 0
Number of bits used for testing: 10000000
Block size: 24
# of blocks: 416666 blocksize: 24 collisions: 5075
```

The test result does not indicate a deviation from random behaviour.

4.3 The Overlapping m-tuple Test

The overlapping m-tuple test splits up the bit sequence into m-tuples of words. Each word contains a fixed number of bits. In the overlapping m-tuple test, the m-tuples are not disjoint; to take the next m-tuple, an m-word-window on the original sequence is shifted by one word. So the next m-tuple consists of $m-1$ shifted words of the previous m-tuple and one new word. Since subsequent m-tuples are not independent, the statistical evaluation is more involved than in the case of the frequency test, but this is handled by the test program. This test is also applied to cyclic shifts of the original sequence.

```
OVERLAPPING M-TUPLE TEST for
NESSIE submission RC6 in OFB mode

Sequencelength = 10000000 bits        Wordlength = 5 bits
m = 2

Shift     p
--------------
  0     77.20%
  1     52.66%
  2     42.52%
  3     49.80%
  4     97.98%

p gives the percentage level of acceptance of the chi-square test
This percentage level gives the probability that a truly random
sequence has a chi-square value greater than the chi-square value
observed in this execution of the test.
```

The result for shift 4 were too good, so we repeated the experiment with another key.

```
OVERLAPPING M-TUPLE TEST for
NESSIE submission RC6 in OFB mode

Sequencelength = 10000000 bits        Wordlength = 5 bits
m = 2

Shift     p
--------------
  0     58.54%
  1     94.94%
```

```
  2      80.81%
  3      68.94%
  4      61.68%

p gives the percentage level of acceptance of the chi-square test
This percentage level gives the probability that a truly random
sequence has a chi-square value greater than the chi-square value
observed in this execution of the test.
```

The test result does not indicate a deviation from random behaviour.

4.4 The Gap Test

The gap test splits up the bit sequence into subsequent, disjoint m-tuples of bits. m is called the word length of the test. The m-tuples are interpreted as binary representations of numbers, and the lengths of gaps, where the numbers are not within a numerical range given as a parameter of the test, are registered and evaluated statistically. The gap test is also applied to cyclic shifts of the original sequence.

```
GAP TEST for
NESSIE submission RC6 in OFB mode

Sequencelength = 10000000 bits        Wordlength = 10 bits
Length of gaps between occurences in the range 256 - 768
Ideal distribution:       mean    variance
                         1.000       2.000
Real distribution:
Shift:             0       1       2       3       4       5       6       7       8       9
            ------------------------------------------------------------------------------
 mean:         1.001   0.997   0.997   1.002   1.001   0.998   1.001   1.000   1.003   1.000
 error:         0.15%  -0.31%  -0.30%   0.18%   0.09%  -0.15%   0.06%   0.02%   0.28%   0.04%
 variance:     2.002   1.990   1.990   2.005   2.006   2.001   2.003   1.999   2.010   1.994
 error:         0.11%  -0.52%  -0.48%   0.25%   0.31%   0.03%   0.15%  -0.06%   0.51%  -0.28%

    p=         48.86%  72.21%  33.61%  53.36%  40.09%  85.92%  96.70%  56.56%  78.57%  10.98%

p gives the percentage level of acceptance of the chi-square test
This percentage level gives the probability that a truly random
sequence has a chi-square value greater than the chi-square value
observed in this execution of the test.
```

The percentage level of acceptance was high for shift 6. However, since we apply a considerable number of statistical tests, it is unavoidable that we get some results with percentage levels of acceptance close to 100% or 0%. In this case, we repeat the test (with different keys) to check whether the result can be reproduced. The second gap test gave the following results:

```
GAP TEST for
NESSIE submission RC6 in OFB mode

Sequencelength = 10000000 bits        Wordlength = 10 bits
Length of gaps between occurences in the range 256 - 768
Ideal distribution:       mean    variance
                         1.000       2.000
Real distribution:
Shift:             0       1       2       3       4       5       6       7       8       9
            ------------------------------------------------------------------------------
 mean:         1.003   1.001   1.001   1.000   1.001   1.003   0.999   1.001   0.999   1.002
 error:         0.28%   0.12%   0.12%  -0.01%   0.09%   0.34%  -0.06%   0.12%  -0.11%   0.23%
 variance:     2.002   2.002   2.009   1.993   2.008   2.008   1.988   1.999   2.004   2.011
 error:         0.11%   0.08%   0.44%  -0.35%   0.39%   0.41%  -0.62%  -0.07%   0.20%   0.54%

    p=         21.82%  93.22%  58.79%  11.97%   6.22%  70.42%  35.47%  60.71%   6.78%  68.73%

p gives the percentage level of acceptance of the chi-square test
This percentage level gives the probability that a truly random
sequence has a chi-square value greater than the chi-square value
observed in this execution of the test.
```

We conclude that the test results do not indicate a deviation from random behaviour.

4.5 The Run Test

The run test splits up the bit sequence into subsequent, disjoint m-tuples of bits. m is called the word length of the test. The m-tuples are interpreted as binary representations of numbers. The lengths of subsequences of consecutive, strictly increasing numbers are evaluated statistically.

```
Run Test for
NESSIE submission RC6 in OFB mode

Number of bits generated and ignored before starting to test: 0
Number of bits used for testing: 10000000
Block size: 16
Maximal run length registered individually: 5
Total of 229597 runs
 114474 runs of length 1  expected: 114800.3
 76480 runs of length 2  expected: 76532.3
 28848 runs of length 3  expected: 28698.7
  7901 runs of length 4  expected: 7652.6
  1593 runs of length 5  expected: 1594.2
   301 runs of length 6 or more expected: 318.8
chisquare = 10.794887 nu = 5
Percentage level of acceptance 5.56
```

The test result does not indicate a deviation from random behaviour.

4.6 The Coupon Collector's Test

The coupon collector's test splits up the bit sequence into subsequent, disjoint m-tuples of bits. m is called the word length of the test. In the test, the number of subsequent m-tuples it takes until all possible 2^m m-tuples have appeared, is evaluated statistically. The coupon collector's test is also applied to cyclic shifts of the original sequence.

```
COUPON COLLECTOR'S TEST for
NESSIE submission RC6 in OFB mode

Sequencelength = 10000000 bits        Wordlength = 8 bits
Ideal distribution:       mean    variance
                       1567.8323   105979.0660
Real distribution:
The results are for cyclic shifts
Shift:                 0        1        2        3        4        5        6        7
            ------------------------------------------------------------------------
 mean:         1568.632 1558.216 1566.053 1566.945 1555.968 1576.689 1564.327 1587.779
 error:           0.05%   -0.61%   -0.11%   -0.06%   -0.76%    0.56%   -0.22%    1.27%
 variance:       113515    98962    95843   113436   102998   111053    92655   123856
 error:           7.11%   -6.62%   -9.56%    7.04%   -2.81%    4.79%  -12.57%   16.87%

    p=            58.40%   87.59%    5.11%   14.25%   96.56%   12.13%   92.87%   80.98%

p gives the percentage level of acceptance of the chi-square test
This percentage level gives the probability that a truly random
sequence has a chi-square value greater than the chi-square value
observed in this execution of the test.
```

The test result does not indicate a deviation from random behaviour.

4.7 The Universal Maurer Test

The universal Maurer test splits up the bit sequence into subsequent, disjoint m-tuples of bits. m is called the blocksize of the test. The test evaluates statistically how many m-tuples later an

m-tuple re-appears in the sequence. The test result of the Maurer test is closely related to the entropy of the bit sequence.

```
Maurer Test for
NESSIE submission RC6 in OFB mode

Number of bits generated and ignored before starting to test: 0
Number of bits used for testing: 1000000
Block size: 8
Initial Blocks= 10000
blocks tested (including initial blocks): 125000
Maurer Test Value: 7.186030
```

For an ideal random number generator, the probability to obtain a Maurer test value of 7.186030 or less is 76.76%. The test result does not indicate a deviation from random behaviour.

4.8 The Poker Test

The poker test splits up the bit sequence into subsequent, disjoint m-tuples of bits. m is called the word length of the test. The sequence of m-tuples is split up into subsequent, disjoint k-tuples of m-tuples. The poker test evaluates statistically how many of the m-tuples in a k-tuple are equal. The poker test is also applied to cyclic shifts of the original sequence.

```
POKER TEST for
NESSIE submission RC6 in OFB mode

Sequencelength = 9999360 bits        Wordlength = 8 bits
Elements in a k-tuple: 128
Ideal distribution:       mean    variance
                        100.8801     13.9923
Real distribution:
Shift:              0       1       2       3       4       5       6       7
            ------------------------------------------------------------------
 mean:       100.923 100.822 100.823 100.857 100.907 100.898 100.917 100.938
 error:        0.04%  -0.06%  -0.06%  -0.02%   0.03%   0.02%   0.04%   0.06%
 variance:    13.766  13.866  13.850  14.181  14.553  14.347  14.411  14.318
 error:        -1.62%  -0.91%  -1.02%   1.35%   4.01%   2.53%   2.99%   2.32%

    p=         84.67%  12.47%   9.05%  60.07%  13.14%  19.70%  35.38%  21.82%

p gives the percentage level of acceptance of the chi-square test
This percentage level gives the probability that a truly random
sequence has a chi-square value greater than the chi-square value
observed in this execution of the test.
```

We conclude that the test results do not indicate a deviation from random behaviour.

4.9 The Fast Spectral Test

The fast spectral test applies the fast Walsh transform to the given sequence. It uses two values derived from the transform to assess the randomness of the sequence.

```
Fast Spectral Test for
NESSIE submission RC6 in OFB mode

The results are:
```

```
The statistic D(4) = 1.840218E+00; percentage level of significance:  96.7%
The statistic D(6) = 2.141422E+00; percentage level of significance:  98.4%
This percentage level gives the probability that a truly random
sequence has a chi-square value greater than the chi-square value
observed in this execution of the test.
```

The statistics were too good, so we repeated the test with another key.

```
Fast Spectral Test for
NESSIE submission RC6 in OFB mode

The results are:

The statistic D(4) = 3.388387E-01; percentage level of significance:  63.3%
The statistic D(6) = 6.890110E-01; percentage level of significance:  75.5%
This percentage level gives the probability that a truly random
sequence has a chi-square value greater than the chi-square value
observed in this execution of the test.
```

The test result does not indicate a deviation from random behaviour.

4.10 The Correlation Test

The correlation test determines in how many places the original sequence and the sequence shifted by n bits have the same value. This is done for all shifts n up to the length of the original sequence. To support the interpretation of the results, for each shift the probability for a sequence of random, independent, and uniformly distributed bits to have this number or less coincidences with its shifted copy is determined. Only values where these probabilities are close to 0 or 1 are printed. The print level is the maximal deviation from 0 or 1 for these probabilities in order to be printed.

```
Correlation Test for
NESSIE submission RC6 in OFB mode

Number of bits generated and ignored before starting to test: 0
Number of bits used for testing: 1000000
Printlevel: 0.000010
shift:0 equal: 1000000 probability: 1.0000000   0e+00
shift:136140 equal: 497842 probability: 0.0000080   8e-06
shift:249191 equal: 502204 probability: 0.9999948   5e-06
shift:274703 equal: 502156 probability: 0.9999919   8e-06
shift:286769 equal: 497862 probability: 0.0000096   1e-05
shift:323328 equal: 497423 probability: 0.0000001   1e-07
shift:410679 equal: 497748 probability: 0.0000034   3e-06
shift:518371 equal: 497747 probability: 0.0000033   3e-06
shift:813570 equal: 497840 probability: 0.0000078   8e-06
```

The test result does not indicate a deviation from random behaviour.

4.11 The Rank Test

In the rank test, the bits of the sequence to test are used to fill square matrices. The bits are treated as elements of the field GF(2), and the ranks of the matrices are evaluated statistically.

```
Rank test for
NESSIE submission RC6 in OFB mode
```

```
Number of bits generated and ignored before starting to test: 0
Number of bits used for testing: 10000000
Order of the matrix: 16
Number of ranks counted individually: 3
 11072 matrices with rank 16, expected: 11280.8
 22775 matrices with rank 15, expected: 22561.3
 5016 matrices with rank 14, expected: 5013.5
 199 matrices with rank 13 or less, expected: 206.4
chisquare = 6.159228 nu = 3
Percentage level of acceptance 10.41
```

The test result does not indicate a deviation from random behaviour.

4.12 The Linear Complexity Test

The linear complexity test uses the Berlekamp Massey algorithm to determine the length of the shortest linear feedback shift register which can produce the given bit sequence. For the linear complexity profile, this is done for the first 1, 2, 3,... bits of the sequence. Some properties of this profile are evaluated.

```
Linear Complexity Test for
NESSIE submission RC6 in OFB mode



-------------------- Final results ------------------

N= 100000      L= 50000      X= 2

N    is the number of input bits.

L    is the linear complexity.

X-1  is the number of bits which has been treated since
     the last change of linear complexity.

------------------------ End ----------------------
The linear complexity profile:

Jumps in the linear complexity profile:


ssl =  99999.000    ssqsl = 498635.000
msl =      3.996    varsl =      3.958


ssh =  50000.000    ssqsh = 150012.000
msh =      1.998    varsh =      2.002


  ssl   is the sum of the sl's
  ssqsl is the sum of the squares of the sl's
  msl   is the mean of the sl's
  varsl is the variance of the sl's
  The number of jumps used in the calculation of msl and varsl is:  25025

  ssh   is the sum of the sh's
  ssqsh is the sum of the squares of the sh's
```

```
  msh   is the mean of the sh's
  varsh is the variance of the sh's
  The number of jumps used in the calculation of msh and varsh is:  25024
maximal step-height 18.000000


  sl  is the steplength
  sh  is the stepheigth
  nj  is the number of jumps
```

The test result does not indicate a deviation from random behaviour.

4.13 The Maximum Order Complexity Test

The maximum order complexity test determines the length of the shortest possibly non-linear feedback shift register which can produce the given bit sequence. For the MOC profile, this is done for the first 1, 2, 3,... bits of the sequence. The changes in this profile are studied.

```
Maximum Order Complexity (MOC) Test for
NESSIE submission RC6 in OFB mode


The changes in the MOC profile:
    3    2   ( 3.17)
   10    6   ( 6.64)
   15    7   ( 7.81)
   25    8   ( 9.29)
   47    9   (11.11)
   64   13   (12.00)
  256   15   (16.00)
  421   16   (17.44)
  465   19   (17.72)
 1005   22   (19.95)
 1896   24   (21.78)
 9921   25   (26.55)
10580   26   (26.74)
26175   29   (29.35)
55335   30   (31.51)
101860   35   (33.27)
623955   36   (38.50)


The number of inputcharacters: 1000000
The number of nodes: 1999960
The number of edges: 2755030

The MOC is: 36
```

For an ideal random number generator, the probability to obtain a MOC of 36 or less is 2.85%. So the test result does not indicate a deviation from random behaviour.

4.14 The Ziv Lempel Complexity Test

The Ziv Lempel complexity test measures how well a bit sequence can be reconstructed from earlier parts of the bit sequence.

```
NESSIE submission RC6 in OFB mode
1000000 input bits of the input file have been handled.
The Ziv Lempel complexity equals 50794.
((1000000 / log2(1000000)) = 50171.665944)

A sequence of length n is considered to be a good pseudo-random
sequence if its Ziv Lempel complexity is greater than n/log2(n).

The maximum length of a component in the history equals 35.
(log2(1000000) = 19.931569)
```

For an ideal random number generator, the probability to have a Ziv Lempel complexity of 50794 or lower is 76.68%. So the test result does not indicate a deviation from random behaviour.

4.15 The Dyadic Complexity Test

The NESSIE dyadic complexity test is an implemenation of the complexity measure suggested by Goretzky and Klapper ([KG97]) for sequences of bits. This measure is cryptologically relevant because feedback shift registers with carry, also described in [KG97], have low dyadic complexity. The tool is documented in the NESSIE document [Dic01].

```
2-adic Complexity Test for
NESSIE submission RC6 in OFB mode

Number of bits generated and ignored before starting to test: 0
Number of bits used for testing: 10000
sequencelength= 10000
2-adic complexity= 4999.24181
```

For an ideal random number generator, the probability to obtain a dyadic complexity of 4999.24181 or less is 29.13%.

We conclude that the test results do not indicate a deviation from random behaviour.

4.16 The Percolation Test

The NESSIE percolation test is the simulation of a forest fire. The bit sequence to be tested determines where trees are standing in the simulated forest. The test evaluates statistically how fast a fire propagates in the simulated forest. The documentation of the test can be found in the NESSIE document [Sch00].

```
PERCOLATION TEST for
NESSIE submission RC6 in OFB mode


Dimensions of the forest lattice: 3
Size in dimension 1: 100
Size in dimension 2: 100
Size in dimension 3: 100
Forest fire executed in a triangular lattice.
Probability for lighting the reachable neighbours (in percent): 100

Result(s) of the single fitting in of 1 forest fire(s):
Percentage level(s) of acceptance:
56.67%
```

The test result does not indicate a deviation from random behaviour.

4.17 The Constant Runs Test

For the constant runs test, the sequence of bits is subdivided into maximal subsequences of consecutive bits with the same value. The frequencies of these runs of the various lengths are evaluated statistically. The tool is documented in the NESSIE document [Ser01].

```
Constant Runs Test for
NESSIE submission RC6 in OFB mode

Number of bits generated and ignored before starting to test: 0
Number of bits used for testing: 10000000
Maximal run length registered individually: 15
Total of 2500473 0-runs
 1249659 0-runs of length    1   expected: 1250236.5
  625759 0-runs of length    2   expected:  625118.2
  312727 0-runs of length    3   expected:  312559.1
  156541 0-runs of length    4   expected:  156279.6
   77733 0-runs of length    5   expected:   78139.8
   39115 0-runs of length    6   expected:   39069.9
   19592 0-runs of length    7   expected:   19534.9
    9516 0-runs of length    8   expected:    9767.5
    4861 0-runs of length    9   expected:    4883.7
    2447 0-runs of length   10   expected:    2441.9
    1327 0-runs of length   11   expected:    1220.9
     596 0-runs of length   12   expected:     610.5
     325 0-runs of length   13   expected:     305.2
     146 0-runs of length   14   expected:     152.6
      71 0-runs of length   15   expected:      76.3
      58 0-runs of length >=16   expected:      76.3
Total of 2500472 1-runs
 1251802 1-runs of length    1   expected: 1250236.0
  623910 1-runs of length    2   expected:  625118.0
  312433 1-runs of length    3   expected:  312559.0
  156011 1-runs of length    4   expected:  156279.5
   77733 1-runs of length    5   expected:   78139.8
   39296 1-runs of length    6   expected:   39069.9
   19580 1-runs of length    7   expected:   19534.9
    9883 1-runs of length    8   expected:    9767.5
    4951 1-runs of length    9   expected:    4883.7
    2458 1-runs of length   10   expected:    2441.9
    1233 1-runs of length   11   expected:    1220.9
     605 1-runs of length   12   expected:     610.5
     273 1-runs of length   13   expected:     305.2
     157 1-runs of length   14   expected:     152.6
      75 1-runs of length   15   expected:      76.3
      72 1-runs of length >=16   expected:      76.3
Chi square value = 40.965649   Number of degrees of freedom = 30
Percentage level of acceptance:  8.75 %
```

The test result does not indicate a deviation from random behaviour.

5 Evaluation of the NESSIE blockcipher RC6 in counter mode

The test descriptions are the same as in the previous section; hence they will be omitted.

5.1 The Frequency Test

```
Frequency Test for
NESSIE submission RC6 in COUNTER mode

Number of bits generated and ignored before starting to test: 0
Number of bits used for testing: 10000000
Block size: 1
sequencelength= 10000000 blocksize= 1
block: 0  count: 4997329
block: 1  count: 5002671
chisquare = 2.853696  nu= 1
Percentage Level of Acceptance:  9.12
```

The test result does not indicate a deviation from random behaviour.

```
Frequency Test for
NESSIE submission RC6 in COUNTER mode

Number of bits generated and ignored before starting to test: 0
Number of bits used for testing: 10000000
Block size: 2
sequencelength= 10000000 blocksize= 2
```

The test result does not indicate a deviation from random behaviour. block: 0 count: 1249985 block: 1 count: 1249980 block: 2 count: 1250756 block: 3 count: 1249279 chisquare = 0.873602 nu= 3 Percentage Level of Acceptance: 83.18

```
Frequency Test for
NESSIE submission RC6 in COUNTER mode

Number of bits generated and ignored before starting to test: 0
Number of bits used for testing: 10000000
Block size: 3
sequencelength= 10000000 blocksize= 3
```

The test result does not indicate a deviation from random behaviour. block: 0 count: 415980 block: 1 count: 416265 block: 2 count: 417162 block: 3 count: 416235 block: 4 count: 417082 block: 5 count: 417829 block: 6 count: 416968 block: 7 count: 415812 chisquare = 8.182359 nu= 7 Percentage Level of Acceptance: 31.68

```
Frequency Test for
NESSIE submission RC6 in COUNTER mode

Number of bits generated and ignored before starting to test: 0
Number of bits used for testing: 10000000
Block size: 4
sequencelength= 10000000 blocksize= 4
```

```
block: 0  count: 156307
block: 1  count: 155700
block: 2  count: 156127
block: 3  count: 155886
block: 4  count: 156963
block: 5  count: 156339
block: 6  count: 156079
block: 7  count: 156090
block: 8  count: 156347
block: 9  count: 156761
block: 10  count: 156324
block: 11  count: 156551
block: 12  count: 155991
block: 13  count: 155979
block: 14  count: 156560
block: 15  count: 155996
chisquare = 10.830400  nu= 15
Percentage Level of Acceptance:  76.45
```

The test result does not indicate a deviation from random behaviour.

```
Frequency Test for
NESSIE submission RC6 in COUNTER mode

Number of bits generated and ignored before starting to test: 0
Number of bits used for testing: 10000000
Block size: 5
sequencelength= 10000000 blocksize= 5
chisquare = 24.396640  nu= 31
Percentage Level of Acceptance:  79.40
```

The test result does not indicate a deviation from random behaviour.

```
Frequency Test for
NESSIE submission RC6 in COUNTER mode

Number of bits generated and ignored before starting to test: 0
Number of bits used for testing: 10000000
Block size: 6
sequencelength= 10000000 blocksize= 6
```

The test result does not indicate a deviation from random behaviour. chisquare = 76.610351 nu= 63 Percentage Level of Acceptance: 11.64

```
Frequency Test for
NESSIE submission RC6 in COUNTER mode

Number of bits generated and ignored before starting to test: 0
Number of bits used for testing: 10000000
Block size: 7
sequencelength= 10000000 blocksize= 7
chisquare = 126.261518  nu= 127
Percentage Level of Acceptance:  50.18
```

The test result does not indicate a deviation from random behaviour.

```
Frequency Test for
NESSIE submission RC6 in COUNTER mode

Number of bits generated and ignored before starting to test: 0
Number of bits used for testing: 10000000
Block size: 8
sequencelength= 10000000 blocksize= 8
chisquare = 239.324160  nu= 255
Percentage Level of Acceptance:  75.15
```

The test result does not indicate a deviation from random behaviour.

```
Frequency Test for
NESSIE submission RC6 in COUNTER mode

Number of bits generated and ignored before starting to test: 0
Number of bits used for testing: 10000000
Block size: 12
sequencelength= 10000000 blocksize= 12
chisquare = 4289.683235  nu= 4095
Percentage Level of Acceptance:  1.68
```

This percentage level of acceptance is too low. Therefore we have repeated the test:

```
Frequency Test for
NESSIE submission RC6 in COUNTER mode

Number of bits generated and ignored before starting to test: 0
Number of bits used for testing: 10000000
Block size: 12
sequencelength= 10000000 blocksize= 12
chisquare = 4148.125418  nu= 4095
Percentage Level of Acceptance:  27.70
```

We conclude that the test results do not indicate a deviation from random behaviour.

```
Frequency Test for
NESSIE submission RC6 in COUNTER mode

Number of bits generated and ignored before starting to test: 0
Number of bits used for testing: 10000000
Block size: 16
sequencelength= 10000000 blocksize= 16
chisquare = 65509.735526  nu= 65535
Percentage Level of Acceptance:  52.71
```

The test result does not indicate a deviation from random behaviour.

5.2 The Collision Test

```
Collision Test for
NESSIE submission RC6 in COUNTER mode

Number of bits generated and ignored before starting to test: 0
Number of bits used for testing: 10000000
Block size: 24
# of blocks: 416666 blocksize: 24 collisions: 5133
```

So the test result does not indicate a deviation from random behaviour.

5.3 The Overlapping m-tuple Test

```
OVERLAPPING M-TUPLE TEST for
NESSIE submission RC6 in COUNTER mode

Sequencelength = 10000000 bits        Wordlength = 5 bits
m = 2

Shift     p
--------------
  0     49.65%
  1     82.48%
  2     73.07%
  3     93.46%
  4     72.79%

p gives the percentage level of acceptance of the chi-square test
This percentage level gives the probability that a truly random
sequence has a chi-square value greater than the chi-square value
observed in this execution of the test.
```

We conclude that the test results do not indicate a deviation from random behaviour.

5.4 The Gap Test

```
GAP TEST for
NESSIE submission RC6 in COUNTER mode

Sequencelength = 10000000 bits        Wordlength = 10 bits
Length of gaps between occurences in the range 256 - 768
Ideal distribution:       mean    variance
                         1.000       2.000
Real distribution:
Shift:             0       1       2       3       4       5       6       7       8       9
            ------------------------------------------------------------------------------
 mean:         0.999   1.000   1.001   1.000   0.999   0.999   0.998   1.003   1.002   0.997
 error:       -0.14%  -0.05%   0.05%  -0.03%  -0.08%  -0.07%  -0.19%   0.26%   0.19%  -0.34%
 variance:     1.993   2.001   1.990   2.003   2.001   2.006   2.010   2.005   1.996   1.994
 error:       -0.35%   0.04%  -0.48%   0.14%   0.05%   0.28%   0.52%   0.26%  -0.22%  -0.28%

    p=        44.94%  30.46%   9.22%  67.73%  54.64%  51.94%  12.49%  15.26%  41.25%  11.80%

p gives the percentage level of acceptance of the chi-square test
This percentage level gives the probability that a truly random
sequence has a chi-square value greater than the chi-square value
observed in this execution of the test.
```

We conclude that the test results do not indicate a deviation from random behaviour.

5.5 The Run Test

```
Run Test for
NESSIE submission RC6 in COUNTER mode

Number of bits generated and ignored before starting to test: 0
Number of bits used for testing: 10000000
Block size: 16
Maximal run length registered individually: 5
Total of 230134 runs
 115355 runs of length 1  expected: 115068.8
```

```
 76610 runs of length 2  expected: 76711.3
 28668 runs of length 3  expected: 28765.9
  7586 runs of length 4  expected: 7670.5
  1607 runs of length 5  expected: 1597.9
   308 runs of length 6 or more expected: 319.6
chisquare = 2.580280 nu = 5
Percentage level of acceptance 76.44
```

The test result does not indicate a deviation from random behaviour.

5.6 The Coupon Collector's Test

```
COUPON COLLECTOR'S TEST for
NESSIE submission RC6 in COUNTER mode

Sequencelength = 10000000 bits        Wordlength = 8 bits
Ideal distribution:       mean    variance
                       1567.8323   105979.0660
Real distribution:
The results are for cyclic shifts
Shift:                 0        1        2        3        4        5        6        7
             ------------------------------------------------------------------------
 mean:         1570.711 1560.380 1570.722 1563.165 1570.942 1564.040 1558.739 1563.519
 error:           0.18%   -0.48%    0.18%   -0.30%    0.20%   -0.24%   -0.58%   -0.28%
 variance:       105222   105869   107528   102580   108598   100159   100431    93655
 error:           -0.71%   -0.10%    1.46%   -3.21%    2.47%   -5.49%   -5.23%  -11.63%

    p=             4.92%   49.81%   95.91%   43.33%   87.49%   87.64%   55.74%   97.84%

p gives the percentage level of acceptance of the chi-square test
This percentage level gives the probability that a truly random
sequence has a chi-square value greater than the chi-square value
observed in this execution of the test.
```

The percentage level of acceptance of shift 7 was too good, therefore the test has been repeated:

```
COUPON COLLECTOR'S TEST for
NESSIE submission RC6 in COUNTER mode

Sequencelength = 10000000 bits        Wordlength = 8 bits
Ideal distribution:       mean    variance
                       1567.8323   105979.0660
Real distribution:
The results are for cyclic shifts
Shift:                 0        1        2        3        4        5        6        7
             ------------------------------------------------------------------------
 mean:         1560.005 1569.823 1589.380 1549.600 1559.311 1580.949 1541.842 1556.034
 error:           -0.50%    0.13%    1.37%   -1.16%   -0.54%    0.84%   -1.66%   -0.75%
 variance:       100783   105888   111143    97174   107756   105799   105796    95811
 error:           -4.90%   -0.09%    4.87%   -8.31%    1.68%   -0.17%   -0.17%   -9.59%

    p=             81.40%   70.00%   60.01%   21.13%   63.31%   66.97%   32.68%   46.42%

p gives the percentage level of acceptance of the chi-square test
This percentage level gives the probability that a truly random
sequence has a chi-square value greater than the chi-square value
observed in this execution of the test.
```

Therefore we conclude that the test results do not indicate a deviation from random behaviour.

5.7 The Universal Maurer Test

```
Maurer Test for
NESSIE submission RC6 in COUNTER mode

Number of bits generated and ignored before starting to test: 0
```

```
Number of bits used for testing: 1000000
Block size: 8
Initial Blocks= 10000
blocks tested (including initial blocks): 125000
Maurer Test Value: 7.184836
```

For an ideal random number generator, the probability to obtain a Maurer test value of 7.184836 or less is 64.34%. So the test result does not indicate a deviation from random behaviour.

5.8 The Poker Test

```
POKER TEST for
NESSIE submission RC6 in COUNTER mode

Sequencelength = 9999360 bits        Wordlength = 8 bits
Elements in a k-tuple: 128
Ideal distribution:       mean    variance
                        100.8801     13.9923
Real distribution:
Shift:             0       1       2       3       4       5       6       7
          ------------------------------------------------------------------
 mean:       100.825 100.828 100.782 100.847 100.844 100.857 100.894 100.915
 error:        -0.05%  -0.05%  -0.10%  -0.03%  -0.04%  -0.02%   0.01%   0.03%
 variance:    14.155  14.048  14.035  13.939  14.110  14.174  13.825  14.164
 error:         1.16%   0.40%   0.30%  -0.38%   0.84%   1.30%  -1.20%   1.23%

    p=         35.00%   3.49%  46.86%  86.54%  93.39%  35.81%  73.70%   6.07%

p gives the percentage level of acceptance of the chi-square test
This percentage level gives the probability that a truly random
sequence has a chi-square value greater than the chi-square value
observed in this execution of the test.
```

We conclude that the test results do not indicate a deviation from random behaviour.

5.9 The Fast Spectral Test

```
Fast Spectral Test for
NESSIE submission RC6 in COUNTER mode


The results are:

The statistic D(4) = -2.242129E-01; percentage level of significance:  41.1%
The statistic D(6) = -2.226682E-01; percentage level of significance:  41.2%
This percentage level gives the probability that a truly random
sequence has a chi-square value greater than the chi-square value
observed in this execution of the test.
```

We conclude that the test results do not indicate a deviation from random behaviour.

5.10 The Correlation Test

```
Correlation Test for
NESSIE submission RC6 in COUNTER mode

Number of bits generated and ignored before starting to test: 0
```

```
Number of bits used for testing: 1000000
Printlevel: 0.000010
shift:0 equal: 1000000 probability: 1.0000000   0e+00
shift:38910 equal: 497762 probability: 0.0000038   4e-06
shift:101626 equal: 502183 probability: 0.9999937   6e-06
shift:243302 equal: 497740 probability: 0.0000031   3e-06
shift:246341 equal: 502218 probability: 0.9999954   5e-06
shift:308967 equal: 502168 probability: 0.9999928   7e-06
shift:348202 equal: 497864 probability: 0.0000097   1e-05
shift:425860 equal: 497750 probability: 0.0000034   3e-06
shift:427017 equal: 497775 probability: 0.0000043   4e-06
shift:488349 equal: 502187 probability: 0.9999939   6e-06
shift:565297 equal: 497819 probability: 0.0000065   6e-06
shift:648232 equal: 497863 probability: 0.0000096   1e-05
shift:707132 equal: 497838 probability: 0.0000077   8e-06
shift:712236 equal: 502296 probability: 0.9999978   2e-06
shift:720840 equal: 497554 probability: 0.0000005   5e-07
shift:736036 equal: 497842 probability: 0.0000080   8e-06
shift:739314 equal: 502208 probability: 0.9999950   5e-06
shift:795130 equal: 497763 probability: 0.0000039   4e-06
shift:861007 equal: 502150 probability: 0.9999915   9e-06
shift:953929 equal: 502233 probability: 0.9999960   4e-06
shift:972269 equal: 502150 probability: 0.9999915   9e-06
shift:972361 equal: 497787 probability: 0.0000048   5e-06
```

The test result does not indicate a deviation from random behaviour.

5.11 The Rank Test

```
Rank test for
NESSIE submission RC6 in COUNTER mode

Number of bits generated and ignored before starting to test: 0
Number of bits used for testing: 10000000
Order of the matrix: 16
Number of ranks counted individually: 3
 11081 matrices with rank 16, expected: 11280.8
 22817 matrices with rank 15, expected: 22561.3
 4973 matrices with rank 14, expected: 5013.5
 191 matrices with rank 13 or less, expected: 206.4
chisquare = 7.919180 nu = 3
Percentage level of acceptance 4.77
```

The test result does not indicate a deviation from random behaviour.

5.12 The Linear Complexity Test

```
Linear Complexity Test for
NESSIE submission RC6 in COUNTER mode

-------------------- Final results ------------------

N= 100000      L= 50000      X= 1

N    is the number of input bits.
```

```
L    is the linear complexity.

X-1  is the number of bits which has been treated since
     the last change of linear complexity.

------------------------- End -----------------------
The linear complexity profile:


Jumps in the linear complexity profile:


ssl =  99999.000    ssqsl = 500867.000
msl =      4.003    varsl =      4.025


ssh =  50001.000    ssqsh = 149861.000
msh =      2.002    varsh =      1.993


  ssl   is the sum of the sl's
  ssqsl is the sum of the squares of the sl's
  msl   is the mean of the sl's
  varsl is the variance of the sl's
  The number of jumps used in the calculation of msl and varsl is:  24979
  The first sl is not counted because it is 0

  ssh   is the sum of the sh's
  ssqsh is the sum of the squares of the sh's
  msh   is the mean of the sh's
  varsh is the variance of the sh's
  The number of jumps used in the calculation of msh and varsh is:  24980
maximal step-height 16.000000


  sl  is the steplength
  sh  is the stepheigth
  nj  is the number of jumps
```

The test result does not indicate a deviation from random behaviour.

5.13 The Maximum Order Complexity Test

```
Maximum Order Complexity (MOC) Test for
NESSIE submission RC6 in COUNTER mode


The changes in the MOC profile:
    2    1   ( 2.00)
    4    2   ( 4.00)
    7    4   ( 5.61)
   15    6   ( 7.81)
   19    7   ( 8.50)
   38   10   (10.50)
   76   15   (12.50)
  212   17   (15.46)
```

```
  452   19   (17.64)
  948   20   (19.78)
 2284   24   (22.31)
 7141   25   (25.60)
17965   26   (28.27)
33591   31   (30.07)
129762   34   (33.97)
266880   35   (36.05)
395427   38   (37.19)


The number of inputcharacters: 1000000
The number of nodes: 1999962
The number of edges: 2755638

The MOC is: 38
```

For an ideal random number generator, the probability to obtain a MOC of 38 or less is 40.78%. So the test result does not indicate a deviation from random behaviour.

5.14 The Ziv Lempel Complexity Test

```
NESSIE submission RC6 in COUNTER mode
1000000 input bits of the input file have been handled.
The Ziv Lempel complexity equals 50815.
((1000000 / log2(1000000)) = 50171.665944)

A sequence of length n is considered to be a good pseudo-random
sequence if its Ziv Lempel complexity is greater than n/log2(n).

The maximum length of a component in the history equals 35.
(log2(1000000) = 19.931569)
```

For an ideal random number generator, the probability to have a Ziv Lempel complexity of 50815 or lower is 96.34%. So the test result does not indicate a deviation from random behaviour.

5.15 The Dyadic Complexity Test

```
2-adic Complexity Test for
NESSIE submission RC6 in COUNTER mode

Number of bits generated and ignored before starting to test: 0
Number of bits used for testing: 10000
sequencelength= 10000
2-adic complexity=  4999.29916
```

For an ideal random number generator, the probability to obtain a dyadic complexity of 4999.29916 or less is 31.39%. So the test result does not indicate a deviation from random behaviour.

5.16 The Percolation Test

```
PERCOLATION TEST for
NESSIE submission RC6 in COUNTER mode
```

```
Dimensions of the forest lattice: 3
Size in dimension 1: 100
Size in dimension 2: 100
Size in dimension 3: 100
Forest fire executed in a triangular lattice.
Probability for lighting the reachable neighbours (in percent): 100

Result(s) of the single fitting in of 1 forest fire(s):
Percentage level(s) of acceptance:
24.97%
```

The test result does not indicate a deviation from random behaviour.

5.17 The Constant Runs Test

```
Constant Runs Test for
NESSIE submission RC6 in COUNTER mode

Number of bits generated and ignored before starting to test: 0
Number of bits used for testing: 10000000
Maximal run length registered individually: 15
Total of 2500625 0-runs
 1251022 0-runs of length    1   expected: 1250312.5
  624997 0-runs of length    2   expected:  625156.2
  312132 0-runs of length    3   expected:  312578.1
  155903 0-runs of length    4   expected:  156289.1
   78470 0-runs of length    5   expected:   78144.5
   38792 0-runs of length    6   expected:   39072.3
   19573 0-runs of length    7   expected:   19536.1
    9905 0-runs of length    8   expected:    9768.1
    4960 0-runs of length    9   expected:    4884.0
    2473 0-runs of length   10   expected:    2442.0
    1197 0-runs of length   11   expected:    1221.0
     589 0-runs of length   12   expected:     610.5
     314 0-runs of length   13   expected:     305.3
     158 0-runs of length   14   expected:     152.6
      71 0-runs of length   15   expected:      76.3
      69 0-runs of length >=16   expected:      76.3
Total of 2500625 1-runs
 1250408 1-runs of length    1   expected: 1250312.5
  625894 1-runs of length    2   expected:  625156.2
  311772 1-runs of length    3   expected:  312578.1
  156343 1-runs of length    4   expected:  156289.1
   78128 1-runs of length    5   expected:   78144.5
   39156 1-runs of length    6   expected:   39072.3
   19711 1-runs of length    7   expected:   19536.1
    9544 1-runs of length    8   expected:    9768.1
    4874 1-runs of length    9   expected:    4884.0
    2319 1-runs of length   10   expected:    2442.0
    1273 1-runs of length   11   expected:    1221.0
     604 1-runs of length   12   expected:     610.5
     297 1-runs of length   13   expected:     305.3
     151 1-runs of length   14   expected:     152.6
```

```
      77 1-runs of length   15   expected:      76.3
      74 1-runs of length >=16   expected:      76.3
Chi square value = 30.384350   Number of degrees of freedom = 30
Percentage level of acceptance: 44.61 %
```

The test result does not indicate a deviation from random behaviour.

6 Conclusion

The statistical test results for the NESSIE submission RC6 do not indicate a deviation from random behaviour.

References

[Bol90] Jean-Paul Boly, *Dependence test*, Tech. report, RIPE Tools for NESSIE Tools-P10-7, 1990.

[Dic91] Markus Dichtl, *The linear factors test*, Tech. report, RIPE Tools for NESSIE Tools-S24-4, 1991.

[Dic01] Markus Dichtl, *The dyadic complexity test*, Tech. report, NES/DOC/SAG/WP2/011/1, 2001.

[KG97] A. Klapper and M. Goresky, *Feedback shift registers, 2-adic span, and combiners with memory*, Journal of Cryptology **10** (1997), no. 2, 111–147.

[Sch00] Sarah Schardt, *The percolation test*, Tech. report, NES/DOC/SAG/WP2/012/1, 2000.

[Sch01a] Marcus Schafheutle, *An introduction to the statistical evaluation of NESSIE blockcipher submissions*, Tech. report, NES/DOC/SAG/WP2/032/1, 2001.

[Sch01b] Marcus Schafheutle, *Software interface layer for calling RIPE streamcipher tests for NESSIE blockcipher submissions applying OFB and counter mode*, Tech. report, NES/DOC/SAG/WP2/030/1, 2001.

[Ser00] Pascale Serf, *The degrees of completeness, of avalanche effect, and of strict avalanche criterion for mars, rc6, rijndael, serpent, and twofish with reduced number of rounds*, Tech. report, NES/DOC/SAG/WP3/003/1, 2000.

[Ser01] Pascale Serf, *The constant runs test*, Tech. report, NES/DOC/SAG/WP2/014/1, 2001.