Internet Engineering Task Force (IETF)
Request for Comments: 6229
Category: Informational
ISSN: 2070-1721

J. Strombergson
SecWorks Sweden AB
S. Josefsson
Simon Josefsson Datakonsult AB

May 2011

# Test Vectors for the Stream Cipher RC4

## Abstract

This document contains test vectors for the stream cipher RC4.

## Status of This Memo

This document is not an Internet Standards Track specification; it is published for informational purposes.

This document is a product of the Internet Engineering Task Force (IETF). It represents the consensus of the IETF community. It has received public review and has been approved for publication by the Internet Engineering Steering Group (IESG). Not all documents approved by the IESG are a candidate for any level of Internet Standard; see Section 2 of RFC 5741.

Information about the current status of this document, any errata, and how to provide feedback on it may be obtained at http://www.rfc-editor.org/info/rfc6229.

Table of Contents



## 1. Introduction

The RC4 [RC4] algorithm is a widely used stream cipher. Test vectors for algorithms are useful for implementers. The RC4 cipher can use different key lengths. Advances in crypto-analysis [FMcG] [MANTIN01] [MIRONOV] [MANTIN05] suggest that initial parts of the stream output need to be discarded. This document contains several test vectors for different key lengths and for different offsets in the stream.

Motivation for this document arose from the implementation of [RFC4345].

The test vectors provided in this document have been collected by generating RC4 keystream output from three separate implementations and comparing the streams. The RC4 implementations used are Libgcrypt 1.4.4 [LIBGCRYPT], Nettle 2.0 [NETTLE], and a custom implementation.

The document contains test vectors for two different keys:

Key 1: The key byte index (starting on one), that is: 0x01, 0x02, 0x03, 0x04,...

Key 2: Generated by hashing the string "Internet Engineering Task Force" with the SHA-256 [SHS] [RFC4634] hash function, using the following command:

```
$ echo -n "Internet Engineering Task Force" | sha256sum
1ada31d5cf688221c109163908ebe51debb46227c6cc8b37641910833222772a
```

The generated string has also been verified using the SHA-256 hash function implementation in OpenSSL (versions 0.9.8l and 1.0.0a) [OPENSSL].

The digest that is generated is then truncated to the appropriate length, keeping the Least Significant Bit (LSB) part of the digest as the key.

The key lengths used in this document are 40, 56, 64, 80, 128, 192, and 256 bits, respectively. The stream offsets used in this document are 0, 256, 512, 768, 1024, 1536, 2048, 3072, and 4096 bytes, respectively. Offset 1536 corresponds to recommendations in [RFC4345]. The offsets 768 and 3072 correspond to recommendations in [SANS].

## 2. Test Vectors for RC4

Key length: 40 bits.
key: 0x0102030405

| | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| DEC | 0 | HEX | 0: | b2 | 39 | 63 | 05 | f0 | 3d | c0 | 27 | cc | c3 | 52 | 4a | 0a | 11 | 18 | a8 |
| DEC | 16 | HEX | 10: | 69 | 82 | 94 | 4f | 18 | fc | 82 | d5 | 89 | c4 | 03 | a4 | 7a | 0d | 09 | 19 |
| DEC | 240 | HEX | f0: | 28 | cb | 11 | 32 | c9 | 6c | e2 | 86 | 42 | 1d | ca | ad | b8 | b6 | 9e | ae |
| DEC | 256 | HEX | 100: | 1c | fc | f6 | 2b | 03 | ed | db | 64 | 1d | 77 | df | cf | 7f | 8d | 8c | 93 |
| DEC | 496 | HEX | 1f0: | 42 | b7 | d0 | cd | d9 | 18 | a8 | a3 | 3d | d5 | 17 | 81 | c8 | 1f | 40 | 41 |
| DEC | 512 | HEX | 200: | 64 | 59 | 84 | 44 | 32 | a7 | da | 92 | 3c | fb | 3e | b4 | 98 | 06 | 61 | f6 |
| DEC | 752 | HEX | 2f0: | ec | 10 | 32 | 7b | de | 2b | ee | fd | 18 | f9 | 27 | 76 | 80 | 45 | 7e | 22 |
| DEC | 768 | HEX | 300: | eb | 62 | 63 | 8d | 4f | 0b | a1 | fe | 9f | ca | 20 | e0 | 5b | f8 | ff | 2b |
| DEC | 1008 | HEX | 3f0: | 45 | 12 | 90 | 48 | e6 | a0 | ed | 0b | 56 | b4 | 90 | 33 | 8f | 07 | 8d | a5 |
| DEC | 1024 | HEX | 400: | 30 | ab | bc | c7 | c2 | 0b | 01 | 60 | 9f | 23 | ee | 2d | 5f | 6b | b7 | df |
| DEC | 1520 | HEX | 5f0: | 32 | 94 | f7 | 44 | d8 | f9 | 79 | 05 | 07 | e7 | 0f | 62 | e5 | bb | ce | ea |
| DEC | 1536 | HEX | 600: | d8 | 72 | 9d | b4 | 18 | 82 | 25 | 9b | ee | 4f | 82 | 53 | 25 | f5 | a1 | 30 |
| DEC | 2032 | HEX | 7f0: | 1e | b1 | 4a | 0c | 13 | b3 | bf | 47 | fa | 2a | 0b | a9 | 3a | d4 | 5b | 8b |
| DEC | 2048 | HEX | 800: | cc | 58 | 2f | 8b | a9 | f2 | 65 | e2 | b1 | be | 91 | 12 | e9 | 75 | d2 | d7 |
| DEC | 3056 | HEX | bf0: | f2 | e3 | 0f | 9b | d1 | 02 | ec | bf | 75 | aa | ad | e9 | bc | 35 | c4 | 3c |
| DEC | 3072 | HEX | c00: | ec | 0e | 11 | c4 | 79 | dc | 32 | 9d | c8 | da | 79 | 68 | fe | 96 | 56 | 81 |
| DEC | 4080 | HEX | ff0: | 06 | 83 | 26 | a2 | 11 | 84 | 16 | d2 | 1f | 9d | 04 | b2 | cd | 1c | a0 | 50 |
| DEC | 4096 | HEX | 1000: | ff | 25 | b5 | 89 | 95 | 99 | 67 | 07 | e5 | 1f | bd | f0 | 8b | 34 | d8 | 75 |

Key length: 56 bits.
key: 0x01020304050607

```
DEC    0 HEX    0:  29 3f 02 d4  7f 37 c9 b6   33 f2 af 52  85 fe b4 6b
DEC   16 HEX   10:  e6 20 f1 39  0d 19 bd 84   e2 e0 fd 75  20 31 af c1
DEC  240 HEX   f0:  91 4f 02 53  1c 92 18 81   0d f6 0f 67  e3 38 15 4c
DEC  256 HEX  100:  d0 fd b5 83  07 3c e8 5a   b8 39 17 74  0e c0 11 d5
DEC  496 HEX  1f0:  75 f8 14 11  e8 71 cf fa   70 b9 0c 74  c5 92 e4 54
DEC  512 HEX  200:  0b b8 72 02  93 8d ad 60   9e 87 a5 a1  b0 79 e5 e4
DEC  752 HEX  2f0:  c2 91 12 46  b6 12 e7 e7   b9 03 df ed  a1 da d8 66
DEC  768 HEX  300:  32 82 8f 91  50 2b 62 91   36 8d e8 08  1d e3 6f c2
DEC 1008 HEX  3f0:  f3 b9 a7 e3  b2 97 bf 9a   d8 04 51 2f  90 63 ef f1
DEC 1024 HEX  400:  8e cb 67 a9  ba 1f 55 a5   a0 67 e2 b0  26 a3 67 6f
DEC 1520 HEX  5f0:  d2 aa 90 2b  d4 2d 0d 7c   fd 34 0c d4  58 10 52 9f
DEC 1536 HEX  600:  78 b2 72 c9  6e 42 ea b4   c6 0b d9 14  e3 9d 06 e3
DEC 2032 HEX  7f0:  f4 33 2f d3  1a 07 93 96   ee 3c ee 3f  2a 4f f0 49
DEC 2048 HEX  800:  05 45 97 81  d4 1f da 7f   30 c1 be 7e  12 46 c6 23
DEC 3056 HEX  bf0:  ad fd 38 68  b8 e5 14 85   d5 e6 10 01  7e 3d d6 09
DEC 3072 HEX  c00:  ad 26 58 1c  0c 5b e4 5f   4c ea 01 db  2f 38 05 d5
DEC 4080 HEX  ff0:  f3 17 2c ef  fc 3b 3d 99   7c 85 cc d5  af 1a 95 0c
DEC 4096 HEX 1000:  e7 4b 0b 97  31 22 7f d3   7c 0e c0 8a  47 dd d8 b8
```

Key length: 64 bits.
key: 0x0102030405060708

```
DEC    0 HEX    0:  97 ab 8a 1b  f0 af b9 61   32 f2 f6 72  58 da 15 a8
DEC   16 HEX   10:  82 63 ef db  45 c4 a1 86   84 ef 87 e6  b1 9e 5b 09
DEC  240 HEX   f0:  96 36 eb c9  84 19 26 f4   f7 d1 f3 62  bd df 6e 18
DEC  256 HEX  100:  d0 a9 90 ff  2c 05 fe f5   b9 03 73 c9  ff 4b 87 0a
DEC  496 HEX  1f0:  73 23 9f 1d  b7 f4 1d 80   b6 43 c0 c5  25 18 ec 63
DEC  512 HEX  200:  16 3b 31 99  23 a6 bd b4   52 7c 62 61  26 70 3c 0f
DEC  752 HEX  2f0:  49 d6 c8 af  0f 97 14 4a   87 df 21 d9  14 72 f9 66
DEC  768 HEX  300:  44 17 3a 10  3b 66 16 c5   d5 ad 1c ee  40 c8 63 d0
DEC 1008 HEX  3f0:  27 3c 9c 4b  27 f3 22 e4   e7 16 ef 53  a4 7d e7 a4
DEC 1024 HEX  400:  c6 d0 e7 b2  26 25 9f a9   02 34 90 b2  61 67 ad 1d
DEC 1520 HEX  5f0:  1f e8 98 67  13 f0 7c 3d   9a e1 c1 63  ff 8c f9 d3
DEC 1536 HEX  600:  83 69 e1 a9  65 61 0b e8   87 fb d0 c7  91 62 aa fb
DEC 2032 HEX  7f0:  0a 01 27 ab  b4 44 84 b9   fb ef 5a bc  ae 1b 57 9f
DEC 2048 HEX  800:  c2 cd ad c6  40 2e 8e e8   66 e1 f3 7b  db 47 e4 2c
DEC 3056 HEX  bf0:  26 b5 1e a3  7d f8 e1 d6   f7 6f c3 b6  6a 74 29 b3
DEC 3072 HEX  c00:  bc 76 83 20  5d 4f 44 3d   c1 f2 9d da  33 15 c8 7b
DEC 4080 HEX  ff0:  d5 fa 5a 34  69 d2 9a aa   f8 3d 23 58  9d b8 c8 5b
DEC 4096 HEX 1000:  3f b4 6e 2c  8f 0f 06 8e   dc e8 cd cd  7d fc 58 62
```

Key length: 80 bits.
key: 0x0102030405060708090a

| | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| DEC | 0 | HEX | 0: | ed | e3 | b0 | 46 | 43 | e5 | 86 | cc | 90 | 7d | c2 | 18 | 51 | 70 | 99 | 02 |
| DEC | 16 | HEX | 10: | 03 | 51 | 6b | a7 | 8f | 41 | 3b | eb | 22 | 3a | a5 | d4 | d2 | df | 67 | 11 |
| DEC | 240 | HEX | f0: | 3c | fd | 6c | b5 | 8e | e0 | fd | de | 64 | 01 | 76 | ad | 00 | 00 | 04 | 4d |
| DEC | 256 | HEX | 100: | 48 | 53 | 2b | 21 | fb | 60 | 79 | c9 | 11 | 4c | 0f | fd | 9c | 04 | a1 | ad |
| DEC | 496 | HEX | 1f0: | 3e | 8c | ea | 98 | 01 | 71 | 09 | 97 | 90 | 84 | b1 | ef | 92 | f9 | 9d | 86 |
| DEC | 512 | HEX | 200: | e2 | 0f | b4 | 9b | db | 33 | 7e | e4 | 8b | 8d | 8d | c0 | f4 | af | ef | fe |
| DEC | 752 | HEX | 2f0: | 5c | 25 | 21 | ea | cd | 79 | 66 | f1 | 5e | 05 | 65 | 44 | be | a0 | d3 | 15 |
| DEC | 768 | HEX | 300: | e0 | 67 | a7 | 03 | 19 | 31 | a2 | 46 | a6 | c3 | 87 | 5d | 2f | 67 | 8a | cb |
| DEC | 1008 | HEX | 3f0: | a6 | 4f | 70 | af | 88 | ae | 56 | b6 | f8 | 75 | 81 | c0 | e2 | 3e | 6b | 08 |
| DEC | 1024 | HEX | 400: | f4 | 49 | 03 | 1d | e3 | 12 | 81 | 4e | c6 | f3 | 19 | 29 | 1f | 4a | 05 | 16 |
| DEC | 1520 | HEX | 5f0: | bd | ae | 85 | 92 | 4b | 3c | b1 | d0 | a2 | e3 | 3a | 30 | c6 | d7 | 95 | 99 |
| DEC | 1536 | HEX | 600: | 8a | 0f | ed | db | ac | 86 | 5a | 09 | bc | d1 | 27 | fb | 56 | 2e | d6 | 0a |
| DEC | 2032 | HEX | 7f0: | b5 | 5a | 0a | 5b | 51 | a1 | 2a | 8b | e3 | 48 | 99 | c3 | e0 | 47 | 51 | 1a |
| DEC | 2048 | HEX | 800: | d9 | a0 | 9c | ea | 3c | e7 | 5f | e3 | 96 | 98 | 07 | 03 | 17 | a7 | 13 | 39 |
| DEC | 3056 | HEX | bf0: | 55 | 22 | 25 | ed | 11 | 77 | f4 | 45 | 84 | ac | 8c | fa | 6c | 4e | b5 | fc |
| DEC | 3072 | HEX | c00: | 7e | 82 | cb | ab | fc | 95 | 38 | 1b | 08 | 09 | 98 | 44 | 21 | 29 | c2 | f8 |
| DEC | 4080 | HEX | ff0: | 1f | 13 | 5e | d1 | 4c | e6 | 0a | 91 | 36 | 9d | 23 | 22 | be | f2 | 5e | 3c |
| DEC | 4096 | HEX | 1000: | 08 | b6 | be | 45 | 12 | 4a | 43 | e2 | eb | 77 | 95 | 3f | 84 | dc | 85 | 53 |

Key length: 128 bits.
key: 0x0102030405060708090a0b0c0d0e0f10

| | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| DEC | 0 | HEX | 0: | 9a | c7 | cc | 9a | 60 | 9d | 1e | f7 | b2 | 93 | 28 | 99 | cd | e4 | 1b | 97 |
| DEC | 16 | HEX | 10: | 52 | 48 | c4 | 95 | 90 | 14 | 12 | 6a | 6e | 8a | 84 | f1 | 1d | 1a | 9e | 1c |
| DEC | 240 | HEX | f0: | 06 | 59 | 02 | e4 | b6 | 20 | f6 | cc | 36 | c8 | 58 | 9f | 66 | 43 | 2f | 2b |
| DEC | 256 | HEX | 100: | d3 | 9d | 56 | 6b | c6 | bc | e3 | 01 | 07 | 68 | 15 | 15 | 49 | f3 | 87 | 3f |
| DEC | 496 | HEX | 1f0: | b6 | d1 | e6 | c4 | a5 | e4 | 77 | 1c | ad | 79 | 53 | 8d | f2 | 95 | fb | 11 |
| DEC | 512 | HEX | 200: | c6 | 8c | 1d | 5c | 55 | 9a | 97 | 41 | 23 | df | 1d | bc | 52 | a4 | 3b | 89 |
| DEC | 752 | HEX | 2f0: | c5 | ec | f8 | 8d | e8 | 97 | fd | 57 | fe | d3 | 01 | 70 | 1b | 82 | a2 | 59 |
| DEC | 768 | HEX | 300: | ec | cb | e1 | 3d | e1 | fc | c9 | 1c | 11 | a0 | b2 | 6c | 0b | c8 | fa | 4d |
| DEC | 1008 | HEX | 3f0: | e7 | a7 | 25 | 74 | f8 | 78 | 2a | e2 | 6a | ab | cf | 9e | bc | d6 | 60 | 65 |
| DEC | 1024 | HEX | 400: | bd | f0 | 32 | 4e | 60 | 83 | dc | c6 | d3 | ce | dd | 3c | a8 | c5 | 3c | 16 |
| DEC | 1520 | HEX | 5f0: | b4 | 01 | 10 | c4 | 19 | 0b | 56 | 22 | a9 | 61 | 16 | b0 | 01 | 7e | d2 | 97 |
| DEC | 1536 | HEX | 600: | ff | a0 | b5 | 14 | 64 | 7e | c0 | 4f | 63 | 06 | b8 | 92 | ae | 66 | 11 | 81 |
| DEC | 2032 | HEX | 7f0: | d0 | 3d | 1b | c0 | 3c | d3 | 3d | 70 | df | f9 | fa | 5d | 71 | 96 | 3e | bd |
| DEC | 2048 | HEX | 800: | 8a | 44 | 12 | 64 | 11 | ea | a7 | 8b | d5 | 1e | 8d | 87 | a8 | 87 | 9b | f5 |
| DEC | 3056 | HEX | bf0: | fa | be | b7 | 60 | 28 | ad | e2 | d0 | e4 | 87 | 22 | e4 | 6c | 46 | 15 | a3 |
| DEC | 3072 | HEX | c00: | c0 | 5d | 88 | ab | d5 | 03 | 57 | f9 | 35 | a6 | 3c | 59 | ee | 53 | 76 | 23 |
| DEC | 4080 | HEX | ff0: | ff | 38 | 26 | 5c | 16 | 42 | c1 | ab | e8 | d3 | c2 | fe | 5e | 57 | 2b | f8 |
| DEC | 4096 | HEX | 1000: | a3 | 6a | 4c | 30 | 1a | e8 | ac | 13 | 61 | 0c | cb | c1 | 22 | 56 | ca | cc |

Key length: 192 bits.
key: 0x0102030405060708090a0b0c0d0e0f101112131415161718

| | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| DEC | 0 | HEX | 0: | 05 | 95 | e5 | 7f | e5 | f0 | bb | 3c | 70 | 6e | da | c8 | a4 | b2 | db | 11 |
| DEC | 16 | HEX | 10: | df | de | 31 | 34 | 4a | 1a | f7 | 69 | c7 | 4f | 07 | 0a | ee | 9e | 23 | 26 |
| DEC | 240 | HEX | f0: | b0 | 6b | 9b | 1e | 19 | 5d | 13 | d8 | f4 | a7 | 99 | 5c | 45 | 53 | ac | 05 |
| DEC | 256 | HEX | 100: | 6b | d2 | 37 | 8e | c3 | 41 | c9 | a4 | 2f | 37 | ba | 79 | f8 | 8a | 32 | ff |
| DEC | 496 | HEX | 1f0: | e7 | 0b | ce | 1d | f7 | 64 | 5a | db | 5d | 2c | 41 | 30 | 21 | 5c | 35 | 22 |
| DEC | 512 | HEX | 200: | 9a | 57 | 30 | c7 | fc | b4 | c9 | af | 51 | ff | da | 89 | c7 | f1 | ad | 22 |
| DEC | 752 | HEX | 2f0: | 04 | 85 | 05 | 5f | d4 | f6 | f0 | d9 | 63 | ef | 5a | b9 | a5 | 47 | 69 | 82 |
| DEC | 768 | HEX | 300: | 59 | 1f | c6 | 6b | cd | a1 | 0e | 45 | 2b | 03 | d4 | 55 | 1f | 6b | 62 | ac |
| DEC | 1008 | HEX | 3f0: | 27 | 53 | cc | 83 | 98 | 8a | fa | 3e | 16 | 88 | a1 | d3 | b4 | 2c | 9a | 02 |
| DEC | 1024 | HEX | 400: | 93 | 61 | 0d | 52 | 3d | 1d | 3f | 00 | 62 | b3 | c2 | a3 | bb | c7 | c7 | f0 |
| DEC | 1520 | HEX | 5f0: | 96 | c2 | 48 | 61 | 0a | ad | ed | fe | af | 89 | 78 | c0 | 3d | e8 | 20 | 5a |
| DEC | 1536 | HEX | 600: | 0e | 31 | 7b | 3d | 1c | 73 | b9 | e9 | a4 | 68 | 8f | 29 | 6d | 13 | 3a | 19 |
| DEC | 2032 | HEX | 7f0: | bd | f0 | e6 | c3 | cc | a5 | b5 | b9 | d5 | 33 | b6 | 9c | 56 | ad | a1 | 20 |
| DEC | 2048 | HEX | 800: | 88 | a2 | 18 | b6 | e2 | ec | e1 | e6 | 24 | 6d | 44 | c7 | 59 | d1 | 9b | 10 |
| DEC | 3056 | HEX | bf0: | 68 | 66 | 39 | 7e | 95 | c1 | 40 | 53 | 4f | 94 | 26 | 34 | 21 | 00 | 6e | 40 |
| DEC | 3072 | HEX | c00: | 32 | cb | 0a | 1e | 95 | 42 | c6 | b3 | b8 | b3 | 98 | ab | c3 | b0 | f1 | d5 |
| DEC | 4080 | HEX | ff0: | 29 | a0 | b8 | ae | d5 | 4a | 13 | 23 | 24 | c6 | 2e | 42 | 3f | 54 | b4 | c8 |
| DEC | 4096 | HEX | 1000: | 3c | b0 | f3 | b5 | 02 | 0a | 98 | b8 | 2a | f9 | fe | 15 | 44 | 84 | a1 | 68 |

Key length: 256 bits.
key: 0x0102030405060708090a0b0c0d0e0f101112131415161718191a1b1c1d1e1f20

| | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| DEC | 0 | HEX | 0: | ea | a6 | bd | 25 | 88 | 0b | f9 | 3d | 3f | 5d | 1e | 4c | a2 | 61 | 1d | 91 |
| DEC | 16 | HEX | 10: | cf | a4 | 5c | 9f | 7e | 71 | 4b | 54 | bd | fa | 80 | 02 | 7c | b1 | 43 | 80 |
| DEC | 240 | HEX | f0: | 11 | 4a | e3 | 44 | de | d7 | 1b | 35 | f2 | e6 | 0f | eb | ad | 72 | 7f | d8 |
| DEC | 256 | HEX | 100: | 02 | e1 | e7 | 05 | 6b | 0f | 62 | 39 | 00 | 49 | 64 | 22 | 94 | 3e | 97 | b6 |
| DEC | 496 | HEX | 1f0: | 91 | cb | 93 | c7 | 87 | 96 | 4e | 10 | d9 | 52 | 7d | 99 | 9c | 6f | 93 | 6b |
| DEC | 512 | HEX | 200: | 49 | b1 | 8b | 42 | f8 | e8 | 36 | 7c | be | b5 | ef | 10 | 4b | a1 | c7 | cd |
| DEC | 752 | HEX | 2f0: | 87 | 08 | 4b | 3b | a7 | 00 | ba | de | 95 | 56 | 10 | 67 | 27 | 45 | b3 | 74 |
| DEC | 768 | HEX | 300: | e7 | a7 | b9 | e9 | ec | 54 | 0d | 5f | f4 | 3b | db | 12 | 79 | 2d | 1b | 35 |
| DEC | 1008 | HEX | 3f0: | c7 | 99 | b5 | 96 | 73 | 8f | 6b | 01 | 8c | 76 | c7 | 4b | 17 | 59 | bd | 90 |
| DEC | 1024 | HEX | 400: | 7f | ec | 5b | fd | 9f | 9b | 89 | ce | 65 | 48 | 30 | 90 | 92 | d7 | e9 | 58 |
| DEC | 1520 | HEX | 5f0: | 40 | f2 | 50 | b2 | 6d | 1f | 09 | 6a | 4a | fd | 4c | 34 | 0a | 58 | 88 | 15 |
| DEC | 1536 | HEX | 600: | 3e | 34 | 13 | 5c | 79 | db | 01 | 02 | 00 | 76 | 76 | 51 | cf | 26 | 30 | 73 |
| DEC | 2032 | HEX | 7f0: | f6 | 56 | ab | cc | f8 | 8d | d8 | 27 | 02 | 7b | 2c | e9 | 17 | d4 | 64 | ec |
| DEC | 2048 | HEX | 800: | 18 | b6 | 25 | 03 | bf | bc | 07 | 7f | ba | bb | 98 | f2 | 0d | 98 | ab | 34 |
| DEC | 3056 | HEX | bf0: | 8a | ed | 95 | ee | 5b | 0d | cb | fb | ef | 4e | b2 | 1d | 3a | 3f | 52 | f9 |
| DEC | 3072 | HEX | c00: | 62 | 5a | 1a | b0 | 0e | e3 | 9a | 53 | 27 | 34 | 6b | dd | b0 | 1a | 9c | 18 |
| DEC | 4080 | HEX | ff0: | a1 | 3a | 7c | 79 | c7 | e1 | 19 | b5 | ab | 02 | 96 | ab | 28 | c3 | 00 | b9 |
| DEC | 4096 | HEX | 1000: | f3 | e4 | c0 | a2 | e0 | 2d | 1d | 01 | f7 | f0 | a7 | 46 | 18 | af | 2b | 48 |

Key length: 40 bits.
key: 0x833222772a

| | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| DEC | 0 | HEX | 0: | 80 | ad | 97 | bd | c9 | 73 | df | 8a | 2e | 87 | 9e | 92 | a4 | 97 | ef | da |
| DEC | 16 | HEX | 10: | 20 | f0 | 60 | c2 | f2 | e5 | 12 | 65 | 01 | d3 | d4 | fe | a1 | 0d | 5f | c0 |
| DEC | 240 | HEX | f0: | fa | a1 | 48 | e9 | 90 | 46 | 18 | 1f | ec | 6b | 20 | 85 | f3 | b2 | 0e | d9 |
| DEC | 256 | HEX | 100: | f0 | da | f5 | ba | b3 | d5 | 96 | 83 | 98 | 57 | 84 | 6f | 73 | fb | fe | 5a |
| DEC | 496 | HEX | 1f0: | 1c | 7e | 2f | c4 | 63 | 92 | 32 | fe | 29 | 75 | 84 | b2 | 96 | 99 | 6b | c8 |
| DEC | 512 | HEX | 200: | 3d | b9 | b2 | 49 | 40 | 6c | c8 | ed | ff | ac | 55 | cc | d3 | 22 | ba | 12 |
| DEC | 752 | HEX | 2f0: | e4 | f9 | f7 | e0 | 06 | 61 | 54 | bb | d1 | 25 | b7 | 45 | 56 | 9b | c8 | 97 |
| DEC | 768 | HEX | 300: | 75 | d5 | ef | 26 | 2b | 44 | c4 | 1a | 9c | f6 | 3a | e1 | 45 | 68 | e1 | b9 |
| DEC | 1008 | HEX | 3f0: | 6d | a4 | 53 | db | f8 | 1e | 82 | 33 | 4a | 3d | 88 | 66 | cb | 50 | a1 | e3 |
| DEC | 1024 | HEX | 400: | 78 | 28 | d0 | 74 | 11 | 9c | ab | 5c | 22 | b2 | 94 | d7 | a9 | bf | a0 | bb |
| DEC | 1520 | HEX | 5f0: | ad | b8 | 9c | ea | 9a | 15 | fb | e6 | 17 | 29 | 5b | d0 | 4b | 8c | a0 | 5c |
| DEC | 1536 | HEX | 600: | 62 | 51 | d8 | 7f | d4 | aa | ae | 9a | 7e | 4a | d5 | c2 | 17 | d3 | f3 | 00 |
| DEC | 2032 | HEX | 7f0: | e7 | 11 | 9b | d6 | dd | 9b | 22 | af | e8 | f8 | 95 | 85 | 43 | 28 | 81 | e2 |
| DEC | 2048 | HEX | 800: | 78 | 5b | 60 | fd | 7e | c4 | e9 | fc | b6 | 54 | 5f | 35 | 0d | 66 | 0f | ab |
| DEC | 3056 | HEX | bf0: | af | ec | c0 | 37 | fd | b7 | b0 | 83 | 8e | b3 | d7 | 0b | cd | 26 | 83 | 82 |
| DEC | 3072 | HEX | c00: | db | c1 | a7 | b4 | 9d | 57 | 35 | 8c | c9 | fa | 6d | 61 | d7 | 3b | 7c | f0 |
| DEC | 4080 | HEX | ff0: | 63 | 49 | d1 | 26 | a3 | 7a | fc | ba | 89 | 79 | 4f | 98 | 04 | 91 | 4f | dc |
| DEC | 4096 | HEX | 1000: | bf | 42 | c3 | 01 | 8c | 2f | 7c | 66 | bf | de | 52 | 49 | 75 | 76 | 81 | 15 |

Key length: 56 bits.
key: 0x1910833222772a

| | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| DEC | 0 | HEX | 0: | bc | 92 | 22 | db | d3 | 27 | 4d | 8f | c6 | 6d | 14 | cc | bd | a6 | 69 | 0b |
| DEC | 16 | HEX | 10: | 7a | e6 | 27 | 41 | 0c | 9a | 2b | e6 | 93 | df | 5b | b7 | 48 | 5a | 63 | e3 |
| DEC | 240 | HEX | f0: | 3f | 09 | 31 | aa | 03 | de | fb | 30 | 0f | 06 | 01 | 03 | 82 | 6f | 2a | 64 |
| DEC | 256 | HEX | 100: | be | aa | 9e | c8 | d5 | 9b | b6 | 81 | 29 | f3 | 02 | 7c | 96 | 36 | 11 | 81 |
| DEC | 496 | HEX | 1f0: | 74 | e0 | 4d | b4 | 6d | 28 | 64 | 8d | 7d | ee | 8a | 00 | 64 | b0 | 6c | fe |
| DEC | 512 | HEX | 200: | 9b | 5e | 81 | c6 | 2f | e0 | 23 | c5 | 5b | e4 | 2f | 87 | bb | f9 | 32 | b8 |
| DEC | 752 | HEX | 2f0: | ce | 17 | 8f | c1 | 82 | 6e | fe | cb | c1 | 82 | f5 | 79 | 99 | a4 | 61 | 40 |
| DEC | 768 | HEX | 300: | 8b | df | 55 | cd | 55 | 06 | 1c | 06 | db | a6 | be | 11 | de | 4a | 57 | 8a |
| DEC | 1008 | HEX | 3f0: | 62 | 6f | 5f | 4d | ce | 65 | 25 | 01 | f3 | 08 | 7d | 39 | c9 | 2c | c3 | 49 |
| DEC | 1024 | HEX | 400: | 42 | da | ac | 6a | 8f | 9a | b9 | a7 | fd | 13 | 7c | 60 | 37 | 82 | 56 | 82 |
| DEC | 1520 | HEX | 5f0: | cc | 03 | fd | b7 | 91 | 92 | a2 | 07 | 31 | 2f | 53 | f5 | d4 | dc | 33 | d9 |
| DEC | 1536 | HEX | 600: | f7 | 0f | 14 | 12 | 2a | 1c | 98 | a3 | 15 | 5d | 28 | b8 | a0 | a8 | a4 | 1d |
| DEC | 2032 | HEX | 7f0: | 2a | 3a | 30 | 7a | b2 | 70 | 8a | 9c | 00 | fe | 0b | 42 | f9 | c2 | d6 | a1 |
| DEC | 2048 | HEX | 800: | 86 | 26 | 17 | 62 | 7d | 22 | 61 | ea | b0 | b1 | 24 | 65 | 97 | ca | 0a | e9 |
| DEC | 3056 | HEX | bf0: | 55 | f8 | 77 | ce | 4f | 2e | 1d | db | bf | 8e | 13 | e2 | cd | e0 | fd | c8 |
| DEC | 3072 | HEX | c00: | 1b | 15 | 56 | cb | 93 | 5f | 17 | 33 | 37 | 70 | 5f | bb | 5d | 50 | 1f | c1 |
| DEC | 4080 | HEX | ff0: | ec | d0 | e9 | 66 | 02 | be | 7f | 8d | 50 | 92 | 81 | 6c | cc | f2 | c2 | e9 |
| DEC | 4096 | HEX | 1000: | 02 | 78 | 81 | fa | b4 | 99 | 3a | 1c | 26 | 20 | 24 | a9 | 4f | ff | 3f | 61 |

Key length: 64 bits.
key: 0x641910833222772a

| | | | | | | |
|---|---|---|---|---|---|---|
| DEC 0 HEX 0: | bb f6 09 de | 94 13 17 2d | 07 66 0c b6 | 80 71 69 26 |
| DEC 16 HEX 10: | 46 10 1a 6d | ab 43 11 5d | 6c 52 2b 4f | e9 36 04 a9 |
| DEC 240 HEX f0: | cb e1 ff f2 | 1c 96 f3 ee | f6 1e 8f e0 | 54 2c bd f0 |
| DEC 256 HEX 100: | 34 79 38 bf | fa 40 09 c5 | 12 cf b4 03 | 4b 0d d1 a7 |
| DEC 496 HEX 1f0: | 78 67 a7 86 | d0 0a 71 47 | 90 4d 76 dd | f1 e5 20 e3 |
| DEC 512 HEX 200: | 8d 3e 9e 1c | ae fc cc b3 | fb f8 d1 8f | 64 12 0b 32 |
| DEC 752 HEX 2f0: | 94 23 37 f8 | fd 76 f0 fa | e8 c5 2d 79 | 54 81 06 72 |
| DEC 768 HEX 300: | b8 54 8c 10 | f5 16 67 f6 | e6 0e 18 2f | a1 9b 30 f7 |
| DEC 1008 HEX 3f0: | 02 11 c7 c6 | 19 0c 9e fd | 12 37 c3 4c | 8f 2e 06 c4 |
| DEC 1024 HEX 400: | bd a6 4f 65 | 27 6d 2a ac | b8 f9 02 12 | 20 3a 80 8e |
| DEC 1520 HEX 5f0: | bd 38 20 f7 | 32 ff b5 3e | c1 93 e7 9d | 33 e2 7c 73 |
| DEC 1536 HEX 600: | d0 16 86 16 | 86 19 07 d4 | 82 e3 6c da | c8 cf 57 49 |
| DEC 2032 HEX 7f0: | 97 b0 f0 f2 | 24 b2 d2 31 | 71 14 80 8f | b0 3a f7 a0 |
| DEC 2048 HEX 800: | e5 96 16 e4 | 69 78 79 39 | a0 63 ce ea | 9a f9 56 d1 |
| DEC 3056 HEX bf0: | c4 7e 0d c1 | 66 09 19 c1 | 11 01 20 8f | 9e 69 aa 1f |
| DEC 3072 HEX c00: | 5a e4 f1 28 | 96 b8 37 9a | 2a ad 89 b5 | b5 53 d6 b0 |
| DEC 4080 HEX ff0: | 6b 6b 09 8d | 0c 29 3b c2 | 99 3d 80 bf | 05 18 b6 d9 |
| DEC 4096 HEX 1000: | 81 70 cc 3c | cd 92 a6 98 | 62 1b 93 9d | d3 8f e7 b9 |

Key length: 80 bits.
key: 0x8b37641910833222772a

| | | | | | | |
|---|---|---|---|---|---|---|
| DEC 0 HEX 0: | ab 65 c2 6e | dd b2 87 60 | 0d b2 fd a1 | 0d 1e 60 5c |
| DEC 16 HEX 10: | bb 75 90 10 | c2 96 58 f2 | c7 2d 93 a2 | d1 6d 29 30 |
| DEC 240 HEX f0: | b9 01 e8 03 | 6e d1 c3 83 | cd 3c 4c 4d | d0 a6 ab 05 |
| DEC 256 HEX 100: | 3d 25 ce 49 | 22 92 4c 55 | f0 64 94 33 | 53 d7 8a 6c |
| DEC 496 HEX 1f0: | 12 c1 aa 44 | bb f8 7e 75 | e6 11 f6 9b | 2c 38 f4 9b |
| DEC 512 HEX 200: | 28 f2 b3 43 | 4b 65 c0 98 | 77 47 00 44 | c6 ea 17 0d |
| DEC 752 HEX 2f0: | bd 9e f8 22 | de 52 88 19 | 61 34 cf 8a | f7 83 93 04 |
| DEC 768 HEX 300: | 67 55 9c 23 | f0 52 15 84 | 70 a2 96 f7 | 25 73 5a 32 |
| DEC 1008 HEX 3f0: | 8b ab 26 fb | c2 c1 2b 0f | 13 e2 ab 18 | 5e ab f2 41 |
| DEC 1024 HEX 400: | 31 18 5a 6d | 69 6f 0c fa | 9b 42 80 8b | 38 e1 32 a2 |
| DEC 1520 HEX 5f0: | 56 4d 3d ae | 18 3c 52 34 | c8 af 1e 51 | 06 1c 44 b5 |
| DEC 1536 HEX 600: | 3c 07 78 a7 | b5 f7 2d 3c | 23 a3 13 5c | 7d 67 b9 f4 |
| DEC 2032 HEX 7f0: | f3 43 69 89 | 0f cf 16 fb | 51 7d ca ae | 44 63 b2 dd |
| DEC 2048 HEX 800: | 02 f3 1c 81 | e8 20 07 31 | b8 99 b0 28 | e7 91 bf a7 |
| DEC 3056 HEX bf0: | 72 da 64 62 | 83 22 8c 14 | 30 08 53 70 | 17 95 61 6f |
| DEC 3072 HEX c00: | 4e 0a 8c 6f | 79 34 a7 88 | e2 26 5e 81 | d6 d0 c8 f4 |
| DEC 4080 HEX ff0: | 43 8d d5 ea | fe a0 11 1b | 6f 36 b4 b9 | 38 da 2a 68 |
| DEC 4096 HEX 1000: | 5f 6b fc 73 | 81 58 74 d9 | 71 00 f0 86 | 97 93 57 d8 |

Key length: 128 bits.
key: 0xebb46227c6cc8b37641910833222772a

| | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| DEC | 0 | HEX | 0: | 72 | 0c | 94 | b6 | 3e | df | 44 | e1 | 31 | d9 | 50 | ca | 21 | 1a | 5a | 30 |
| DEC | 16 | HEX | 10: | c3 | 66 | fd | ea | cf | 9c | a8 | 04 | 36 | be | 7c | 35 | 84 | 24 | d2 | 0b |
| DEC | 240 | HEX | f0: | b3 | 39 | 4a | 40 | aa | bf | 75 | cb | a4 | 22 | 82 | ef | 25 | a0 | 05 | 9f |
| DEC | 256 | HEX | 100: | 48 | 47 | d8 | 1d | a4 | 94 | 2d | bc | 24 | 9d | ef | c4 | 8c | 92 | 2b | 9f |
| DEC | 496 | HEX | 1f0: | 08 | 12 | 8c | 46 | 9f | 27 | 53 | 42 | ad | da | 20 | 2b | 2b | 58 | da | 95 |
| DEC | 512 | HEX | 200: | 97 | 0d | ac | ef | 40 | ad | 98 | 72 | 3b | ac | 5d | 69 | 55 | b8 | 17 | 61 |
| DEC | 752 | HEX | 2f0: | 3c | b8 | 99 | 93 | b0 | 7b | 0c | ed | 93 | de | 13 | d2 | a1 | 10 | 13 | ac |
| DEC | 768 | HEX | 300: | ef | 2d | 67 | 6f | 15 | 45 | c2 | c1 | 3d | c6 | 80 | a0 | 2f | 4a | db | fe |
| DEC | 1008 | HEX | 3f0: | b6 | 05 | 95 | 51 | 4f | 24 | bc | 9f | e5 | 22 | a6 | ca | d7 | 39 | 36 | 44 |
| DEC | 1024 | HEX | 400: | b5 | 15 | a8 | c5 | 01 | 17 | 54 | f5 | 90 | 03 | 05 | 8b | db | 81 | 51 | 4e |
| DEC | 1520 | HEX | 5f0: | 3c | 70 | 04 | 7e | 8c | bc | 03 | 8e | 3b | 98 | 20 | db | 60 | 1d | a4 | 95 |
| DEC | 1536 | HEX | 600: | 11 | 75 | da | 6e | e7 | 56 | de | 46 | a5 | 3e | 2b | 07 | 56 | 60 | b7 | 70 |
| DEC | 2032 | HEX | 7f0: | 00 | a5 | 42 | bb | a0 | 21 | 11 | cc | 2c | 65 | b3 | 8e | bd | ba | 58 | 7e |
| DEC | 2048 | HEX | 800: | 58 | 65 | fd | bb | 5b | 48 | 06 | 41 | 04 | e8 | 30 | b3 | 80 | f2 | ae | de |
| DEC | 3056 | HEX | bf0: | 34 | b2 | 1a | d2 | ad | 44 | e9 | 99 | db | 2d | 7f | 08 | 63 | f0 | d9 | b6 |
| DEC | 3072 | HEX | c00: | 84 | a9 | 21 | 8f | c3 | 6e | 8a | 5f | 2c | cf | be | ae | 53 | a2 | 7d | 25 |
| DEC | 4080 | HEX | ff0: | a2 | 22 | 1a | 11 | b8 | 33 | cc | b4 | 98 | a5 | 95 | 40 | f0 | 54 | 5f | 4a |
| DEC | 4096 | HEX | 1000: | 5b | be | b4 | 78 | 7d | 59 | e5 | 37 | 3f | db | ea | 6c | 6f | 75 | c2 | 9b |

Key length: 192 bits.
key: 0xc109163908ebe51debb46227c6cc8b37641910833222772a

| | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| DEC | 0 | HEX | 0: | 54 | b6 | 4e | 6b | 5a | 20 | b5 | e2 | ec | 84 | 59 | 3d | c7 | 98 | 9d | a7 |
| DEC | 16 | HEX | 10: | c1 | 35 | ee | e2 | 37 | a8 | 54 | 65 | ff | 97 | dc | 03 | 92 | 4f | 45 | ce |
| DEC | 240 | HEX | f0: | cf | cc | 92 | 2f | b4 | a1 | 4a | b4 | 5d | 61 | 75 | aa | bb | f2 | d2 | 01 |
| DEC | 256 | HEX | 100: | 83 | 7b | 87 | e2 | a4 | 46 | ad | 0e | f7 | 98 | ac | d0 | 2b | 94 | 12 | 4f |
| DEC | 496 | HEX | 1f0: | 17 | a6 | db | d6 | 64 | 92 | 6a | 06 | 36 | b3 | f4 | c3 | 7a | 4f | 46 | 94 |
| DEC | 512 | HEX | 200: | 4a | 5f | 9f | 26 | ae | ee | d4 | d4 | a2 | 5f | 63 | 2d | 30 | 52 | 33 | d9 |
| DEC | 752 | HEX | 2f0: | 80 | a3 | d0 | 1e | f0 | 0c | 8e | 9a | 42 | 09 | c1 | 7f | 4e | eb | 35 | 8c |
| DEC | 768 | HEX | 300: | d1 | 5e | 7d | 5f | fa | aa | bc | 02 | 07 | bf | 20 | 0a | 11 | 77 | 93 | a2 |
| DEC | 1008 | HEX | 3f0: | 34 | 96 | 82 | bf | 58 | 8e | aa | 52 | d0 | aa | 15 | 60 | 34 | 6a | ea | fa |
| DEC | 1024 | HEX | 400: | f5 | 85 | 4c | db | 76 | c8 | 89 | e3 | ad | 63 | 35 | 4e | 5f | 72 | 75 | e3 |
| DEC | 1520 | HEX | 5f0: | 53 | 2c | 7c | ec | cb | 39 | df | 32 | 36 | 31 | 84 | 05 | a4 | b1 | 27 | 9c |
| DEC | 1536 | HEX | 600: | ba | ef | e6 | d9 | ce | b6 | 51 | 84 | 22 | 60 | e0 | d1 | e0 | 5e | 3b | 90 |
| DEC | 2032 | HEX | 7f0: | e8 | 2d | 8c | 6d | b5 | 4e | 3c | 63 | 3f | 58 | 1c | 95 | 2b | a0 | 42 | 07 |
| DEC | 2048 | HEX | 800: | 4b | 16 | e5 | 0a | bd | 38 | 1b | d7 | 09 | 00 | a9 | cd | 9a | 62 | cb | 23 |
| DEC | 3056 | HEX | bf0: | 36 | 82 | ee | 33 | bd | 14 | 8b | d9 | f5 | 86 | 56 | cd | 8f | 30 | d9 | fb |
| DEC | 3072 | HEX | c00: | 1e | 5a | 0b | 84 | 75 | 04 | 5d | 9b | 20 | b2 | 62 | 86 | 24 | ed | fd | 9e |
| DEC | 4080 | HEX | ff0: | 63 | ed | d6 | 84 | fb | 82 | 62 | 82 | fe | 52 | 8f | 9c | 0e | 92 | 37 | bc |
| DEC | 4096 | HEX | 1000: | e4 | dd | 2e | 98 | d6 | 96 | 0f | ae | 0b | 43 | 54 | 54 | 56 | 74 | 33 | 91 |

```
 Key length: 256 bits.
 key: 0x1ada31d5cf688221c109163908ebe51debb46227c6cc8b37641910833222772a

 DEC    0 HEX    0:  dd 5b cb 00  18 e9 22 d4   94 75 9d 7c  39 5d 02 d3
 DEC   16 HEX   10:  c8 44 6f 8f  77 ab f7 37   68 53 53 eb  89 a1 c9 eb
 DEC  240 HEX   f0:  af 3e 30 f9  c0 95 04 59   38 15 15 75  c3 fb 90 98
 DEC  256 HEX  100:  f8 cb 62 74  db 99 b8 0b   1d 20 12 a9  8e d4 8f 0e
 DEC  496 HEX  1f0:  25 c3 00 5a  1c b8 5d e0   76 25 98 39  ab 71 98 ab
 DEC  512 HEX  200:  9d cb c1 83  e8 cb 99 4b   72 7b 75 be  31 80 76 9c
 DEC  752 HEX  2f0:  a1 d3 07 8d  fa 91 69 50   3e d9 d4 49  1d ee 4e b2
 DEC  768 HEX  300:  85 14 a5 49  58 58 09 6f   59 6e 4b cd  66 b1 06 65
 DEC 1008 HEX  3f0:  5f 40 d5 9e  c1 b0 3b 33   73 8e fa 60  b2 25 5d 31
 DEC 1024 HEX  400:  34 77 c7 f7  64 a4 1b ac   ef f9 0b f1  4f 92 b7 cc
 DEC 1520 HEX  5f0:  ac 4e 95 36  8d 99 b9 eb   78 b8 da 8f  81 ff a7 95
 DEC 1536 HEX  600:  8c 3c 13 f8  c2 38 8b b7   3f 38 57 6e  65 b7 c4 46
 DEC 2032 HEX  7f0:  13 c4 b9 c1  df b6 65 79   ed dd 8a 28  0b 9f 73 16
 DEC 2048 HEX  800:  dd d2 78 20  55 01 26 69   8e fa ad c6  4b 64 f6 6e
 DEC 3056 HEX  bf0:  f0 8f 2e 66  d2 8e d1 43   f3 a2 37 cf  9d e7 35 59
 DEC 3072 HEX  c00:  9e a3 6c 52  55 31 b8 80   ba 12 43 34  f5 7b 0b 70
 DEC 4080 HEX  ff0:  d5 a3 9e 3d  fc c5 02 80   ba c4 a6 b5  aa 0d ca 7d
 DEC 4096 HEX 1000:  37 0b 1c 1f  e6 55 91 6d   97 fd 0d 47  ca 1d 72 b8
```

## 3. Security Considerations

The RC4 algorithm does not meet the basic criteria required for an encryption algorithm, as its output is distinguishable from random. The use of RC4 continues to be recommended against; in particular, its use in new specifications is discouraged. This note is intended only to aid the interoperability of existing specifications that make use of RC4.

## 4. Copying Conditions

This document is intended to be considered a Code Component, and is thus effectively available under the Simplified BSD License.

## 5. References

### 5.1. Normative References

[RC4] Schneier, B., "Applied Cryptography: Protocols, Algorithms, and Source Code in C", Second Edition, John Wiley and Sons, New York, NY, 1996.

### 5.2. Informative References

[RFC4345] Harris, B., "Improved Arcfour Modes for the Secure Shell (SSH) Transport Layer Protocol", RFC 4345, January 2006.

[RFC4634] Eastlake 3rd, D. and T. Hansen, "US Secure Hash Algorithms (SHA and HMAC-SHA)", RFC 4634, July 2006.

[FMcG] Fluhrer, S. and D. McGrew, "Statistical Analysis of the Alleged RC4 Keystream Generator", <http://www.mindspring.com/~dmcgrew/rc4-03.pdf>.

[LIBGCRYPT] Koch, W., "Libgcrypt", <http://directory.fsf.org/project/libgcrypt/>.

[MANTIN01] Mantin, I., "Analysis of the Stream Cipher RC4", <http://www.wisdom.weizmann.ac.il/~itsik/RC4/Papers/Mantin1.zip>.

[MANTIN05] Mantin, I., "Predicting and Distinguishing Attacks on RC4 Keystream Generator", Proceedings of EUROCRYPT 2005, <http://www.iacr.org/cryptodb/archive/2005/EUROCRYPT/2597/2597.pdf>.

[MIRONOV] Mironov, I., "(Not So) Random Shuffles of RC4", <http://eprint.iacr.org/2002/067.pdf>.

[NETTLE] Moeller, N., "Nettle - a low-level crypto library", <http://www.gnu.org/software/nettle/>.

[OPENSSL] OpenSSL Team, "The OpenSSL Project", <http://www.openssl.org/>.

[SANS] Hopwood, D., "Standard Cryptographic Algorithm Naming (SANS) entry on RC4", <http://www.users.zetnet.co.uk/hopwood/crypto/scan/cs.html#RC4>.

[SHS] National Institute of Standards and Technology (NIST), "FIPS Publication 180-3: Secure Hash Standard (SHS)", October 2008, <http://csrc.nist.gov/publications/fips/fips180-3/fips180-3_final.pdf>.

## Authors' Addresses

Joachim Strombergson
SecWorks Sweden AB
Hogenvagen 5A
Savedalen 433 63
SE

EMail: joachim@secworks.se

Simon Josefsson
Simon Josefsson Datakonsult AB
Hagagatan 24
Stockholm 113 47
SE

EMail: simon@josefsson.org
URI: http://josefsson.org/