

Network Working Group
Internet-Draft
Intended status: Informational
Expires: July 4, 2014

J. Strombergson
Secworks Sweden AB
December 31, 2013

Test Vectors for the Stream Cipher ChaCha
draft-strombergson-chacha-test-vectors-01

Abstract

This document contains test vectors for the stream cipher ChaCha using 8, 12 and 20 rounds as well as 128 and 256 bit keys.

Status of this Memo

This Internet-Draft is submitted in full conformance with the provisions of [BCP 78](#) and [BCP 79](#).

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at <http://datatracker.ietf.org/drafts/current/>.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

This Internet-Draft will expire on July 4, 2014.

Copyright Notice

Copyright (c) 2013 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to [BCP 78](#) and the IETF Trust's Legal Provisions Relating to IETF Documents (<http://trustee.ietf.org/license-info>) in effect on the date of publication of this document. Please review these documents carefully, as they describe your rights and restrictions with respect to this document. Code Components extracted from this document must include Simplified BSD License text as described in Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the Simplified BSD License.

Internet-Draft Test Vectors for the Stream Cipher ChaCha December 2013

Table of Contents

1.	Introduction	3
2.	Description of the test Vectors	3
3.	Test vectors for ChaCha	4
4.	Security Considerations	41
5.	IANA Considerations	41
6.	Copying conditions	41
7.	References	41
7.1.	Normative References	41
7.2.	Informative References	42
	Author's Address	42

Internet-Draft Test Vectors for the Stream Cipher ChaCha December 2013

1. Introduction

The ChaCha [[ChaCha](#)] algorithm is a fairly new stream cipher that is getting some attention. ChaCha has been proposed as a replacement for RC4 [[RC4](#)] and ChaCha is also used in a few protocols.

In order to efficiently implement the algorithm and ensure interoperability between different implementations, it is of great importance to be able to verify that a given implementation is functionally correct. Test vectors aids this verification by providing a known correct answer.

Unfortunately, for ChaCha there are no test vectors published. This Internet Draft tries to rectify this by providing test vectors for ChaCha.

2. Description of the test Vectors

The test vectors describes in this document is given as a number of test cases. For each test case there is a number of test vectors and known answers. The test vectors in a test case has been generated with support for:

- 128 and 256 bit keys
- 8, 12 and 20 rounds

This means that for a given test case there are 6 different test vectors. Each of these test vectors contains the keystream for two 64 byte blocks.

The test vectors in this I-D has been generated by a simple generator based on the chacha.c [[chacha.c](#)] reference model by Daniel J Bernstein. The generator has been verified to generate the same values as the reference model. reference model.

All zero input data blocks, that is 64 bytes with the value of 0x00 has been used during generation. Since ChaCha is a stream cipher and encryption, decryption is done by XOR-ing the data with the keystream. By using all zero data blocks we get the keystream itself.

The random key in Test Case 8 has been generated by the following command. For 128 bit key only the first 16 bytes are used.

```
$ echo -n "All your base are belong to us" | openssl dgst -sha256
c46ec1b18ce8a878725a37e780dfb7351f68ed2e194c79fbc6aebec1a667975d
```

The random IV in Test Case 8 has been generated by the following command. Only the first eight bytes are used.

```
$ echo -n "Internet Engineering Task Force" | openssl dgst -sha256
1ada31d5cf688221c109163908ebe51debb46227c6cc8b37641910833222772a
```

The test vector generator is available as a stand alone c program in the `chacha_testvectors` [[chacha_testvectors](#)] project on Github.

3. Test vectors for ChaCha

TC1: All zero key and IV.

```
Key:    0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00
        0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00
IV:     0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00
Rounds: 8
```

Internal state after init:

```
state[00 - 01] = 0x61707865 0x3120646e
state[02 - 03] = 0x79622d36 0x6b206574
state[04 - 05] = 0x00000000 0x00000000
state[06 - 07] = 0x00000000 0x00000000
state[08 - 09] = 0x00000000 0x00000000
state[10 - 11] = 0x00000000 0x00000000
state[12 - 13] = 0x00000000 0x00000000
state[14 - 15] = 0x00000000 0x00000000
```

Keystream block :
0xe2 0x8a 0x5f 0xa4 0xa6 0x7f 0x8c 0x5d
0xef 0xed 0x3e 0x6f 0xb7 0x30 0x34 0x86
0xaa 0x84 0x27 0xd3 0x14 0x19 0xa7 0x29
0x57 0x2d 0x77 0x79 0x53 0x49 0x11 0x20
0xb6 0x4a 0xb8 0xe7 0x2b 0x8d 0xeb 0x85
0xcd 0x6a 0xea 0x7c 0xb6 0x08 0x9a 0x10
0x18 0x24 0xbe 0xeb 0x08 0x81 0x4a 0x42
0x8a 0xab 0x1f 0xa2 0xc8 0x16 0x08 0x1b

Keystream block 1:
0x8a 0x26 0xaf 0x44 0x8a 0x1b 0xa9 0x06
0x36 0x8f 0xd8 0xc8 0x38 0x31 0xc1 0x8c
0xec 0x8c 0xed 0x81 0x1a 0x02 0x8e 0x67
0x5b 0x8d 0x2b 0xe8 0xfc 0xe0 0x81 0x16
0x5c 0xea 0xe9 0xf1 0xd1 0xb7 0xa9 0x75
0x49 0x77 0x49 0x48 0x05 0x69 0xce 0xb8
0x3d 0xe6 0xa0 0xa5 0x87 0xd4 0x98 0x4f
0x19 0x92 0x5f 0x5d 0x33 0x8e 0x43 0x0d

Key: 0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00
0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00
IV: 0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00
Rounds: 12

Internal state after init:
state[00 - 01] = 0x61707865 0x3120646e
state[02 - 03] = 0x79622d36 0x6b206574
state[04 - 05] = 0x00000000 0x00000000
state[06 - 07] = 0x00000000 0x00000000
state[08 - 09] = 0x00000000 0x00000000
state[10 - 11] = 0x00000000 0x00000000
state[12 - 13] = 0x00000000 0x00000000
state[14 - 15] = 0x00000000 0x00000000

Keystream block :
0xe1 0x04 0x7b 0xa9 0x47 0x6b 0xf8 0xff
0x31 0x2c 0x01 0xb4 0x34 0x5a 0x7d 0x8c
0xa5 0x79 0x2b 0x0a 0xd4 0x67 0x31 0x3f
0x1d 0xc4 0x12 0xb5 0xfd 0xce 0x32 0x41
0x0d 0xea 0x8b 0x68 0xbd 0x77 0x4c 0x36
0xa9 0x20 0xf0 0x92 0xa0 0x4d 0x3f 0x95

```
0x27 0x4f 0xbe 0xff 0x97 0xbc 0x84 0x91
0xfc 0xef 0x37 0xf8 0x59 0x70 0xb4 0x50
```

Keystream block 1:

```
0x1d 0x43 0xb6 0x1a 0x8f 0x7e 0x19 0xfc
0xed 0xde 0xf3 0x68 0xae 0x6b 0xfb 0x11
0x10 0x1b 0xd9 0xfd 0x3e 0x4d 0x12 0x7d
0xe3 0x0d 0xb2 0xdb 0x1b 0x47 0x2e 0x76
0x42 0x68 0x03 0xa4 0x5e 0x15 0xb9 0x62
0x75 0x19 0x86 0xef 0x1d 0x9d 0x50 0xf5
0x98 0xa5 0xdc 0xdc 0x9f 0xa5 0x29 0xa2
0x83 0x57 0x99 0x1e 0x78 0x4e 0xa2 0x0f
```

```
Key:      0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00
          0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00
IV:       0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00
Rounds: 20
```

Internal state after init:

```
state[00 - 01] = 0x61707865 0x3120646e
state[02 - 03] = 0x79622d36 0x6b206574
state[04 - 05] = 0x00000000 0x00000000
state[06 - 07] = 0x00000000 0x00000000
state[08 - 09] = 0x00000000 0x00000000
state[10 - 11] = 0x00000000 0x00000000
```

```
state[12 - 13] = 0x00000000 0x00000000
state[14 - 15] = 0x00000000 0x00000000
```

Keystream block :

```
0x89 0x67 0x09 0x52 0x60 0x83 0x64 0xfd
0x00 0xb2 0xf9 0x09 0x36 0xf0 0x31 0xc8
0xe7 0x56 0xe1 0x5d 0xba 0x04 0xb8 0x49
0x3d 0x00 0x42 0x92 0x59 0xb2 0x0f 0x46
0xcc 0x04 0xf1 0x11 0x24 0x6b 0x6c 0x2c
0xe0 0x66 0xbe 0x3b 0xfb 0x32 0xd9 0xaa
0x0f 0xdd 0xfb 0xc1 0x21 0x23 0xd4 0xb9
0xe4 0x4f 0x34 0xdc 0xa0 0x5a 0x10 0x3f
```

Keystream block 1:

```
0x6c 0xd1 0x35 0xc2 0x87 0x8c 0x83 0x2b
```

```
0x58 0x96 0xb1 0x34 0xf6 0x14 0x2a 0x9d
0x4d 0x8d 0x0d 0x8f 0x10 0x26 0xd2 0x0a
0x0a 0x81 0x51 0x2c 0xbc 0xe6 0xe9 0x75
0x8a 0x71 0x43 0xd0 0x21 0x97 0x80 0x22
0xa3 0x84 0x14 0x1a 0x80 0xce 0xa3 0x06
0x2f 0x41 0xf6 0x7a 0x75 0x2e 0x66 0xad
0x34 0x11 0x98 0x4c 0x78 0x7e 0x30 0xad
```

```
Key:      0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00
          0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00
          0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00
          0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00
IV:       0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00
Rounds:  8
```

```
Internal state after init:
state[00 - 01] = 0x61707865 0x3320646e
state[02 - 03] = 0x79622d32 0x6b206574
state[04 - 05] = 0x00000000 0x00000000
state[06 - 07] = 0x00000000 0x00000000
state[08 - 09] = 0x00000000 0x00000000
state[10 - 11] = 0x00000000 0x00000000
state[12 - 13] = 0x00000000 0x00000000
state[14 - 15] = 0x00000000 0x00000000
```

```
Keystream block :
0x3e 0x00 0xef 0x2f 0x89 0x5f 0x40 0xd6
0x7f 0x5b 0xb8 0xe8 0x1f 0x09 0xa5 0xa1
0x2c 0x84 0x0e 0xc3 0xce 0x9a 0x7f 0x3b
0x18 0x1b 0xe1 0x88 0xef 0x71 0x1a 0x1e
0x98 0x4c 0xe1 0x72 0xb9 0x21 0x6f 0x41
0x9f 0x44 0x53 0x67 0x45 0x6d 0x56 0x19
```

```
0x31 0x4a 0x42 0xa3 0xda 0x86 0xb0 0x01
0x38 0x7b 0xfd 0xb8 0x0e 0x0c 0xfe 0x42
```

```
Keystream block 1:
0xd2 0xae 0xfa 0x0d 0xea 0xa5 0xc1 0x51
0xbf 0x0a 0xdb 0x6c 0x01 0xf2 0xa5 0xad
0xc0 0xfd 0x58 0x12 0x59 0xf9 0xa2 0xaa
0xdc 0xf2 0x0f 0x8f 0xd5 0x66 0xa2 0x6b
```

0x50 0x32 0xec 0x38 0xbb 0xc5 0xda 0x98
0xee 0x0c 0x6f 0x56 0x8b 0x87 0x2a 0x65
0xa0 0x8a 0xbf 0x25 0x1d 0xeb 0x21 0xbb
0x4b 0x56 0xe5 0xd8 0x82 0x1e 0x68 0xaa

Key: 0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00
0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00
0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00
0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00
IV: 0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00
Rounds: 12

Internal state after init:
state[00 - 01] = 0x61707865 0x3320646e
state[02 - 03] = 0x79622d32 0x6b206574
state[04 - 05] = 0x00000000 0x00000000
state[06 - 07] = 0x00000000 0x00000000
state[08 - 09] = 0x00000000 0x00000000
state[10 - 11] = 0x00000000 0x00000000
state[12 - 13] = 0x00000000 0x00000000
state[14 - 15] = 0x00000000 0x00000000

Keystream block :
0x9b 0xf4 0x9a 0x6a 0x07 0x55 0xf9 0x53
0x81 0x1f 0xce 0x12 0x5f 0x26 0x83 0xd5
0x04 0x29 0xc3 0xbb 0x49 0xe0 0x74 0x14
0x7e 0x00 0x89 0xa5 0x2e 0xae 0x15 0x5f
0x05 0x64 0xf8 0x79 0xd2 0x7a 0xe3 0xc0
0x2c 0xe8 0x28 0x34 0xac 0xfa 0x8c 0x79
0x3a 0x62 0x9f 0x2c 0xa0 0xde 0x69 0x19
0x61 0x0b 0xe8 0x2f 0x41 0x13 0x26 0xbe

Keystream block 1:
0x0b 0xd5 0x88 0x41 0x20 0x3e 0x74 0xfe
0x86 0xfc 0x71 0x33 0x8c 0xe0 0x17 0x3d
0xc6 0x28 0xeb 0xb7 0x19 0xbd 0xcb 0xcc
0x15 0x15 0x85 0x21 0x4c 0xc0 0x89 0xb4
0x42 0x25 0x8d 0xcd 0xa1 0x4c 0xf1 0x11
0xc6 0x02 0xb8 0x97 0x1b 0x8c 0xc8 0x43

0xe9 0x1e 0x46 0xca 0x90 0x51 0x51 0xc0

0x27 0x44 0xa6 0xb0 0x17 0xe6 0x93 0x16

Key: 0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00
0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00
0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00
0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00
IV: 0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00
Rounds: 20

Internal state after init:
state[00 - 01] = 0x61707865 0x3320646e
state[02 - 03] = 0x79622d32 0x6b206574
state[04 - 05] = 0x00000000 0x00000000
state[06 - 07] = 0x00000000 0x00000000
state[08 - 09] = 0x00000000 0x00000000
state[10 - 11] = 0x00000000 0x00000000
state[12 - 13] = 0x00000000 0x00000000
state[14 - 15] = 0x00000000 0x00000000

Keystream block :
0x76 0xb8 0xe0 0xad 0xa0 0xf1 0x3d 0x90
0x40 0x5d 0x6a 0xe5 0x53 0x86 0xbd 0x28
0xbd 0xd2 0x19 0xb8 0xa0 0x8d 0xed 0x1a
0xa8 0x36 0xef 0xcc 0x8b 0x77 0x0d 0xc7
0xda 0x41 0x59 0x7c 0x51 0x57 0x48 0x8d
0x77 0x24 0xe0 0x3f 0xb8 0xd8 0x4a 0x37
0x6a 0x43 0xb8 0xf4 0x15 0x18 0xa1 0x1c
0xc3 0x87 0xb6 0x69 0xb2 0xee 0x65 0x86

Keystream block 1:
0x9f 0x07 0xe7 0xbe 0x55 0x51 0x38 0x7a
0x98 0xba 0x97 0x7c 0x73 0x2d 0x08 0x0d
0xcb 0x0f 0x29 0xa0 0x48 0xe3 0x65 0x69
0x12 0xc6 0x53 0x3e 0x32 0xee 0x7a 0xed
0x29 0xb7 0x21 0x76 0x9c 0xe6 0x4e 0x43
0xd5 0x71 0x33 0xb0 0x74 0xd8 0x39 0xd5
0x31 0xed 0x1f 0x28 0x51 0x0a 0xfb 0x45
0xac 0xe1 0x0a 0x1f 0x4b 0x79 0x4d 0x6f

TC2: Single bit in key set. All zero IV.

Key: 0x01 0x00 0x00 0x00 0x00 0x00 0x00 0x00
0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00
IV: 0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00
Rounds: 8

Internal state after init:

```
state[00 - 01] = 0x61707865 0x3120646e
state[02 - 03] = 0x79622d36 0x6b206574
state[04 - 05] = 0x00000001 0x00000000
state[06 - 07] = 0x00000000 0x00000000
state[08 - 09] = 0x00000001 0x00000000
state[10 - 11] = 0x00000000 0x00000000
state[12 - 13] = 0x00000000 0x00000000
state[14 - 15] = 0x00000000 0x00000000
```

Keystream block :

```
0x03 0xa7 0x66 0x98 0x88 0x60 0x5a 0x07
0x65 0xe8 0x35 0x74 0x75 0xe5 0x86 0x73
0xf9 0x4f 0xc8 0x16 0x1d 0xa7 0x6c 0x2a
0x3a 0xa2 0xf3 0xca 0xf9 0xfe 0x54 0x49
0xe0 0xfc 0xf3 0x8e 0xb8 0x82 0x65 0x6a
0xf8 0x3d 0x43 0x0d 0x41 0x09 0x27 0xd5
0x5c 0x97 0x2a 0xc4 0xc9 0x2a 0xb9 0xda
0x37 0x13 0xe1 0x9f 0x76 0x1e 0xaa 0x14
```

Keystream block 1:

```
0x71 0x38 0xc2 0x5c 0x8a 0x7c 0xe3 0xd5
0xe7 0x54 0x67 0x46 0xff 0xd2 0xe3 0x51
0x5c 0xe6 0xa4 0xb1 0xb2 0xd3 0xf3 0x80
0x13 0x86 0x68 0xed 0x39 0xfa 0x92 0xf8
0xa1 0xae 0xe3 0x62 0x58 0xe0 0x5f 0xae
0x6f 0x56 0x66 0x73 0x51 0x17 0x65 0xfd
0xb5 0x9e 0x05 0x16 0x3d 0x55 0xa7 0x08
0xc5 0xf9 0xbc 0x45 0x04 0x51 0x24 0xcb
```

Key: 0x01 0x00 0x00 0x00 0x00 0x00 0x00 0x00

0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00

IV: 0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00

Rounds: 12

Internal state after init:

```
state[00 - 01] = 0x61707865 0x3120646e
state[02 - 03] = 0x79622d36 0x6b206574
state[04 - 05] = 0x00000001 0x00000000
state[06 - 07] = 0x00000000 0x00000000
state[08 - 09] = 0x00000001 0x00000000
state[10 - 11] = 0x00000000 0x00000000
state[12 - 13] = 0x00000000 0x00000000
state[14 - 15] = 0x00000000 0x00000000
```

Keystream block :
0x2a 0x86 0x5a 0x3b 0x89 0x99 0xfa 0x83

Internet-Draft Test Vectors for the Stream Cipher ChaCha December 2013

0xae 0x8a 0xac 0xf3 0x3f 0xc6 0xbe 0x4f
0x32 0xc8 0xaa 0x97 0x62 0x73 0x8d 0x26
0x96 0x32 0x70 0x05 0x2f 0x4e 0xef 0x8b
0x86 0xaf 0x75 0x8f 0x78 0x67 0x56 0x0a
0xf6 0xd0 0xee 0xb9 0x73 0xb5 0x54 0x2b
0xb2 0x4c 0x8a 0xbc 0xea 0xc8 0xb1 0xf3
0x6d 0x02 0x69 0x63 0xd6 0xc8 0xa9 0xb2

Keystream block 1:
0xd8 0x2c 0xe0 0xca 0xd3 0x7d 0x51 0xb1
0x05 0x2c 0x33 0x14 0x4a 0x30 0xa8 0x23
0x9c 0x9f 0xca 0x62 0x84 0xac 0x5e 0xa7
0x50 0xbe 0xbb 0x2d 0x22 0x4d 0xbb 0x39
0xaa 0x4e 0x7a 0xcd 0x51 0x1f 0x8c 0xef
0x15 0xa5 0xc4 0x90 0x59 0x0e 0x38 0xe9
0x63 0x97 0xc0 0x6c 0xd2 0x1c 0x38 0x9c
0xb8 0xb1 0x15 0x9c 0x24 0x0c 0x9c 0x0e

Key: 0x01 0x00 0x00 0x00 0x00 0x00 0x00 0x00
0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00
IV: 0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00
Rounds: 20

Internal state after init:
state[00 - 01] = 0x61707865 0x3120646e
state[02 - 03] = 0x79622d36 0x6b206574
state[04 - 05] = 0x00000001 0x00000000
state[06 - 07] = 0x00000000 0x00000000
state[08 - 09] = 0x00000001 0x00000000
state[10 - 11] = 0x00000000 0x00000000
state[12 - 13] = 0x00000000 0x00000000
state[14 - 15] = 0x00000000 0x00000000

Keystream block :
0xae 0x56 0x06 0x0d 0x04 0xf5 0xb5 0x97
0x89 0x7f 0xf2 0xaf 0x13 0x88 0xdb 0xce
0xff 0x5a 0x2a 0x49 0x20 0x33 0x5d 0xc1
0x7a 0x3c 0xb1 0xb1 0xb1 0x0f 0xbe 0x70

0xec 0xe8 0xf4 0x86 0x4d 0x8c 0x7c 0xdf
0x00 0x76 0x45 0x3a 0x82 0x91 0xc7 0xdb
0xeb 0x3a 0xa9 0xc9 0xd1 0x0e 0x8c 0xa3
0x6b 0xe4 0x44 0x93 0x76 0xed 0x7c 0x42

Keystream block 1:

0xfc 0x3d 0x47 0x1c 0x34 0xa3 0x6f 0xbb
0xf6 0x16 0xbc 0x0a 0x0e 0x7c 0x52 0x30
0x30 0xd9 0x44 0xf4 0x3e 0xc3 0xe7 0x8d

0xd6 0xa1 0x24 0x66 0x54 0x7c 0xb4 0xf7
0xb3 0xce 0xbd 0x0a 0x50 0x05 0xe7 0x62
0xe5 0x62 0xd1 0x37 0x5b 0x7a 0xc4 0x45
0x93 0xa9 0x91 0xb8 0x5d 0x1a 0x60 0xfb
0xa2 0x03 0x5d 0xfa 0xa2 0xa6 0x42 0xd5

Key: 0x01 0x00 0x00 0x00 0x00 0x00 0x00 0x00
0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00
0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00
0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00

IV: 0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00

Rounds: 8

Internal state after init:

state[00 - 01] = 0x61707865 0x3320646e
state[02 - 03] = 0x79622d32 0x6b206574
state[04 - 05] = 0x00000001 0x00000000
state[06 - 07] = 0x00000000 0x00000000
state[08 - 09] = 0x00000000 0x00000000
state[10 - 11] = 0x00000000 0x00000000
state[12 - 13] = 0x00000000 0x00000000
state[14 - 15] = 0x00000000 0x00000000

Keystream block :

0xcf 0x5e 0xe9 0xa0 0x49 0x4a 0xa9 0x61
0x3e 0x05 0xd5 0xed 0x72 0x5b 0x80 0x4b
0x12 0xf4 0xa4 0x65 0xee 0x63 0x5a 0xcc
0x3a 0x31 0x1d 0xe8 0x74 0x04 0x89 0xea
0x28 0x9d 0x04 0xf4 0x3c 0x75 0x18 0xdb
0x56 0xeb 0x44 0x33 0xe4 0x98 0xa1 0x23
0x8c 0xd8 0x46 0x4d 0x37 0x63 0xdd 0xbb

0x92 0x22 0xee 0x3b 0xd8 0xfa 0xe3 0xc8

Keystream block 1:

0xb4 0x35 0x5a 0x7d 0x93 0xdd 0x88 0x67
0x08 0x9e 0xe6 0x43 0x55 0x8b 0x95 0x75
0x4e 0xfa 0x2b 0xd1 0xa8 0xa1 0xe2 0xd7
0x5b 0xcd 0xb3 0x20 0x15 0x54 0x26 0x38
0x29 0x19 0x41 0xfe 0xb4 0x99 0x65 0x58
0x7c 0x4f 0xdf 0xe2 0x19 0xcf 0x0e 0xc1
0x32 0xa6 0xcd 0x4d 0xc0 0x67 0x39 0x2e
0x67 0x98 0x2f 0xe5 0x32 0x78 0xc0 0xb4

Key: 0x01 0x00 0x00 0x00 0x00 0x00 0x00 0x00
0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00
0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00

0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00
IV: 0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00
Rounds: 12

Internal state after init:

state[00 - 01] = 0x61707865 0x3320646e
state[02 - 03] = 0x79622d32 0x6b206574
state[04 - 05] = 0x00000001 0x00000000
state[06 - 07] = 0x00000000 0x00000000
state[08 - 09] = 0x00000000 0x00000000
state[10 - 11] = 0x00000000 0x00000000
state[12 - 13] = 0x00000000 0x00000000
state[14 - 15] = 0x00000000 0x00000000

Keystream block :

0x12 0x05 0x6e 0x59 0x5d 0x56 0xb0 0xf6
0xee 0xf0 0x90 0xf0 0xcd 0x25 0xa2 0x09
0x49 0x24 0x8c 0x27 0x90 0x52 0x5d 0x0f
0x93 0x02 0x18 0xff 0x0b 0x4d 0xdd 0x10
0xa6 0x00 0x22 0x39 0xd9 0xa4 0x54 0xe2
0x9e 0x10 0x7a 0x7d 0x06 0xfe 0xfd 0xfe
0xf0 0x21 0x0f 0xeb 0xa0 0x44 0xf9 0xf2
0x9b 0x17 0x72 0xc9 0x60 0xdc 0x29 0xc0

Keystream block 1:

```
0x0c 0x73 0x66 0xc5 0xcb 0xc6 0x04 0x24
0x0e 0x66 0x5e 0xb0 0x2a 0x69 0x37 0x2a
0x7a 0xf9 0x79 0xb2 0x6f 0xbb 0x78 0x09
0x2a 0xc7 0xc4 0xb8 0x80 0x29 0xa7 0xc8
0x54 0x51 0x3b 0xc2 0x17 0xbb 0xfc 0x7d
0x90 0x43 0x2e 0x30 0x8e 0xba 0x15 0xaf
0xc6 0x5a 0xeb 0x48 0xef 0x10 0x0d 0x56
0x01 0xe6 0xaf 0xba 0x25 0x71 0x17 0xa9
```

```
Key:    0x01 0x00 0x00 0x00 0x00 0x00 0x00 0x00
        0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00
        0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00
        0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00
IV:     0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00
Rounds: 20
```

```
Internal state after init:
state[00 - 01] = 0x61707865 0x3320646e
state[02 - 03] = 0x79622d32 0x6b206574
state[04 - 05] = 0x00000001 0x00000000
state[06 - 07] = 0x00000000 0x00000000
state[08 - 09] = 0x00000000 0x00000000
```

```
state[10 - 11] = 0x00000000 0x00000000
state[12 - 13] = 0x00000000 0x00000000
state[14 - 15] = 0x00000000 0x00000000
```

```
Keystream block :
0xc5 0xd3 0x0a 0x7c 0xe1 0xec 0x11 0x93
0x78 0xc8 0x4f 0x48 0x7d 0x77 0x5a 0x85
0x42 0xf1 0x3e 0xce 0x23 0x8a 0x94 0x55
0xe8 0x22 0x9e 0x88 0x8d 0xe8 0x5b 0xbd
0x29 0xeb 0x63 0xd0 0xa1 0x7a 0x5b 0x99
0x9b 0x52 0xda 0x22 0xbe 0x40 0x23 0xeb
0x07 0x62 0x0a 0x54 0xf6 0xfa 0x6a 0xd8
0x73 0x7b 0x71 0xeb 0x04 0x64 0xda 0xc0
```

```
Keystream block 1:
0x10 0xf6 0x56 0xe6 0xd1 0xfd 0x55 0x05
0x3e 0x50 0xc4 0x87 0x5c 0x99 0x30 0xa3
0x3f 0x6d 0x02 0x63 0xbd 0x14 0xdf 0xd6
```

```
0xab 0x8c 0x70 0x52 0x1c 0x19 0x33 0x8b
0x23 0x08 0xb9 0x5c 0xf8 0xd0 0xbb 0x7d
0x20 0x2d 0x21 0x02 0x78 0x0e 0xa3 0x52
0x8f 0x1c 0xb4 0x85 0x60 0xf7 0x6b 0x20
0xf3 0x82 0xb9 0x42 0x50 0x0f 0xce 0xac
```

TC3: Single bit in IV set. All zero key.

```
-----
Key:    0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00
        0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00
IV:     0x01 0x00 0x00 0x00 0x00 0x00 0x00 0x00
Rounds: 8
```

Internal state after init:

```
state[00 - 01] = 0x61707865 0x3120646e
state[02 - 03] = 0x79622d36 0x6b206574
state[04 - 05] = 0x00000000 0x00000000
state[06 - 07] = 0x00000000 0x00000000
state[08 - 09] = 0x00000000 0x00000000
state[10 - 11] = 0x00000000 0x00000000
state[12 - 13] = 0x00000000 0x00000000
state[14 - 15] = 0x00000001 0x00000000
```

Keystream block :

```
0x25 0xf5 0xbe 0xc6 0x68 0x39 0x16 0xff
0x44 0xbc 0xcd 0x12 0xd1 0x02 0xe6 0x92
0x17 0x66 0x63 0xf4 0xca 0xc5 0x3e 0x71
0x95 0x09 0xca 0x74 0xb6 0xb2 0xee 0xc8
0x5d 0xa4 0x23 0x6f 0xb2 0x99 0x02 0x01
```

```
0x2a 0xdc 0x8f 0x0d 0x86 0xc8 0x18 0x7d
0x25 0xcd 0x1c 0x48 0x69 0x66 0x93 0x0d
0x02 0x04 0xc4 0xee 0x88 0xa6 0xab 0x35
```

Keystream block 1:

```
0x5a 0x6c 0x99 0x76 0xc7 0xbc 0x6e 0x78
0xba 0xf3 0x10 0x8c 0x53 0x64 0xef 0x42
0xb9 0x3b 0x35 0xd2 0x69 0x4d 0x2d 0xdf
0x72 0xa4 0xfc 0x7e 0xcd 0xb9 0x68 0xfc
0xfe 0x16 0xbe 0xdb 0x8d 0x48 0x10 0x2f
0xb5 0x4f 0x1c 0xe3 0x63 0x6e 0x91 0x4c
```

0x0e 0x2d 0xad 0xc7 0xca 0xa2 0xab 0x19
0x29 0x73 0x3a 0x92 0x63 0x32 0x5e 0x72

Key: 0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00
0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00

IV: 0x01 0x00 0x00 0x00 0x00 0x00 0x00 0x00

Rounds: 12

Internal state after init:

state[00 - 01] = 0x61707865 0x3120646e
state[02 - 03] = 0x79622d36 0x6b206574
state[04 - 05] = 0x00000000 0x00000000
state[06 - 07] = 0x00000000 0x00000000
state[08 - 09] = 0x00000000 0x00000000
state[10 - 11] = 0x00000000 0x00000000
state[12 - 13] = 0x00000000 0x00000000
state[14 - 15] = 0x00000001 0x00000000

Keystream block :

0x91 0xcd 0xb2 0xf1 0x80 0xbc 0x89 0xcf
0xe8 0x6b 0x8b 0x68 0x71 0xcd 0x6b 0x3a
0xf6 0x1a 0xbf 0x6e 0xba 0x01 0x63 0x5d
0xb6 0x19 0xc4 0x0a 0x0b 0x2e 0x19 0xed
0xfa 0x8c 0xe5 0xa9 0xbd 0x7f 0x53 0xcc
0x2c 0x9b 0xcf 0xea 0x18 0x1e 0x97 0x54
0xa9 0xe2 0x45 0x73 0x1f 0x65 0x8c 0xc2
0x82 0xc2 0xae 0x1c 0xab 0x1a 0xe0 0x2c

Keystream block 1:

0x43 0x66 0xd2 0x88 0xf0 0xf8 0x8e 0x00
0x16 0x80 0xbc 0x02 0xf1 0xb1 0x9a 0x96
0x37 0xa2 0x61 0xa1 0x3b 0xd8 0x3e 0x31
0x2f 0x37 0x58 0xea 0x89 0xba 0x72 0x22
0x3d 0x65 0xb1 0xcd 0x40 0xce 0xa4 0x78
0xb2 0x0f 0x4e 0x2b 0xbb 0x9a 0x98 0xea
0x05 0xfa 0xbc 0x05 0xf8 0x6d 0xf9 0xa2

0x89 0x32 0x6d 0x37 0x9a 0xfb 0x99 0xb9

Key: 0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00


```
0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00
IV:    0x01 0x00 0x00 0x00 0x00 0x00 0x00 0x00
Rounds: 20
```

```
Internal state after init:
state[00 - 01] = 0x61707865 0x3120646e
state[02 - 03] = 0x79622d36 0x6b206574
state[04 - 05] = 0x00000000 0x00000000
state[06 - 07] = 0x00000000 0x00000000
state[08 - 09] = 0x00000000 0x00000000
state[10 - 11] = 0x00000000 0x00000000
state[12 - 13] = 0x00000000 0x00000000
state[14 - 15] = 0x00000001 0x00000000
```

```
Keystream block :
0x16 0x63 0x87 0x9e 0xb3 0xf2 0xc9 0x94
0x9e 0x23 0x88 0xca 0xa3 0x43 0xd3 0x61
0xbb 0x13 0x27 0x71 0x24 0x5a 0xe6 0xd0
0x27 0xca 0x9c 0xb0 0x10 0xdc 0x1f 0xa7
0x17 0x8d 0xc4 0x1f 0x82 0x78 0xbc 0x1f
0x64 0xb3 0xf1 0x27 0x69 0xa2 0x40 0x97
0xf4 0x0d 0x63 0xa8 0x63 0x66 0xbd 0xb3
0x6a 0xc0 0x8a 0xbe 0x60 0xc0 0x7f 0xe8
```

```
Keystream block 1:
0xb0 0x57 0x37 0x5c 0x89 0x14 0x44 0x08
0xcc 0x74 0x46 0x24 0xf6 0x9f 0x7f 0x4c
0xcb 0xd9 0x33 0x66 0xc9 0x2f 0xc4 0xdf
0xca 0xda 0x65 0xf1 0xb9 0x59 0xd8 0xc6
0x4d 0xfc 0x50 0xde 0x71 0x1f 0xb4 0x64
0x16 0xc2 0x55 0x3c 0xc6 0x0f 0x21 0xbb
0xfd 0x00 0x64 0x91 0xcb 0x17 0x88 0x8b
0x4f 0xb3 0x52 0x1c 0x4f 0xdd 0x87 0x45
```

```
Key:    0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00
        0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00
        0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00
        0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00
IV:    0x01 0x00 0x00 0x00 0x00 0x00 0x00 0x00
Rounds: 8
```

```
Internal state after init:
state[00 - 01] = 0x61707865 0x3320646e
```

```
state[02 - 03] = 0x79622d32 0x6b206574
state[04 - 05] = 0x00000000 0x00000000
state[06 - 07] = 0x00000000 0x00000000
state[08 - 09] = 0x00000000 0x00000000
state[10 - 11] = 0x00000000 0x00000000
state[12 - 13] = 0x00000000 0x00000000
state[14 - 15] = 0x00000001 0x00000000
```

Keystream block :

```
0x2b 0x8f 0x4b 0xb3 0x79 0x83 0x06 0xca
0x51 0x30 0xd4 0x7c 0x4f 0x8d 0x4e 0xd1
0x3a 0xa0 0xed 0xcc 0xc1 0xbe 0x69 0x42
0x09 0x0f 0xae 0xec 0xa0 0xd7 0x59 0x9b
0x7f 0xf0 0xfe 0x61 0x6b 0xb2 0x5a 0xa0
0x15 0x3a 0xd6 0xfd 0xc8 0x8b 0x95 0x49
0x03 0xc2 0x24 0x26 0xd4 0x78 0xb9 0x7b
0x22 0xb8 0xf9 0xb1 0xdb 0x00 0xcf 0x06
```

Keystream block 1:

```
0x47 0x0b 0xdf 0xfb 0xc4 0x88 0xa8 0xb7
0xc7 0x01 0xeb 0xf4 0x06 0x1d 0x75 0xc5
0x96 0x91 0x86 0x49 0x7c 0x95 0x36 0x78
0x09 0xaf 0xa8 0x0b 0xd8 0x43 0xb0 0x40
0xa7 0x9a 0xbc 0x6e 0x73 0xa9 0x17 0x57
0xf1 0xdb 0x73 0xc8 0xea 0xcf 0xa5 0x43
0xb3 0x8f 0x28 0x9d 0x06 0x5a 0xb2 0xf3
0x03 0x2d 0x37 0x7b 0x8c 0x37 0xfe 0x46
```

```
Key:    0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00
        0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00
        0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00
        0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00
```

```
IV:    0x01 0x00 0x00 0x00 0x00 0x00 0x00 0x00
```

Rounds: 12

Internal state after init:

```
state[00 - 01] = 0x61707865 0x3320646e
state[02 - 03] = 0x79622d32 0x6b206574
state[04 - 05] = 0x00000000 0x00000000
state[06 - 07] = 0x00000000 0x00000000
state[08 - 09] = 0x00000000 0x00000000
state[10 - 11] = 0x00000000 0x00000000
state[12 - 13] = 0x00000000 0x00000000
state[14 - 15] = 0x00000001 0x00000000
```

Keystream block :

0x64 0xb8 0xbd 0xf8 0x7b 0x82 0x8c 0x4b

Internet-Draft Test Vectors for the Stream Cipher ChaCha December 2013

0x6d 0xba 0xf7 0xef 0x69 0x8d 0xe0 0x3d
0xf8 0xb3 0x3f 0x63 0x57 0x14 0x41 0x8f
0x98 0x36 0xad 0xe5 0x9b 0xe1 0x29 0x69
0x46 0xc9 0x53 0xa0 0xf3 0x8e 0xcf 0xfc
0x9e 0xcb 0x98 0xe8 0x1d 0x5d 0x99 0xa5
0xed 0xfc 0x8f 0x9a 0x0a 0x45 0xb9 0xe4
0x1e 0xf3 0xb3 0x1f 0x02 0x8f 0x1d 0x0f

Keystream block 1:

0x55 0x9d 0xb4 0xa7 0xf2 0x22 0xc4 0x42
0xfe 0x23 0xb9 0xa2 0x59 0x6a 0x88 0x28
0x51 0x22 0xee 0x4f 0x13 0x63 0x89 0x6e
0xa7 0x7c 0xa1 0x50 0x91 0x2a 0xc7 0x23
0xbf 0xf0 0x4b 0x02 0x6a 0x2f 0x80 0x7e
0x03 0xb2 0x9c 0x02 0x07 0x7d 0x7b 0x06
0xfc 0x1a 0xb9 0x82 0x7c 0x13 0xc8 0x01
0x3a 0x6d 0x83 0xbd 0x3b 0x52 0xa2 0x6f

Key: 0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00
0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00
0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00
0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00

IV: 0x01 0x00 0x00 0x00 0x00 0x00 0x00 0x00

Rounds: 20

Internal state after init:

state[00 - 01] = 0x61707865 0x3320646e
state[02 - 03] = 0x79622d32 0x6b206574
state[04 - 05] = 0x00000000 0x00000000
state[06 - 07] = 0x00000000 0x00000000
state[08 - 09] = 0x00000000 0x00000000
state[10 - 11] = 0x00000000 0x00000000
state[12 - 13] = 0x00000000 0x00000000
state[14 - 15] = 0x00000001 0x00000000

Keystream block :

0xef 0x3f 0xdf 0xd6 0xc6 0x15 0x78 0xfb
0xf5 0xcf 0x35 0xbd 0x3d 0xd3 0x3b 0x80
0x09 0x63 0x16 0x34 0xd2 0x1e 0x42 0xac

0x33 0x96 0x0b 0xd1 0x38 0xe5 0x0d 0x32
0x11 0x1e 0x4c 0xaf 0x23 0x7e 0xe5 0x3c
0xa8 0xad 0x64 0x26 0x19 0x4a 0x88 0x54
0x5d 0xdc 0x49 0x7a 0x0b 0x46 0x6e 0x7d
0x6b 0xbd 0xb0 0x04 0x1b 0x2f 0x58 0x6b

Keystream block 1:

0x53 0x05 0xe5 0xe4 0x4a 0xff 0x19 0xb2

0x35 0x93 0x61 0x44 0x67 0x5e 0xfb 0xe4
0x40 0x9e 0xb7 0xe8 0xe5 0xf1 0x43 0x0f
0x5f 0x58 0x36 0xae 0xb4 0x9b 0xb5 0x32
0x8b 0x01 0x7c 0x4b 0x9d 0xc1 0x1f 0x8a
0x03 0x86 0x3f 0xa8 0x03 0xdc 0x71 0xd5
0x72 0x6b 0x2b 0x6b 0x31 0xaa 0x32 0x70
0x8a 0xfe 0x5a 0xf1 0xd6 0xb6 0x90 0x58

TC4: All bits in key and IV are set.

Key: 0xff 0xff 0xff 0xff 0xff 0xff 0xff 0xff
0xff 0xff 0xff 0xff 0xff 0xff 0xff 0xff
IV: 0xff 0xff 0xff 0xff 0xff 0xff 0xff 0xff
Rounds: 8

Internal state after init:

state[00 - 01] = 0x61707865 0x3120646e
state[02 - 03] = 0x79622d36 0x6b206574
state[04 - 05] = 0xffffffff 0xffffffff
state[06 - 07] = 0xffffffff 0xffffffff
state[08 - 09] = 0xffffffff 0xffffffff
state[10 - 11] = 0xffffffff 0xffffffff
state[12 - 13] = 0x00000000 0x00000000
state[14 - 15] = 0xffffffff 0xffffffff

Keystream block :

0x22 0x04 0xd5 0xb8 0x1c 0xe6 0x62 0x19
0x3e 0x00 0x96 0x60 0x34 0xf9 0x13 0x02
0xf1 0x4a 0x3f 0xb0 0x47 0xf5 0x8b 0x6e
0x6e 0xf0 0xd7 0x21 0x13 0x23 0x04 0x16
0x3e 0x0f 0xb6 0x40 0xd7 0x6f 0xf9 0xc3
0xb9 0xcd 0x99 0x99 0x6e 0x6e 0x38 0xfa

0xd1 0x3f 0x0e 0x31 0xc8 0x22 0x44 0xd3
0x3a 0xbb 0xc1 0xb1 0x1e 0x8b 0xf1 0x2d

Keystream block 1:

0x9a 0x81 0xd7 0x8e 0x9e 0x56 0x60 0x4d
0xdf 0xae 0x13 0x69 0x21 0xf5 0x1c 0x9d
0x81 0xae 0x15 0x11 0x9d 0xb8 0xe7 0x56
0xdd 0x28 0x02 0x44 0x93 0xee 0x57 0x1d
0x36 0x3a 0xe4 0xbb 0xcd 0x6e 0x7d 0x30
0x0f 0x99 0xd2 0x67 0x3a 0xeb 0x92 0xcc
0xfc 0x6e 0x43 0xa3 0x8d 0xc3 0x1b 0xac
0xd6 0x6b 0x28 0xf1 0x7b 0x22 0xb2 0x8a

Key: 0xff 0xff 0xff 0xff 0xff 0xff 0xff 0xff

0xff 0xff 0xff 0xff 0xff 0xff 0xff 0xff
IV: 0xff 0xff 0xff 0xff 0xff 0xff 0xff 0xff
Rounds: 12

Internal state after init:

state[00 - 01] = 0x61707865 0x3120646e
state[02 - 03] = 0x79622d36 0x6b206574
state[04 - 05] = 0xffffffff 0xffffffff
state[06 - 07] = 0xffffffff 0xffffffff
state[08 - 09] = 0xffffffff 0xffffffff
state[10 - 11] = 0xffffffff 0xffffffff
state[12 - 13] = 0x00000000 0x00000000
state[14 - 15] = 0xffffffff 0xffffffff

Keystream block :

0x60 0xe3 0x49 0xe6 0x0c 0x38 0xb3 0x28
0xc4 0xba 0xab 0x90 0xd4 0x4a 0x7c 0x72
0x76 0x62 0x77 0x0d 0x36 0x35 0x0d 0x65
0xa1 0x43 0x3b 0xd9 0x2b 0x00 0xec 0xf4
0x83 0xd5 0x59 0x7d 0x7a 0x61 0x62 0x58
0xec 0x3c 0x5d 0x5b 0x30 0xe1 0xc5 0xc8
0x5c 0x5d 0xfe 0x2f 0x92 0x42 0x3b 0x8e
0x36 0x87 0x0f 0x31 0x85 0xb6 0xad 0xd9

Keystream block 1:

0xf3 0x4d 0xab 0x6c 0x2b 0xc5 0x51 0x89

```
0x8f 0xbd 0xcd 0xfc 0x78 0x3f 0x09 0x17
0x1c 0xc8 0xb5 0x9a 0x8b 0x28 0x52 0x98
0x3c 0x3a 0x9b 0x91 0xd2 0x9b 0x57 0x61
0x12 0x46 0x4a 0x9d 0x8e 0x05 0x02 0x63
0xe9 0x89 0x90 0x6f 0x42 0xc7 0xef 0xca
0xc8 0xa7 0x0a 0x85 0xbb 0x7f 0xf2 0x21
0x12 0x73 0xfb 0xd4 0xca 0xd9 0x61 0x42
```

```
Key:      0xff 0xff 0xff 0xff 0xff 0xff 0xff 0xff
          0xff 0xff 0xff 0xff 0xff 0xff 0xff 0xff
IV:       0xff 0xff 0xff 0xff 0xff 0xff 0xff 0xff
Rounds: 20
```

```
Internal state after init:
state[00 - 01] = 0x61707865 0x3120646e
state[02 - 03] = 0x79622d36 0x6b206574
state[04 - 05] = 0xffffffff 0xffffffff
state[06 - 07] = 0xffffffff 0xffffffff
state[08 - 09] = 0xffffffff 0xffffffff
state[10 - 11] = 0xffffffff 0xffffffff
state[12 - 13] = 0x00000000 0x00000000
```

```
state[14 - 15] = 0xffffffff 0xffffffff
```

```
Keystream block :
0x99 0x29 0x47 0xc3 0x96 0x61 0x26 0xa0
0xe6 0x60 0xa3 0xe9 0x5d 0xb0 0x48 0xde
0x09 0x1f 0xb9 0xe0 0x18 0x5b 0x1e 0x41
0xe4 0x10 0x15 0xbb 0x7e 0xe5 0x01 0x50
0x39 0x9e 0x47 0x60 0xb2 0x62 0xf9 0xd5
0x3f 0x26 0xd8 0xdd 0x19 0xe5 0x6f 0x5c
0x50 0x6a 0xe0 0xc3 0x61 0x9f 0xa6 0x7f
0xb0 0xc4 0x08 0x10 0x6d 0x02 0x03 0xee
```

```
Keystream block 1:
0x40 0xea 0x3c 0xfa 0x61 0xfa 0x32 0xa2
0xfd 0xa8 0xd1 0x23 0x8a 0x21 0x35 0xd9
0xd4 0x17 0x87 0x75 0x24 0x0f 0x99 0x00
0x70 0x64 0xa6 0xa7 0xf0 0xc7 0x31 0xb6
0x7c 0x22 0x7c 0x52 0xef 0x79 0x6b 0x6b
0xed 0x9f 0x90 0x59 0xba 0x06 0x14 0xbc
```

0xf6 0xdd 0x6e 0x38 0x91 0x7f 0x3b 0x15
0x0e 0x57 0x63 0x75 0xbe 0x50 0xed 0x67

Key: 0xff 0xff 0xff 0xff 0xff 0xff 0xff 0xff
0xff 0xff 0xff 0xff 0xff 0xff 0xff 0xff
0xff 0xff 0xff 0xff 0xff 0xff 0xff 0xff
0xff 0xff 0xff 0xff 0xff 0xff 0xff 0xff
IV: 0xff 0xff 0xff 0xff 0xff 0xff 0xff 0xff
Rounds: 8

Internal state after init:
state[00 - 01] = 0x61707865 0x3320646e
state[02 - 03] = 0x79622d32 0x6b206574
state[04 - 05] = 0xffffffff 0xffffffff
state[06 - 07] = 0xffffffff 0xffffffff
state[08 - 09] = 0xffffffff 0xffffffff
state[10 - 11] = 0xffffffff 0xffffffff
state[12 - 13] = 0x00000000 0x00000000
state[14 - 15] = 0xffffffff 0xffffffff

Keystream block :
0xe1 0x63 0xbb 0xf8 0xc9 0xa7 0x39 0xd1
0x89 0x25 0xee 0x83 0x62 0xda 0xd2 0xcd
0xc9 0x73 0xdf 0x05 0x22 0x5a 0xfb 0x2a
0xa2 0x63 0x96 0xf2 0xa9 0x84 0x9a 0x4a
0x44 0x5e 0x05 0x47 0xd3 0x1c 0x16 0x23
0xc5 0x37 0xdf 0x4b 0xa8 0x5c 0x70 0xa9
0x88 0x4a 0x35 0xbc 0xbf 0x3d 0xfa 0xb0

0x77 0xe9 0x8b 0x0f 0x68 0x13 0x5f 0x54

Keystream block 1:
0x81 0xd4 0x93 0x3f 0x8b 0x32 0x2a 0xc0
0xcd 0x76 0x2c 0x27 0x23 0x5c 0xe2 0xb3
0x15 0x34 0xe0 0x24 0x4a 0x9a 0x2f 0x1f
0xd5 0xe9 0x44 0x98 0xd4 0x7f 0xf1 0x08
0x79 0x0c 0x00 0x9c 0xf9 0xe1 0xa3 0x48
0x03 0x2a 0x76 0x94 0xcb 0x28 0x02 0x4c
0xd9 0x6d 0x34 0x98 0x36 0x1e 0xdb 0x17
0x85 0xaf 0x75 0x2d 0x18 0x7a 0xb5 0x4b

Key: 0xff 0xff 0xff 0xff 0xff 0xff 0xff 0xff
0xff 0xff 0xff 0xff 0xff 0xff 0xff 0xff
0xff 0xff 0xff 0xff 0xff 0xff 0xff 0xff
0xff 0xff 0xff 0xff 0xff 0xff 0xff 0xff
IV: 0xff 0xff 0xff 0xff 0xff 0xff 0xff 0xff
Rounds: 12

Internal state after init:
state[00 - 01] = 0x61707865 0x3320646e
state[02 - 03] = 0x79622d32 0x6b206574
state[04 - 05] = 0xffffffff 0xffffffff
state[06 - 07] = 0xffffffff 0xffffffff
state[08 - 09] = 0xffffffff 0xffffffff
state[10 - 11] = 0xffffffff 0xffffffff
state[12 - 13] = 0x00000000 0x00000000
state[14 - 15] = 0xffffffff 0xffffffff

Keystream block :
0x04 0xbf 0x88 0xda 0xe8 0xe4 0x7a 0x22
0x8f 0xa4 0x7b 0x7e 0x63 0x79 0x43 0x4b
0xa6 0x64 0xa7 0xd2 0x8f 0x4d 0xab 0x84
0xe5 0xf8 0xb4 0x64 0xad 0xd2 0x0c 0x3a
0xca 0xa6 0x9c 0x5a 0xb2 0x21 0xa2 0x3a
0x57 0xeb 0x5f 0x34 0x5c 0x96 0xf4 0xd1
0x32 0x2d 0x0a 0x2f 0xf7 0xa9 0xcd 0x43
0x40 0x1c 0xd5 0x36 0x63 0x9a 0x61 0x5a

Keystream block 1:
0x5c 0x94 0x29 0xb5 0x5c 0xa3 0xc1 0xb5
0x53 0x54 0x55 0x96 0x69 0xa1 0x54 0xac
0xa4 0x6c 0xd7 0x61 0xc4 0x1a 0xb8 0xac
0xe3 0x85 0x36 0x3b 0x95 0x67 0x5f 0x06
0x8e 0x18 0xdb 0x5a 0x67 0x3c 0x11 0x29
0x1b 0xd4 0x18 0x78 0x92 0xa9 0xa3 0xa3
0x35 0x14 0xf3 0x71 0x2b 0x26 0xc1 0x30

0x26 0x10 0x32 0x98 0xed 0x76 0xbc 0x9a

Key: 0xff 0xff 0xff 0xff 0xff 0xff 0xff 0xff
0xff 0xff 0xff 0xff 0xff 0xff 0xff 0xff


```
      0xff 0xff 0xff 0xff 0xff 0xff 0xff 0xff
      0xff 0xff 0xff 0xff 0xff 0xff 0xff 0xff
IV:    0xff 0xff 0xff 0xff 0xff 0xff 0xff 0xff
Rounds: 20
```

```
Internal state after init:
state[00 - 01] = 0x61707865 0x3320646e
state[02 - 03] = 0x79622d32 0x6b206574
state[04 - 05] = 0xffffffff 0xffffffff
state[06 - 07] = 0xffffffff 0xffffffff
state[08 - 09] = 0xffffffff 0xffffffff
state[10 - 11] = 0xffffffff 0xffffffff
state[12 - 13] = 0x00000000 0x00000000
state[14 - 15] = 0xffffffff 0xffffffff
```

```
Keystream block :
0xd9 0xbf 0x3f 0x6b 0xce 0x6e 0xd0 0xb5
0x42 0x54 0x55 0x77 0x67 0xfb 0x57 0x44
0x3d 0xd4 0x77 0x89 0x11 0xb6 0x06 0x05
0x5c 0x39 0xcc 0x25 0xe6 0x74 0xb8 0x36
0x3f 0xea 0xbc 0x57 0xfd 0xe5 0x4f 0x79
0x0c 0x52 0xc8 0xae 0x43 0x24 0x0b 0x79
0xd4 0x90 0x42 0xb7 0x77 0xbf 0xd6 0xcb
0x80 0xe9 0x31 0x27 0x0b 0x7f 0x50 0xeb
```

```
Keystream block 1:
0x5b 0xac 0x2a 0xcd 0x86 0xa8 0x36 0xc5
0xdc 0x98 0xc1 0x16 0xc1 0x21 0x7e 0xc3
0x1d 0x3a 0x63 0xa9 0x45 0x13 0x19 0xf0
0x97 0xf3 0xb4 0xd6 0xda 0xb0 0x77 0x87
0x19 0x47 0x7d 0x24 0xd2 0x4b 0x40 0x3a
0x12 0x24 0x1d 0x7c 0xca 0x06 0x4f 0x79
0x0f 0x1d 0x51 0xcc 0xaf 0xf6 0xb1 0x66
0x7d 0x4b 0xbc 0xa1 0x95 0x8c 0x43 0x06
```

TC5: Every even bit set in key and IV.

```
-----
Key:    0x55 0x55 0x55 0x55 0x55 0x55 0x55 0x55
      0x55 0x55 0x55 0x55 0x55 0x55 0x55 0x55
IV:    0x55 0x55 0x55 0x55 0x55 0x55 0x55 0x55
Rounds: 8
```

Internal state after init:

```
state[00 - 01] = 0x61707865 0x3120646e
state[02 - 03] = 0x79622d36 0x6b206574
state[04 - 05] = 0x55555555 0x55555555
state[06 - 07] = 0x55555555 0x55555555
state[08 - 09] = 0x55555555 0x55555555
state[10 - 11] = 0x55555555 0x55555555
state[12 - 13] = 0x00000000 0x00000000
state[14 - 15] = 0x55555555 0x55555555
```

Keystream block :

```
0xf0 0xa2 0x3b 0xc3 0x62 0x70 0xe1 0x8e
0xd0 0x69 0x1d 0xc3 0x84 0x37 0x4b 0x9b
0x2c 0x5c 0xb6 0x01 0x10 0xa0 0x3f 0x56
0xfa 0x48 0xa9 0xfb 0xba 0xd9 0x61 0xaa
0x6b 0xab 0x4d 0x89 0x2e 0x96 0x26 0x1b
0x6f 0x1a 0x09 0x19 0x51 0x4a 0xe5 0x6f
0x86 0xe0 0x66 0xe1 0x7c 0x71 0xa4 0x17
0x6a 0xc6 0x84 0xaf 0x1c 0x93 0x19 0x96
```

Keystream block 1:

```
0x95 0x0f 0x75 0x4e 0x72 0x8b 0xd0 0x61
0xd1 0x76 0xec 0xf5 0x71 0xc6 0x2a 0x5e
0xa5 0xc7 0x76 0x69 0x7b 0x31 0x93 0xd3
0xea 0x94 0xcf 0x17 0xd7 0xf0 0xa1 0x4e
0x50 0x48 0x59 0xd1 0xa6 0x7c 0x24 0x8a
0xb2 0x98 0xbe 0x3b 0xb7 0xed 0xed 0x3a
0x23 0xf6 0x1b 0x6c 0x5b 0xd1 0xa5 0xa4
0xcf 0xc8 0x4b 0xfc 0x3d 0x29 0x5a 0xc5
```

Key: 0x55 0x55 0x55 0x55 0x55 0x55 0x55 0x55

0x55 0x55 0x55 0x55 0x55 0x55 0x55 0x55

IV: 0x55 0x55 0x55 0x55 0x55 0x55 0x55 0x55

Rounds: 12

Internal state after init:

```
state[00 - 01] = 0x61707865 0x3120646e
state[02 - 03] = 0x79622d36 0x6b206574
state[04 - 05] = 0x55555555 0x55555555
state[06 - 07] = 0x55555555 0x55555555
state[08 - 09] = 0x55555555 0x55555555
state[10 - 11] = 0x55555555 0x55555555
state[12 - 13] = 0x00000000 0x00000000
state[14 - 15] = 0x55555555 0x55555555
```

Keystream block :

```
0x90 0xec 0x7a 0x49 0xee 0x0b 0x20 0xa8
```

Internet-Draft Test Vectors for the Stream Cipher ChaCha December 2013

```
0x08 0xaf 0x3d 0x46 0x3c 0x1f 0xac 0x6c
0x2a 0x7c 0x89 0x7c 0xe8 0xf6 0xe6 0x0d
0x79 0x3b 0x62 0xdd 0xbe 0xbc 0xf9 0x80
0xac 0x91 0x7f 0x09 0x1e 0x52 0x95 0x2d
0xb0 0x63 0xb1 0xd2 0xb9 0x47 0xde 0x04
0xaa 0xc0 0x87 0x19 0x0c 0xa9 0x9a 0x35
0xb5 0xea 0x50 0x1e 0xb5 0x35 0xd5 0x70
```

Keystream block 1:

```
0x8f 0x78 0xcc 0xea 0x3d 0x94 0x52 0x58
0x44 0x50 0x10 0x1a 0xc4 0x95 0xcd 0x16
0x6e 0xfd 0x69 0x42 0x6b 0x47 0xfa 0x6e
0x8e 0x78 0x89 0x21 0xf2 0x9e 0x3d 0x54
0x73 0x64 0xb9 0x52 0x91 0x31 0x73 0xa5
0xba 0xc5 0x00 0xe8 0x9d 0x8c 0x66 0xc6
0xce 0x51 0xed 0x62 0x6d 0x0d 0xa8 0xdc
0x94 0xde 0xec 0x92 0x12 0x5e 0xa4 0x8d
```

```
Key:      0x55 0x55 0x55 0x55 0x55 0x55 0x55 0x55
          0x55 0x55 0x55 0x55 0x55 0x55 0x55 0x55
IV:       0x55 0x55 0x55 0x55 0x55 0x55 0x55 0x55
Rounds: 20
```

Internal state after init:

```
state[00 - 01] = 0x61707865 0x3120646e
state[02 - 03] = 0x79622d36 0x6b206574
state[04 - 05] = 0x55555555 0x55555555
state[06 - 07] = 0x55555555 0x55555555
state[08 - 09] = 0x55555555 0x55555555
state[10 - 11] = 0x55555555 0x55555555
state[12 - 13] = 0x00000000 0x00000000
state[14 - 15] = 0x55555555 0x55555555
```

Keystream block :

```
0x35 0x7d 0x7d 0x94 0xf9 0x66 0x77 0x8f
0x58 0x15 0xa2 0x05 0x1d 0xcb 0x04 0x13
0x3b 0x26 0xb0 0xea 0xd9 0xf5 0x7d 0xd0
0x99 0x27 0x83 0x7b 0xc3 0x06 0x7e 0x4b
0x6b 0xf2 0x99 0xad 0x81 0xf7 0xf5 0x0c
0x8d 0xa8 0x3c 0x78 0x10 0xbf 0xc1 0x7b
0xb6 0xf4 0x81 0x3a 0xb6 0xc3 0x26 0x95
```

0x70 0x45 0xfd 0x3f 0xd5 0xe1 0x99 0x15

Keystream block 1:

0xec 0x74 0x4a 0x6b 0x9b 0xf8 0xcb 0xdc
0xb3 0x6d 0x8b 0x6a 0x54 0x99 0xc6 0x8a
0x08 0xef 0x7b 0xe6 0xcc 0x1e 0x93 0xf2

Internet-Draft Test Vectors for the Stream Cipher ChaCha December 2013

0xf5 0xbc 0xd2 0xca 0xd4 0xe4 0x7c 0x18
0xa3 0xe5 0xd9 0x4b 0x56 0x66 0x38 0x2c
0x6d 0x13 0x0d 0x82 0x2d 0xd5 0x6a 0xac
0xb0 0xf8 0x19 0x52 0x78 0xe7 0xb2 0x92
0x49 0x5f 0x09 0x86 0x8d 0xdf 0x12 0xcc

Key: 0x55 0x55 0x55 0x55 0x55 0x55 0x55 0x55
0x55 0x55 0x55 0x55 0x55 0x55 0x55 0x55
0x55 0x55 0x55 0x55 0x55 0x55 0x55 0x55
0x55 0x55 0x55 0x55 0x55 0x55 0x55 0x55
IV: 0x55 0x55 0x55 0x55 0x55 0x55 0x55 0x55
Rounds: 8

Internal state after init:

state[00 - 01] = 0x61707865 0x3320646e
state[02 - 03] = 0x79622d32 0x6b206574
state[04 - 05] = 0x55555555 0x55555555
state[06 - 07] = 0x55555555 0x55555555
state[08 - 09] = 0x55555555 0x55555555
state[10 - 11] = 0x55555555 0x55555555
state[12 - 13] = 0x00000000 0x00000000
state[14 - 15] = 0x55555555 0x55555555

Keystream block :

0x7c 0xb7 0x82 0x14 0xe4 0xd3 0x46 0x5b
0x6d 0xc6 0x2c 0xf7 0xa1 0x53 0x8c 0x88
0x99 0x69 0x52 0xb4 0xfb 0x72 0xcb 0x61
0x05 0xf1 0x24 0x3c 0xe3 0x44 0x2e 0x29
0x75 0xa5 0x9e 0xbc 0xd2 0xb2 0xa5 0x98
0x29 0x0d 0x75 0x38 0x49 0x1f 0xe6 0x5b
0xdb 0xfe 0xfd 0x06 0x0d 0x88 0x79 0x81
0x20 0xa7 0x0d 0x04 0x9d 0xc2 0x67 0x7d

Keystream block 1:

```
0xd4 0x8f 0xf5 0xa2 0x51 0x3e 0x49 0x7a
0x5d 0x54 0x80 0x2d 0x74 0x84 0xc4 0xf1
0x08 0x39 0x44 0xd8 0xd0 0xd1 0x4d 0x64
0x82 0xce 0x09 0xf7 0xe5 0xeb 0xf2 0x0b
0x29 0x80 0x7d 0x62 0xc3 0x18 0x74 0xd0
0x2f 0x5d 0x3c 0xc8 0x53 0x81 0xa7 0x45
0xec 0xbc 0x60 0x52 0x52 0x05 0xe3 0x00
0xa7 0x69 0x61 0xbf 0xe5 0x1a 0xc0 0x7c
```

```
Key:    0x55 0x55 0x55 0x55 0x55 0x55 0x55 0x55
        0x55 0x55 0x55 0x55 0x55 0x55 0x55 0x55
        0x55 0x55 0x55 0x55 0x55 0x55 0x55 0x55
```

```
        0x55 0x55 0x55 0x55 0x55 0x55 0x55 0x55
IV:    0x55 0x55 0x55 0x55 0x55 0x55 0x55 0x55
Rounds: 12
```

Internal state after init:

```
state[00 - 01] = 0x61707865 0x3320646e
state[02 - 03] = 0x79622d32 0x6b206574
state[04 - 05] = 0x55555555 0x55555555
state[06 - 07] = 0x55555555 0x55555555
state[08 - 09] = 0x55555555 0x55555555
state[10 - 11] = 0x55555555 0x55555555
state[12 - 13] = 0x00000000 0x00000000
state[14 - 15] = 0x55555555 0x55555555
```

Keystream block :

```
0xa6 0x00 0xf0 0x77 0x27 0xff 0x93 0xf3
0xda 0x00 0xdd 0x74 0xcc 0x3e 0x8b 0xfb
0x5c 0xa7 0x30 0x2f 0x6a 0x0a 0x29 0x44
0x95 0x3d 0xe0 0x04 0x50 0xee 0xcd 0x40
0xb8 0x60 0xf6 0x60 0x49 0xf2 0xea 0xed
0x63 0xb2 0xef 0x39 0xcc 0x31 0x0d 0x2c
0x48 0x8f 0x5d 0x9a 0x24 0x1b 0x61 0x5d
0xc0 0xab 0x70 0xf9 0x21 0xb9 0x1b 0x95
```

Keystream block 1:

```
0x14 0x0e 0xff 0x4a 0xa4 0x95 0xac 0x61
0x28 0x9b 0x6b 0xc5 0x7d 0xe0 0x72 0x41
0x9d 0x09 0xda 0xa7 0xa7 0x24 0x39 0x90
```

```
0xda 0xf3 0x48 0xa8 0xf2 0x83 0x1e 0x59
0x7c 0xf3 0x79 0xb3 0xb2 0x84 0xf0 0x0b
0xda 0x27 0xa4 0xc6 0x80 0x85 0x37 0x4a
0x8a 0x5c 0x38 0xde 0xd6 0x2d 0x11 0x41
0xca 0xe0 0xbb 0x83 0x8d 0xdc 0x22 0x32
```

```
Key:    0x55 0x55 0x55 0x55 0x55 0x55 0x55 0x55
        0x55 0x55 0x55 0x55 0x55 0x55 0x55 0x55
        0x55 0x55 0x55 0x55 0x55 0x55 0x55 0x55
        0x55 0x55 0x55 0x55 0x55 0x55 0x55 0x55
IV:     0x55 0x55 0x55 0x55 0x55 0x55 0x55 0x55
Rounds: 20
```

```
Internal state after init:
state[00 - 01] = 0x61707865 0x3320646e
state[02 - 03] = 0x79622d32 0x6b206574
state[04 - 05] = 0x55555555 0x55555555
state[06 - 07] = 0x55555555 0x55555555
state[08 - 09] = 0x55555555 0x55555555
```

Internet-Draft Test Vectors for the Stream Cipher ChaCha December 2013

```
state[10 - 11] = 0x55555555 0x55555555
state[12 - 13] = 0x00000000 0x00000000
state[14 - 15] = 0x55555555 0x55555555
```

```
Keystream block :
0xbe 0xa9 0x41 0x1a 0xa4 0x53 0xc5 0x43
0x4a 0x5a 0xe8 0xc9 0x28 0x62 0xf5 0x64
0x39 0x68 0x55 0xa9 0xea 0x6e 0x22 0xd6
0xd3 0xb5 0x0a 0xe1 0xb3 0x66 0x33 0x11
0xa4 0xa3 0x60 0x6c 0x67 0x1d 0x60 0x5c
0xe1 0x6c 0x3a 0xec 0xe8 0xe6 0x1e 0xa1
0x45 0xc5 0x97 0x75 0x01 0x7b 0xee 0x2f
0xa6 0xf8 0x8a 0xfc 0x75 0x80 0x69 0xf7
```

```
Keystream block 1:
0xe0 0xb8 0xf6 0x76 0xe6 0x44 0x21 0x6f
0x4d 0x2a 0x34 0x22 0xd7 0xfa 0x36 0xc6
0xc4 0x93 0x1a 0xca 0x95 0x0e 0x9d 0xa4
0x27 0x88 0xe6 0xd0 0xb6 0xd1 0xcd 0x83
0x8e 0xf6 0x52 0xe9 0x7b 0x14 0x5b 0x14
0x87 0x1e 0xae 0x6c 0x68 0x04 0xc7 0x00
```

0x4d 0xb5 0xac 0x2f 0xce 0x4c 0x68 0xc7
0x26 0xd0 0x04 0xb1 0x0f 0xca 0xba 0x86

TC6: Every odd bit set in key and IV.

Key: 0xaa 0xaa 0xaa 0xaa 0xaa 0xaa 0xaa 0xaa
0xaa 0xaa 0xaa 0xaa 0xaa 0xaa 0xaa 0xaa
IV: 0xaa 0xaa 0xaa 0xaa 0xaa 0xaa 0xaa 0xaa
Rounds: 8

Internal state after init:
state[00 - 01] = 0x61707865 0x3120646e
state[02 - 03] = 0x79622d36 0x6b206574
state[04 - 05] = 0aaaaaaaa 0aaaaaaaa
state[06 - 07] = 0aaaaaaaa 0aaaaaaaa
state[08 - 09] = 0aaaaaaaa 0aaaaaaaa
state[10 - 11] = 0aaaaaaaa 0aaaaaaaa
state[12 - 13] = 0x00000000 0x00000000
state[14 - 15] = 0aaaaaaaa 0aaaaaaaa

Keystream block :
0x31 0x2d 0x95 0xc0 0xbc 0x38 0xef 0xf4
0x94 0x2d 0xb2 0xd5 0x0b 0xdc 0x50 0x0a
0x30 0x64 0x1e 0xf7 0x13 0x2d 0xb1 0xa8
0xae 0x83 0x8b 0x3b 0xea 0x3a 0x7a 0xb0
0x38 0x15 0xd7 0xa4 0xcc 0x09 0xdb 0xf5

0x88 0x2a 0x34 0x33 0xd7 0x43 0xac 0xed
0x48 0x13 0x6e 0xba 0xb7 0x32 0x99 0x50
0x68 0x55 0xc0 0xf5 0x43 0x7a 0x36 0xc6

Keystream block 1:
0xef 0x5a 0xd3 0xd6 0xa4 0xf6 0xc3 0x5d
0x9d 0x66 0xc2 0xe3 0x40 0x05 0xb9 0x1b
0xbb 0xe3 0x09 0x9e 0x13 0x5a 0x00 0xce
0x2f 0x70 0x07 0x45 0xbe 0x62 0x53 0x19
0x58 0x24 0xd4 0xb1 0x9f 0x69 0x73 0x1b
0x61 0x77 0xe6 0x24 0x35 0x8c 0x79 0x77
0xe6 0x75 0x52 0xf5 0x19 0xb4 0x70 0xe3
0xf7 0xa8 0xec 0x96 0x5d 0xc3 0xbe 0xda

Key: 0xaa 0xaa 0xaa 0xaa 0xaa 0xaa 0xaa 0xaa
0xaa 0xaa 0xaa 0xaa 0xaa 0xaa 0xaa 0xaa
IV: 0xaa 0xaa 0xaa 0xaa 0xaa 0xaa 0xaa 0xaa
Rounds: 12

Internal state after init:
state[00 - 01] = 0x61707865 0x3120646e
state[02 - 03] = 0x79622d36 0x6b206574
state[04 - 05] = 0xaaaaaaaa 0xaaaaaaaa
state[06 - 07] = 0xaaaaaaaa 0xaaaaaaaa
state[08 - 09] = 0xaaaaaaaa 0xaaaaaaaa
state[10 - 11] = 0xaaaaaaaa 0xaaaaaaaa
state[12 - 13] = 0x00000000 0x00000000
state[14 - 15] = 0xaaaaaaaa 0xaaaaaaaa

Keystream block :
0x05 0x7f 0xe8 0x4f 0xea 0xd1 0x3c 0x24
0xb7 0x6b 0xb2 0xa6 0xfd 0xde 0x66 0xf2
0x68 0x8e 0x8e 0xb6 0x26 0x82 0x75 0xc2
0x2c 0x6b 0xcb 0x90 0xb8 0x56 0x16 0xd7
0xfe 0x4d 0x31 0x93 0xa1 0x03 0x6b 0x70
0xd7 0xfb 0x86 0x4f 0x01 0x45 0x36 0x41
0x85 0x10 0x29 0xec 0xdb 0x60 0xac 0x38
0x79 0xf5 0x64 0x96 0xf1 0x62 0x13 0xf4

Keystream block 1:
0xe9 0xe6 0x19 0x45 0xb8 0xd8 0x54 0xa1
0x74 0x9a 0x7c 0x1f 0xc5 0xfb 0x58 0x4d
0xcf 0xc6 0x8c 0x55 0x8e 0x6e 0xfe 0x04
0x5b 0x51 0xd5 0x13 0xeb 0xeb 0x09 0x3f
0xbe 0x91 0xd7 0xba 0x36 0xdc 0x6f 0x0c
0x8c 0x7c 0xfa 0x66 0x65 0x4a 0xd9 0x9d
0x64 0xc3 0x42 0xbb 0x30 0x47 0x36 0x8b

0x7e 0xdd 0xdf 0x83 0x6c 0x72 0x53 0xcc

Key: 0xaa 0xaa 0xaa 0xaa 0xaa 0xaa 0xaa 0xaa
0xaa 0xaa 0xaa 0xaa 0xaa 0xaa 0xaa 0xaa
IV: 0xaa 0xaa 0xaa 0xaa 0xaa 0xaa 0xaa 0xaa
Rounds: 20

Internal state after init:
state[00 - 01] = 0x61707865 0x3120646e
state[02 - 03] = 0x79622d36 0x6b206574
state[04 - 05] = 0xaaaaaaaa 0xaaaaaaaa
state[06 - 07] = 0xaaaaaaaa 0xaaaaaaaa
state[08 - 09] = 0xaaaaaaaa 0xaaaaaaaa
state[10 - 11] = 0xaaaaaaaa 0xaaaaaaaa
state[12 - 13] = 0x00000000 0x00000000
state[14 - 15] = 0xaaaaaaaa 0xaaaaaaaa

Keystream block :
0xfc 0x79 0xac 0xbd 0x58 0x52 0x61 0x03
0x86 0x27 0x76 0xaa 0xb2 0x0f 0x3b 0x7d
0x8d 0x31 0x49 0xb2 0xfa 0xb6 0x57 0x66
0x29 0x93 0x16 0xb6 0xe5 0xb1 0x66 0x84
0xde 0x5d 0xe5 0x48 0xc1 0xb7 0xd0 0x83
0xef 0xd9 0xe3 0x05 0x23 0x19 0xe0 0xc6
0x25 0x41 0x41 0xda 0x04 0xa6 0x58 0x6d
0xf8 0x00 0xf6 0x4d 0x46 0xb0 0x1c 0x87

Keystream block 1:
0x1f 0x05 0xbc 0x67 0xe0 0x76 0x28 0xeb
0xe6 0xf6 0x86 0x5a 0x21 0x77 0xe0 0xb6
0x6a 0x55 0x8a 0xa7 0xcc 0x1e 0x8f 0xf1
0xa9 0x8d 0x27 0xf7 0x07 0x1f 0x83 0x35
0xef 0xce 0x45 0x37 0xbb 0x0e 0xf7 0xb5
0x73 0xb3 0x2f 0x32 0x76 0x5f 0x29 0x00
0x7d 0xa5 0x3b 0xba 0x62 0xe7 0xa4 0x4d
0x00 0x6f 0x41 0xeb 0x28 0xfe 0x15 0xd6

Key: 0xaa 0xaa 0xaa 0xaa 0xaa 0xaa 0xaa 0xaa
0xaa 0xaa 0xaa 0xaa 0xaa 0xaa 0xaa 0xaa
0xaa 0xaa 0xaa 0xaa 0xaa 0xaa 0xaa 0xaa
0xaa 0xaa 0xaa 0xaa 0xaa 0xaa 0xaa 0xaa
IV: 0xaa 0xaa 0xaa 0xaa 0xaa 0xaa 0xaa 0xaa
Rounds: 8

Internal state after init:
state[00 - 01] = 0x61707865 0x3320646e

```
state[02 - 03] = 0x79622d32 0x6b206574
state[04 - 05] = 0xaaaaaaaa 0xaaaaaaaa
state[06 - 07] = 0xaaaaaaaa 0xaaaaaaaa
state[08 - 09] = 0xaaaaaaaa 0xaaaaaaaa
state[10 - 11] = 0xaaaaaaaa 0xaaaaaaaa
state[12 - 13] = 0x00000000 0x00000000
state[14 - 15] = 0xaaaaaaaa 0xaaaaaaaa
```

Keystream block :

```
0x40 0xf9 0xab 0x86 0xc8 0xf9 0xa1 0xa0
0xcd 0xc0 0x5a 0x75 0xe5 0x53 0x1b 0x61
0x2d 0x71 0xef 0x7f 0x0c 0xf9 0xe3 0x87
0xdf 0x6e 0xd6 0x97 0x2f 0x0a 0xae 0x21
0x31 0x1a 0xa5 0x81 0xf8 0x16 0xc9 0x0e
0x8a 0x99 0xde 0x99 0x0b 0x6b 0x95 0xaa
0xc9 0x24 0x50 0xf4 0xe1 0x12 0x71 0x26
0x67 0xb8 0x04 0xc9 0x9e 0x9c 0x6e 0xda
```

Keystream block 1:

```
0xf8 0xd1 0x44 0xf5 0x60 0xc8 0xc0 0xea
0x36 0x88 0x0d 0x3b 0x77 0x87 0x4c 0x9a
0x91 0x03 0xd1 0x47 0xf6 0xde 0xd3 0x86
0x28 0x48 0x01 0xa4 0xee 0x15 0x8e 0x5e
0xa4 0xf9 0xc0 0x93 0xfc 0x55 0xfd 0x34
0x4c 0x33 0x34 0x9d 0xc5 0xb6 0x99 0xe2
0x1d 0xc8 0x3b 0x42 0x96 0xf9 0x2e 0xe3
0xec 0xab 0xf3 0xd5 0x1f 0x95 0xfe 0x3f
```

```
Key:    0xaa 0xaa 0xaa 0xaa 0xaa 0xaa 0xaa 0xaa
        0xaa 0xaa 0xaa 0xaa 0xaa 0xaa 0xaa 0xaa
        0xaa 0xaa 0xaa 0xaa 0xaa 0xaa 0xaa 0xaa
        0xaa 0xaa 0xaa 0xaa 0xaa 0xaa 0xaa 0xaa
```

```
IV:    0xaa 0xaa 0xaa 0xaa 0xaa 0xaa 0xaa 0xaa
```

Rounds: 12

Internal state after init:

```
state[00 - 01] = 0x61707865 0x3320646e
state[02 - 03] = 0x79622d32 0x6b206574
state[04 - 05] = 0xaaaaaaaa 0xaaaaaaaa
state[06 - 07] = 0xaaaaaaaa 0xaaaaaaaa
state[08 - 09] = 0xaaaaaaaa 0xaaaaaaaa
state[10 - 11] = 0xaaaaaaaa 0xaaaaaaaa
state[12 - 13] = 0x00000000 0x00000000
state[14 - 15] = 0xaaaaaaaa 0xaaaaaaaa
```

Keystream block :

```
0x85 0x65 0x05 0xb0 0x1d 0x3b 0x47 0xaa
```

Internet-Draft Test Vectors for the Stream Cipher ChaCha December 2013

```
0xe0 0x3d 0x6a 0x97 0xaa 0x0f 0x03 0x3a
0x9a 0xdc 0xc9 0x43 0x77 0xba 0xbd 0x86
0x08 0x86 0x4f 0xb3 0xf6 0x25 0xb6 0xe3
0x14 0xf0 0x86 0x15 0x8f 0x9f 0x72 0x5d
0x81 0x1e 0xeb 0x95 0x3b 0x7f 0x74 0x70
0x76 0xe4 0xc3 0xf6 0x39 0xfa 0x84 0x1f
0xad 0x6c 0x9a 0x70 0x9e 0x62 0x13 0x97
```

Keystream block 1:

```
0x6d 0xd6 0xee 0x9b 0x5e 0x1e 0x2e 0x67
0x6b 0x1c 0x9e 0x2b 0x82 0xc2 0xe9 0x6c
0x16 0x48 0x43 0x7b 0xff 0x2f 0x01 0x26
0xb7 0x4e 0x8c 0xe0 0xa9 0xb0 0x6d 0x17
0x20 0xac 0x0b 0x6f 0x09 0x08 0x6f 0x28
0xbc 0x20 0x15 0x87 0xf0 0x53 0x5e 0xd9
0x38 0x52 0x70 0xd0 0x8b 0x4a 0x93 0x82
0xf1 0x8f 0x82 0xdb 0xde 0x18 0x21 0x0e
```

```
Key:    0xaa 0xaa 0xaa 0xaa 0xaa 0xaa 0xaa 0xaa
        0xaa 0xaa 0xaa 0xaa 0xaa 0xaa 0xaa 0xaa
        0xaa 0xaa 0xaa 0xaa 0xaa 0xaa 0xaa 0xaa
        0xaa 0xaa 0xaa 0xaa 0xaa 0xaa 0xaa 0xaa
IV:     0xaa 0xaa 0xaa 0xaa 0xaa 0xaa 0xaa 0xaa
Rounds: 20
```

Internal state after init:

```
state[00 - 01] = 0x61707865 0x3320646e
state[02 - 03] = 0x79622d32 0x6b206574
state[04 - 05] = 0aaaaaaaa 0aaaaaaaa
state[06 - 07] = 0aaaaaaaa 0aaaaaaaa
state[08 - 09] = 0aaaaaaaa 0aaaaaaaa
state[10 - 11] = 0aaaaaaaa 0aaaaaaaa
state[12 - 13] = 0x00000000 0x00000000
state[14 - 15] = 0aaaaaaaa 0aaaaaaaa
```

Keystream block :

```
0x9a 0xa2 0xa9 0xf6 0x56 0xef 0xde 0x5a
0xa7 0x59 0x1c 0x5f 0xed 0x4b 0x35 0xae
0xa2 0x89 0x5d 0xec 0x7c 0xb4 0x54 0x3b
0x9e 0x9f 0x21 0xf5 0xe7 0xbc 0xbc 0xf3
0xc4 0x3c 0x74 0x8a 0x97 0x08 0x88 0xf8
0x24 0x83 0x93 0xa0 0x9d 0x43 0xe0 0xb7
```

0xe1 0x64 0xbc 0x4d 0x0b 0x0f 0xb2 0x40
0xa2 0xd7 0x21 0x15 0xc4 0x80 0x89 0x06

Keystream block 1:

0x72 0x18 0x44 0x89 0x44 0x05 0x45 0xd0

Internet-Draft Test Vectors for the Stream Cipher ChaCha December 2013

0x21 0xd9 0x7e 0xf6 0xb6 0x93 0xdf 0xe5
0xb2 0xc1 0x32 0xd4 0x7e 0x6f 0x04 0x1c
0x90 0x63 0x65 0x1f 0x96 0xb6 0x23 0xe6
0x2a 0x11 0x99 0x9a 0x23 0xb6 0xf7 0xc4
0x61 0xb2 0x15 0x30 0x26 0xad 0x5e 0x86
0x6a 0x2e 0x59 0x7e 0xd0 0x7b 0x84 0x01
0xde 0xc6 0x3a 0x09 0x34 0xc6 0xb2 0xa9

TC7: Sequence patterns in key and IV.

Key: 0x00 0x11 0x22 0x33 0x44 0x55 0x66 0x77
0x88 0x99 0xaa 0xbb 0xcc 0xdd 0xee 0xff
IV: 0x0f 0x1e 0x2d 0x3c 0x4b 0x5a 0x69 0x78
Rounds: 8

Internal state after init:

state[00 - 01] = 0x61707865 0x3120646e
state[02 - 03] = 0x79622d36 0x6b206574
state[04 - 05] = 0x33221100 0x77665544
state[06 - 07] = 0xbbaa9988 0xffeeddcc
state[08 - 09] = 0x33221100 0x77665544
state[10 - 11] = 0xbbaa9988 0xffeeddcc
state[12 - 13] = 0x00000000 0x00000000
state[14 - 15] = 0x3c2d1e0f 0x78695a4b

Keystream block :

0x29 0x56 0x0d 0x28 0x0b 0x45 0x28 0x40
0x0a 0x8f 0x4b 0x79 0x53 0x69 0xfb 0x3a
0x01 0x10 0x55 0x99 0xe9 0xf1 0xed 0x58
0x27 0x9c 0xfc 0x9e 0xce 0x2d 0xc5 0xf9
0x9f 0x1c 0x2e 0x52 0xc9 0x82 0x38 0xf5
0x42 0xa5 0xc0 0xa8 0x81 0xd8 0x50 0xb6
0x15 0xd3 0xac 0xd9 0xfb 0xdb 0x02 0x6e
0x93 0x68 0x56 0x5d 0xa5 0x0e 0x0d 0x49

Keystream block 1:

```
0xdd 0x5b 0xe8 0xef 0x74 0x24 0x8b 0x3e
0x25 0x1d 0x96 0x5d 0x8f 0xcb 0x21 0xe7
0xcf 0xe2 0x04 0xd4 0x00 0x78 0x06 0xfb
0xee 0x3c 0xe9 0x4c 0x74 0xbf 0xba 0xd2
0xc1 0x1c 0x62 0x1b 0xa0 0x48 0x14 0x7c
0x5c 0xaa 0x94 0xd1 0x82 0xcc 0xff 0x6f
0xd5 0xcf 0x44 0xad 0xf9 0x6e 0x3d 0x68
0x28 0x1b 0xb4 0x96 0x76 0xaf 0x87 0xe7
```

Key: 0x00 0x11 0x22 0x33 0x44 0x55 0x66 0x77

```
0x88 0x99 0xaa 0xbb 0xcc 0xdd 0xee 0xff
IV: 0x0f 0x1e 0x2d 0x3c 0x4b 0x5a 0x69 0x78
Rounds: 12
```

Internal state after init:

```
state[00 - 01] = 0x61707865 0x3120646e
state[02 - 03] = 0x79622d36 0x6b206574
state[04 - 05] = 0x33221100 0x77665544
state[06 - 07] = 0xbbaa9988 0xffeeddcc
state[08 - 09] = 0x33221100 0x77665544
state[10 - 11] = 0xbbaa9988 0xffeeddcc
state[12 - 13] = 0x00000000 0x00000000
state[14 - 15] = 0x3c2d1e0f 0x78695a4b
```

Keystream block :

```
0x5e 0xdd 0xc2 0xd9 0x42 0x8f 0xce 0xee
0xc5 0x0a 0x52 0xa9 0x64 0xea 0xe0 0xff
0xb0 0x4b 0x2d 0xe0 0x06 0xa9 0xb0 0x4c
0xff 0x36 0x8f 0xfa 0x92 0x11 0x16 0xb2
0xe8 0xe2 0x64 0xba 0xbd 0x2e 0xfa 0x0d
0xe4 0x3e 0xf2 0xe3 0xb6 0xd0 0x65 0xe8
0xf7 0xc0 0xa1 0x78 0x37 0xb0 0xa4 0x0e
0xb0 0xe2 0xc7 0xa3 0x74 0x2c 0x87 0x53
```

Keystream block 1:

```
0xed 0xe5 0xf3 0xf6 0xd1 0x9b 0xe5 0x54
0x67 0x5e 0x50 0x6a 0x77 0x5c 0x63 0xf0
0x94 0xd4 0x96 0x5c 0x31 0x93 0x19 0xdc
0xd7 0x50 0x6f 0x45 0x7b 0x11 0x7b 0x84
```

```
0xb1 0x0b 0x24 0x6e 0x95 0x6c 0x2d 0xa8
0x89 0x8a 0x65 0x6c 0xee 0xf3 0xf7 0xb7
0x16 0x45 0xb1 0x9f 0x70 0x1d 0xb8 0x44
0x85 0xce 0x51 0x21 0xf0 0xf6 0x17 0xef
```

```
Key:      0x00 0x11 0x22 0x33 0x44 0x55 0x66 0x77
          0x88 0x99 0xaa 0xbb 0xcc 0xdd 0xee 0xff
IV:      0x0f 0x1e 0x2d 0x3c 0x4b 0x5a 0x69 0x78
Rounds: 20
```

```
Internal state after init:
state[00 - 01] = 0x61707865 0x3120646e
state[02 - 03] = 0x79622d36 0x6b206574
state[04 - 05] = 0x33221100 0x77665544
state[06 - 07] = 0xbbaa9988 0xffeeddcc
state[08 - 09] = 0x33221100 0x77665544
state[10 - 11] = 0xbbaa9988 0xffeeddcc
state[12 - 13] = 0x00000000 0x00000000
```

```
state[14 - 15] = 0x3c2d1e0f 0x78695a4b
```

Keystream block :

```
0xd1 0xab 0xf6 0x30 0x46 0x7e 0xb4 0xf6
0x7f 0x1c 0xfb 0x47 0xcd 0x62 0x6a 0xae
0x8a 0xfe 0xdb 0xbe 0x4f 0xf8 0xfc 0x5f
0xe9 0xcf 0xae 0x30 0x7e 0x74 0xed 0x45
0x1f 0x14 0x04 0x42 0x5a 0xd2 0xb5 0x45
0x69 0xd5 0xf1 0x81 0x48 0x93 0x99 0x71
0xab 0xb8 0xfa 0xfc 0x88 0xce 0x4a 0xc7
0xfe 0x1c 0x3d 0x1f 0x7a 0x1e 0xb7 0xca
```

Keystream block 1:

```
0xe7 0x6c 0xa8 0x7b 0x61 0xa9 0x71 0x35
0x41 0x49 0x77 0x60 0xdd 0x9a 0xe0 0x59
0x35 0x0c 0xad 0x0d 0xce 0xdf 0xaa 0x80
0xa8 0x83 0x11 0x9a 0x1a 0x6f 0x98 0x7f
0xd1 0xce 0x91 0xfd 0x8e 0xe0 0x82 0x80
0x34 0xb4 0x11 0x20 0x0a 0x97 0x45 0xa2
0x85 0x55 0x44 0x75 0xd1 0x2a 0xfc 0x04
0x88 0x7f 0xef 0x35 0x16 0xd1 0x2a 0x2c
```

Key: 0x00 0x11 0x22 0x33 0x44 0x55 0x66 0x77
0x88 0x99 0xaa 0xbb 0xcc 0xdd 0xee 0xff
0xff 0xee 0xdd 0xcc 0xbb 0xaa 0x99 0x88
0x77 0x66 0x55 0x44 0x33 0x22 0x11 0x00
IV: 0x0f 0x1e 0x2d 0x3c 0x4b 0x5a 0x69 0x78
Rounds: 8

Internal state after init:

state[00 - 01] = 0x61707865 0x3320646e
state[02 - 03] = 0x79622d32 0x6b206574
state[04 - 05] = 0x33221100 0x77665544
state[06 - 07] = 0xbbaa9988 0xffeeddcc
state[08 - 09] = 0xccddeeff 0x8899aabb
state[10 - 11] = 0x44556677 0x00112233
state[12 - 13] = 0x00000000 0x00000000
state[14 - 15] = 0x3c2d1e0f 0x78695a4b

Keystream block :

0xdb 0x43 0xad 0x9d 0x1e 0x84 0x2d 0x12
0x72 0xe4 0x53 0x0e 0x27 0x6b 0x3f 0x56
0x8f 0x88 0x59 0xb3 0xf7 0xcf 0x6d 0x9d
0x2c 0x74 0xfa 0x53 0x80 0x8c 0xb5 0x15
0x7a 0x8e 0xbf 0x46 0xad 0x3d 0xcc 0x4b
0x6c 0x7d 0xad 0xde 0x13 0x17 0x84 0xb0
0x12 0x0e 0x0e 0x22 0xf6 0xd5 0xf9 0xff

0xa7 0x40 0x7d 0x4a 0x21 0xb6 0x95 0xd9

Keystream block 1:

0xc5 0xdd 0x30 0xbf 0x55 0x61 0x2f 0xab
0x9b 0xdd 0x11 0x89 0x20 0xc1 0x98 0x16
0x47 0x0c 0x7f 0x5d 0xcd 0x42 0x32 0x5d
0xbb 0xed 0x8c 0x57 0xa5 0x62 0x81 0xc1
0x44 0xcb 0x0f 0x03 0xe8 0x1b 0x30 0x04
0x62 0x4e 0x06 0x50 0xa1 0xce 0x5a 0xfa
0xf9 0xa7 0xcd 0x81 0x63 0xf6 0xdb 0xd7
0x26 0x02 0x25 0x7d 0xd9 0x6e 0x47 0x1e

Key: 0x00 0x11 0x22 0x33 0x44 0x55 0x66 0x77
0x88 0x99 0xaa 0xbb 0xcc 0xdd 0xee 0xff

```
0xff 0xee 0xdd 0xcc 0xbb 0xaa 0x99 0x88
0x77 0x66 0x55 0x44 0x33 0x22 0x11 0x00
IV:    0x0f 0x1e 0x2d 0x3c 0x4b 0x5a 0x69 0x78
Rounds: 12
```

```
Internal state after init:
state[00 - 01] = 0x61707865 0x3320646e
state[02 - 03] = 0x79622d32 0x6b206574
state[04 - 05] = 0x33221100 0x77665544
state[06 - 07] = 0xbbaa9988 0xffeeddcc
state[08 - 09] = 0xccddeeff 0x8899aabb
state[10 - 11] = 0x44556677 0x00112233
state[12 - 13] = 0x00000000 0x00000000
state[14 - 15] = 0x3c2d1e0f 0x78695a4b
```

```
Keystream block :
0x7e 0xd1 0x2a 0x3a 0x63 0x91 0x2a 0xe9
0x41 0xba 0x6d 0x4c 0x0d 0x5e 0x86 0x2e
0x56 0x8b 0x0e 0x55 0x89 0x34 0x69 0x35
0x50 0x5f 0x06 0x4b 0x8c 0x26 0x98 0xdb
0xf7 0xd8 0x50 0x66 0x7d 0x8e 0x67 0xbe
0x63 0x9f 0x3b 0x4f 0x6a 0x16 0xf9 0x2e
0x65 0xea 0x80 0xf6 0xc7 0x42 0x94 0x45
0xda 0x1f 0xc2 0xc1 0xb9 0x36 0x50 0x40
```

```
Keystream block 1:
0xe3 0x2e 0x50 0xc4 0x10 0x6f 0x3b 0x3d
0xa1 0xce 0x7c 0xcb 0x1e 0x71 0x40 0xb1
0x53 0x49 0x3c 0x0f 0x3a 0xd9 0xa9 0xbc
0xff 0x07 0x7e 0xc4 0x59 0x6f 0x1d 0x0f
0x29 0xbf 0x9c 0xba 0xa5 0x02 0x82 0x0f
0x73 0x2a 0xf5 0xa9 0x3c 0x49 0xee 0xe3
0x3d 0x1c 0x4f 0x12 0xaf 0x3b 0x42 0x97
```

```
0xaf 0x91 0xfe 0x41 0xea 0x9e 0x94 0xa2
```

```
Key:    0x00 0x11 0x22 0x33 0x44 0x55 0x66 0x77
        0x88 0x99 0xaa 0xbb 0xcc 0xdd 0xee 0xff
        0xff 0xee 0xdd 0xcc 0xbb 0xaa 0x99 0x88
        0x77 0x66 0x55 0x44 0x33 0x22 0x11 0x00
IV:     0x0f 0x1e 0x2d 0x3c 0x4b 0x5a 0x69 0x78
```


Rounds: 20

Internal state after init:

```
state[00 - 01] = 0x61707865 0x3320646e
state[02 - 03] = 0x79622d32 0x6b206574
state[04 - 05] = 0x33221100 0x77665544
state[06 - 07] = 0xbbaa9988 0xffeeddcc
state[08 - 09] = 0xccddeeff 0x8899aabb
state[10 - 11] = 0x44556677 0x00112233
state[12 - 13] = 0x00000000 0x00000000
state[14 - 15] = 0x3c2d1e0f 0x78695a4b
```

Keystream block :

```
0x9f 0xad 0xf4 0x09 0xc0 0x08 0x11 0xd0
0x04 0x31 0xd6 0x7e 0xfb 0xd8 0x8f 0xba
0x59 0x21 0x8d 0x5d 0x67 0x08 0xb1 0xd6
0x85 0x86 0x3f 0xab 0xbb 0x0e 0x96 0x1e
0xea 0x48 0x0f 0xd6 0xfb 0x53 0x2b 0xfd
0x49 0x4b 0x21 0x51 0x01 0x50 0x57 0x42
0x3a 0xb6 0x0a 0x63 0xfe 0x4f 0x55 0xf7
0xa2 0x12 0xe2 0x16 0x7c 0xca 0xb9 0x31
```

Keystream block 1:

```
0xfb 0xfd 0x29 0xcf 0x7b 0xc1 0xd2 0x79
0xed 0xdf 0x25 0xdd 0x31 0x6b 0xb8 0x84
0x3d 0x6e 0xde 0xe0 0xbd 0x1e 0xf1 0x21
0xd1 0x2f 0xa1 0x7c 0xbc 0x2c 0x57 0x4c
0xcc 0xab 0x5e 0x27 0x51 0x67 0xb0 0x8b
0xd6 0x86 0xf8 0xa0 0x9d 0xf8 0x7e 0xc3
0xff 0xb3 0x53 0x61 0xb9 0x4e 0xbf 0xa1
0x3f 0xec 0x0e 0x48 0x89 0xd1 0x8d 0xa5
```

TC8: key: 'All your base are belong to us!', IV: 'IETF2013'

```
-----
Key:    0xc4 0x6e 0xc1 0xb1 0x8c 0xe8 0xa8 0x78
        0x72 0x5a 0x37 0xe7 0x80 0xdf 0xb7 0x35
IV:     0x1a 0xda 0x31 0xd5 0xcf 0x68 0x82 0x21
Rounds: 8
```

Internal state after init:

```
state[00 - 01] = 0x61707865 0x3120646e
state[02 - 03] = 0x79622d36 0x6b206574
state[04 - 05] = 0xb1c16ec4 0x78a8e88c
state[06 - 07] = 0xe7375a72 0x35b7df80
state[08 - 09] = 0xb1c16ec4 0x78a8e88c
state[10 - 11] = 0xe7375a72 0x35b7df80
state[12 - 13] = 0x00000000 0x00000000
state[14 - 15] = 0xd531da1a 0x218268cf
```

Keystream block :

```
0x6a 0x87 0x01 0x08 0x85 0x9f 0x67 0x91
0x18 0xf3 0xe2 0x05 0xe2 0xa5 0x6a 0x68
0x26 0xef 0x5a 0x60 0xa4 0x10 0x2a 0xc8
0xd4 0x77 0x00 0x59 0xfc 0xb7 0xc7 0xba
0xe0 0x2f 0x5c 0xe0 0x04 0xa6 0xbf 0xbb
0xea 0x53 0x01 0x4d 0xd8 0x21 0x07 0xc0
0xaa 0x1c 0x7c 0xe1 0x1b 0x7d 0x78 0xf2
0xd5 0x0b 0xd3 0x60 0x2b 0xbd 0x25 0x94
```

Keystream block 1:

```
0x05 0x60 0xbb 0x6a 0x84 0x28 0x9e 0x0b
0x38 0xf5 0xdd 0x21 0xd6 0xef 0x6d 0x77
0x37 0xe3 0xec 0x0f 0xb7 0x72 0xda 0x2c
0x71 0xc2 0x39 0x77 0x62 0xe5 0xdb 0xbb
0xf4 0x49 0xe3 0xd1 0x63 0x9c 0xcb 0xfa
0x3e 0x06 0x9c 0x4d 0x87 0x1e 0xd6 0x39
0x5b 0x22 0xaa 0xf3 0x5c 0x8d 0xa6 0xde
0x2d 0xec 0x3d 0x77 0x88 0x0d 0xa8 0xe8
```

```
Key:      0xc4 0x6e 0xc1 0xb1 0x8c 0xe8 0xa8 0x78
          0x72 0x5a 0x37 0xe7 0x80 0xdf 0xb7 0x35
IV:       0x1a 0xda 0x31 0xd5 0xcf 0x68 0x82 0x21
Rounds: 12
```

Internal state after init:

```
state[00 - 01] = 0x61707865 0x3120646e
state[02 - 03] = 0x79622d36 0x6b206574
state[04 - 05] = 0xb1c16ec4 0x78a8e88c
state[06 - 07] = 0xe7375a72 0x35b7df80
state[08 - 09] = 0xb1c16ec4 0x78a8e88c
state[10 - 11] = 0xe7375a72 0x35b7df80
state[12 - 13] = 0x00000000 0x00000000
state[14 - 15] = 0xd531da1a 0x218268cf
```

Keystream block :

```
0xb0 0x2b 0xd8 0x1e 0xb5 0x5c 0x8f 0x68
```

0xb5 0xe9 0xca 0x4e 0x30 0x70 0x79 0xbc
0x22 0x5b 0xd2 0x20 0x07 0xed 0xdc 0x67
0x02 0x80 0x18 0x20 0x70 0x9c 0xe0 0x98
0x07 0x04 0x6a 0x0d 0x2a 0xa5 0x52 0xbf
0xdb 0xb4 0x94 0x66 0x17 0x6d 0x56 0xe3
0x2d 0x51 0x9e 0x10 0xf5 0xad 0x5f 0x27
0x46 0xe2 0x41 0xe0 0x9b 0xdf 0x99 0x59

Keystream block 1:

0x17 0xbe 0x08 0x73 0xed 0xde 0x9a 0xf5
0xb8 0x62 0x46 0x44 0x1c 0xe4 0x10 0x19
0x5b 0xae 0xde 0x41 0xf8 0xbd 0xab 0x6a
0xd2 0x53 0x22 0x63 0x82 0xee 0x38 0x3e
0x34 0x72 0xf9 0x45 0xa5 0xe6 0xbd 0x62
0x8c 0x7a 0x58 0x2b 0xcf 0x8f 0x89 0x98
0x70 0x59 0x6a 0x58 0xda 0xb8 0x3b 0x51
0xa5 0x0c 0x7d 0xbb 0x4f 0x3e 0x6e 0x76

Key: 0xc4 0x6e 0xc1 0xb1 0x8c 0xe8 0xa8 0x78
0x72 0x5a 0x37 0xe7 0x80 0xdf 0xb7 0x35
IV: 0x1a 0xda 0x31 0xd5 0xcf 0x68 0x82 0x21
Rounds: 20

Internal state after init:

state[00 - 01] = 0x61707865 0x3120646e
state[02 - 03] = 0x79622d36 0x6b206574
state[04 - 05] = 0xb1c16ec4 0x78a8e88c
state[06 - 07] = 0xe7375a72 0x35b7df80
state[08 - 09] = 0xb1c16ec4 0x78a8e88c
state[10 - 11] = 0xe7375a72 0x35b7df80
state[12 - 13] = 0x00000000 0x00000000
state[14 - 15] = 0xd531da1a 0x218268cf

Keystream block :

0x82 0x6a 0xbd 0xd8 0x44 0x60 0xe2 0xe9
0x34 0x9f 0x0e 0xf4 0xaf 0x5b 0x17 0x9b
0x42 0x6e 0x4b 0x2d 0x10 0x9a 0x9c 0x5b
0xb4 0x40 0x00 0xae 0x51 0xbe 0xa9 0x0a
0x49 0x6b 0xee 0xef 0x62 0xa7 0x68 0x50
0xff 0x3f 0x04 0x02 0xc4 0xdd 0xc9 0x9f
0x6d 0xb0 0x7f 0x15 0x1c 0x1c 0x0d 0xfa
0xc2 0xe5 0x65 0x65 0xd6 0x28 0x96 0x25

Keystream block 1:

0x5b 0x23 0x13 0x2e 0x7b 0x46 0x9c 0x7b

0xfb 0x88 0xfa 0x95 0xd4 0x4c 0xa5 0xae
0x3e 0x45 0xe8 0x48 0xa4 0x10 0x8e 0x98

Internet-Draft Test Vectors for the Stream Cipher ChaCha December 2013

0xba 0xd7 0xa9 0xeb 0x15 0x51 0x27 0x84
0xa6 0xa9 0xe6 0xe5 0x91 0xdc 0xe6 0x74
0x12 0x0a 0xca 0xf9 0x04 0x0f 0xf5 0x0f
0xf3 0xac 0x30 0xcc 0xfb 0x5e 0x14 0x20
0x4f 0x5e 0x42 0x68 0xb9 0x0a 0x88 0x04

Key: 0xc4 0x6e 0xc1 0xb1 0x8c 0xe8 0xa8 0x78
0x72 0x5a 0x37 0xe7 0x80 0xdf 0xb7 0x35
0x1f 0x68 0xed 0x2e 0x19 0x4c 0x79 0xfb
0xc6 0xae 0xbe 0xe1 0xa6 0x67 0x97 0x5d
IV: 0x1a 0xda 0x31 0xd5 0xcf 0x68 0x82 0x21
Rounds: 8

Internal state after init:

state[00 - 01] = 0x61707865 0x3320646e
state[02 - 03] = 0x79622d32 0x6b206574
state[04 - 05] = 0xb1c16ec4 0x78a8e88c
state[06 - 07] = 0xe7375a72 0x35b7df80
state[08 - 09] = 0x2eed681f 0xfb794c19
state[10 - 11] = 0xe1beaec6 0x5d9767a6
state[12 - 13] = 0x00000000 0x00000000
state[14 - 15] = 0xd531da1a 0x218268cf

Keystream block :

0x83 0x87 0x51 0xb4 0x2d 0x8d 0xdd 0x8a
0x3d 0x77 0xf4 0x88 0x25 0xa2 0xba 0x75
0x2c 0xf4 0x04 0x7c 0xb3 0x08 0xa5 0x97
0x8e 0xf2 0x74 0x97 0x3b 0xe3 0x74 0xc9
0x6a 0xd8 0x48 0x06 0x58 0x71 0x41 0x7b
0x08 0xf0 0x34 0xe6 0x81 0xfe 0x46 0xa9
0x3f 0x7d 0x5c 0x61 0xd1 0x30 0x66 0x14
0xd4 0xaa 0xf2 0x57 0xa7 0xcf 0xf0 0x8b

Keystream block 1:

0x16 0xf2 0xfd 0xa1 0x70 0xcc 0x18 0xa4
0xb5 0x8a 0x26 0x67 0xed 0x96 0x27 0x74
0xaf 0x79 0x2a 0x6e 0x7f 0x3c 0x77 0x99
0x25 0x40 0x71 0x1a 0x7a 0x13 0x6d 0x7e

0x8a 0x2f 0x8d 0x3f 0x93 0x81 0x67 0x09
0xd4 0x5a 0x3f 0xa5 0xf8 0xce 0x72 0xfd
0xe1 0x5b 0xe7 0xb8 0x41 0xac 0xba 0x3a
0x2a 0xbd 0x55 0x72 0x28 0xd9 0xfe 0x4f

Key: 0xc4 0x6e 0xc1 0xb1 0x8c 0xe8 0xa8 0x78
0x72 0x5a 0x37 0xe7 0x80 0xdf 0xb7 0x35
0x1f 0x68 0xed 0x2e 0x19 0x4c 0x79 0xfb

Internet-Draft Test Vectors for the Stream Cipher ChaCha December 2013

0xc6 0xae 0xbe 0xe1 0xa6 0x67 0x97 0x5d
IV: 0x1a 0xda 0x31 0xd5 0xcf 0x68 0x82 0x21
Rounds: 12

Internal state after init:

state[00 - 01] = 0x61707865 0x3320646e
state[02 - 03] = 0x79622d32 0x6b206574
state[04 - 05] = 0xb1c16ec4 0x78a8e88c
state[06 - 07] = 0xe7375a72 0x35b7df80
state[08 - 09] = 0x2eed681f 0xfb794c19
state[10 - 11] = 0xe1beaec6 0x5d9767a6
state[12 - 13] = 0x00000000 0x00000000
state[14 - 15] = 0xd531da1a 0x218268cf

Keystream block :

0x14 0x82 0x07 0x27 0x84 0xbc 0x6d 0x06
0xb4 0xe7 0x3b 0xdc 0x11 0x8b 0xc0 0x10
0x3c 0x79 0x76 0x78 0x6c 0xa9 0x18 0xe0
0x69 0x86 0xaa 0x25 0x1f 0x7e 0x9c 0xc1
0xb2 0x74 0x9a 0x0a 0x16 0xee 0x83 0xb4
0x24 0x2d 0x2e 0x99 0xb0 0x8d 0x7c 0x20
0x09 0x2b 0x80 0xbc 0x46 0x6c 0x87 0x28
0x3b 0x61 0xb1 0xb3 0x9d 0x0f 0xfb 0xab

Keystream block 1:

0xd9 0x4b 0x11 0x6b 0xc1 0xeb 0xdb 0x32
0x9b 0x9e 0x4f 0x62 0x0d 0xb6 0x95 0x54
0x4a 0x8e 0x3d 0x9b 0x68 0x47 0x3d 0x0c
0x97 0x5a 0x46 0xad 0x96 0x6e 0xd6 0x31
0xe4 0x2a 0xff 0x53 0x0a 0xd5 0xea 0xc7
0xd8 0x04 0x7a 0xdf 0xa1 0xe5 0x11 0x3c
0x91 0xf3 0xe3 0xb8 0x83 0xf1 0xd1 0x89

0xac 0x1c 0x8f 0xe0 0x7b 0xa5 0xa4 0x2b

Key: 0xc4 0x6e 0xc1 0xb1 0x8c 0xe8 0xa8 0x78
0x72 0x5a 0x37 0xe7 0x80 0xdf 0xb7 0x35
0x1f 0x68 0xed 0x2e 0x19 0x4c 0x79 0xfb
0xc6 0xae 0xbe 0xe1 0xa6 0x67 0x97 0x5d
IV: 0x1a 0xda 0x31 0xd5 0xcf 0x68 0x82 0x21
Rounds: 20

Internal state after init:
state[00 - 01] = 0x61707865 0x3320646e
state[02 - 03] = 0x79622d32 0x6b206574
state[04 - 05] = 0xb1c16ec4 0x78a8e88c
state[06 - 07] = 0xe7375a72 0x35b7df80
state[08 - 09] = 0x2eed681f 0xfb794c19

state[10 - 11] = 0xe1beaec6 0x5d9767a6
state[12 - 13] = 0x00000000 0x00000000
state[14 - 15] = 0xd531da1a 0x218268cf

Keystream block :
0xf6 0x3a 0x89 0xb7 0x5c 0x22 0x71 0xf9
0x36 0x88 0x16 0x54 0x2b 0xa5 0x2f 0x06
0xed 0x49 0x24 0x17 0x92 0x30 0x2b 0x00
0xb5 0xe8 0xf8 0x0a 0xe9 0xa4 0x73 0xaf
0xc2 0x5b 0x21 0x8f 0x51 0x9a 0xf0 0xfd
0xd4 0x06 0x36 0x2e 0x8d 0x69 0xde 0x7f
0x54 0xc6 0x04 0xa6 0xe0 0x0f 0x35 0x3f
0x11 0x0f 0x77 0x1b 0xdc 0xa8 0xab 0x92

Keystream block 1:
0xe5 0xfb 0xc3 0x4e 0x60 0xa1 0xd9 0xa9
0xdb 0x17 0x34 0x5b 0x0a 0x40 0x27 0x36
0x85 0x3b 0xf9 0x10 0xb0 0x60 0xbd 0xf1
0xf8 0x97 0xb6 0x29 0x0f 0x01 0xd1 0x38
0xae 0x2c 0x4c 0x90 0x22 0x5b 0xa9 0xea
0x14 0xd5 0x18 0xf5 0x59 0x29 0xde 0xa0
0x98 0xca 0x7a 0x6c 0xcf 0xe6 0x12 0x27
0x05 0x3c 0x84 0xe4 0x9a 0x4a 0x33 0x32

[4.](#) Security Considerations

None.

[5.](#) IANA Considerations

None.

[6.](#) Copying conditions

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

[7.](#) References

[7.1.](#) Normative References

[ChaCha] Bernstein, DJ., "ChaCha, a variant of Salsa20",
WWW <http://cr.yp.to/chacha/chacha-20080128.pdf>.

[RC4] Schneier, B., "Applied Cryptography, second edition,
[section 17.1](#), page 397".

[7.2.](#) Informative References

[FIPS.180-2.2002]
National Institute of Standards and Technology, "Secure Hash Standard", FIPS PUB 180-2, August 2002, <<http://csrc.nist.gov/publications/fips/fips180-2/fips180-2.pdf>>.

[chacha.c]
Bernstein, DJ., "The ChaCha family of stream ciphers",
WWW <http://cr.yp.to/chacha.html>.

[chacha_testvectors]
Strombergson, J., "chacha_testvectors",
WWW https://github.com/secworks/chacha_testvectors/.

Author's Address

Joachim Strombergson
Secworks Sweden AB
Hoegenvaegen 5A
Saevedalen 433 63
SE

Email: joachim@secworks.se
URI: <http://secworks.se/>