Algorithm: **MCSSHA-8**

Principal submitter: **Mikhail Maslennikov**

Revision: August 18, 2014

SECURE HASH ALGORITHM MCSSHA-8

Table of Contents

1. INTRODUCTION

This document specifies secure hash algorithm MCSSHA-8. This algorithms is iterative, one-way hash functions that can process a message to produce a condensed representation called a *message digest*. These algorithms enable the determination of a message's integrity: any change to the message will, with a very high probability, result in a different message digest. This property is useful in the generation and verification of digital signatures and message authentication codes, and in the generation of random numbers (bits).

MCSSHA-8 algorithm can be described in three stages: preprocessing, pre-hash computation and final hash computation. Each stage change *Shift Registry state* (SR-state) and final SR-state is message digest.

Preprocessing setting initial SR-state to be used in the hash computation. Initial SR-state not depended from message and padding not used in MCSSHA-8 algorithms. The pre-hash computation generates *pre-final SR-state* from the message. The final hash computation generates message digest – final SR-state - from pre-final SR-state.

MCSSHA-8 algorithm in many respects is similar to previous algorithms MCSSHA 3 - 7 of same family MCSSHA. Distinctions consist only in length of the Shift Registry for pre-hash computation and a method of generation of the final message digest for final stage. Also in MCSSHA-8 digest length can take any value from 32 to 512 bits (from 4 to 64 bytes).

2. DEFINITIONS

2.1 Glossary of Terms and Acronyms

Bit	A binary digit having a value of 0 or 1.
Byte	A group of eight bits.
Hash bit length (h)	Length (in bits) of the message digest. It may be any value from 32 to 512.
Hash byte length (H)	Length (in bytes) of the message digest. It may be any value from 4 to 64.
Shift Registry length (N)	Integer value.
Shift Registry state (SR state)	A group of N bytes.
Initial SR state	SR state before pre-hash computation.
Shift Registry point (SR point)	Digit from 0 to N-1.
SR points	A group of four SR points
Initial SR points	SR points before pre-hash computation.
Shift Registry Substitution	A group of 256 bytes where all values are various.
Shift Registry step (SR step)	Transformation of a SR state during one step.
Input byte for SR step	Byte that use SR step.
Message	A group of bits.
Message length in bits	Number of bits in message.
Message length in bytes	Number of full bytes in message.
Message remain bits	Message’s last bits not included in the last byte.

2.2 Algorithm Parameters, Symbols, and Terms

2.2.1 Parameters

The following parameters are used in MCSSHA-8 algorithm specifications in this document.

h	Hash bit length
H	Hash byte length, H = h/8.
M	Message to be hashed.
l	Length of the message *M*, in bits.
L	Length of the message M, in bytes, *L* = *l*/8.
r	Number of message remain bits, i.e. *r* = *l* - 8*L.*

m_i byte number i in message M.

$M=m_1,m_2,\ldots,m_L$ Message M as byte sequence.

π Shift Registry Substitution.

p_1,p_2,p_3,p_4 set of SR points. The number of point always 4, the values of points changes step by step.

Δ delay in pre-hash computation, i.e. number of SR steps without input byte during one byte computation.

2.2.2 Symbols

The following symbols are used in MCSSHA-8 algorithm specifications.

$+$ Addition on the module 256.

$-$ Subtraction on the module 256.

$\pi(y)$ Replacement byte *y* on substitution *π*.

$a(\mathrm{mod}\ N)$ Reduction of value *a* on the module *N*.

3. NOTATION AND CONVENTIONS

3.1 Substitution

The following terminology related to substitution will be used.

A byte is an element of the hex set {00,01,…,09,0A,…,0F,10, …,FF}.

$\pi(y)$ Replacement byte y on substitution π. If substitution π is group of 256 bytes where all values are various, for example 30, 60, ..., 5F, then π(00) = 30, π(01) = 60, …, π(FF) = 5F.

3.2 Shift Registry Steps

The following terminology related to SR steps will be used.

$Y = (y_0,y_1, \ldots,y_{N-1})$ SR state before step.

$P=(p_1,p_2,p_3,p_4)$ SR points before step.

p Changeable position: $p= (p_4+1)(\text{mod } N)$.

x Input byte for step.

4. FUNCTIONS AND CONSTANTS

This section defines the functions and constants that are used by MCSSHA algorithms. All stages of MCSSHA algorithms consists from SR steps and each step change SR state and SR points. SR substitution п is constant and same for each step.

4.1 Constants

SR substitution п is same for any MCSSHA algorithm's parameters. This is group of 256 bytes where all values are various. In hex, these group are

```
30 60 67 B5 43 EA 93 25 48 0D 18 6F 28 7A FE B6
D5 9C 23 86 52 42 F7 FD F6 9B EE 99 91 BC 2A 63
A1 A0 57 3C 39 D2 EC 71 45 CB 41 DC 0B 5B C2 36
01 55 7D FB ED 83 8F 31 C0 4C 08 E3 9D C1 D3 E9
B8 BD AE 0F E7 70 5A EB 4D 29 F9 A9 3D 26 46 06
D0 50 A5 BE 66 90 F4 20 E4 33 27 E2 AB EF 68 54
37 6A DB BB D8 7B 69 C4 F2 BF 85 C7 A6 B4 9A DD
72 34 E8 FC D6 21 98 96 32 CA 49 B3 F3 97 8E 2F
00 B0 10 1A 77 38 CF 51 BA 1F 22 AC 62 89 76 C3
02 6E 2C 47 3A 5C 1B 56 8A 5D 03 16 74 58 79 09
D7 F5 0A 92 4F 87 CD DA 8C C9 9E 3B 12 6B 53 FF
80 B7 F8 D9 F1 5E AF E0 05 A4 14 2B A3 CC 6C 7C
78 AA 95 84 61 A8 CE 13 88 FA 59 4E B9 C8 4B 24
D1 07 94 2E DF B1 17 A2 1D 4A C6 AD 15 19 35 7F
81 44 0C 9F 75 7E D4 82 DE E6 E1 2D 3E 73 11 8B
C5 A7 F0 6D 1C 64 0E 04 40 1E 8D E5 3F B2 65 5F
```

4.2 Functions

Let's $Y=(y_0,y_1, \dots,y_{N-1})$- SR state, $P=(p_1,p_2,p_3,p_4)$ – SR points, x – input byte, p – changeable position *before* SR step.

Each step use functions F1(Y,P,x) and F2(P), that are defined as follow:

$$F1(Y,P,x) = (y_0,y_1, \dots,y_{p-1},z,y_{p+1},\dots,y_{N-1}) \qquad 0 < p < N-1$$
$$F1(Y,P,x) = (z,y_1,y_2, \dots,y_{N-1}) \qquad p = 0$$
$$F1(Y,P,x) = (y_0,y_1, \dots,y_{N-2},z) \qquad p = N-1$$

where z = п($y_{p1} - y_{p2} - y_{p3} + y_{p4}$) + x.

$$F2(P) = ((p_1+1)(\mathrm{mod}\ N), (p_2+1)(\mathrm{mod}\ N), (p_3+1)(\mathrm{mod}\ N), (p_4+1)(\mathrm{mod}\ N)).$$

SR state F1(Y,P,x) and SR point F2(P) become SR state and SR points *after* SR step.

5. PREPROCESSING

Preprocessing shall take place before hash computation begins. In this stage MCSSHA algorithm set initial SR state and points for pre-hash computation as follow:

If N – SR length for pre-hash computation, then each SR byte number i, i from 0 to N-1, set value i during preprocessing.

For SR points p_1,p_2,p_3,p_4

p_1 = 0;
p_2 = 1;
p_3 = N-4;
p_4 = N-1.

Note, that SR length N and hash length H during preprocessing and pre-hash computation linked as follows from table below:

Table 1. SR length N and hash length H for preprocessing and pre-hash computation.

H – hash length in bytes	**N – SR length**
4	8
From 5 to 8	16
From 9 to 16	32
From 17 to 32	64
From 33 to 64	128

6. PRE-HASH COMPUTATION

Pre-hash computation prepare SR state that depended from all message's bits except remain bits.
For each byte m_i from message M pre-hash computation perform steps:

Step 1: SR step with input byte m_i.

Delay Steps: SR step with input byte 0.

As default, delay value Δ for MCSSHA-8 algorithm is 3.
Thus, as default pre-hash computation for message M and length in bytes L consist from 4L steps.

WARNING!

For values Δ below 2 (0 or 1) algorithm MCSSHA-8 can't be used as hash function, because in this cases it's possible to find collisions!

7. FINAL HASH COMPUTATION

Final hash computation use SR with length H.

7.1 Preparing input sequence for SR.

Let's $a_1,a_2,\ldots,a_r$ – remain bits from message M, B = $(b_1,b_2,\ldots,b_n)$ – n bits from SR state after pre-hash computation, where n = 8*N. Also B = $(B_1,B_2,\ldots,B_N)$ – sequence in bytes.

Input sequence Z for SR have length H and, if remain bits absent, will be as follow:

$$Z = B_N,B_{N-1},B_{N-4},B_{N-5},B_{N-8},B_{N-9},\ldots$$

If remain bits present, it in bits will be as follow:

$$Z = a_1,a_2,\ldots,a_r,\ b_n,b_{n-1},\ldots,b_{n-15},b_{n-31},b_{n-32},\ldots,b_{n-47},b_{n-63},\ldots$$

Final input sequence Z1 = Z | H (add message digest length to the end of the sequence Z)

7.2 Preparing final digest.

Preparing final digest use SR with length H and input sequence Z1 with length H + 1. Initial SR state is 0,1,2,...,H-1, initial SR points:

$p_1 = 0$;
$p_2 = 1$;
$p_3 = H-4$;
$p_4 = H-1$
for H >= 6,

$p_1 = 0$;
$p_2 = 1$;
$p_3 = 2$;
$p_4 = H-1$
for H = 4 or 5.

9. ESTIMATED COMPUTATIONAL EFFICIENCY AND MEMORY REQUIREMENTS

During work of algorithm all operations are carried out extremely with bytes. Any operations with words - group of either 32 bits (4 bytes) or 64 bits (8 bytes) – not used. So algorithm can be realized on any kind of processors: 8-bits, 16-bits, 32-bits and 64-bits. Efficiency depended from processor's architecture.

9.1 Memory Requirement

Algorithm not use message's padding, so it's memory requirements includes only memory for Shift Registry parameters: state, points and substitution.
For any hash length algorithm use memory:

- for SR substitution	256 bytes;
- for SR points	4 bytes.

For SR state it's necessary N bytes.

9.2 Computation Efficiency

Following data compare MCSSHA-3 and MCSSHA-6 speed with another hash algorithms speed. The source codes for this algorithms were copied from OpenSSL web site (http://www.openssl.org/source) and from First Round SHA-3 Candidates (http://csrc.nist.gov/groups/ST/hash/sha-3/Round1/submissions_rnd1.html).

64-bits OS
MS Windows 7 OS, 64-bits, i73537U CPU @ 2.00 GHz 2.50 GHz.

Algorithm	Hash length (in bits)	Text length (in bytes)	Number of tests	Time (sec)
SHA-224	224	1	1000000	2,9
MCSSHA-3	224	1	1000000	3,6
MCSSHA-6	224	1	1000000	4,3
MCSSHA-8	224	1	1000000	2,0
Skein	224	1	1000000	3,6
MD6	224	1	1000000	29,8
Keccak	224	1	1000000	7,4
Blake	224	1	1000000	4,2
SHA-224	224	100	1000000	5,6
MCSSHA-3	224	100	1000000	11,6
MCSSHA-6	224	100	1000000	12,5
MCSSHA-8	224	100	1000000	10,6
Skein	224	100	1000000	8,7
MD6	224	100	1000000	29,8
Keccak	224	100	1000000	7,5
Blake	224	100	1000000	8,5
SHA-224	224	100000	1000	4,5
MCSSHA-3	224	100000	1000	8,1
MCSSHA-6	224	100000	1000	8,1
MCSSHA-8	224	100000	1000	8,5
Skein	224	100000	1000	5,0
MD6	224	100000	1000	7,0
Keccak	224	100000	1000	5,6
Blake	224	100000	1000	6,0
SHA-512	512	1	1000000	7,6
MCSSHA-3	512	1	1000000	6,5
MCSSHA-6	512	1	1000000	6,8
MCSSHA-8	512	1	1000000	3,8
Skein	512	1	1000000	6,4
MD6	512	1	1000000	48,6
Keccak	512	1	1000000	7,5
Blake	512	1	1000000	9,1
SHA-512	512	100	1000000	8,1
MCSSHA-3	512	100	1000000	14,3
MCSSHA-6	512	100	1000000	14,7
MCSSHA-8	512	100	1000000	12,4
Skein	512	100	1000000	9,7
MD6	512	100	1000000	48,6
Keccak	512	100	1000000	14,5
Blake	512	100	1000000	9,1

SHA-512	512	100000	1000	5,5
MCSSHA-3	512	100000	1000	8,0
MCSSHA-6	512	100000	1000	7,9
MCSSHA-8	512	100000	1000	8,6
Skein	512	100000	1000	4,7
MD6	512	100000	1000	12,1
Keccak	512	100000	1000	11,0
Blake	512	100000	1000	7,0

10. ADDITIONAL CRYPTOGRAPHY FEATURES

10.1 Hash value independence.

The method of constructing hash functions type MCSSHA suggests independence of the hash values $H_i(M)$ and $H_j(M)$ for any same message M and different $i \neq j$, where $H_i(m)$ – hash value length i from message M. In particular, values $H_i(M)$ and $H_{i+1}(M)$ are independence, i.e. if you know $H_{i+1}(M)$ and M – unknown, the problem of finding $H_i(M)$ is very difficult. For example, if you use Password Based Key Derivation Function (PBKDF) with hash iterations, where all hashes have same length, so in this case enough to get one hash-transformation table for all hashes values and you can calculate KDF for any value of iteration count. If you use during PBKDF's MCSSHA-type hash iterations hash values with different length, you need several tables.

10.2 Encrypt algorithm MCSSHA-type.

We can use MCSSHA-type transformation for constructing fast encrypt algorithm. In this case instead message M we applied to the SR-input session key, start SR-state – open block text, final SR-state – encrypted block text. Design and selection of parameters such encrypt algorithms are the subject of the future researches.

11. Appendix A. Calculating hash examples.

In all this examples message *M* be the 24-bit (3-byte) ASCII string "**abc**", which is equivalent to the following hex string: 61 62 63.

11.1 Pre-hash computation for hash bit length 224 and 256, delay=3.

This is SR states for steps in pre-hash computation. 0 – initial SR state. SR length is 64.

Stage 1. Preprocessing. Initial SR state.

0.

```
00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F 10 11 12 13 14 15 16 17 18 19 1A 1B 1C 1D 1E 1F
20 21 22 23 24 25 26 27 28 29 2A 2B 2C 2D 2E 2F 30 31 32 33 34 35 36 37 38 39 3A 3B 3C 3D 3E 3F
```

Stage 2. Pre-hash computation – 12 steps

Input byte 61

1.

```
C8 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F 10 11 12 13 14 15 16 17 18 19 1A 1B 1C 1D 1E 1F
20 21 22 23 24 25 26 27 28 29 2A 2B 2C 2D 2E 2F 30 31 32 33 34 35 36 37 38 39 3A 3B 3C 3D 3E 3F
```

2.

```
C8 22 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F 10 11 12 13 14 15 16 17 18 19 1A 1B 1C 1D 1E 1F
20 21 22 23 24 25 26 27 28 29 2A 2B 2C 2D 2E 2F 30 31 32 33 34 35 36 37 38 39 3A 3B 3C 3D 3E 3F
```

3.

```
C8 22 9F 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F 10 11 12 13 14 15 16 17 18 19 1A 1B 1C 1D 1E 1F
20 21 22 23 24 25 26 27 28 29 2A 2B 2C 2D 2E 2F 30 31 32 33 34 35 36 37 38 39 3A 3B 3C 3D 3E 3F
```

4.

```
C8 22 9F 54 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F 10 11 12 13 14 15 16 17 18 19 1A 1B 1C 1D 1E 1F
20 21 22 23 24 25 26 27 28 29 2A 2B 2C 2D 2E 2F 30 31 32 33 34 35 36 37 38 39 3A 3B 3C 3D 3E 3F
```

Input byte 62

5.

```
C8 22 9F 54 0E 05 06 07 08 09 0A 0B 0C 0D 0E 0F 10 11 12 13 14 15 16 17 18 19 1A 1B 1C 1D 1E 1F
20 21 22 23 24 25 26 27 28 29 2A 2B 2C 2D 2E 2F 30 31 32 33 34 35 36 37 38 39 3A 3B 3C 3D 3E 3F
```

6.

```
C8 22 9F 54 0E 2D 06 07 08 09 0A 0B 0C 0D 0E 0F 10 11 12 13 14 15 16 17 18 19 1A 1B 1C 1D 1E 1F
20 21 22 23 24 25 26 27 28 29 2A 2B 2C 2D 2E 2F 30 31 32 33 34 35 36 37 38 39 3A 3B 3C 3D 3E 3F
```

7.

```
C8 22 9F 54 0E 2D 89 07 08 09 0A 0B 0C 0D 0E 0F 10 11 12 13 14 15 16 17 18 19 1A 1B 1C 1D 1E 1F
20 21 22 23 24 25 26 27 28 29 2A 2B 2C 2D 2E 2F 30 31 32 33 34 35 36 37 38 39 3A 3B 3C 3D 3E 3F
```

8.

```
C8 22 9F 54 0E 2D 89 ED 08 09 0A 0B 0C 0D 0E 0F 10 11 12 13 14 15 16 17 18 19 1A 1B 1C 1D 1E 1F
20 21 22 23 24 25 26 27 28 29 2A 2B 2C 2D 2E 2F 30 31 32 33 34 35 36 37 38 39 3A 3B 3C 3D 3E 3F
```

Input byte 63

9.

```
C8 22 9F 54 0E 2D 89 ED 98 09 0A 0B 0C 0D 0E 0F 10 11 12 13 14 15 16 17 18 19 1A 1B 1C 1D 1E 1F
20 21 22 23 24 25 26 27 28 29 2A 2B 2C 2D 2E 2F 30 31 32 33 34 35 36 37 38 39 3A 3B 3C 3D 3E 3F
```

10.

```
C8 22 9F 54 0E 2D 89 ED 98 85 0A 0B 0C 0D 0E 0F 10 11 12 13 14 15 16 17 18 19 1A 1B 1C 1D 1E 1F
20 21 22 23 24 25 26 27 28 29 2A 2B 2C 2D 2E 2F 30 31 32 33 34 35 36 37 38 39 3A 3B 3C 3D 3E 3F
```

11.

```
C8 22 9F 54 0E 2D 89 ED 98 85 E5 0B 0C 0D 0E 0F 10 11 12 13 14 15 16 17 18 19 1A 1B 1C 1D 1E 1F
20 21 22 23 24 25 26 27 28 29 2A 2B 2C 2D 2E 2F 30 31 32 33 34 35 36 37 38 39 3A 3B 3C 3D 3E 3F
```

12.

```
C8 22 9F 54 0E 2D 89 ED 98 85 E5 04 0C 0D 0E 0F 10 11 12 13 14 15 16 17 18 19 1A 1B 1C 1D 1E 1F
```

```
20 21 22 23 24 25 26 27 28 29 2A 2B 2C 2D 2E 2F 30 31 32 33 34 35 36 37 38 39 3A 3B 3C 3D 3E 3F
```

11.2 Pre-hash computation for hash bit length 384 and 512, delay=3.

This is SR states for steps in pre-hash computation. 0 – initial SR state. SR length is 128.

Stage 1. Preprocessing. Initial SR state.

```
0.
00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F 10 11 12 13 14 15 16 17 18 19 1A 1B 1C 1D 1E 1F
20 21 22 23 24 25 26 27 28 29 2A 2B 2C 2D 2E 2F 30 31 32 33 34 35 36 37 38 39 3A 3B 3C 3D 3E 3F
40 41 42 43 44 45 46 47 48 49 4A 4B 4C 4D 4E 4F 50 51 52 53 54 55 56 57 58 59 5A 5B 5C 5D 5E 5F
60 61 62 63 64 65 66 67 68 69 6A 6B 6C 6D 6E 6F 70 71 72 73 74 75 76 77 78 79 7A 7B 7C 7D 7E 7F
```

Stage 2. Pre-hash computation – 12 steps

Input byte 61

```
1.
C8 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F 10 11 12 13 14 15 16 17 18 19 1A 1B 1C 1D 1E 1F
20 21 22 23 24 25 26 27 28 29 2A 2B 2C 2D 2E 2F 30 31 32 33 34 35 36 37 38 39 3A 3B 3C 3D 3E 3F
40 41 42 43 44 45 46 47 48 49 4A 4B 4C 4D 4E 4F 50 51 52 53 54 55 56 57 58 59 5A 5B 5C 5D 5E 5F
60 61 62 63 64 65 66 67 68 69 6A 6B 6C 6D 6E 6F 70 71 72 73 74 75 76 77 78 79 7A 7B 7C 7D 7E 7F

2.
C8 F9 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F 10 11 12 13 14 15 16 17 18 19 1A 1B 1C 1D 1E 1F
20 21 22 23 24 25 26 27 28 29 2A 2B 2C 2D 2E 2F 30 31 32 33 34 35 36 37 38 39 3A 3B 3C 3D 3E 3F
40 41 42 43 44 45 46 47 48 49 4A 4B 4C 4D 4E 4F 50 51 52 53 54 55 56 57 58 59 5A 5B 5C 5D 5E 5F
60 61 62 63 64 65 66 67 68 69 6A 6B 6C 6D 6E 6F 70 71 72 73 74 75 76 77 78 79 7A 7B 7C 7D 7E 7F

3.
C8 F9 49 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F 10 11 12 13 14 15 16 17 18 19 1A 1B 1C 1D 1E 1F
20 21 22 23 24 25 26 27 28 29 2A 2B 2C 2D 2E 2F 30 31 32 33 34 35 36 37 38 39 3A 3B 3C 3D 3E 3F
40 41 42 43 44 45 46 47 48 49 4A 4B 4C 4D 4E 4F 50 51 52 53 54 55 56 57 58 59 5A 5B 5C 5D 5E 5F
60 61 62 63 64 65 66 67 68 69 6A 6B 6C 6D 6E 6F 70 71 72 73 74 75 76 77 78 79 7A 7B 7C 7D 7E 7F

4.
C8 F9 49 FA 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F 10 11 12 13 14 15 16 17 18 19 1A 1B 1C 1D 1E 1F
20 21 22 23 24 25 26 27 28 29 2A 2B 2C 2D 2E 2F 30 31 32 33 34 35 36 37 38 39 3A 3B 3C 3D 3E 3F
40 41 42 43 44 45 46 47 48 49 4A 4B 4C 4D 4E 4F 50 51 52 53 54 55 56 57 58 59 5A 5B 5C 5D 5E 5F
60 61 62 63 64 65 66 67 68 69 6A 6B 6C 6D 6E 6F 70 71 72 73 74 75 76 77 78 79 7A 7B 7C 7D 7E 7F
```

Input byte 62

```
5.
C8 F9 49 FA B7 05 06 07 08 09 0A 0B 0C 0D 0E 0F 10 11 12 13 14 15 16 17 18 19 1A 1B 1C 1D 1E 1F
20 21 22 23 24 25 26 27 28 29 2A 2B 2C 2D 2E 2F 30 31 32 33 34 35 36 37 38 39 3A 3B 3C 3D 3E 3F
40 41 42 43 44 45 46 47 48 49 4A 4B 4C 4D 4E 4F 50 51 52 53 54 55 56 57 58 59 5A 5B 5C 5D 5E 5F
60 61 62 63 64 65 66 67 68 69 6A 6B 6C 6D 6E 6F 70 71 72 73 74 75 76 77 78 79 7A 7B 7C 7D 7E 7F

6.
C8 F9 49 FA B7 CC 06 07 08 09 0A 0B 0C 0D 0E 0F 10 11 12 13 14 15 16 17 18 19 1A 1B 1C 1D 1E 1F
20 21 22 23 24 25 26 27 28 29 2A 2B 2C 2D 2E 2F 30 31 32 33 34 35 36 37 38 39 3A 3B 3C 3D 3E 3F
40 41 42 43 44 45 46 47 48 49 4A 4B 4C 4D 4E 4F 50 51 52 53 54 55 56 57 58 59 5A 5B 5C 5D 5E 5F
60 61 62 63 64 65 66 67 68 69 6A 6B 6C 6D 6E 6F 70 71 72 73 74 75 76 77 78 79 7A 7B 7C 7D 7E 7F

7.
C8 F9 49 FA B7 CC 10 07 08 09 0A 0B 0C 0D 0E 0F 10 11 12 13 14 15 16 17 18 19 1A 1B 1C 1D 1E 1F
20 21 22 23 24 25 26 27 28 29 2A 2B 2C 2D 2E 2F 30 31 32 33 34 35 36 37 38 39 3A 3B 3C 3D 3E 3F
40 41 42 43 44 45 46 47 48 49 4A 4B 4C 4D 4E 4F 50 51 52 53 54 55 56 57 58 59 5A 5B 5C 5D 5E 5F
60 61 62 63 64 65 66 67 68 69 6A 6B 6C 6D 6E 6F 70 71 72 73 74 75 76 77 78 79 7A 7B 7C 7D 7E 7F

8.
C8 F9 49 FA B7 CC 10 42 08 09 0A 0B 0C 0D 0E 0F 10 11 12 13 14 15 16 17 18 19 1A 1B 1C 1D 1E 1F
20 21 22 23 24 25 26 27 28 29 2A 2B 2C 2D 2E 2F 30 31 32 33 34 35 36 37 38 39 3A 3B 3C 3D 3E 3F
40 41 42 43 44 45 46 47 48 49 4A 4B 4C 4D 4E 4F 50 51 52 53 54 55 56 57 58 59 5A 5B 5C 5D 5E 5F
60 61 62 63 64 65 66 67 68 69 6A 6B 6C 6D 6E 6F 70 71 72 73 74 75 76 77 78 79 7A 7B 7C 7D 7E 7F
```

Input byte 63

```
9.
C8 F9 49 FA B7 CC 10 42 85 09 0A 0B 0C 0D 0E 0F 10 11 12 13 14 15 16 17 18 19 1A 1B 1C 1D 1E 1F
20 21 22 23 24 25 26 27 28 29 2A 2B 2C 2D 2E 2F 30 31 32 33 34 35 36 37 38 39 3A 3B 3C 3D 3E 3F
40 41 42 43 44 45 46 47 48 49 4A 4B 4C 4D 4E 4F 50 51 52 53 54 55 56 57 58 59 5A 5B 5C 5D 5E 5F
60 61 62 63 64 65 66 67 68 69 6A 6B 6C 6D 6E 6F 70 71 72 73 74 75 76 77 78 79 7A 7B 7C 7D 7E 7F

10.
C8 F9 49 FA B7 CC 10 42 85 05 0A 0B 0C 0D 0E 0F 10 11 12 13 14 15 16 17 18 19 1A 1B 1C 1D 1E 1F
20 21 22 23 24 25 26 27 28 29 2A 2B 2C 2D 2E 2F 30 31 32 33 34 35 36 37 38 39 3A 3B 3C 3D 3E 3F
40 41 42 43 44 45 46 47 48 49 4A 4B 4C 4D 4E 4F 50 51 52 53 54 55 56 57 58 59 5A 5B 5C 5D 5E 5F
60 61 62 63 64 65 66 67 68 69 6A 6B 6C 6D 6E 6F 70 71 72 73 74 75 76 77 78 79 7A 7B 7C 7D 7E 7F

11.
C8 F9 49 FA B7 CC 10 42 85 05 1C 0B 0C 0D 0E 0F 10 11 12 13 14 15 16 17 18 19 1A 1B 1C 1D 1E 1F
20 21 22 23 24 25 26 27 28 29 2A 2B 2C 2D 2E 2F 30 31 32 33 34 35 36 37 38 39 3A 3B 3C 3D 3E 3F
40 41 42 43 44 45 46 47 48 49 4A 4B 4C 4D 4E 4F 50 51 52 53 54 55 56 57 58 59 5A 5B 5C 5D 5E 5F
60 61 62 63 64 65 66 67 68 69 6A 6B 6C 6D 6E 6F 70 71 72 73 74 75 76 77 78 79 7A 7B 7C 7D 7E 7F

12.
C8 F9 49 FA B7 CC 10 42 85 05 1C 4A 0C 0D 0E 0F 10 11 12 13 14 15 16 17 18 19 1A 1B 1C 1D 1E 1F
20 21 22 23 24 25 26 27 28 29 2A 2B 2C 2D 2E 2F 30 31 32 33 34 35 36 37 38 39 3A 3B 3C 3D 3E 3F
40 41 42 43 44 45 46 47 48 49 4A 4B 4C 4D 4E 4F 50 51 52 53 54 55 56 57 58 59 5A 5B 5C 5D 5E 5F
60 61 62 63 64 65 66 67 68 69 6A 6B 6C 6D 6E 6F 70 71 72 73 74 75 76 77 78 79 7A 7B 7C 7D 7E 7F
```

11.3 Final hash computation for hash bit length 224.

SR state before final hash computation

```
C8 22 9F 54 0E 2D 89 ED 98 85 E5 04 0C 0D 0E 0F 10 11 12 13 14 15 16 17 18 19 1A 1B 1C 1D 1E 1F
20 21 22 23 24 25 26 27 28 29 2A 2B 2C 2D 2E 2F 30 31 32 33 34 35 36 37 38 39 3A 3B 3C 3D 3E 3F
```

Input sequence

```
04 E5 ED 89 54 9F 3F 3E 3B 3A 37 36 33 32 2F 2E 2B 2A 27 26 23 22 1F 1E 1B 1A 17 16 1C
```

Initial SR state.

```
0.
00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F 10 11 12 13 14 15 16 17 18 19 1A 1B
```

Calculating SR state. Total 29 steps.

```
1.
6B 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F 10 11 12 13 14 15 16 17 18 19 1A 1B
2.
6B 35 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F 10 11 12 13 14 15 16 17 18 19 1A 1B
3.
6B 35 DB 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F 10 11 12 13 14 15 16 17 18 19 1A 1B
4.
6B 35 DB 05 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F 10 11 12 13 14 15 16 17 18 19 1A 1B
5.
6B 35 DB 05 B1 05 06 07 08 09 0A 0B 0C 0D 0E 0F 10 11 12 13 14 15 16 17 18 19 1A 1B
6.
6B 35 DB 05 B1 52 06 07 08 09 0A 0B 0C 0D 0E 0F 10 11 12 13 14 15 16 17 18 19 1A 1B
7.
6B 35 DB 05 B1 52 D7 07 08 09 0A 0B 0C 0D 0E 0F 10 11 12 13 14 15 16 17 18 19 1A 1B
8.
6B 35 DB 05 B1 52 D7 45 08 09 0A 0B 0C 0D 0E 0F 10 11 12 13 14 15 16 17 18 19 1A 1B
9.
6B 35 DB 05 B1 52 D7 45 82 09 0A 0B 0C 0D 0E 0F 10 11 12 13 14 15 16 17 18 19 1A 1B
10.
6B 35 DB 05 B1 52 D7 45 82 70 0A 0B 0C 0D 0E 0F 10 11 12 13 14 15 16 17 18 19 1A 1B
11.
6B 35 DB 05 B1 52 D7 45 82 70 C1 0B 0C 0D 0E 0F 10 11 12 13 14 15 16 17 18 19 1A 1B
12.
6B 35 DB 05 B1 52 D7 45 82 70 C1 E9 0C 0D 0E 0F 10 11 12 13 14 15 16 17 18 19 1A 1B
13.
6B 35 DB 05 B1 52 D7 45 82 70 C1 E9 9C 0D 0E 0F 10 11 12 13 14 15 16 17 18 19 1A 1B
14.
```

```
6B 35 DB 05 B1 52 D7 45 82 70 C1 E9 9C 0E 0E 0F 10 11 12 13 14 15 16 17 18 19 1A 1B
15.
6B 35 DB 05 B1 52 D7 45 82 70 C1 E9 9C 0E 6C 0F 10 11 12 13 14 15 16 17 18 19 1A 1B
16.
6B 35 DB 05 B1 52 D7 45 82 70 C1 E9 9C 0E 6C 3E 10 11 12 13 14 15 16 17 18 19 1A 1B
17.
6B 35 DB 05 B1 52 D7 45 82 70 C1 E9 9C 0E 6C 3E 20 11 12 13 14 15 16 17 18 19 1A 1B
18.
6B 35 DB 05 B1 52 D7 45 82 70 C1 E9 9C 0E 6C 3E 20 C6 12 13 14 15 16 17 18 19 1A 1B
19.
6B 35 DB 05 B1 52 D7 45 82 70 C1 E9 9C 0E 6C 3E 20 C6 5A 13 14 15 16 17 18 19 1A 1B
20.
6B 35 DB 05 B1 52 D7 45 82 70 C1 E9 9C 0E 6C 3E 20 C6 5A BF 14 15 16 17 18 19 1A 1B
21.
6B 35 DB 05 B1 52 D7 45 82 70 C1 E9 9C 0E 6C 3E 20 C6 5A BF 9C 15 16 17 18 19 1A 1B
22.
6B 35 DB 05 B1 52 D7 45 82 70 C1 E9 9C 0E 6C 3E 20 C6 5A BF 9C D3 16 17 18 19 1A 1B
23.
6B 35 DB 05 B1 52 D7 45 82 70 C1 E9 9C 0E 6C 3E 20 C6 5A BF 9C D3 51 17 18 19 1A 1B
24.
6B 35 DB 05 B1 52 D7 45 82 70 C1 E9 9C 0E 6C 3E 20 C6 5A BF 9C D3 51 8C 18 19 1A 1B
25.
6B 35 DB 05 B1 52 D7 45 82 70 C1 E9 9C 0E 6C 3E 20 C6 5A BF 9C D3 51 8C A6 19 1A 1B
26.
6B 35 DB 05 B1 52 D7 45 82 70 C1 E9 9C 0E 6C 3E 20 C6 5A BF 9C D3 51 8C A6 AE 1A 1B
27.
6B 35 DB 05 B1 52 D7 45 82 70 C1 E9 9C 0E 6C 3E 20 C6 5A BF 9C D3 51 8C A6 AE C2 1B
28.
6B 35 DB 05 B1 52 D7 45 82 70 C1 E9 9C 0E 6C 3E 20 C6 5A BF 9C D3 51 8C A6 AE C2 EA
29.
65 35 DB 05 B1 52 D7 45 82 70 C1 E9 9C 0E 6C 3E 20 C6 5A BF 9C D3 51 8C A6 AE C2 EA
```

Final message digest:
65 35 DB 05 B1 52 D7 45 82 70 C1 E9 9C 0E 6C 3E 20 C6 5A BF 9C D3 51 8C A6 AE C2 EA

11.4 Final hash computation for hash bit length 256.

SR state before final hash computation

```
C8 22 9F 54 0E 2D 89 ED 98 85 E5 04 0C 0D 0E 0F 10 11 12 13 14 15 16 17 18 19 1A 1B 1C 1D 1E 1F
20 21 22 23 24 25 26 27 28 29 2A 2B 2C 2D 2E 2F 30 31 32 33 34 35 36 37 38 39 3A 3B 3C 3D 3E 3F
```

Input sequence

```
04 E5 ED 89 54 9F 3F 3E 3B 3A 37 36 33 32 2F 2E 2B 2A 27 26 23 22 1F 1E 1B 1A 17 16 13 12 0F 0E
20
```

Initial SR state.

```
0.
00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F 10 11 12 13 14 15 16 17 18 19 1A 1B 1C 1D 1E 1F
```

Calculating SR state. Total 33 steps.

```
1.
6B 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F 10 11 12 13 14 15 16 17 18 19 1A 1B 1C 1D 1E 1F
2.
6B 0B 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F 10 11 12 13 14 15 16 17 18 19 1A 1B 1C 1D 1E 1F
3.
6B 0B 2B 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F 10 11 12 13 14 15 16 17 18 19 1A 1B 1C 1D 1E 1F
4.
6B 0B 2B F8 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F 10 11 12 13 14 15 16 17 18 19 1A 1B 1C 1D 1E 1F
5.
6B 0B 2B F8 B6 05 06 07 08 09 0A 0B 0C 0D 0E 0F 10 11 12 13 14 15 16 17 18 19 1A 1B 1C 1D 1E 1F
6.
6B 0B 2B F8 B6 3D 06 07 08 09 0A 0B 0C 0D 0E 0F 10 11 12 13 14 15 16 17 18 19 1A 1B 1C 1D 1E 1F
7.
6B 0B 2B F8 B6 3D DB 07 08 09 0A 0B 0C 0D 0E 0F 10 11 12 13 14 15 16 17 18 19 1A 1B 1C 1D 1E 1F
8.
6B 0B 2B F8 B6 3D DB 4A 08 09 0A 0B 0C 0D 0E 0F 10 11 12 13 14 15 16 17 18 19 1A 1B 1C 1D 1E 1F
```

```
9.
6B 0B 2B F8 B6 3D DB 4A 82 09 0A 0B 0C 0D 0E 0F 10 11 12 13 14 15 16 17 18 19 1A 1B 1C 1D 1E 1F
10.
6B 0B 2B F8 B6 3D DB 4A 82 21 0A 0B 0C 0D 0E 0F 10 11 12 13 14 15 16 17 18 19 1A 1B 1C 1D 1E 1F
11.
6B 0B 2B F8 B6 3D DB 4A 82 21 A7 0B 0C 0D 0E 0F 10 11 12 13 14 15 16 17 18 19 1A 1B 1C 1D 1E 1F
12.
6B 0B 2B F8 B6 3D DB 4A 82 21 A7 E1 0C 0D 0E 0F 10 11 12 13 14 15 16 17 18 19 1A 1B 1C 1D 1E 1F
13.
6B 0B 2B F8 B6 3D DB 4A 82 21 A7 E1 9B 0D 0E 0F 10 11 12 13 14 15 16 17 18 19 1A 1B 1C 1D 1E 1F
14.
6B 0B 2B F8 B6 3D DB 4A 82 21 A7 E1 9B FC 0E 0F 10 11 12 13 14 15 16 17 18 19 1A 1B 1C 1D 1E 1F
15.
6B 0B 2B F8 B6 3D DB 4A 82 21 A7 E1 9B FC 95 0F 10 11 12 13 14 15 16 17 18 19 1A 1B 1C 1D 1E 1F
16.
6B 0B 2B F8 B6 3D DB 4A 82 21 A7 E1 9B FC 95 07 10 11 12 13 14 15 16 17 18 19 1A 1B 1C 1D 1E 1F
17.
6B 0B 2B F8 B6 3D DB 4A 82 21 A7 E1 9B FC 95 07 F2 11 12 13 14 15 16 17 18 19 1A 1B 1C 1D 1E 1F
18.
6B 0B 2B F8 B6 3D DB 4A 82 21 A7 E1 9B FC 95 07 F2 8E 12 13 14 15 16 17 18 19 1A 1B 1C 1D 1E 1F
19.
6B 0B 2B F8 B6 3D DB 4A 82 21 A7 E1 9B FC 95 07 F2 8E 67 13 14 15 16 17 18 19 1A 1B 1C 1D 1E 1F
20.
6B 0B 2B F8 B6 3D DB 4A 82 21 A7 E1 9B FC 95 07 F2 8E 67 7A 14 15 16 17 18 19 1A 1B 1C 1D 1E 1F
21.
6B 0B 2B F8 B6 3D DB 4A 82 21 A7 E1 9B FC 95 07 F2 8E 67 7A 74 15 16 17 18 19 1A 1B 1C 1D 1E 1F
22.
6B 0B 2B F8 B6 3D DB 4A 82 21 A7 E1 9B FC 95 07 F2 8E 67 7A 74 A0 16 17 18 19 1A 1B 1C 1D 1E 1F
23.
6B 0B 2B F8 B6 3D DB 4A 82 21 A7 E1 9B FC 95 07 F2 8E 67 7A 74 A0 DF 17 18 19 1A 1B 1C 1D 1E 1F
24.
6B 0B 2B F8 B6 3D DB 4A 82 21 A7 E1 9B FC 95 07 F2 8E 67 7A 74 A0 DF F6 18 19 1A 1B 1C 1D 1E 1F
25.
6B 0B 2B F8 B6 3D DB 4A 82 21 A7 E1 9B FC 95 07 F2 8E 67 7A 74 A0 DF F6 CB 19 1A 1B 1C 1D 1E 1F
26.
6B 0B 2B F8 B6 3D DB 4A 82 21 A7 E1 9B FC 95 07 F2 8E 67 7A 74 A0 DF F6 CB 5B 1A 1B 1C 1D 1E 1F
27.
6B 0B 2B F8 B6 3D DB 4A 82 21 A7 E1 9B FC 95 07 F2 8E 67 7A 74 A0 DF F6 CB 5B CA 1B 1C 1D 1E 1F
28.
6B 0B 2B F8 B6 3D DB 4A 82 21 A7 E1 9B FC 95 07 F2 8E 67 7A 74 A0 DF F6 CB 5B CA 44 1C 1D 1E 1F
29.
6B 0B 2B F8 B6 3D DB 4A 82 21 A7 E1 9B FC 95 07 F2 8E 67 7A 74 A0 DF F6 CB 5B CA 44 45 1D 1E 1F
30.
6B 0B 2B F8 B6 3D DB 4A 82 21 A7 E1 9B FC 95 07 F2 8E 67 7A 74 A0 DF F6 CB 5B CA 44 45 F8 1E 1F
31.
6B 0B 2B F8 B6 3D DB 4A 82 21 A7 E1 9B FC 95 07 F2 8E 67 7A 74 A0 DF F6 CB 5B CA 44 45 F8 6A 1F
32.
6B 0B 2B F8 B6 3D DB 4A 82 21 A7 E1 9B FC 95 07 F2 8E 67 7A 74 A0 DF F6 CB 5B CA 44 45 F8 6A D4
33.
AB 0B 2B F8 B6 3D DB 4A 82 21 A7 E1 9B FC 95 07 F2 8E 67 7A 74 A0 DF F6 CB 5B CA 44 45 F8 6A D4
```

Final message digest:
AB 0B 2B F8 B6 3D DB 4A 82 21 A7 E1 9B FC 95 07 F2 8E 67 7A 74 A0 DF F6 CB 5B CA 44 45 F8 6A D4

11.5 Final hash computation for hash bit length 384.

SR state before final hash computation

```
C8 F9 49 FA B7 CC 10 42 85 05 1C 4A 0C 0D 0E 0F 10 11 12 13 14 15 16 17 18 19 1A 1B 1C 1D 1E 1F
20 21 22 23 24 25 26 27 28 29 2A 2B 2C 2D 2E 2F 30 31 32 33 34 35 36 37 38 39 3A 3B 3C 3D 3E 3F
40 41 42 43 44 45 46 47 48 49 4A 4B 4C 4D 4E 4F 50 51 52 53 54 55 56 57 58 59 5A 5B 5C 5D 5E 5F
60 61 62 63 64 65 66 67 68 69 6A 6B 6C 6D 6E 6F 70 71 72 73 74 75 76 77 78 79 7A 7B 7C 7D 7E 7F
```

Input sequence

```
4A 1C 42 10 FA 49 7F 7E 7B 7A 77 76 73 72 6F 6E 6B 6A 67 66 63 62 5F 5E 5B 5A 57 56 53 52 4F 4E
4B 4A 47 46 43 42 3F 3E 3B 3A 37 36 33 32 2F 2E 30
```

```
Initial SR state.

0.
00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F 10 11 12 13 14 15 16 17 18 19 1A 1B 1C 1D 1E 1F
20 21 22 23 24 25 26 27 28 29 2A 2B 2C 2D 2E 2F

Calculating SR state. Total 49 steps.

1.
B1 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F 10 11 12 13 14 15 16 17 18 19 1A 1B 1C 1D 1E 1F
20 21 22 23 24 25 26 27 28 29 2A 2B 2C 2D 2E 2F
2.
B1 36 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F 10 11 12 13 14 15 16 17 18 19 1A 1B 1C 1D 1E 1F
20 21 22 23 24 25 26 27 28 29 2A 2B 2C 2D 2E 2F
3.
B1 36 67 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F 10 11 12 13 14 15 16 17 18 19 1A 1B 1C 1D 1E 1F
20 21 22 23 24 25 26 27 28 29 2A 2B 2C 2D 2E 2F
4.
B1 36 67 41 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F 10 11 12 13 14 15 16 17 18 19 1A 1B 1C 1D 1E 1F
20 21 22 23 24 25 26 27 28 29 2A 2B 2C 2D 2E 2F
5.
B1 36 67 41 BD 05 06 07 08 09 0A 0B 0C 0D 0E 0F 10 11 12 13 14 15 16 17 18 19 1A 1B 1C 1D 1E 1F
20 21 22 23 24 25 26 27 28 29 2A 2B 2C 2D 2E 2F
6.
B1 36 67 41 BD 18 06 07 08 09 0A 0B 0C 0D 0E 0F 10 11 12 13 14 15 16 17 18 19 1A 1B 1C 1D 1E 1F
20 21 22 23 24 25 26 27 28 29 2A 2B 2C 2D 2E 2F
7.
B1 36 67 41 BD 18 FF 07 08 09 0A 0B 0C 0D 0E 0F 10 11 12 13 14 15 16 17 18 19 1A 1B 1C 1D 1E 1F
20 21 22 23 24 25 26 27 28 29 2A 2B 2C 2D 2E 2F
8.
B1 36 67 41 BD 18 FF 4A 08 09 0A 0B 0C 0D 0E 0F 10 11 12 13 14 15 16 17 18 19 1A 1B 1C 1D 1E 1F
20 21 22 23 24 25 26 27 28 29 2A 2B 2C 2D 2E 2F
9.
B1 36 67 41 BD 18 FF 4A DD 09 0A 0B 0C 0D 0E 0F 10 11 12 13 14 15 16 17 18 19 1A 1B 1C 1D 1E 1F
20 21 22 23 24 25 26 27 28 29 2A 2B 2C 2D 2E 2F
10.
B1 36 67 41 BD 18 FF 4A DD DB 0A 0B 0C 0D 0E 0F 10 11 12 13 14 15 16 17 18 19 1A 1B 1C 1D 1E 1F
20 21 22 23 24 25 26 27 28 29 2A 2B 2C 2D 2E 2F
11.
B1 36 67 41 BD 18 FF 4A DD DB 24 0B 0C 0D 0E 0F 10 11 12 13 14 15 16 17 18 19 1A 1B 1C 1D 1E 1F
20 21 22 23 24 25 26 27 28 29 2A 2B 2C 2D 2E 2F
12.
B1 36 67 41 BD 18 FF 4A DD DB 24 C0 0C 0D 0E 0F 10 11 12 13 14 15 16 17 18 19 1A 1B 1C 1D 1E 1F
20 21 22 23 24 25 26 27 28 29 2A 2B 2C 2D 2E 2F
13.
B1 36 67 41 BD 18 FF 4A DD DB 24 C0 7F 0D 0E 0F 10 11 12 13 14 15 16 17 18 19 1A 1B 1C 1D 1E 1F
20 21 22 23 24 25 26 27 28 29 2A 2B 2C 2D 2E 2F
14.
B1 36 67 41 BD 18 FF 4A DD DB 24 C0 7F 04 0E 0F 10 11 12 13 14 15 16 17 18 19 1A 1B 1C 1D 1E 1F
20 21 22 23 24 25 26 27 28 29 2A 2B 2C 2D 2E 2F
15.
B1 36 67 41 BD 18 FF 4A DD DB 24 C0 7F 04 EE 0F 10 11 12 13 14 15 16 17 18 19 1A 1B 1C 1D 1E 1F
20 21 22 23 24 25 26 27 28 29 2A 2B 2C 2D 2E 2F
16.
B1 36 67 41 BD 18 FF 4A DD DB 24 C0 7F 04 EE C9 10 11 12 13 14 15 16 17 18 19 1A 1B 1C 1D 1E 1F
20 21 22 23 24 25 26 27 28 29 2A 2B 2C 2D 2E 2F
17.
B1 36 67 41 BD 18 FF 4A DD DB 24 C0 7F 04 EE C9 94 11 12 13 14 15 16 17 18 19 1A 1B 1C 1D 1E 1F
20 21 22 23 24 25 26 27 28 29 2A 2B 2C 2D 2E 2F
18.
B1 36 67 41 BD 18 FF 4A DD DB 24 C0 7F 04 EE C9 94 2D 12 13 14 15 16 17 18 19 1A 1B 1C 1D 1E 1F
20 21 22 23 24 25 26 27 28 29 2A 2B 2C 2D 2E 2F
19.
B1 36 67 41 BD 18 FF 4A DD DB 24 C0 7F 04 EE C9 94 2D 3A 13 14 15 16 17 18 19 1A 1B 1C 1D 1E 1F
20 21 22 23 24 25 26 27 28 29 2A 2B 2C 2D 2E 2F
20.
B1 36 67 41 BD 18 FF 4A DD DB 24 C0 7F 04 EE C9 94 2D 3A D8 14 15 16 17 18 19 1A 1B 1C 1D 1E 1F
20 21 22 23 24 25 26 27 28 29 2A 2B 2C 2D 2E 2F
21.
B1 36 67 41 BD 18 FF 4A DD DB 24 C0 7F 04 EE C9 94 2D 3A D8 72 15 16 17 18 19 1A 1B 1C 1D 1E 1F
20 21 22 23 24 25 26 27 28 29 2A 2B 2C 2D 2E 2F
```

```
22.
B1 36 67 41 BD 18 FF 4A DD DB 24 C0 7F 04 EE C9 94 2D 3A D8 72 49 16 17 18 19 1A 1B 1C 1D 1E 1F
20 21 22 23 24 25 26 27 28 29 2A 2B 2C 2D 2E 2F
23.
B1 36 67 41 BD 18 FF 4A DD DB 24 C0 7F 04 EE C9 94 2D 3A D8 72 49 5D 17 18 19 1A 1B 1C 1D 1E 1F
20 21 22 23 24 25 26 27 28 29 2A 2B 2C 2D 2E 2F
24.
B1 36 67 41 BD 18 FF 4A DD DB 24 C0 7F 04 EE C9 94 2D 3A D8 72 49 5D D5 18 19 1A 1B 1C 1D 1E 1F
20 21 22 23 24 25 26 27 28 29 2A 2B 2C 2D 2E 2F
25.
B1 36 67 41 BD 18 FF 4A DD DB 24 C0 7F 04 EE C9 94 2D 3A D8 72 49 5D D5 36 19 1A 1B 1C 1D 1E 1F
20 21 22 23 24 25 26 27 28 29 2A 2B 2C 2D 2E 2F
26.
B1 36 67 41 BD 18 FF 4A DD DB 24 C0 7F 04 EE C9 94 2D 3A D8 72 49 5D D5 36 98 1A 1B 1C 1D 1E 1F
20 21 22 23 24 25 26 27 28 29 2A 2B 2C 2D 2E 2F
27.
B1 36 67 41 BD 18 FF 4A DD DB 24 C0 7F 04 EE C9 94 2D 3A D8 72 49 5D D5 36 98 5F 1B 1C 1D 1E 1F
20 21 22 23 24 25 26 27 28 29 2A 2B 2C 2D 2E 2F
28.
B1 36 67 41 BD 18 FF 4A DD DB 24 C0 7F 04 EE C9 94 2D 3A D8 72 49 5D D5 36 98 5F 75 1C 1D 1E 1F
20 21 22 23 24 25 26 27 28 29 2A 2B 2C 2D 2E 2F
29.
B1 36 67 41 BD 18 FF 4A DD DB 24 C0 7F 04 EE C9 94 2D 3A D8 72 49 5D D5 36 98 5F 75 26 1D 1E 1F
20 21 22 23 24 25 26 27 28 29 2A 2B 2C 2D 2E 2F
30.
B1 36 67 41 BD 18 FF 4A DD DB 24 C0 7F 04 EE C9 94 2D 3A D8 72 49 5D D5 36 98 5F 75 26 DB 1E 1F
20 21 22 23 24 25 26 27 28 29 2A 2B 2C 2D 2E 2F
31.
B1 36 67 41 BD 18 FF 4A DD DB 24 C0 7F 04 EE C9 94 2D 3A D8 72 49 5D D5 36 98 5F 75 26 DB 02 1F
20 21 22 23 24 25 26 27 28 29 2A 2B 2C 2D 2E 2F
32.
B1 36 67 41 BD 18 FF 4A DD DB 24 C0 7F 04 EE C9 94 2D 3A D8 72 49 5D D5 36 98 5F 75 26 DB 02 B0
20 21 22 23 24 25 26 27 28 29 2A 2B 2C 2D 2E 2F
33.
B1 36 67 41 BD 18 FF 4A DD DB 24 C0 7F 04 EE C9 94 2D 3A D8 72 49 5D D5 36 98 5F 75 26 DB 02 B0
6A 21 22 23 24 25 26 27 28 29 2A 2B 2C 2D 2E 2F
34.
B1 36 67 41 BD 18 FF 4A DD DB 24 C0 7F 04 EE C9 94 2D 3A D8 72 49 5D D5 36 98 5F 75 26 DB 02 B0
6A C0 22 23 24 25 26 27 28 29 2A 2B 2C 2D 2E 2F
35.
B1 36 67 41 BD 18 FF 4A DD DB 24 C0 7F 04 EE C9 94 2D 3A D8 72 49 5D D5 36 98 5F 75 26 DB 02 B0
6A C0 13 23 24 25 26 27 28 29 2A 2B 2C 2D 2E 2F
36.
B1 36 67 41 BD 18 FF 4A DD DB 24 C0 7F 04 EE C9 94 2D 3A D8 72 49 5D D5 36 98 5F 75 26 DB 02 B0
6A C0 13 21 24 25 26 27 28 29 2A 2B 2C 2D 2E 2F
37.
B1 36 67 41 BD 18 FF 4A DD DB 24 C0 7F 04 EE C9 94 2D 3A D8 72 49 5D D5 36 98 5F 75 26 DB 02 B0
6A C0 13 21 F2 25 26 27 28 29 2A 2B 2C 2D 2E 2F
38.
B1 36 67 41 BD 18 FF 4A DD DB 24 C0 7F 04 EE C9 94 2D 3A D8 72 49 5D D5 36 98 5F 75 26 DB 02 B0
6A C0 13 21 F2 97 26 27 28 29 2A 2B 2C 2D 2E 2F
39.
B1 36 67 41 BD 18 FF 4A DD DB 24 C0 7F 04 EE C9 94 2D 3A D8 72 49 5D D5 36 98 5F 75 26 DB 02 B0
6A C0 13 21 F2 97 59 27 28 29 2A 2B 2C 2D 2E 2F
40.
B1 36 67 41 BD 18 FF 4A DD DB 24 C0 7F 04 EE C9 94 2D 3A D8 72 49 5D D5 36 98 5F 75 26 DB 02 B0
6A C0 13 21 F2 97 59 6F 28 29 2A 2B 2C 2D 2E 2F
41.
B1 36 67 41 BD 18 FF 4A DD DB 24 C0 7F 04 EE C9 94 2D 3A D8 72 49 5D D5 36 98 5F 75 26 DB 02 B0
6A C0 13 21 F2 97 59 6F 2E 29 2A 2B 2C 2D 2E 2F
42.
B1 36 67 41 BD 18 FF 4A DD DB 24 C0 7F 04 EE C9 94 2D 3A D8 72 49 5D D5 36 98 5F 75 26 DB 02 B0
6A C0 13 21 F2 97 59 6F 2E 55 2A 2B 2C 2D 2E 2F
43.
B1 36 67 41 BD 18 FF 4A DD DB 24 C0 7F 04 EE C9 94 2D 3A D8 72 49 5D D5 36 98 5F 75 26 DB 02 B0
6A C0 13 21 F2 97 59 6F 2E 55 1C 2B 2C 2D 2E 2F
44.
B1 36 67 41 BD 18 FF 4A DD DB 24 C0 7F 04 EE C9 94 2D 3A D8 72 49 5D D5 36 98 5F 75 26 DB 02 B0
6A C0 13 21 F2 97 59 6F 2E 55 1C 48 2C 2D 2E 2F
45.
B1 36 67 41 BD 18 FF 4A DD DB 24 C0 7F 04 EE C9 94 2D 3A D8 72 49 5D D5 36 98 5F 75 26 DB 02 B0
6A C0 13 21 F2 97 59 6F 2E 55 1C 48 CE 2D 2E 2F
46.
B1 36 67 41 BD 18 FF 4A DD DB 24 C0 7F 04 EE C9 94 2D 3A D8 72 49 5D D5 36 98 5F 75 26 DB 02 B0
```

```
6A C0 13 21 F2 97 59 6F 2E 55 1C 48 CE 64 2E 2F
47.
B1 36 67 41 BD 18 FF 4A DD DB 24 C0 7F 04 EE C9 94 2D 3A D8 72 49 5D D5 36 98 5F 75 26 DB 02 B0
6A C0 13 21 F2 97 59 6F 2E 55 1C 48 CE 64 1A 2F
48.
B1 36 67 41 BD 18 FF 4A DD DB 24 C0 7F 04 EE C9 94 2D 3A D8 72 49 5D D5 36 98 5F 75 26 DB 02 B0
6A C0 13 21 F2 97 59 6F 2E 55 1C 48 CE 64 1A FE
49.
6B 36 67 41 BD 18 FF 4A DD DB 24 C0 7F 04 EE C9 94 2D 3A D8 72 49 5D D5 36 98 5F 75 26 DB 02 B0
6A C0 13 21 F2 97 59 6F 2E 55 1C 48 CE 64 1A FE
```

Final message digest:
6B 36 67 41 BD 18 FF 4A DD DB 24 C0 7F 04 EE C9 94 2D 3A D8 72 49 5D D5 36 98 5F 75 26 DB 02 B0
6A C0 13 21 F2 97 59 6F 2E 55 1C 48 CE 64 1A FE

11.6 Final hash computation for hash bit length 512.

SR state before final hash computation

```
C8 F9 49 FA B7 CC 10 42 85 05 1C 4A 0C 0D 0E 0F 10 11 12 13 14 15 16 17 18 19 1A 1B 1C 1D 1E 1F
20 21 22 23 24 25 26 27 28 29 2A 2B 2C 2D 2E 2F 30 31 32 33 34 35 36 37 38 39 3A 3B 3C 3D 3E 3F
40 41 42 43 44 45 46 47 48 49 4A 4B 4C 4D 4E 4F 50 51 52 53 54 55 56 57 58 59 5A 5B 5C 5D 5E 5F
60 61 62 63 64 65 66 67 68 69 6A 6B 6C 6D 6E 6F 70 71 72 73 74 75 76 77 78 79 7A 7B 7C 7D 7E 7F
```

Input sequence

```
4A 1C 42 10 FA 49 7F 7E 7B 7A 77 76 73 72 6F 6E 6B 6A 67 66 63 62 5F 5E 5B 5A 57 56 53 52 4F 4E
4B 4A 47 46 43 42 3F 3E 3B 3A 37 36 33 32 2F 2E 2B 2A 27 26 23 22 1F 1E 1B 1A 17 16 13 12 0F 0E
40
```

Initial SR state.

```
0.
00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F 10 11 12 13 14 15 16 17 18 19 1A 1B 1C 1D 1E 1F
20 21 22 23 24 25 26 27 28 29 2A 2B 2C 2D 2E 2F 30 31 32 33 34 35 36 37 38 39 3A 3B 3C 3D 3E 3F
```

Calculating SR state. Total 65 steps.

```
1.
B1 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F 10 11 12 13 14 15 16 17 18 19 1A 1B 1C 1D 1E 1F
20 21 22 23 24 25 26 27 28 29 2A 2B 2C 2D 2E 2F 30 31 32 33 34 35 36 37 38 39 3A 3B 3C 3D 3E 3F
2.
B1 18 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F 10 11 12 13 14 15 16 17 18 19 1A 1B 1C 1D 1E 1F
20 21 22 23 24 25 26 27 28 29 2A 2B 2C 2D 2E 2F 30 31 32 33 34 35 36 37 38 39 3A 3B 3C 3D 3E 3F
3.
B1 18 8C 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F 10 11 12 13 14 15 16 17 18 19 1A 1B 1C 1D 1E 1F
20 21 22 23 24 25 26 27 28 29 2A 2B 2C 2D 2E 2F 30 31 32 33 34 35 36 37 38 39 3A 3B 3C 3D 3E 3F
4.
B1 18 8C 4D 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F 10 11 12 13 14 15 16 17 18 19 1A 1B 1C 1D 1E 1F
20 21 22 23 24 25 26 27 28 29 2A 2B 2C 2D 2E 2F 30 31 32 33 34 35 36 37 38 39 3A 3B 3C 3D 3E 3F
5.
B1 18 8C 4D 10 05 06 07 08 09 0A 0B 0C 0D 0E 0F 10 11 12 13 14 15 16 17 18 19 1A 1B 1C 1D 1E 1F
20 21 22 23 24 25 26 27 28 29 2A 2B 2C 2D 2E 2F 30 31 32 33 34 35 36 37 38 39 3A 3B 3C 3D 3E 3F
6.
B1 18 8C 4D 10 4D 06 07 08 09 0A 0B 0C 0D 0E 0F 10 11 12 13 14 15 16 17 18 19 1A 1B 1C 1D 1E 1F
20 21 22 23 24 25 26 27 28 29 2A 2B 2C 2D 2E 2F 30 31 32 33 34 35 36 37 38 39 3A 3B 3C 3D 3E 3F
7.
B1 18 8C 4D 10 4D F7 07 08 09 0A 0B 0C 0D 0E 0F 10 11 12 13 14 15 16 17 18 19 1A 1B 1C 1D 1E 1F
20 21 22 23 24 25 26 27 28 29 2A 2B 2C 2D 2E 2F 30 31 32 33 34 35 36 37 38 39 3A 3B 3C 3D 3E 3F
8.
B1 18 8C 4D 10 4D F7 47 08 09 0A 0B 0C 0D 0E 0F 10 11 12 13 14 15 16 17 18 19 1A 1B 1C 1D 1E 1F
20 21 22 23 24 25 26 27 28 29 2A 2B 2C 2D 2E 2F 30 31 32 33 34 35 36 37 38 39 3A 3B 3C 3D 3E 3F
9.
B1 18 8C 4D 10 4D F7 47 0A 09 0A 0B 0C 0D 0E 0F 10 11 12 13 14 15 16 17 18 19 1A 1B 1C 1D 1E 1F
20 21 22 23 24 25 26 27 28 29 2A 2B 2C 2D 2E 2F 30 31 32 33 34 35 36 37 38 39 3A 3B 3C 3D 3E 3F
10.
```

```
B1 18 8C 4D 10 4D F7 47 0A 1D 0A 0B 0C 0D 0E 0F 10 11 12 13 14 15 16 17 18 19 1A 1B 1C 1D 1E 1F
20 21 22 23 24 25 26 27 28 29 2A 2B 2C 2D 2E 2F 30 31 32 33 34 35 36 37 38 39 3A 3B 3C 3D 3E 3F
11.
B1 18 8C 4D 10 4D F7 47 0A 1D 49 0B 0C 0D 0E 0F 10 11 12 13 14 15 16 17 18 19 1A 1B 1C 1D 1E 1F
20 21 22 23 24 25 26 27 28 29 2A 2B 2C 2D 2E 2F 30 31 32 33 34 35 36 37 38 39 3A 3B 3C 3D 3E 3F
12.
B1 18 8C 4D 10 4D F7 47 0A 1D 49 D6 0C 0D 0E 0F 10 11 12 13 14 15 16 17 18 19 1A 1B 1C 1D 1E 1F
20 21 22 23 24 25 26 27 28 29 2A 2B 2C 2D 2E 2F 30 31 32 33 34 35 36 37 38 39 3A 3B 3C 3D 3E 3F
13.
B1 18 8C 4D 10 4D F7 47 0A 1D 49 D6 C1 0D 0E 0F 10 11 12 13 14 15 16 17 18 19 1A 1B 1C 1D 1E 1F
20 21 22 23 24 25 26 27 28 29 2A 2B 2C 2D 2E 2F 30 31 32 33 34 35 36 37 38 39 3A 3B 3C 3D 3E 3F
14.
B1 18 8C 4D 10 4D F7 47 0A 1D 49 D6 C1 04 0E 0F 10 11 12 13 14 15 16 17 18 19 1A 1B 1C 1D 1E 1F
20 21 22 23 24 25 26 27 28 29 2A 2B 2C 2D 2E 2F 30 31 32 33 34 35 36 37 38 39 3A 3B 3C 3D 3E 3F
15.
B1 18 8C 4D 10 4D F7 47 0A 1D 49 D6 C1 04 83 0F 10 11 12 13 14 15 16 17 18 19 1A 1B 1C 1D 1E 1F
20 21 22 23 24 25 26 27 28 29 2A 2B 2C 2D 2E 2F 30 31 32 33 34 35 36 37 38 39 3A 3B 3C 3D 3E 3F
16.
B1 18 8C 4D 10 4D F7 47 0A 1D 49 D6 C1 04 83 80 10 11 12 13 14 15 16 17 18 19 1A 1B 1C 1D 1E 1F
20 21 22 23 24 25 26 27 28 29 2A 2B 2C 2D 2E 2F 30 31 32 33 34 35 36 37 38 39 3A 3B 3C 3D 3E 3F
17.
B1 18 8C 4D 10 4D F7 47 0A 1D 49 D6 C1 04 83 80 D7 11 12 13 14 15 16 17 18 19 1A 1B 1C 1D 1E 1F
20 21 22 23 24 25 26 27 28 29 2A 2B 2C 2D 2E 2F 30 31 32 33 34 35 36 37 38 39 3A 3B 3C 3D 3E 3F
18.
B1 18 8C 4D 10 4D F7 47 0A 1D 49 D6 C1 04 83 80 D7 FE 12 13 14 15 16 17 18 19 1A 1B 1C 1D 1E 1F
20 21 22 23 24 25 26 27 28 29 2A 2B 2C 2D 2E 2F 30 31 32 33 34 35 36 37 38 39 3A 3B 3C 3D 3E 3F
19.
B1 18 8C 4D 10 4D F7 47 0A 1D 49 D6 C1 04 83 80 D7 FE B0 13 14 15 16 17 18 19 1A 1B 1C 1D 1E 1F
20 21 22 23 24 25 26 27 28 29 2A 2B 2C 2D 2E 2F 30 31 32 33 34 35 36 37 38 39 3A 3B 3C 3D 3E 3F
20.
B1 18 8C 4D 10 4D F7 47 0A 1D 49 D6 C1 04 83 80 D7 FE B0 9C 14 15 16 17 18 19 1A 1B 1C 1D 1E 1F
20 21 22 23 24 25 26 27 28 29 2A 2B 2C 2D 2E 2F 30 31 32 33 34 35 36 37 38 39 3A 3B 3C 3D 3E 3F
21.
B1 18 8C 4D 10 4D F7 47 0A 1D 49 D6 C1 04 83 80 D7 FE B0 9C C4 15 16 17 18 19 1A 1B 1C 1D 1E 1F
20 21 22 23 24 25 26 27 28 29 2A 2B 2C 2D 2E 2F 30 31 32 33 34 35 36 37 38 39 3A 3B 3C 3D 3E 3F
22.
B1 18 8C 4D 10 4D F7 47 0A 1D 49 D6 C1 04 83 80 D7 FE B0 9C C4 0A 16 17 18 19 1A 1B 1C 1D 1E 1F
20 21 22 23 24 25 26 27 28 29 2A 2B 2C 2D 2E 2F 30 31 32 33 34 35 36 37 38 39 3A 3B 3C 3D 3E 3F
23.
B1 18 8C 4D 10 4D F7 47 0A 1D 49 D6 C1 04 83 80 D7 FE B0 9C C4 0A 92 17 18 19 1A 1B 1C 1D 1E 1F
20 21 22 23 24 25 26 27 28 29 2A 2B 2C 2D 2E 2F 30 31 32 33 34 35 36 37 38 39 3A 3B 3C 3D 3E 3F
24.
B1 18 8C 4D 10 4D F7 47 0A 1D 49 D6 C1 04 83 80 D7 FE B0 9C C4 0A 92 C2 18 19 1A 1B 1C 1D 1E 1F
20 21 22 23 24 25 26 27 28 29 2A 2B 2C 2D 2E 2F 30 31 32 33 34 35 36 37 38 39 3A 3B 3C 3D 3E 3F
25.
B1 18 8C 4D 10 4D F7 47 0A 1D 49 D6 C1 04 83 80 D7 FE B0 9C C4 0A 92 C2 0D 19 1A 1B 1C 1D 1E 1F
20 21 22 23 24 25 26 27 28 29 2A 2B 2C 2D 2E 2F 30 31 32 33 34 35 36 37 38 39 3A 3B 3C 3D 3E 3F
26.
B1 18 8C 4D 10 4D F7 47 0A 1D 49 D6 C1 04 83 80 D7 FE B0 9C C4 0A 92 C2 0D C1 1A 1B 1C 1D 1E 1F
20 21 22 23 24 25 26 27 28 29 2A 2B 2C 2D 2E 2F 30 31 32 33 34 35 36 37 38 39 3A 3B 3C 3D 3E 3F
27.
B1 18 8C 4D 10 4D F7 47 0A 1D 49 D6 C1 04 83 80 D7 FE B0 9C C4 0A 92 C2 0D C1 19 1B 1C 1D 1E 1F
20 21 22 23 24 25 26 27 28 29 2A 2B 2C 2D 2E 2F 30 31 32 33 34 35 36 37 38 39 3A 3B 3C 3D 3E 3F
28.
B1 18 8C 4D 10 4D F7 47 0A 1D 49 D6 C1 04 83 80 D7 FE B0 9C C4 0A 92 C2 0D C1 19 4A 1C 1D 1E 1F
20 21 22 23 24 25 26 27 28 29 2A 2B 2C 2D 2E 2F 30 31 32 33 34 35 36 37 38 39 3A 3B 3C 3D 3E 3F
29.
B1 18 8C 4D 10 4D F7 47 0A 1D 49 D6 C1 04 83 80 D7 FE B0 9C C4 0A 92 C2 0D C1 19 4A F0 1D 1E 1F
20 21 22 23 24 25 26 27 28 29 2A 2B 2C 2D 2E 2F 30 31 32 33 34 35 36 37 38 39 3A 3B 3C 3D 3E 3F
30.
B1 18 8C 4D 10 4D F7 47 0A 1D 49 D6 C1 04 83 80 D7 FE B0 9C C4 0A 92 C2 0D C1 19 4A F0 14 1E 1F
20 21 22 23 24 25 26 27 28 29 2A 2B 2C 2D 2E 2F 30 31 32 33 34 35 36 37 38 39 3A 3B 3C 3D 3E 3F
31.
B1 18 8C 4D 10 4D F7 47 0A 1D 49 D6 C1 04 83 80 D7 FE B0 9C C4 0A 92 C2 0D C1 19 4A F0 14 DC 1F
20 21 22 23 24 25 26 27 28 29 2A 2B 2C 2D 2E 2F 30 31 32 33 34 35 36 37 38 39 3A 3B 3C 3D 3E 3F
32.
B1 18 8C 4D 10 4D F7 47 0A 1D 49 D6 C1 04 83 80 D7 FE B0 9C C4 0A 92 C2 0D C1 19 4A F0 14 DC BC
20 21 22 23 24 25 26 27 28 29 2A 2B 2C 2D 2E 2F 30 31 32 33 34 35 36 37 38 39 3A 3B 3C 3D 3E 3F
33.
B1 18 8C 4D 10 4D F7 47 0A 1D 49 D6 C1 04 83 80 D7 FE B0 9C C4 0A 92 C2 0D C1 19 4A F0 14 DC BC
99 21 22 23 24 25 26 27 28 29 2A 2B 2C 2D 2E 2F 30 31 32 33 34 35 36 37 38 39 3A 3B 3C 3D 3E 3F
34.
B1 18 8C 4D 10 4D F7 47 0A 1D 49 D6 C1 04 83 80 D7 FE B0 9C C4 0A 92 C2 0D C1 19 4A F0 14 DC BC
99 C1 22 23 24 25 26 27 28 29 2A 2B 2C 2D 2E 2F 30 31 32 33 34 35 36 37 38 39 3A 3B 3C 3D 3E 3F
```

```
35.
B1 18 8C 4D 10 4D F7 47 0A 1D 49 D6 C1 04 83 80 D7 FE B0 9C C4 0A 92 C2 0D C1 19 4A F0 14 DC BC
99 C1 BC 23 24 25 26 27 28 29 2A 2B 2C 2D 2E 2F 30 31 32 33 34 35 36 37 38 39 3A 3B 3C 3D 3E 3F
36.
B1 18 8C 4D 10 4D F7 47 0A 1D 49 D6 C1 04 83 80 D7 FE B0 9C C4 0A 92 C2 0D C1 19 4A F0 14 DC BC
99 C1 BC A5 24 25 26 27 28 29 2A 2B 2C 2D 2E 2F 30 31 32 33 34 35 36 37 38 39 3A 3B 3C 3D 3E 3F
37.
B1 18 8C 4D 10 4D F7 47 0A 1D 49 D6 C1 04 83 80 D7 FE B0 9C C4 0A 92 C2 0D C1 19 4A F0 14 DC BC
99 C1 BC A5 B2 25 26 27 28 29 2A 2B 2C 2D 2E 2F 30 31 32 33 34 35 36 37 38 39 3A 3B 3C 3D 3E 3F
38.
B1 18 8C 4D 10 4D F7 47 0A 1D 49 D6 C1 04 83 80 D7 FE B0 9C C4 0A 92 C2 0D C1 19 4A F0 14 DC BC
99 C1 BC A5 B2 07 26 27 28 29 2A 2B 2C 2D 2E 2F 30 31 32 33 34 35 36 37 38 39 3A 3B 3C 3D 3E 3F
39.
B1 18 8C 4D 10 4D F7 47 0A 1D 49 D6 C1 04 83 80 D7 FE B0 9C C4 0A 92 C2 0D C1 19 4A F0 14 DC BC
99 C1 BC A5 B2 07 38 27 28 29 2A 2B 2C 2D 2E 2F 30 31 32 33 34 35 36 37 38 39 3A 3B 3C 3D 3E 3F
40.
B1 18 8C 4D 10 4D F7 47 0A 1D 49 D6 C1 04 83 80 D7 FE B0 9C C4 0A 92 C2 0D C1 19 4A F0 14 DC BC
99 C1 BC A5 B2 07 38 6A 28 29 2A 2B 2C 2D 2E 2F 30 31 32 33 34 35 36 37 38 39 3A 3B 3C 3D 3E 3F
41.
B1 18 8C 4D 10 4D F7 47 0A 1D 49 D6 C1 04 83 80 D7 FE B0 9C C4 0A 92 C2 0D C1 19 4A F0 14 DC BC
99 C1 BC A5 B2 07 38 6A 1B 29 2A 2B 2C 2D 2E 2F 30 31 32 33 34 35 36 37 38 39 3A 3B 3C 3D 3E 3F
42.
B1 18 8C 4D 10 4D F7 47 0A 1D 49 D6 C1 04 83 80 D7 FE B0 9C C4 0A 92 C2 0D C1 19 4A F0 14 DC BC
99 C1 BC A5 B2 07 38 6A 1B C0 2A 2B 2C 2D 2E 2F 30 31 32 33 34 35 36 37 38 39 3A 3B 3C 3D 3E 3F
43.
B1 18 8C 4D 10 4D F7 47 0A 1D 49 D6 C1 04 83 80 D7 FE B0 9C C4 0A 92 C2 0D C1 19 4A F0 14 DC BC
99 C1 BC A5 B2 07 38 6A 1B C0 88 2B 2C 2D 2E 2F 30 31 32 33 34 35 36 37 38 39 3A 3B 3C 3D 3E 3F
44.
B1 18 8C 4D 10 4D F7 47 0A 1D 49 D6 C1 04 83 80 D7 FE B0 9C C4 0A 92 C2 0D C1 19 4A F0 14 DC BC
99 C1 BC A5 B2 07 38 6A 1B C0 88 F2 2C 2D 2E 2F 30 31 32 33 34 35 36 37 38 39 3A 3B 3C 3D 3E 3F
45.
B1 18 8C 4D 10 4D F7 47 0A 1D 49 D6 C1 04 83 80 D7 FE B0 9C C4 0A 92 C2 0D C1 19 4A F0 14 DC BC
99 C1 BC A5 B2 07 38 6A 1B C0 88 F2 4A 2D 2E 2F 30 31 32 33 34 35 36 37 38 39 3A 3B 3C 3D 3E 3F
46.
B1 18 8C 4D 10 4D F7 47 0A 1D 49 D6 C1 04 83 80 D7 FE B0 9C C4 0A 92 C2 0D C1 19 4A F0 14 DC BC
99 C1 BC A5 B2 07 38 6A 1B C0 88 F2 4A 51 2E 2F 30 31 32 33 34 35 36 37 38 39 3A 3B 3C 3D 3E 3F
47.
B1 18 8C 4D 10 4D F7 47 0A 1D 49 D6 C1 04 83 80 D7 FE B0 9C C4 0A 92 C2 0D C1 19 4A F0 14 DC BC
99 C1 BC A5 B2 07 38 6A 1B C0 88 F2 4A 51 B7 2F 30 31 32 33 34 35 36 37 38 39 3A 3B 3C 3D 3E 3F
48.
B1 18 8C 4D 10 4D F7 47 0A 1D 49 D6 C1 04 83 80 D7 FE B0 9C C4 0A 92 C2 0D C1 19 4A F0 14 DC BC
99 C1 BC A5 B2 07 38 6A 1B C0 88 F2 4A 51 B7 8F 30 31 32 33 34 35 36 37 38 39 3A 3B 3C 3D 3E 3F
49.
B1 18 8C 4D 10 4D F7 47 0A 1D 49 D6 C1 04 83 80 D7 FE B0 9C C4 0A 92 C2 0D C1 19 4A F0 14 DC BC
99 C1 BC A5 B2 07 38 6A 1B C0 88 F2 4A 51 B7 8F 12 31 32 33 34 35 36 37 38 39 3A 3B 3C 3D 3E 3F
50.
B1 18 8C 4D 10 4D F7 47 0A 1D 49 D6 C1 04 83 80 D7 FE B0 9C C4 0A 92 C2 0D C1 19 4A F0 14 DC BC
99 C1 BC A5 B2 07 38 6A 1B C0 88 F2 4A 51 B7 8F 12 A2 32 33 34 35 36 37 38 39 3A 3B 3C 3D 3E 3F
51.
B1 18 8C 4D 10 4D F7 47 0A 1D 49 D6 C1 04 83 80 D7 FE B0 9C C4 0A 92 C2 0D C1 19 4A F0 14 DC BC
99 C1 BC A5 B2 07 38 6A 1B C0 88 F2 4A 51 B7 8F 12 A2 08 33 34 35 36 37 38 39 3A 3B 3C 3D 3E 3F
52.
B1 18 8C 4D 10 4D F7 47 0A 1D 49 D6 C1 04 83 80 D7 FE B0 9C C4 0A 92 C2 0D C1 19 4A F0 14 DC BC
99 C1 BC A5 B2 07 38 6A 1B C0 88 F2 4A 51 B7 8F 12 A2 08 58 34 35 36 37 38 39 3A 3B 3C 3D 3E 3F
53.
B1 18 8C 4D 10 4D F7 47 0A 1D 49 D6 C1 04 83 80 D7 FE B0 9C C4 0A 92 C2 0D C1 19 4A F0 14 DC BC
99 C1 BC A5 B2 07 38 6A 1B C0 88 F2 4A 51 B7 8F 12 A2 08 58 93 35 36 37 38 39 3A 3B 3C 3D 3E 3F
54.
B1 18 8C 4D 10 4D F7 47 0A 1D 49 D6 C1 04 83 80 D7 FE B0 9C C4 0A 92 C2 0D C1 19 4A F0 14 DC BC
99 C1 BC A5 B2 07 38 6A 1B C0 88 F2 4A 51 B7 8F 12 A2 08 58 93 E7 36 37 38 39 3A 3B 3C 3D 3E 3F
55.
B1 18 8C 4D 10 4D F7 47 0A 1D 49 D6 C1 04 83 80 D7 FE B0 9C C4 0A 92 C2 0D C1 19 4A F0 14 DC BC
99 C1 BC A5 B2 07 38 6A 1B C0 88 F2 4A 51 B7 8F 12 A2 08 58 93 E7 54 37 38 39 3A 3B 3C 3D 3E 3F
56.
B1 18 8C 4D 10 4D F7 47 0A 1D 49 D6 C1 04 83 80 D7 FE B0 9C C4 0A 92 C2 0D C1 19 4A F0 14 DC BC
99 C1 BC A5 B2 07 38 6A 1B C0 88 F2 4A 51 B7 8F 12 A2 08 58 93 E7 54 03 38 39 3A 3B 3C 3D 3E 3F
57.
B1 18 8C 4D 10 4D F7 47 0A 1D 49 D6 C1 04 83 80 D7 FE B0 9C C4 0A 92 C2 0D C1 19 4A F0 14 DC BC
99 C1 BC A5 B2 07 38 6A 1B C0 88 F2 4A 51 B7 8F 12 A2 08 58 93 E7 54 03 F8 39 3A 3B 3C 3D 3E 3F
58.
B1 18 8C 4D 10 4D F7 47 0A 1D 49 D6 C1 04 83 80 D7 FE B0 9C C4 0A 92 C2 0D C1 19 4A F0 14 DC BC
99 C1 BC A5 B2 07 38 6A 1B C0 88 F2 4A 51 B7 8F 12 A2 08 58 93 E7 54 03 F8 EF 3A 3B 3C 3D 3E 3F
59.
B1 18 8C 4D 10 4D F7 47 0A 1D 49 D6 C1 04 83 80 D7 FE B0 9C C4 0A 92 C2 0D C1 19 4A F0 14 DC BC
```

```
99 C1 BC A5 B2 07 38 6A 1B C0 88 F2 4A 51 B7 8F 12 A2 08 58 93 E7 54 03 F8 EF 1A 3B 3C 3D 3E 3F
60.
B1 18 8C 4D 10 4D F7 47 0A 1D 49 D6 C1 04 83 80 D7 FE B0 9C C4 0A 92 C2 0D C1 19 4A F0 14 DC BC
99 C1 BC A5 B2 07 38 6A 1B C0 88 F2 4A 51 B7 8F 12 A2 08 58 93 E7 54 03 F8 EF 1A 0D 3C 3D 3E 3F
61.
B1 18 8C 4D 10 4D F7 47 0A 1D 49 D6 C1 04 83 80 D7 FE B0 9C C4 0A 92 C2 0D C1 19 4A F0 14 DC BC
99 C1 BC A5 B2 07 38 6A 1B C0 88 F2 4A 51 B7 8F 12 A2 08 58 93 E7 54 03 F8 EF 1A 0D 65 3D 3E 3F
62.
B1 18 8C 4D 10 4D F7 47 0A 1D 49 D6 C1 04 83 80 D7 FE B0 9C C4 0A 92 C2 0D C1 19 4A F0 14 DC BC
99 C1 BC A5 B2 07 38 6A 1B C0 88 F2 4A 51 B7 8F 12 A2 08 58 93 E7 54 03 F8 EF 1A 0D 65 33 3E 3F
63.
B1 18 8C 4D 10 4D F7 47 0A 1D 49 D6 C1 04 83 80 D7 FE B0 9C C4 0A 92 C2 0D C1 19 4A F0 14 DC BC
99 C1 BC A5 B2 07 38 6A 1B C0 88 F2 4A 51 B7 8F 12 A2 08 58 93 E7 54 03 F8 EF 1A 0D 65 33 05 3F
64.
B1 18 8C 4D 10 4D F7 47 0A 1D 49 D6 C1 04 83 80 D7 FE B0 9C C4 0A 92 C2 0D C1 19 4A F0 14 DC BC
99 C1 BC A5 B2 07 38 6A 1B C0 88 F2 4A 51 B7 8F 12 A2 08 58 93 E7 54 03 F8 EF 1A 0D 65 33 05 DD
65.
DC 18 8C 4D 10 4D F7 47 0A 1D 49 D6 C1 04 83 80 D7 FE B0 9C C4 0A 92 C2 0D C1 19 4A F0 14 DC BC
99 C1 BC A5 B2 07 38 6A 1B C0 88 F2 4A 51 B7 8F 12 A2 08 58 93 E7 54 03 F8 EF 1A 0D 65 33 05 DD
```

Final message digest:
DC 18 8C 4D 10 4D F7 47 0A 1D 49 D6 C1 04 83 80 D7 FE B0 9C C4 0A 92 C2 0D C1 19 4A F0 14 DC BC 99 C1 BC A5 B2 07 38 6A 1B C0 88 F2 4A 51 B7 8F 12 A2 08 58 93 E7 54 03 F8 EF 1A 0D 65 33 05 DD

12. Appendix B. CAT and MCT tests (delay=3).

```
# ShortMsgKAT_224.txt
# Algorithm Name: MCSSHA-8
# Principal Submitter: Mikhail Maslennikov

Len = 0
Msg = 00
MD = 37A0735A10133C76AA49533F612347479DE8F2B805A704BB6DB6C2FD

Len = 1
Msg = 00
MD = EA455E4B7C2A673275905A06150A109EC9FBEE930598D25CFB62C8E5

Len = 2
Msg = C0
MD = 9160FEDA1F3994705B6BA1CB6656793340AD81ECC0E8EDF47E1FD74A

Len = 3
Msg = C0
MD = E239F1182CD63BBD47575E3C602C8C6A501FEFDA619FC13620E1240E

Len = 4
Msg = 80
MD = 2CC4ACB5FCA467EA95B7E864EDF58A041848AD3DDADFB663DA7DAEA3

Len = 5
Msg = 48
MD = 5D140F462DAFBA955500E1026314AE54D5709A48B8A3F897C518D332

Len = 6
Msg = 50
MD = C2544431B2CBA7EDD0FFD88D4B453E0C0090C897834C7212BE70EAC9

# LongMsgKAT_224.txt
# Algorithm Name: MCSSHA-8
# Principal Submitter: Mikhail Maslennikov

Len = 2048
Msg                                                                      =
724627916C50338643E6996F07877EAFD96BDF01DA7E991D4155B9BE1295EA7D21C9391F4C4A41C75F77E5D273
89253393725F1427F57914B273AB862B9E31DABCE506E558720520D33352D119F699E784F9E548FF91BC35CA147
042128709820D69A8287EA3257857615EB0321270E94B84F446942765CE882B191FAEE7E1C87E0F0BD4E0CD8A9
27703524B559B769CA4ECE1F6DBF313FDCF67C572EC4185C1A88E86EC11B6454B371980020F19633B6B95BD280
```

```
E4FBCB0161E1A82470320CEC6ECFA25AC73D09F1536F286D3F9DACAFB2CD1D0CE72D64D197F5C7520B3CCB2FD
74EB72664BA93853EF41EABF52F015DD591500D018DD162815CC993595B195
MD = C29EC9BF3A0CC472F34C5F52F0F97CABC1213FD79FA8A7951DD0783C
Len = 2111
Msg =
919FE5E7F35F64A7487649E564771DBBF10AE204ECC2181312D1A79FB579297C94F0DB9EAAE9E009A4F02057AF2
C973C5DAFA7B60154371A5D2C8E992FB6429176F8424B1A866BC1D1BED00438E97FAB42040DCACDEF7CA9FC20
33059B8898BB40CCFB2634B051797BDF3B915C503EC81839AD01E0F4F2F871EFF2008D40011730BE7A47888E79
55A806876BE120CB0F3A139A3620154ECC6482A70F5629F6A9D3341BE6FBBF48E5AA0C53589A04F057DD44268A
FFCABF75ADFC549F73F454264D46A98CCA80E3000C7446853DD5B430C9344E87E3230555B09FB3E7E64B5AD398
9293AC0FEEC0E75F909696F028A5525D26DDEA5D2B2C813FB3613DFF38CE23209285CC77C60860
MD = E61BB5A4866C44931670FDF4283D2562F8F090CD8773788E6CE36638
Len = 2174
Msg =
BD687B6D6684949FBD52A8196DF5D5927B403DEE88A47E4E4B52071BDDA6A6284A9EA1EB84950BA17A60277B0
FEA83C930E5619D5A6D232901B9D3A696662C7FD5F1349B494BC166C67B717C06D03E9FB05DB9EE292D4792F4
59E0ACC08369E3D14684CFF388C940F30738FB71D97EFEB51C7DB553CB85B6FC18429815EC71420822151BB8F5
135DD698EFE3D3118963EE194F94682DFA62EC9D3BCB5F826DA790779704DF2AC5C8A9FA2B50A42A87ED2FBAD
F1E1C8E55689531786A9858DE9E88009E56873FD2D431FCFC99B85574342DC7E78406678BDE94B9A06974DFF15
4EAC3BC7977AC7C123EBCDAC0641A69B792058BA373EDD1BA45E3339C2ABC032993B25F4E3BFA3D5FF620C621
D94C40F8
MD = 0BBA15610E74B885FB2FA6FCCB2AE119A0F595BE446733E92E4334DF
Len = 2237
Msg =
D13409007A6B3242CBAD4CE01D9AED77EFEF0A7725B96A30097EA092FA1E49A136DE03F3F348464C9BEA033216
F380440C7EC81E284738DCC640D485ED32F5D7DD1CF936C1677CBB3CDD8E0E001783FD5A3F388AE6EF7085FF9
A22FA722C7FCCF4CDC239B200D5D11884B565D01C84E4D563C6623C241C5AE0812CE8F9201BBADE48198378A3
E232EF3E10C03022620A266D0A346A6A22F202333A94D2CEF495DBA102B133B8237449C3350BF80EE51B6EE8A9
72CCFC3ED5FD7790444DA253922EEF6C611180F91DF1B6E58E843D318D94A958A017590B14D383C0F385F9CF25
14E8AE1EA749795E10F991E3FB744C6030EF6B02989E8EFFBF8E8BF31FC39B692C517C7C012ECBD0E0785BDEF48
01C4E036C98C6CD0C9328
MD = A8F6DA9F6DC568D8ACBE4222383DDB1EF8280CC5DDF0028CF2192617
Len = 2300
Msg =
68F891C11459B2E9B71774E2B8A2A5C3C9CC36072E3498498496F1C7901684F3E9DACF13A3F1BAE22140DEE525
3732E4D4196B534F675264B53D38659727797F0A18910CCB5B48FE2346C2E998B6537357AF8D15826FCB57BA80
4FE143E765F4680A0B28A9E3716A59ABC60EF253E357A4784FF1BE4680C82D797813CE50355D8FDB3C75936CC3
3E1717B99D9A8ADE9D0EA9172662B708EBCBC31C05064FE67B287C56D01C12411E9B890AD16238B36E192B15C
D86D26F4EFDE5B523D71656F5CEA6CA73BDC04FEB973D303BBAF4C0264761092E23220CEB8359FC91C1D918FB
3F32DBBA92DEAC1C71DA8BC4BE806803F6E7970FA64721C645EED4C2BED7EEFA2B720931FDBD6C67B83756B1C
E51C51F839C250AD900B9D49FE5188FC4A2B5D0
MD = D29770B3A0EF11E720240EBA3357825803EA61CDDC55349AE297FB64
Len = 2363
Msg =
7D9222C58DC49F14BFD7198A9A1C338D17201C007822A91DCD262860364CA1DA8C0056033EB58E406E36D5A4F
6F7E9D98BE57126C9FE7676B58FDF0F9899432FF78DE2AB65C9000071EBA6967123F97BA3DC1F3825D3C8C5148
EAD7AEF0334F40CB0F6B982CB7C99CA39E1B4B2E3A3541683D1EC5560466F52175518390D38C7461C116DB2D5
6EF913784D2E8B20959BBD6F8F3282C597D94A1EDBFA8F25089E9D2E8DC465EAD90FA23E4388BD6BAFE226327
49B7AAEA53D5CBCF9678227ADC3F4109F1849AC2539B6F2B25B4D8EDAB41E8BFCFC337728DC48A8EA5119115F
C1B133300D68231C96A9D518F6DC3CA51581309C53F49510FE18F608A215069D41F2CFC84E53A9347FD723DFF9
D3F5006F7C0B18441A29BDEF7725920260B1613C6532A0A994B488E0
MD = 270CA5799DC7755E02901443454CA832B94F20C9B65E99D232FDCCB3
Len = 2426
Msg =
FC447A550FC565F964337521DBD6481FF6C4FEC25A2BC946230C0021570E75B0E3D50320AB24C4949CB4EA7ED6
D14D10E1EB9CB4116461A743D49F337597F12D09945285647B249A2AE3EBF69F1FC62A36532B2FC89ECED5B48A
C27A0E18AF8B0F023BE5C00FF0BF8C16F412B34D4AE9ECD2963583FA268ED439B4640FFCC57384EF066362E23D
2F0712F9658CB7B7F56F548C4A3C7DB51D8FF4430D14CE1042221254CAA4BF009B197E6F74B42067E95E42D6C8
F2D37AA5522F5594D61745BA28C8F302E007316282985730FBCB8BDAB0C5A3693BEEC32C0D57AD20D3394B7AC
72831FF5DDFC8208E09057AB9E9EE2FAC208E9FCB6D0B567C4DDED41ED286678DB3860B230C9A52C577867EC3
5A17EF902E258CD8314F36875D97543088679415FD0D7C2A9CB6CAEE76A2A1DC294700
MD = 81DA03068C74D99D41ACFFC2E69543302D9EA82D0D241ED7D27EA2C8
```

```
# ExtremelyLongMsgKAT_224.txt
# Algorithm Name: MCSSHA-8
# Principal Submitter: Mikhail Maslennikov

Repeat = 16777216
Text = abcdefghbcdefghicdefghijdefghijkefghijklfghijklmghijklmnhijklmno
MD = 9ABA8A8F5C043EEBD02E0D0EC2D4A4668A3F5B155F7F78D0D0665E64
```

```
# MonteCarlo_224.txt
# Algorithm Name: MCSSHA-8
# Principal Submitter: Mikhail Maslennikov

Seed =
6CD4C0C5CB2CA2A0F1D1AECEBAC03B52E64EA03D1A1654372936545B92BBC5484A59DB74BB60F9C40CEB1A5A
A35A6FAFE80349E14C253A4E8B1D77612DDD81ACE926AE8B0AF6E53176DBFFCC2A6B88C6BD765F939D3D178A9
BDE9EF3AA131C61E31C1E42CDFAF4B4DCDE579A37E150EFBEF5555B4C1CB40439D835A724E2FAE7

j = 0
MD = 3818DF31AD5C227586D9E7DB61BCE604B73FCD755BB03ACEF08806DC

j = 1
MD = CBF2FBCBFA9BF272686FA9A619672ABBD9F7AB5DCBD9DB28E33C864E

j = 2
MD = AA3833D61FB26A740660492070F06B210B7ED5A32A0C380CBE13C74F

j = 3
MD = 9A507FF52EC2CF34D305C91E57BF9313AD2583C47483C8DCF5CEBA04

j = 4
MD = 7C875DCE5F13621CBBD0F6C3F168F1F431B4F1CD5162136B3A6A9A7D

j = 5
MD = 794139C648980375F98665EBAFE0961AE48F694178BEA91D3F33D325

j = 6
MD = E795296E9EBF5DBB20D29E02123330AD9380D236DDE310E5DCAFDEE9



# ShortMsgKAT_256.txt
# Algorithm Name: MCSSHA-8
# Principal Submitter: Mikhail Maslennikov

Len = 0
Msg = 00
MD = 85F885B535D359C4A535D8B03F334A7F08FD1361FBC8041CB090B70DB2A61402

Len = 1
Msg = 00
MD = 9491051B551FB423DF137DC8F1ACD3A9EF3DCCE427715885F6FE8C18A3D27171

Len = 2
Msg = C0
MD = AFC55BB1D6A2E6B997E7BAFA64BCE83B9E0BDDBB16DDE335ADE73722579EE940

Len = 3
Msg = C0
MD = 48BC1FC69C65364312F73D83B650E71F355835A51FB00BDD0D8CC100307240B5

Len = 4
Msg = 80
MD = 9FAC6CF08DF4B4B7ED32795C3C7F4CBD21E63EB164085BFA7CECE232FE0C2BF2

Len = 5
Msg = 48
MD = 022584B10166F5A85E7DC2F4AD6F435FC718CFB543F97B40CF29DB5BFCCCF525

Len = 6
Msg = 50
MD = 7859006D461A73B6A5DE3D7B59E5729A40A379A19F416B46156A9D2040CD4E27



# LongMsgKAT_256.txt
# Algorithm Name: MCSSHA-8
# Principal Submitter: Mikhail Maslennikov
```

```
Len = 2048
Msg =
724627916C50338643E6996F07877EAFD96BDF01DA7E991D4155B9BE1295EA7D21C9391F4C4A41C75F77E5D273
89253393725F1427F57914B273AB862B9E31DABCE506E558720520D33352D119F699E784F9E548FF91BC35CA147
042128709820D69A8287EA3257857615EB0321270E94B84F446942765CE882B191FAEE7E1C87E0F0BD4E0CD8A9
27703524B559B769CA4ECE1F6DBF313FDCF67C572EC4185C1A88E86EC11B6454B371980020F19633B6B95BD280
E4FBCB0161E1A82470320CEC6ECFA25AC73D09F1536F286D3F9DACAFB2CD1D0CE72D64D197F5C7520B3CCB2FD
74EB72664BA93853EF41EABF52F015DD591500D018DD162815CC993595B195
MD = A35F673FCA7B9CDA78B7FCB46B402EAA80F77858FF3681B6684FFB9DD9AF0482
Len = 2111
Msg =
919FE5E7F35F64A7487649E564771DBBF10AE204ECC2181312D1A79FB579297C94F0DB9EAAE9E009A4F02057AF2
C973C5DAFA7B60154371A5D2C8E992FB6429176F8424B1A866BC1D1BED00438E97FAB42040DCACDEF7CA9FC20
33059B8898BB40CCFB2634B051797BDF3B915C503EC81839AD01E0F4F2F871EFF2008D40011730BE7A47888E79
55A806876BE120CB0F3A139A3620154ECC6482A70F5629F6A9D3341BE6FBBF48E5AA0C53589A04F057DD44268A
FFCABF75ADFC549F73F454264D46A98CCA80E3000C7446853DD5B430C9344E87E3230555B09FB3E7E64B5AD398
9293AC0FEEC0E75F909696F028A5525D26DDEA5D2B2C813FB3613DFF38CE23209285CC77C60860
MD = 1079ACA9B5CA5164413F946BDA608A8B2C2A4063378055972DB53585D420645F
Len = 2174
Msg =
BD687B6D6684949FBD52A8196DF5D5927B403DEE88A47E4E4B52071BDDA6A6284A9EA1EB84950BA17A60277B0
FEA83C930E5619D5A6D232901B9D3A696662C7FD5F1349B494BC166C67B717C06D03E9FB05DB9EE292D4792F4
59E0ACC08369E3D14684CFF388C940F30738FB71D97EFEB51C7DB553CB85B6FC18429815EC71420822151BB8F5
135DD698EFE3D3118963EE194F94682DFA62EC9D3BCB5F826DA790779704DF2AC5C8A9FA2B50A42A87ED2FBAD
F1E1C8E55689531786A9858DE9E88009E56873FD2D431FCFC99B85574342DC7E78406678BDE94B9A06974DFF15
4EAC3BC7977AC7C123EBCDAC0641A69B792058BA373EDD1BA45E3339C2ABC032993B25F4E3BFA3D5FF620C621
D94C40F8
MD = 59548F207557633F5D4AE265C0356C3712E90264D83262C51D56EB6EABB6DDDC
Len = 2237
Msg =
D13409007A6B3242CBAD4CE01D9AED77EFEF0A7725B96A30097EA092FA1E49A136DE03F3F348464C9BEA033216
F380440C7EC81E284738DCC640D485ED32F5D7DD1CF936C1677CBB3CDD8E0E001783FD5A3F388AE6EF7085FF9
A22FA722C7FCCF4CDC239B200D5D11884B565D01C84E4D563C6623C241C5AE0812CE8F9201BBADE48198378A3
E232EF3E10C03022620A266D0A346A6A22F202333A94D2CEF495DBA102B133B8237449C3350BF80EE51B6EE8A9
72CCFC3ED5FD7790444DA253922EEF6C611180F91DF1B6E58E843D318D94A958A017590B14D383C0F385F9CF25
14E8AE1EA749795E10F991E3FB744C6030EF6B02989E8EFFBF8E8BF31FC39B692C517C7C012ECBD0E0785BDEF48
01C4E036C98C6CD0C9328
MD = CB352476A4C7913E848D9747AC9D38DECF69D0F9EF37CC83E60C18EE28EE50AE
Len = 2300
Msg =
68F891C11459B2E9B71774E2B8A2A5C3C9CC36072E3498498496F1C7901684F3E9DACF13A3F1BAE22140DEE525
3732E4D4196B534F675264B53D38659727797F0A18910CCB5B48FE2346C2E998B6537357AF8D15826FCB57BA80
4FE143E765F4680A0B28A9E3716A59ABC60EF253E357A4784FF1BE4680C82D797813CE50355D8FDB3C75936CC3
3E1717B99D9A8ADE9D0EA9172662B708EBCBC31C05064FE67B287C56D01C12411E9B890AD16238B36E192B15C
D86D26F4EFDE5B523D71656F5CEA6CA73BDC04FEB973D303BBAF4C0264761092E23220CEB8359FC91C1D918FB
3F32DBBA92DEAC1C71DA8BC4BE806803F6E7970FA64721C645EED4C2BED7EEFA2B720931FDBD6C67B83756B1C
E51C51F839C250AD900B9D49FE5188FC4A2B5D0
MD = 1265D72D175E5231618A1CAFFC8DA7490779A4AC318EAD614C01DE96BEED96E4
Len = 2363
Msg =
7D9222C58DC49F14BFD7198A9A1C338D17201C007822A91DCD262860364CA1DA8C0056033EB58E406E36D5A4F
6F7E9D98BE57126C9FE7676B58FDF0F9899432FF78DE2AB65C9000071EBA6967123F97BA3DC1F3825D3C8C5148
EAD7AEF0334F40CB0F6B982CB7C99CA39E1B4B2E3A3541683D1EC5560466F52175518390D38C7461C116DB2D5
6EF913784D2E8B20959BBD6F8F3282C597D94A1EDBFA8F25089E9D2E8DC465EAD90FA23E4388BD6BAFE226327
49B7AAEA53D5CBCF9678227ADC3F4109F1849AC2539B6F2B25B4D8EDAB41E8BFCFC337728DC48A8EA5119115F
C1B133300D68231C96A9D518F6DC3CA51581309C53F49510FE18F608A215069D41F2CFC84E53A9347FD723DFF9
D3F5006F7C0B18441A29BDEF7725920260B1613C6532A0A994B488E0
MD = 2BF19242F57A57CB3B00B2B92497ECD77356125EE1171B517637AA6C7266680B
Len = 2426
Msg =
FC447A550FC565F964337521DBD6481FF6C4FEC25A2BC946230C0021570E75B0E3D50320AB24C4949CB4EA7ED6
D14D10E1EB9CB4116461A743D49F337597F12D09945285647B249A2AE3EBF69F1FC62A36532B2FC89ECED5B48A
C27A0E18AF8B0F023BE5C00FF0BF8C16F412B34D4AE9ECD2963583FA268ED439B4640FFCC57384EF066362E23D
2F0712F9658CB7B7F56F548C4A3C7DB51D8FF4430D14CE1042221254CAA4BF009B197E6F74B42067E95E42D6C8
F2D37AA5522F5594D61745BA28C8F302E007316282985730FBCB8BDAB0C5A3693BEEC32C0D57AD20D3394B7AC
72831FF5DDFC8208E09057AB9E9EE2FAC208E9FCB6D0B567C4DDED41ED286678DB3860B230C9A52C577867EC3
5A17EF902E258CD8314F36875D97543088679415FD0D7C2A9CB6CAEE76A2A1DC294700
MD = B299D004AFFF2942987D292C2D4811A59A985035B180A1D9499B6C5A3F493F21


# ExtremelyLongMsgKAT_256.txt
# Algorithm Name: MCSSHA-8
# Principal Submitter: Mikhail Maslennikov
```

```
Repeat = 16777216
Text = abcdefghbcdefghicdefghijdefghijkefghijklfghijklmghijklmnhijklmno
MD = E38645C76DE3CCDB0E21E896528E5DD830D68AB06C78AF5AD17A44D1BB2945C5



# MonteCarlo_256.txt
# Algorithm Name: MCSSHA-8
# Principal Submitter: Mikhail Maslennikov

Seed                                                                                                  =
6CD4C0C5CB2CA2A0F1D1AECEBAC03B52E64EA03D1A1654372936545B92BBC5484A59DB74BB60F9C40CEB1A5A
A35A6FAFE80349E14C253A4E8B1D77612DDD81ACE926AE8B0AF6E53176DBFFCC2A6B88C6BD765F939D3D178A9
BDE9EF3AA131C61E31C1E42CDFAF4B4DCDE579A37E150EFBEF5555B4C1CB40439D835A724E2FAE7

j = 0
MD = C03144041DB1414E046694984DFFD43CBFDA1B5E66C517CF79708A2987C23F7B

j = 1
MD = C5903B51898A3B026757088FA6B43A3F17F12E05CB0AEE426455527D237BC78A

j = 2
MD = A56DEB5F4968F61222F33C0B1F19725D0AC17056A654D8E62F839F403891665E

j = 3
MD = 68247FE6E3E6F36EE3A12C1FF5D991AF73BC2E9380BE268AF6F45E41610A669B

j = 4
MD = 4B35EF94B9FB8B7425CE9B0362885FBF507E17A0CFCA36FC9CD94842082AE827

j = 5
MD = 4C1A39227B21931214CDCFB1B68FAA719158B4964314C512B2916DC1025B08D4

j = 6
MD = 689AC672D0E15B47EEE438A797528F48D096D2BB42ECC88F828F9C676220C0DB


# ShortMsgKAT_384.txt
# Algorithm Name: MCSSHA-8
# Principal Submitter: Mikhail Maslennikov

Len = 0
Msg = 00
MD                                                                                                    =
EB83E13170B407236766D369C79D5DCF84323ADF7EFFB4314739C24C8A160133CB2F961560370A4EA2B3B71CF1
E759F1

Len = 1
Msg = 00
MD                                                                                                    =
D8F1D2C7DC9C3380C9C2ABF63E6645F7347782CF2E5ACB8E7B4818C47014065E923653B9076C0F29B79015C22B
9611AE

Len = 2
Msg = C0
MD                                                                                                    =
AED56BC1E6B2F6C9A7F7CA0A74CCF84BAE1BEDCB26EDF345BDF7473267AEF99E1EAC8650E250864F314C32D6D
87536F1

Len = 3
Msg = C0
MD                                                                                                    =
A73717F1622FCBB8DD582F05BDC4069C801681E09E3B6EF3AFE5611DFCDF5F258CF924CC2F69ADE72510A06A2B
D219F0

Len = 4
Msg = 80
MD                                                                                                    =
286F9F942EE3767B63253982D0142CFFE78990B7C95E2D5686651520018A3ACFEB2A6E2C5B744DD454711EDB71
D15AAA

Len = 5
Msg = 48
```

```
MD =
BB72026F7670679FD83F157CE5C245A3DE9318B0D92A4EF28869600E8ADB7BC094FE019110556FB2867A897037
DCD6B8

Len = 6
Msg = 50
MD =
9C1FBE6387A1E57D2D69D33D5F01F43C9EF1B82019CE9B963CF1C9AADD4A19A702DC8D6AAC00C05CC78AB23C
7E098C9F


# LongMsgKAT_384.txt
# Algorithm Name: MCSSHA-8
# Principal Submitter: Mikhail Maslennikov

Len = 2048
Msg =
724627916C50338643E6996F07877EAFD96BDF01DA7E991D4155B9BE1295EA7D21C9391F4C4A41C75F77E5D273
89253393725F1427F57914B273AB862B9E31DABCE506E558720520D33352D119F699E784F9E548FF91BC35CA147
042128709820D69A8287EA3257857615EB0321270E94B84F446942765CE882B191FAEE7E1C87E0F0BD4E0CD8A9
27703524B559B769CA4ECE1F6DBF313FDCF67C572EC4185C1A88E86EC11B6454B371980020F19633B6B95BD280
E4FBCB0161E1A82470320CEC6ECFA25AC73D09F1536F286D3F9DACAFB2CD1D0CE72D64D197F5C7520B3CCB2FD
74EB72664BA93853EF41EABF52F015DD591500D018DD162815CC993595B195
MD =
8459D4BFCE99FCEB6429ACB0FA87F3BEB81F48B38EC6EAE5CC7CAA05A2F93765D0D0F68794672D6DCE818D525
704122B
Len = 2111
Msg =
919FE5E7F35F64A7487649E564771DBBF10AE204ECC2181312D1A79FB579297C94F0DB9EAAE9E009A4F02057AF2
C973C5DAFA7B60154371A5D2C8E992FB6429176F8424B1A866BC1D1BED00438E97FAB42040DCACDEF7CA9FC20
33059B8898BB40CCFB2634B051797BDF3B915C503EC81839AD01E0F4F2F871EFF2008D40011730BE7A47888E79
55A806876BE120CB0F3A139A3620154ECC6482A70F5629F6A9D3341BE6FBBF48E5AA0C53589A04F057DD44268A
FFCABF75ADFC549F73F454264D46A98CCA80E3000C7446853DD5B430C9344E87E3230555B09FB3E7E64B5AD398
9293AC0FEEC0E75F909696F028A5525D26DDEA5D2B2C813FB3613DFF38CE23209285CC77C60860
MD =
CCB6D277C1C8F43E964652193EC7D4329474272EEC0A66B14E1804D7A5035F25E3CBF488DE582482466B9EE62B
98307A
Len = 2174
Msg =
BD687B6D6684949FBD52A8196DF5D5927B403DEE88A47E4E4B52071BDDA6A6284A9EA1EB84950BA17A60277B0
FEA83C930E5619D5A6D232901B9D3A696662C7FD5F1349B494BC166C67B717C06D03E9FB05DB9EE292D4792F4
59E0ACC08369E3D14684CFF388C940F30738FB71D97EFEB51C7DB553CB85B6FC18429815EC71420822151BB8F5
135DD698EFE3D3118963EE194F94682DFA62EC9D3BCB5F826DA790779704DF2AC5C8A9FA2B50A42A87ED2FBAD
F1E1C8E55689531786A9858DE9E88009E56873FD2D431FCFC99B85574342DC7E78406678BDE94B9A06974DFF15
4EAC3BC7977AC7C123EBCDAC0641A69B792058BA373EDD1BA45E3339C2ABC032993B25F4E3BFA3D5FF620C621
D94C40F8
MD =
6D6AFBBE6BFAF56825853C10795EE6ABF84A3DBFE6791292D767FA41E13E677118BB28199E4463FE2FEC7E36250
24F64
Len = 2237
Msg =
D13409007A6B3242CBAD4CE01D9AED77EFEF0A7725B96A30097EA092FA1E49A136DE03F3F348464C9BEA033216
F380440C7EC81E284738DCC640D485ED32F5D7DD1CF936C1677CBB3CDD8E0E001783FD5A3F388AE6EF7085FF9
A22FA722C7FCCF4CDC239B200D5D11884B565D01C84E4D563C6623C241C5AE0812CE8F9201BBADE48198378A3
E232EF3E10C03022620A266D0A346A6A22F202333A94D2CEF495DBA102B133B8237449C3350BF80EE51B6EE8A9
72CCFC3ED5FD7790444DA253922EEF6C611180F91DF1B6E58E843D318D94A958A017590B14D383C0F385F9CF25
14E8AE1EA749795E10F991E3FB744C6030EF6B02989E8EFFBF8E8BF31FC39B692C517C7C012ECBD0E0785BDEF48
01C4E036C98C6CD0C9328
MD =
8DB02BD7E2ABFC7E2AFFAD47669BCEF43C1A4912A8276D5AB12A1C5EA6866FBFCE1CF46C9D9DF5B61D6C074E1
E9433FC
Len = 2300
Msg =
68F891C11459B2E9B71774E2B8A2A5C3C9CC36072E3498498496F1C7901684F3E9DACF13A3F1BAE22140DEE525
3732E4D4196B534F675264B53D38659727797F0A18910CCB5B48FE2346C2E998B6537357AF8D15826FCB57BA80
4FE143E765F4680A0B28A9E3716A59ABC60EF253E357A4784FF1BE4680C82D797813CE50355D8FDB3C75936CC3
3E1717B99D9A8ADE9D0EA9172662B708EBCBC31C05064FE67B287C56D01C12411E9B890AD16238B36E192B15C
D86D26F4EFDE5B523D71656F5CEA6CA73BDC04FEB973D303BBAF4C0264761092E23220CEB8359FC91C1D918FB
3F32DBBA92DEAC1C71DA8BC4BE806803F6E7970FA64721C645EED4C2BED7EEFA2B720931FDBD6C67B83756B1C
E51C51F839C250AD900B9D49FE5188FC4A2B5D0
MD =
1E409EBDAA3C3B53E0A13FBA8B462EAF9CCE188BA6AC6958A373904428C2A0D104E4AE070BB93654319D7E773
9359950
Len = 2363
```

```
Msg =
7D9222C58DC49F14BFD7198A9A1C338D17201C007822A91DCD262860364CA1DA8C0056033EB58E406E36D5A4F
6F7E9D98BE57126C9FE7676B58FDF0F9899432FF78DE2AB65C9000071EBA6967123F97BA3DC1F3825D3C8C5148
EAD7AEF0334F40CB0F6B982CB7C99CA39E1B4B2E3A3541683D1EC5560466F52175518390D38C7461C116DB2D5
6EF913784D2E8B20959BBD6F8F3282C597D94A1EDBFA8F25089E9D2E8DC465EAD90FA23E4388BD6BAFE226327
49B7AAEA53D5CBCF9678227ADC3F4109F1849AC2539B6F2B25B4D8EDAB41E8BFCFC337728DC48A8EA5119115F
C1B133300D68231C96A9D518F6DC3CA51581309C53F49510FE18F608A215069D41F2CFC84E53A9347FD723DFF9
D3F5006F7C0B18441A29BDEF7725920260B1613C6532A0A994B488E0
MD =
3A429C9377F12D8B7FDDEF88758C6A48D43FF0455BC37A2225250B99FA13928CD538CB80E0DE8A616E80711088
9DAFC3
Len = 2426
Msg =
FC447A550FC565F964337521DBD6481FF6C4FEC25A2BC946230C0021570E75B0E3D50320AB24C4949CB4EA7ED6
D14D10E1EB9CB4116461A743D49F337597F12D09945285647B249A2AE3EBF69F1FC62A36532B2FC89ECED5B48A
C27A0E18AF8B0F023BE5C00FF0BF8C16F412B34D4AE9ECD2963583FA268ED439B4640FFCC57384EF066362E23D
2F0712F9658CB7B7F56F548C4A3C7DB51D8FF4430D14CE1042221254CAA4BF009B197E6F74B42067E95E42D6C8
F2D37AA5522F5594D61745BA28C8F302E007316282985730FBCB8BDAB0C5A3693BEEC32C0D57AD20D3394B7AC
72831FF5DDFC8208E09057AB9E9EE2FAC208E9FCB6D0B567C4DDED41ED286678DB3860B230C9A52C577867EC3
5A17EF902E258CD8314F36875D97543088679415FD0D7C2A9CB6CAEE76A2A1DC294700
MD =
5199AA1F589395E036003E5C9586DF0AC2B6AAE9A347FB0B9BB92D04492A5F06EB17622B4D2A604B24BC04DA2
0C26207


# ExtremelyLongMsgKAT_384.txt
# Algorithm Name: MCSSHA-8
# Principal Submitter: Mikhail Maslennikov

Repeat = 16777216
Text = abcdefghbcdefghicdefghijdefghijkefghijklfghijklmghijklmnhijklmno
MD =
78968B6C508C46412F0C390778EE1FB59D10919FFA3559A451DE2BF4BA65FBB7F555EB6AAA9E53004AD879C679
D5EC13


# MonteCarlo_384.txt
# Algorithm Name: MCSSHA-8
# Principal Submitter: Mikhail Maslennikov

Seed =
6CD4C0C5CB2CA2A0F1D1AECEBAC03B52E64EA03D1A1654372936545B92BBC5484A59DB74BB60F9C40CEB1A5A
A35A6FAFE80349E14C253A4E8B1D77612DDD81ACE926AE8B0AF6E53176DBFFCC2A6B88C6BD765F939D3D178A9
BDE9EF3AA131C61E31C1E42CDFAF4B4DCDE579A37E150EFBEF5555B4C1CB40439D835A724E2FAE7

j = 0
MD =
93A41902BAA88742DD15EE5983328208F689B5A52F94AFEB0F5DA994E4BD9593F0EAE00605D1EF3234191DA9DE
464065

j = 1
MD =
F704157F15C099B12C766866EC201B3314A02624D128DCFEF627B4382202A007D3CDFDCB57FDD59D653C01595
2A7235B

j = 2
MD =
E1D08CF43114C24A0DB53FAF9A6FC04887C62E2CC7D89856C4344A2E0E00A62CBD514C0C2546560E2671F1F11B
EDF09F

j = 3
MD =
2EDF91961B3EA09308A6C4C21EC90CA83ADEB6EA2591FF80928FF067599418774B2491FB16F6617F04606270E7B
87E5C

j = 4
MD =
0E3EF8707735302FE46FF44EE0B31C12360E47E5989D185D48AA396C3BC45EDF74B4405CF52EBFC2B1AA50D7A9
A0F74B

j = 5
MD =
F7339D1AF8586D362B6A58DE1B996AB4DCAA3962ABA86DF1E560E46482D5759A44FC66B482D51C62A0808F3B9
81C935F
```

```
j = 6
MD =
BE2FA51551DB738C2CA4C62B8EDF92EA1D01EB59FFEAA55E6192F73E64ABF5C98E476B9E9CEB07255BF7A5EA8E
5BC98C



# ShortMsgKAT_512.txt
# Algorithm Name: MCSSHA-8
# Principal Submitter: Mikhail Maslennikov

Len = 0
Msg = 00
MD =
650AC9996F4EEA42035F41CFB5F654D99BAD3FD5A3BA9C20429FB2B868CEDC7E81366EC546ECCA75F171F83A74
8D5D7962FD24B8A7DF27AC52F656D307DB7A32

Len = 1
Msg = 00
MD =
31B1253B753FD443FF339DE811CCF3C90F5DEC04479178A5161EAC38C3F29185C9B6566E6A74D5026DD7757DC
93A72ADAE8B031DA526603775CDAB8172D2ED6B

Len = 2
Msg = C0
MD =
AC277C7B8AB87F912EFC8DBF9B52F924513C4439179B881AFA3B8AAF822B67B0EA3BBC3D32DBB6FED97D58FDC
5B46A6E132FE7F8FA1E13B263AA9DA36A3D893F

Len = 3
Msg = C0
MD =
DC2F94D5C744CD72EBBA0BF7BB1CA135152BEA5CA41C1FFF70A71A571CBE5ACF3FE7299A6D1EE251E48D6301D
5CF8B83AE1825580BD2D4154E943DD25A88B925

Len = 4
Msg = 80
MD =
0E77A77B09E528490FC170A2D24B2C5535DB38C151965461DA033765C6096B1E433F11A3F7532026E4F410987B
41638BD74DC794447F414385DA6A9C9713EC25

Len = 5
Msg = 48
MD =
DDD11F5AAD68002269AB116CBA39A44C8054F1295EC763E6E313717CDCC2025232D61F9225FF30F1DFF88485D
8B82CE68AFF843057D86E59F075032151E57499

Len = 6
Msg = 50
MD =
A4461E22A8471EB2D6330B91BDBC19DE2A3176C3F3075BA348F5961D0840E26E83AA0B60FD81F956ACFD6DA3B
6A19317BF38C76BA3E1F39D66B3B423CB19F072



# LongMsgKAT_512.txt
# Algorithm Name: MCSSHA-8
# Principal Submitter: Mikhail Maslennikov

Len = 2048
Msg =
724627916C50338643E6996F07877EAFD96BDF01DA7E991D4155B9BE1295EA7D21C9391F4C4A41C75F77E5D273
89253393725F1427F57914B273AB862B9E31DABCE506E558720520D33352D119F699E784F9E548FF91BC35CA147
042128709820D69A8287EA3257857615EB0321270E94B84F446942765CE882B191FAEE7E1C87E0F0BD4E0CD8A9
27703524B559B769CA4ECE1F6DBF313FDCF67C572EC4185C1A88E86EC11B6454B371980020F19633B6B95BD280
E4FBCB0161E1A82470320CEC6ECFA25AC73D09F1536F286D3F9DACAFB2CD1D0CE72D64D197F5C7520B3CCB2FD
74EB72664BA93853EF41EABF52F015DD591500D018DD162815CC993595B195
MD =
297753F6A4CEE4C1642C8C915CEC819B070C8E84F4AEB6AB87AF7C7555AE46E1E779E9AA7A138693A75FECD319
F7922837730321ADFF7F21C52F82890C39EADE
Len = 2111
Msg =
919FE5E7F35F64A7487649E564771DBBF10AE204ECC2181312D1A79FB579297C94F0DB9EAAE9E009A4F02057AF2
```

```
C973C5DAFA7B60154371A5D2C8E992FB6429176F8424B1A866BC1D1BED00438E97FAB42040DCACDEF7CA9FC20
33059B8898BB40CCFB2634B051797BDF3B915C503EC81839AD01E0F4F2F871EFF2008D40011730BE7A47888E79
55A806876BE120CB0F3A139A3620154ECC6482A70F5629F6A9D3341BE6FBBF48E5AA0C53589A04F057DD44268A
FFCABF75ADFC549F73F454264D46A98CCA80E3000C7446853DD5B430C9344E87E3230555B09FB3E7E64B5AD398
9293AC0FEEC0E75F909696F028A5525D26DDEA5D2B2C813FB3613DFF38CE23209285CC77C60860
MD                                                                                        =
36D59C187429F295446CCC224789A1ACFFDC26DCA4879171A6334203967C4682E12446C10E1B483BBF8A01F5A5
0A5A9BC6B5041CE062E93B4660DD5076A9F440
Len = 2174
Msg                                                                                       =
BD687B6D6684949FBD52A8196DF5D5927B403DEE88A47E4E4B52071BDDA6A6284A9EA1EB84950BA17A60277B0
FEA83C930E5619D5A6D232901B9D3A696662C7FD5F1349B494BC166C67B717C06D03E9FB05DB9EE292D4792F4
59E0ACC08369E3D14684CFF388C940F30738FB71D97EFEB51C7DB553CB85B6FC18429815EC71420822151BB8F5
135DD698EFE3D3118963EE194F94682DFA62EC9D3BCB5F826DA790779704DF2AC5C8A9FA2B50A42A87ED2FBAD
F1E1C8E55689531786A9858DE9E88009E56873FD2D431FCFC99B85574342DC7E78406678BDE94B9A06974DFF15
4EAC3BC7977AC7C123EBCDAC0641A69B792058BA373EDD1BA45E3339C2ABC032993B25F4E3BFA3D5FF620C621
D94C40F8
MD                                                                                        =
C6B5B0E213B9D83DB14856D884D4DD3DA81B433B44A8073BAAD865487A690D008DAD7352CFD8A2DB4A3F38B
256396576E34954C724DCCAB313B8FD4F30016163
Len = 2237
Msg                                                                                       =
D13409007A6B3242CBAD4CE01D9AED77EFEF0A7725B96A30097EA092FA1E49A136DE03F3F348464C9BEA033216
F380440C7EC81E284738DCC640D485ED32F5D7DD1CF936C1677CBB3CDD8E0E001783FD5A3F388AE6EF7085FF9
A22FA722C7FCCF4CDC239B200D5D11884B565D01C84E4D563C6623C241C5AE0812CE8F9201BBADE48198378A3
E232EF3E10C03022620A266D0A346A6A22F202333A94D2CEF495DBA102B133B8237449C3350BF80EE51B6EE8A9
72CCFC3ED5FD7790444DA253922EEF6C611180F91DF1B6E58E843D318D94A958A017590B14D383C0F385F9CF25
14E8AE1EA749795E10F991E3FB744C6030EF6B02989E8EFFBF8E8BF31FC39B692C517C7C012ECBD0E0785BDEF48
01C4E036C98C6CD0C9328
MD                                                                                        =
3D969BD4DE41547470337B18AFE51A8564D14FA6B4AA7B12E9DE5471E5664CB0318AA36F06507B6BFF90C10E1B
FF92DE589954AEAC98556F353AA548357A777A
Len = 2300
Msg                                                                                       =
68F891C11459B2E9B71774E2B8A2A5C3C9CC36072E3498498496F1C7901684F3E9DACF13A3F1BAE22140DEE525
3732E4D4196B534F675264B53D38659727797F0A18910CCB5B48FE2346C2E998B6537357AF8D15826FCB57BA80
4FE143E765F4680A0B28A9E3716A59ABC60EF253E357A4784FF1BE4680C82D797813CE50355D8FDB3C75936CC3
3E1717B99D9A8ADE9D0EA9172662B708EBCBC31C05064FE67B287C56D01C12411E9B890AD16238B36E192B15C
D86D26F4EFDE5B523D71656F5CEA6CA73BDC04FEB973D303BBAF4C0264761092E23220CEB8359FC91C1D918FB
3F32DBBA92DEAC1C71DA8BC4BE806803F6E7970FA64721C645EED4C2BED7EEFA2B720931FDBD6C67B83756B1C
E51C51F839C250AD900B9D49FE5188FC4A2B5D0
MD                                                                                        =
0F31F21B7EBAF68209552C567EA5CD4B193AB558686521C75476E9B3B97FA75C828E73E90D5BA041DF2115DA56
0CF856E010D8C27CD375B616E6AAAB7FA200A1
Len = 2363
Msg                                                                                       =
7D9222C58DC49F14BFD7198A9A1C338D17201C007822A91DCD262860364CA1DA8C0056033EB58E406E36D5A4F
6F7E9D98BE57126C9FE7676B58FDF0F9899432FF78DE2AB65C9000071EBA6967123F97BA3DC1F3825D3C8C5148
EAD7AEF0334F40CB0F6B982CB7C99CA39E1B4B2E3A3541683D1EC5560466F52175518390D38C7461C116DB2D5
6EF913784D2E8B20959BBD6F8F3282C597D94A1EDBFA8F25089E9D2E8DC465EAD90FA23E4388BD6BAFE226327
49B7AAEA53D5CBCF9678227ADC3F4109F1849AC2539B6F2B25B4D8EDAB41E8BFCFC337728DC48A8EA5119115F
C1B133300D68231C96A9D518F6DC3CA51581309C53F49510FE18F608A215069D41F2CFC84E53A9347FD723DFF9
D3F5006F7C0B18441A29BDEF7725920260B1613C6532A0A994B488E0
MD                                                                                        =
C56F178F494E56FCF15E15C334E7FD50D9FBC353B30A4073D343D4F228A94C7F5B4584F07C93652AD92D20BE08
3E8F6074BB6D895949C1DAE8081574627860E3
Len = 2426
Msg                                                                                       =
FC447A550FC565F964337521DBD6481FF6C4FEC25A2BC946230C0021570E75B0E3D50320AB24C4949CB4EA7ED6
D14D10E1EB9CB4116461A743D49F337597F12D09945285647B249A2AE3EBF69F1FC62A36532B2FC89ECED5B48A
C27A0E18AF8B0F023BE5C00FF0BF8C16F412B34D4AE9ECD2963583FA268ED439B4640FFCC57384EF066362E23D
2F0712F9658CB7B7F56F548C4A3C7DB51D8FF4430D14CE1042221254CAA4BF009B197E6F74B42067E95E42D6C8
F2D37AA5522F5594D61745BA28C8F302E007316282985730FBCB8BDAB0C5A3693BEEC32C0D57AD20D3394B7AC
72831FF5DDFC8208E09057AB9E9EE2FAC208E9FCB6D0B567C4DDED41ED286678DB3860B230C9A52C577867EC3
5A17EF902E258CD8314F36875D97543088679415FD0D7C2A9CB6CAEE76A2A1DC294700
MD                                                                                        =
979BD0D8E864FE91711E1C8F7F835DC29ACA3978D0F32B67F2604E38C7D0D035FC7B202ABFB6A9EC7D6CB72E4
2B8C61BA540E2F6C250B83C4092E9570AB08E96



# ExtremelyLongMsgKAT_512.txt
# Algorithm Name: MCSSHA-8
# Principal Submitter: Mikhail Maslennikov

Repeat = 16777216
Text = abcdefghbcdefghicdefghijdefghijkefghijklfghijklmghijklmnhijklmno
MD =
B54DC5C258001ED96AC19BAD84BCCF582EF16C78C356ADED5384CB3E91E001B927EC99EEA2969A5DCECEFD9D
11AC5D3F18B310F81D22CA41FB8CB26AF6B60F23



# MonteCarlo_512.txt
# Algorithm Name: MCSSHA-8
# Principal Submitter: Mikhail Maslennikov

Seed =
6CD4C0C5CB2CA2A0F1D1AECEBAC03B52E64EA03D1A1654372936545B92BBC5484A59DB74BB60F9C40CEB1A5A
A35A6FAFE80349E14C253A4E8B1D77612DDD81ACE926AE8B0AF6E53176DBFFCC2A6B88C6BD765F939D3D178A9
BDE9EF3AA131C61E31C1E42CDFAF4B4DCDE579A37E150EFBEF5555B4C1CB40439D835A724E2FAE7

j = 0
MD =
E7D79D51450C1CB6C41753EDD971E2C9D08BC89011CFDAE1EE82F348B865F195786431ADFDF884C921484AB53
DAC2F0260222A740263992290C7A77C60A0B287

j = 1
MD =
D09AD2F1B92D34A890C4EB151657D9AC22235B3B562399CFBCF6174DAFCC274069A76E45D6F6B5B4DD3CF5538
EB92E092632AD6E8319CA781437A4AB9B2E7F81

j = 2
MD =
93919E78E8171D9896F2ACF931C261EBD92A2DFD3926CF3183D7DEF8EA72ED246C22E425DE3709FBDCD9090D0
12B73C0AB9EF122E6117D96ADDD0BAACCF3335D

j = 3
MD =
68FB138A561FC4F838EC1F871C318A87722F086743664B0C1328366F1E4B980845CF7559498FEEC25E441AA8031
0395C0F20E1CB8D40332F881954D3AB4CBA78

j = 4
MD =
CB15F41966354ADB2A145D4C719CD29D3E62566E54A4D36F04199A4F6895762B9E36EAB2E505D2CD8C017C01F
6798AF1CA23DEFEA11092DCDD430AF536DAC5EB

j = 5
MD =
FE29995B675D46DE5706271915B52B1DA16AC7A49D5F8DC3A20469360E5CFC60E6F0099087743F14CD105133B3
1C60C905596AF33189CF1AB5A7623D427DE0A1

j = 6
MD =
43ED2EFF2DD151169A23A886CC55242491EB784684BAFD513BB42802628753E6322379F5C4A64A62381C63F194
7A3B11132376112374EF3CCC311757FB49BACB
```