Algorithm: **MCSSHA-8**
Principal submitter: **Mikhail Maslennikov**

Revision: February 15, 2014

SECURE HASH ALGORITHM MCSSHA-8

Table of Contents

1. INTRODUCTION 2
2. DEFINITIONS 3
2.1 Glossary of Terms and Acronyms 3
2.2 Algorithm Parameters, Symbols, and Terms 3
2.2.1 Parameters 3
2.2.2 Symbols 4
3. NOTATION AND CONVENTIONS 5
3.1 Substitution 5
3.2 Shift Registry Steps 5
4. FUNCTIONS AND CONSTANTS 6
4.1 Constants 6
4.2 Functions 6
5. PREPROCESSING 7
6. PRE-HASH COMPUTATION 8
7. FINAL HASH COMPUTATION 9
7.1 Preparing input sequence for first digest. 9
7.2 Preparing first digest. 9
7.3 Preparing input sequence for second digest. 9
7.4 Preparing second digest. 10
7.5 Preparing final digest. 10
9. ESTIMATED COMPUTATIONAL EFFICIENCY AND MEMORY REQUIREMENTS 10
9.1 Memory Requirement 10
9.2 Computation Efficiency 10
10. Appendix A. Calculating hash examples. 12
10.1 Pre-hash computation for hash bit length 224 and 256, delay=3. 12
10.2 Pre-hash computation for hash bit length 384 and 512, delay=3. 13
10.3 Final hash computation for hash bit length 224. 14
10.4 Final hash computation for hash bit length 256. 16
10.5 Final hash computation for hash bit length 384. 19
10.6 Final hash computation for hash bit length 512. 23
11. Appendix B. CAT and MCT tests (delay=3). 30

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.

$M=m_1,m_2,...,m_L$ 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.

$a(mod\ N)$ 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}.

π(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: $p= (p_4+1) \pmod N$.

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 π is constant and same for each step.

4.1 Constants

SR substitution π 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 $Y=(y_0,y_1, \ldots,y_{N-1})$- 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:

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

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

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

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. In final stage MCSSHA-8 algorithm calculate two digests D1 and D2 length of H bytes each. Then this digests are added bit by bit mod 2.

7.1 Preparing input sequence for first digest.

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

Input sequence Z1 for SR have length H and, if remain bits absent, will be as follow:

$$Z1 = B_N,B_{N-1},B_{N-4},B_{N-5},B_{N-8},B_{N-9},...$$

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

$$Z1 = a_1,a_2,...,a_r,\ b_n,b_{n-1},...,b_{n-15},b_{n-32},b_{n-33},...,b_{n-47},b_{n-64},...$$

Final input sequence for first digest is Z1 | H (add message digest length to the end of the sequence Z1)

7.2 Preparing first digest.

Preparing first digest D1 use SR with length H and input sequence Z1 | H 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.

7.3 Preparing input sequence for second digest.

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

Input sequence Z2 for SR have length H and, if remain bits absent, will be as follow:

$$Z2 = B_{N-2},B_{N-3},B_{N-6},B_{N-7},B_{N-10},B_{N-11},...$$

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

$$Z2 = a_1,a_2,...,a_r,\ b_{n-16},b_{n-17},...,b_{n-31},b_{n-48},b_{n-49},...,b_{n-63},b_{n-80},...$$

Final input sequence for second digests is Z2 | H (add message digest length to the end of the sequence Z2)

7.4 Preparing second digest.

Preparing second digest D2 use SR with length H and input sequence Z2 | H 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.

7.5 Preparing final digest.

Final digest D is result of bitwise addition D1 and D2.

$$D = D1 \oplus D2$$

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	3,0
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	11,9
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	9,3
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	6,8
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	15,4
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	9,5
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. 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.

10.1 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

10.2 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

10.3 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 for D1

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

First 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

Input sequence for D2
85 98 2D 0E 22 C8 3D 3C 39 38 35 34 31 30 2D 2C 29 28 25 24 21 20 1D 1C 19 18 15 14

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.
EC 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.
EC 2C 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.
EC 2C C9 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.
EC 2C C9 79 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.
EC 2C C9 79 84 05 06 07 08 09 0A 0B 0C 0D 0E 0F 10 11 12 13 14 15 16 17 18 19 1A 1B
6.
EC 2C C9 79 84 E8 06 07 08 09 0A 0B 0C 0D 0E 0F 10 11 12 13 14 15 16 17 18 19 1A 1B
7.
EC 2C C9 79 84 E8 67 07 08 09 0A 0B 0C 0D 0E 0F 10 11 12 13 14 15 16 17 18 19 1A 1B
8.
EC 2C C9 79 84 E8 67 AF 08 09 0A 0B 0C 0D 0E 0F 10 11 12 13 14 15 16 17 18 19 1A 1B
9.
EC 2C C9 79 84 E8 67 AF 7A 09 0A 0B 0C 0D 0E 0F 10 11 12 13 14 15 16 17 18 19 1A 1B
10.
EC 2C C9 79 84 E8 67 AF 7A A6 0A 0B 0C 0D 0E 0F 10 11 12 13 14 15 16 17 18 19 1A 1B
11.
EC 2C C9 79 84 E8 67 AF 7A A6 08 0B 0C 0D 0E 0F 10 11 12 13 14 15 16 17 18 19 1A 1B
12.
EC 2C C9 79 84 E8 67 AF 7A A6 08 18 0C 0D 0E 0F 10 11 12 13 14 15 16 17 18 19 1A 1B
13.
EC 2C C9 79 84 E8 67 AF 7A A6 08 18 89 0D 0E 0F 10 11 12 13 14 15 16 17 18 19 1A 1B
14.

EC 2C C9 79 84 E8 67 AF 7A A6 08 18 89 3C 0E 0F 10 11 12 13 14 15 16 17 18 19 1A 1B
15.
EC 2C C9 79 84 E8 67 AF 7A A6 08 18 89 3C 28 0F 10 11 12 13 14 15 16 17 18 19 1A 1B
16.
EC 2C C9 79 84 E8 67 AF 7A A6 08 18 89 3C 28 E2 10 11 12 13 14 15 16 17 18 19 1A 1B
17.
EC 2C C9 79 84 E8 67 AF 7A A6 08 18 89 3C 28 E2 0D 11 12 13 14 15 16 17 18 19 1A 1B
18.
EC 2C C9 79 84 E8 67 AF 7A A6 08 18 89 3C 28 E2 0D F9 12 13 14 15 16 17 18 19 1A 1B
19.
EC 2C C9 79 84 E8 67 AF 7A A6 08 18 89 3C 28 E2 0D F9 F6 13 14 15 16 17 18 19 1A 1B
20.
EC 2C C9 79 84 E8 67 AF 7A A6 08 18 89 3C 28 E2 0D F9 F6 AA 14 15 16 17 18 19 1A 1B
21.
EC 2C C9 79 84 E8 67 AF 7A A6 08 18 89 3C 28 E2 0D F9 F6 AA 95 15 16 17 18 19 1A 1B
22.
EC 2C C9 79 84 E8 67 AF 7A A6 08 18 89 3C 28 E2 0D F9 F6 AA 95 36 16 17 18 19 1A 1B
23.
EC 2C C9 79 84 E8 67 AF 7A A6 08 18 89 3C 28 E2 0D F9 F6 AA 95 36 06 17 18 19 1A 1B
24.
EC 2C C9 79 84 E8 67 AF 7A A6 08 18 89 3C 28 E2 0D F9 F6 AA 95 36 06 FE 18 19 1A 1B
25.
EC 2C C9 79 84 E8 67 AF 7A A6 08 18 89 3C 28 E2 0D F9 F6 AA 95 36 06 FE 0B 19 1A 1B
26.
EC 2C C9 79 84 E8 67 AF 7A A6 08 18 89 3C 28 E2 0D F9 F6 AA 95 36 06 FE 0B F7 1A 1B
27.
EC 2C C9 79 84 E8 67 AF 7A A6 08 18 89 3C 28 E2 0D F9 F6 AA 95 36 06 FE 0B F7 DA 1B
28.
EC 2C C9 79 84 E8 67 AF 7A A6 08 18 89 3C 28 E2 0D F9 F6 AA 95 36 06 FE 0B F7 DA 83
29.
DC 2C C9 79 84 E8 67 AF 7A A6 08 18 89 3C 28 E2 0D F9 F6 AA 95 36 06 FE 0B F7 DA 83

Second digest:
DC 2C C9 79 84 E8 67 AF 7A A6 08 18 89 3C 28 E2 0D F9 F6 AA 95 36 06 FE 0B F7 DA 83

Final digest:
B9 19 12 7C 35 BA B0 EA F8 D6 C9 F1 15 32 44 DC 2D 3F AC 15 09 E5 57 72 AD 59 18 69

10.4 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 for D1

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

First 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 D**4**

Input sequence for D2

85 98 2D 0E 22 C8 3D 3C 39 38 35 34 31 30 2D 2C 29 28 25 24 21 20 1D 1C 19 18 15 14 11 10 0D 0C 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.

EC 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.
EC E3 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.
EC E3 8E 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.
EC E3 8E A8 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.
EC E3 8E A8 4D 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.
EC E3 8E A8 4D 87 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.
EC E3 8E A8 4D 87 7D 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.
EC E3 8E A8 4D 87 7D 1B 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.
EC E3 8E A8 4D 87 7D 1B 01 09 0A 0B 0C 0D 0E 0F 10 11 12 13 14 15 16 17 18 19 1A 1B 1C 1D 1E 1F
10.
EC E3 8E A8 4D 87 7D 1B 01 02 0A 0B 0C 0D 0E 0F 10 11 12 13 14 15 16 17 18 19 1A 1B 1C 1D 1E 1F
11.
EC E3 8E A8 4D 87 7D 1B 01 02 AC 0B 0C 0D 0E 0F 10 11 12 13 14 15 16 17 18 19 1A 1B 1C 1D 1E 1F
12.
EC E3 8E A8 4D 87 7D 1B 01 02 AC 36 0C 0D 0E 0F 10 11 12 13 14 15 16 17 18 19 1A 1B 1C 1D 1E 1F
13.
EC E3 8E A8 4D 87 7D 1B 01 02 AC 36 1E 0D 0E 0F 10 11 12 13 14 15 16 17 18 19 1A 1B 1C 1D 1E 1F
14.
EC E3 8E A8 4D 87 7D 1B 01 02 AC 36 1E C9 0E 0F 10 11 12 13 14 15 16 17 18 19 1A 1B 1C 1D 1E 1F
15.
EC E3 8E A8 4D 87 7D 1B 01 02 AC 36 1E C9 BE 0F 10 11 12 13 14 15 16 17 18 19 1A 1B 1C 1D 1E 1F
16.
EC E3 8E A8 4D 87 7D 1B 01 02 AC 36 1E C9 BE 7D 10 11 12 13 14 15 16 17 18 19 1A 1B 1C 1D 1E 1F
17.
EC E3 8E A8 4D 87 7D 1B 01 02 AC 36 1E C9 BE 7D 91 11 12 13 14 15 16 17 18 19 1A 1B 1C 1D 1E 1F
18.
EC E3 8E A8 4D 87 7D 1B 01 02 AC 36 1E C9 BE 7D 91 3B 12 13 14 15 16 17 18 19 1A 1B 1C 1D 1E 1F
19.
EC E3 8E A8 4D 87 7D 1B 01 02 AC 36 1E C9 BE 7D 91 3B 18 13 14 15 16 17 18 19 1A 1B 1C 1D 1E 1F
20.
EC E3 8E A8 4D 87 7D 1B 01 02 AC 36 1E C9 BE 7D 91 3B 18 27 14 15 16 17 18 19 1A 1B 1C 1D 1E 1F
21.
EC E3 8E A8 4D 87 7D 1B 01 02 AC 36 1E C9 BE 7D 91 3B 18 27 7D 15 16 17 18 19 1A 1B 1C 1D 1E 1F
22.
EC E3 8E A8 4D 87 7D 1B 01 02 AC 36 1E C9 BE 7D 91 3B 18 27 7D DD 16 17 18 19 1A 1B 1C 1D 1E 1F
23.
EC E3 8E A8 4D 87 7D 1B 01 02 AC 36 1E C9 BE 7D 91 3B 18 27 7D DD 7E 17 18 19 1A 1B 1C 1D 1E 1F
24.
EC E3 8E A8 4D 87 7D 1B 01 02 AC 36 1E C9 BE 7D 91 3B 18 27 7D DD 7E 10 18 19 1A 1B 1C 1D 1E 1F
25.
EC E3 8E A8 4D 87 7D 1B 01 02 AC 36 1E C9 BE 7D 91 3B 18 27 7D DD 7E 10 45 19 1A 1B 1C 1D 1E 1F
26.
EC E3 8E A8 4D 87 7D 1B 01 02 AC 36 1E C9 BE 7D 91 3B 18 27 7D DD 7E 10 45 DC 1A 1B 1C 1D 1E 1F
27.
EC E3 8E A8 4D 87 7D 1B 01 02 AC 36 1E C9 BE 7D 91 3B 18 27 7D DD 7E 10 45 DC 04 1B 1C 1D 1E 1F
28.
EC E3 8E A8 4D 87 7D 1B 01 02 AC 36 1E C9 BE 7D 91 3B 18 27 7D DD 7E 10 45 DC 04 81 1C 1D 1E 1F
29.
EC E3 8E A8 4D 87 7D 1B 01 02 AC 36 1E C9 BE 7D 91 3B 18 27 7D DD 7E 10 45 DC 04 81 F4 1D 1E 1F
30.
EC E3 8E A8 4D 87 7D 1B 01 02 AC 36 1E C9 BE 7D 91 3B 18 27 7D DD 7E 10 45 DC 04 81 F4 0D 1E 1F
31.
EC E3 8E A8 4D 87 7D 1B 01 02 AC 36 1E C9 BE 7D 91 3B 18 27 7D DD 7E 10 45 DC 04 81 F4 0D 55 1F
32.
EC E3 8E A8 4D 87 7D 1B 01 02 AC 36 1E C9 BE 7D 91 3B 18 27 7D DD 7E 10 45 DC 04 81 F4 0D 55 31
33.
7A E3 8E A8 4D 87 7D 1B 01 02 AC 36 1E C9 BE 7D 91 3B 18 27 7D DD 7E 10 45 DC 04 81 F4 0D 55 31

Second message digest:
7A E3 8E A8 4D 87 7D 1B 01 02 AC 36 1E C9 BE 7D 91 3B 18 27 7D DD 7E 10 45 DC 04 81 F4 0D 55 31

Final digest:
D1 E8 A5 50 FB BA A6 51 83 23 0B D7 85 35 2B 7A 63 B5 7F 5D 09 7D A1 E6 8E 87 CE C5 B1 F5 3F E5

10.5 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 for D1

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

First 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

Input sequence for D2
05 85 CC B7 F9 C8 7D 7C 79 78 75 74 71 70 6D 6C 69 68 65 64 61 60 5D 5C 59 58 55 54 51 50 4D 4C 49 48 45
44 41 40 3D 3C 39 38 35 34 31 30 2D 2C 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.
6C 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.
6C 58 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.
6C 58 97 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.
6C 58 97 7B 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.
6C 58 97 7B F7 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.
6C 58 97 7B F7 41 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.
6C 58 97 7B F7 41 46 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.
6C 58 97 7B F7 41 46 D5 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.
6C 58 97 7B F7 41 46 D5 92 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.
6C 58 97 7B F7 41 46 D5 92 48 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.
6C 58 97 7B F7 41 46 D5 92 48 D5 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.
6C 58 97 7B F7 41 46 D5 92 48 D5 D3 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.
6C 58 97 7B F7 41 46 D5 92 48 D5 D3 29 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.
6C 58 97 7B F7 41 46 D5 92 48 D5 D3 29 F1 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.
6C 58 97 7B F7 41 46 D5 92 48 D5 D3 29 F1 06 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.
6C 58 97 7B F7 41 46 D5 92 48 D5 D3 29 F1 06 E9 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.
6C 58 97 7B F7 41 46 D5 92 48 D5 D3 29 F1 06 E9 E5 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.
6C 58 97 7B F7 41 46 D5 92 48 D5 D3 29 F1 06 E9 E5 D5 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.
6C 58 97 7B F7 41 46 D5 92 48 D5 D3 29 F1 06 E9 E5 D5 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
20.
6C 58 97 7B F7 41 46 D5 92 48 D5 D3 29 F1 06 E9 E5 D5 B0 32 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.
6C 58 97 7B F7 41 46 D5 92 48 D5 D3 29 F1 06 E9 E5 D5 B0 32 9E 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.
6C 58 97 7B F7 41 46 D5 92 48 D5 D3 29 F1 06 E9 E5 D5 B0 32 9E E8 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.
6C 58 97 7B F7 41 46 D5 92 48 D5 D3 29 F1 06 E9 E5 D5 B0 32 9E E8 8E 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.
6C 58 97 7B F7 41 46 D5 92 48 D5 D3 29 F1 06 E9 E5 D5 B0 32 9E E8 8E 3E 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.
6C 58 97 7B F7 41 46 D5 92 48 D5 D3 29 F1 06 E9 E5 D5 B0 32 9E E8 8E 3E 62 19 1A 1B 1C 1D 1E 1F 20 21 22 23 24 25 26 27 28 29 2A 2B 2C 2D 2E 2F
26.
6C 58 97 7B F7 41 46 D5 92 48 D5 D3 29 F1 06 E9 E5 D5 B0 32 9E E8 8E 3E 62 22 1A 1B 1C 1D 1E 1F 20 21 22 23 24 25 26 27 28 29 2A 2B 2C 2D 2E 2F
27.
6C 58 97 7B F7 41 46 D5 92 48 D5 D3 29 F1 06 E9 E5 D5 B0 32 9E E8 8E 3E 62 22 9C 1B 1C 1D 1E 1F 20 21 22 23 24 25 26 27 28 29 2A 2B 2C 2D 2E 2F
28.
6C 58 97 7B F7 41 46 D5 92 48 D5 D3 29 F1 06 E9 E5 D5 B0 32 9E E8 8E 3E 62 22 9C 43 1C 1D 1E 1F 20 21 22 23 24 25 26 27 28 29 2A 2B 2C 2D 2E 2F
29.
6C 58 97 7B F7 41 46 D5 92 48 D5 D3 29 F1 06 E9 E5 D5 B0 32 9E E8 8E 3E 62 22 9C 43 D2 1D 1E 1F 20 21 22 23 24 25 26 27 28 29 2A 2B 2C 2D 2E 2F
30.
6C 58 97 7B F7 41 46 D5 92 48 D5 D3 29 F1 06 E9 E5 D5 B0 32 9E E8 8E 3E 62 22 9C 43 D2 4F 1E 1F 20 21 22 23 24 25 26 27 28 29 2A 2B 2C 2D 2E 2F
31.
6C 58 97 7B F7 41 46 D5 92 48 D5 D3 29 F1 06 E9 E5 D5 B0 32 9E E8 8E 3E 62 22 9C 43 D2 4F 45 1F 20 21 22 23 24 25 26 27 28 29 2A 2B 2C 2D 2E 2F
32.
6C 58 97 7B F7 41 46 D5 92 48 D5 D3 29 F1 06 E9 E5 D5 B0 32 9E E8 8E 3E 62 22 9C 43 D2 4F 45 AC 20 21 22 23 24 25 26 27 28 29 2A 2B 2C 2D 2E 2F
33.
6C 58 97 7B F7 41 46 D5 92 48 D5 D3 29 F1 06 E9 E5 D5 B0 32 9E E8 8E 3E 62 22 9C 43 D2 4F 45 AC 93 21 22 23 24 25 26 27 28 29 2A 2B 2C 2D 2E 2F
34.

6C 58 97 7B F7 41 46 D5 92 48 D5 D3 29 F1 06 E9 E5 D5 B0 32 9E E8 8E 3E 62 22 9C 43 D2 4F 45 AC 93 57 22 23
24 25 26 27 28 29 2A 2B 2C 2D 2E 2F
35.
6C 58 97 7B F7 41 46 D5 92 48 D5 D3 29 F1 06 E9 E5 D5 B0 32 9E E8 8E 3E 62 22 9C 43 D2 4F 45 AC 93 57 E1 23
24 25 26 27 28 29 2A 2B 2C 2D 2E 2F
36.
6C 58 97 7B F7 41 46 D5 92 48 D5 D3 29 F1 06 E9 E5 D5 B0 32 9E E8 8E 3E 62 22 9C 43 D2 4F 45 AC 93 57 E1 31
24 25 26 27 28 29 2A 2B 2C 2D 2E 2F
37.
6C 58 97 7B F7 41 46 D5 92 48 D5 D3 29 F1 06 E9 E5 D5 B0 32 9E E8 8E 3E 62 22 9C 43 D2 4F 45 AC 93 57 E1 31
99 25 26 27 28 29 2A 2B 2C 2D 2E 2F
38.
6C 58 97 7B F7 41 46 D5 92 48 D5 D3 29 F1 06 E9 E5 D5 B0 32 9E E8 8E 3E 62 22 9C 43 D2 4F 45 AC 93 57 E1 31
99 FD 26 27 28 29 2A 2B 2C 2D 2E 2F
39.
6C 58 97 7B F7 41 46 D5 92 48 D5 D3 29 F1 06 E9 E5 D5 B0 32 9E E8 8E 3E 62 22 9C 43 D2 4F 45 AC 93 57 E1 31
99 FD D6 27 28 29 2A 2B 2C 2D 2E 2F
40.
6C 58 97 7B F7 41 46 D5 92 48 D5 D3 29 F1 06 E9 E5 D5 B0 32 9E E8 8E 3E 62 22 9C 43 D2 4F 45 AC 93 57 E1 31
99 FD D6 8B 28 29 2A 2B 2C 2D 2E 2F
41.
6C 58 97 7B F7 41 46 D5 92 48 D5 D3 29 F1 06 E9 E5 D5 B0 32 9E E8 8E 3E 62 22 9C 43 D2 4F 45 AC 93 57 E1 31
99 FD D6 8B E0 29 2A 2B 2C 2D 2E 2F
42.
6C 58 97 7B F7 41 46 D5 92 48 D5 D3 29 F1 06 E9 E5 D5 B0 32 9E E8 8E 3E 62 22 9C 43 D2 4F 45 AC 93 57 E1 31
99 FD D6 8B E0 44 2A 2B 2C 2D 2E 2F
43.
6C 58 97 7B F7 41 46 D5 92 48 D5 D3 29 F1 06 E9 E5 D5 B0 32 9E E8 8E 3E 62 22 9C 43 D2 4F 45 AC 93 57 E1 31
99 FD D6 8B E0 44 E9 2B 2C 2D 2E 2F
44.
6C 58 97 7B F7 41 46 D5 92 48 D5 D3 29 F1 06 E9 E5 D5 B0 32 9E E8 8E 3E 62 22 9C 43 D2 4F 45 AC 93 57 E1 31
99 FD D6 8B E0 44 E9 23 2C 2D 2E 2F
45.
6C 58 97 7B F7 41 46 D5 92 48 D5 D3 29 F1 06 E9 E5 D5 B0 32 9E E8 8E 3E 62 22 9C 43 D2 4F 45 AC 93 57 E1 31
99 FD D6 8B E0 44 E9 23 DF 2D 2E 2F
46.
6C 58 97 7B F7 41 46 D5 92 48 D5 D3 29 F1 06 E9 E5 D5 B0 32 9E E8 8E 3E 62 22 9C 43 D2 4F 45 AC 93 57 E1 31
99 FD D6 8B E0 44 E9 23 DF 33 2E 2F
47.
6C 58 97 7B F7 41 46 D5 92 48 D5 D3 29 F1 06 E9 E5 D5 B0 32 9E E8 8E 3E 62 22 9C 43 D2 4F 45 AC 93 57 E1 31
99 FD D6 8B E0 44 E9 23 DF 33 56 2F
48.
6C 58 97 7B F7 41 46 D5 92 48 D5 D3 29 F1 06 E9 E5 D5 B0 32 9E E8 8E 3E 62 22 9C 43 D2 4F 45 AC 93 57 E1 31
99 FD D6 8B E0 44 E9 23 DF 33 56 3A
49.
0D 58 97 7B F7 41 46 D5 92 48 D5 D3 29 F1 06 E9 E5 D5 B0 32 9E E8 8E 3E 62 22 9C 43 D2 4F 45 AC 93 57 E1 31
99 FD D6 8B E0 44 E9 23 DF 33 56 3A

Second message digest:
0D 58 97 7B F7 41 46 D5 92 48 D5 D3 29 F1 06 E9 E5 D5 B0 32 9E E8 8E 3E 62 22 9C 43 D2 4F 45 AC 93 57 E1 31
99 FD D6 8B E0 44 E9 23 DF 33 56 3A

Final digest:
**66 6E F0 3A 4A 59 B9 9F 4F 93 F1 13 56 F5 E8 20 71 F8 8A EA EC A1 D3 EB 54 BA C3 36 F4 94 47 1C F9
97 F2 10 6B 6A 8F E4 CE 11 F5 6B 11 57 4C C4**

10.6 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 for D1

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

First 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

Input sequence for D2

05 85 CC B7 F9 C8 7D 7C 79 78 75 74 71 70 6D 6C 69 68 65 64 61 60 5D 5C 59 58 55 54 51 50 4D 4C
49 48 45 44 41 40 3D 3C 39 38 35 34 31 30 2D 2C 29 28 25 24 21 20 1D 1C 19 18 15 14 11 10 0D 0C
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.
6C 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.
6C 47 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.
6C 47 14 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.
6C 47 14 96 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.
6C 47 14 96 C4 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.
6C 47 14 96 C4 BB 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.
6C 47 14 96 C4 BB 4A 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.
6C 47 14 96 C4 BB 4A 55 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.
6C 47 14 96 C4 BB 4A 55 7B 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.
6C 47 14 96 C4 BB 4A 55 7B F4 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.
6C 47 14 96 C4 BB 4A 55 7B F4 3E 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.
6C 47 14 96 C4 BB 4A 55 7B F4 3E 52 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.
6C 47 14 96 C4 BB 4A 55 7B F4 3E 52 88 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.
6C 47 14 96 C4 BB 4A 55 7B F4 3E 52 88 B7 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.
6C 47 14 96 C4 BB 4A 55 7B F4 3E 52 88 B7 9F 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.
6C 47 14 96 C4 BB 4A 55 7B F4 3E 52 88 B7 9F A9 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.
6C 47 14 96 C4 BB 4A 55 7B F4 3E 52 88 B7 9F A9 0A 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.
6C 47 14 96 C4 BB 4A 55 7B F4 3E 52 88 B7 9F A9 0A 0D 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.
6C 47 14 96 C4 BB 4A 55 7B F4 3E 52 88 B7 9F A9 0A 0D 19 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.
6C 47 14 96 C4 BB 4A 55 7B F4 3E 52 88 B7 9F A9 0A 0D 19 41 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.
6C 47 14 96 C4 BB 4A 55 7B F4 3E 52 88 B7 9F A9 0A 0D 19 41 F0 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.

6C 47 14 96 C4 BB 4A 55 7B F4 3E 52 88 B7 9F A9 0A 0D 19 41 F0 6C 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.
6C 47 14 96 C4 BB 4A 55 7B F4 3E 52 88 B7 9F A9 0A 0D 19 41 F0 6C 02 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.
6C 47 14 96 C4 BB 4A 55 7B F4 3E 52 88 B7 9F A9 0A 0D 19 41 F0 6C 02 D4 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.
6C 47 14 96 C4 BB 4A 55 7B F4 3E 52 88 B7 9F A9 0A 0D 19 41 F0 6C 02 D4 F8 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.
6C 47 14 96 C4 BB 4A 55 7B F4 3E 52 88 B7 9F A9 0A 0D 19 41 F0 6C 02 D4 F8 04 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.
6C 47 14 96 C4 BB 4A 55 7B F4 3E 52 88 B7 9F A9 0A 0D 19 41 F0 6C 02 D4 F8 04 B5 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.
6C 47 14 96 C4 BB 4A 55 7B F4 3E 52 88 B7 9F A9 0A 0D 19 41 F0 6C 02 D4 F8 04 B5 D5 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.
6C 47 14 96 C4 BB 4A 55 7B F4 3E 52 88 B7 9F A9 0A 0D 19 41 F0 6C 02 D4 F8 04 B5 D5 66 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.
6C 47 14 96 C4 BB 4A 55 7B F4 3E 52 88 B7 9F A9 0A 0D 19 41 F0 6C 02 D4 F8 04 B5 D5 66 BA 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.
6C 47 14 96 C4 BB 4A 55 7B F4 3E 52 88 B7 9F A9 0A 0D 19 41 F0 6C 02 D4 F8 04 B5 D5 66 BA 90 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.
6C 47 14 96 C4 BB 4A 55 7B F4 3E 52 88 B7 9F A9 0A 0D 19 41 F0 6C 02 D4 F8 04 B5 D5 66 BA 90 60
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.
6C 47 14 96 C4 BB 4A 55 7B F4 3E 52 88 B7 9F A9 0A 0D 19 41 F0 6C 02 D4 F8 04 B5 D5 66 BA 90 60
67 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.
6C 47 14 96 C4 BB 4A 55 7B F4 3E 52 88 B7 9F A9 0A 0D 19 41 F0 6C 02 D4 F8 04 B5 D5 66 BA 90 60
67 5A 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.
6C 47 14 96 C4 BB 4A 55 7B F4 3E 52 88 B7 9F A9 0A 0D 19 41 F0 6C 02 D4 F8 04 B5 D5 66 BA 90 60
67 5A 3F 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.
6C 47 14 96 C4 BB 4A 55 7B F4 3E 52 88 B7 9F A9 0A 0D 19 41 F0 6C 02 D4 F8 04 B5 D5 66 BA 90 60
67 5A 3F 79 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.
6C 47 14 96 C4 BB 4A 55 7B F4 3E 52 88 B7 9F A9 0A 0D 19 41 F0 6C 02 D4 F8 04 B5 D5 66 BA 90 60
67 5A 3F 79 DD 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.
6C 47 14 96 C4 BB 4A 55 7B F4 3E 52 88 B7 9F A9 0A 0D 19 41 F0 6C 02 D4 F8 04 B5 D5 66 BA 90 60
67 5A 3F 79 DD 50 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.
6C 47 14 96 C4 BB 4A 55 7B F4 3E 52 88 B7 9F A9 0A 0D 19 41 F0 6C 02 D4 F8 04 B5 D5 66 BA 90 60
67 5A 3F 79 DD 50 12 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.
6C 47 14 96 C4 BB 4A 55 7B F4 3E 52 88 B7 9F A9 0A 0D 19 41 F0 6C 02 D4 F8 04 B5 D5 66 BA 90 60
7 5A 3F 79 DD 50 12 C6 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.
6C 47 14 96 C4 BB 4A 55 7B F4 3E 52 88 B7 9F A9 0A 0D 19 41 F0 6C 02 D4 F8 04 B5 D5 66 BA 90 60
67 5A 3F 79 DD 50 12 C6 17 29 2A 2B 2C 2D 2E 2F 30 31 32 33 34 35 36 37 38 39 3A 3B 3C 3D 3E 3F
42.
6C 47 14 96 C4 BB 4A 55 7B F4 3E 52 88 B7 9F A9 0A 0D 19 41 F0 6C 02 D4 F8 04 B5 D5 66 BA 90 60
67 5A 3F 79 DD 50 12 C6 17 06 2A 2B 2C 2D 2E 2F 30 31 32 33 34 35 36 37 38 39 3A 3B 3C 3D 3E 3F
43.
6C 47 14 96 C4 BB 4A 55 7B F4 3E 52 88 B7 9F A9 0A 0D 19 41 F0 6C 02 D4 F8 04 B5 D5 66 BA 90 60
67 5A 3F 79 DD 50 12 C6 17 06 A2 2B 2C 2D 2E 2F 30 31 32 33 34 35 36 37 38 39 3A 3B 3C 3D 3E 3F
44.
6C 47 14 96 C4 BB 4A 55 7B F4 3E 52 88 B7 9F A9 0A 0D 19 41 F0 6C 02 D4 F8 04 B5 D5 66 BA 90 60
67 5A 3F 79 DD 50 12 C6 17 06 A2 E1 2C 2D 2E 2F 30 31 32 33 34 35 36 37 38 39 3A 3B 3C 3D 3E 3F
45.
6C 47 14 96 C4 BB 4A 55 7B F4 3E 52 88 B7 9F A9 0A 0D 19 41 F0 6C 02 D4 F8 04 B5 D5 66 BA 90 60
67 5A 3F 79 DD 50 12 C6 17 06 A2 E1 2B 2D 2E 2F 30 31 32 33 34 35 36 37 38 39 3A 3B 3C 3D 3E 3F
46.
6C 47 14 96 C4 BB 4A 55 7B F4 3E 52 88 B7 9F A9 0A 0D 19 41 F0 6C 02 D4 F8 04 B5 D5 66 BA 90 60
67 5A 3F 79 DD 50 12 C6 17 06 A2 E1 2B 69 2E 2F 30 31 32 33 34 35 36 37 38 39 3A 3B 3C 3D 3E 3F

47.
6C 47 14 96 C4 BB 4A 55 7B F4 3E 52 88 B7 9F A9 0A 0D 19 41 F0 6C 02 D4 F8 04 B5 D5 66 BA 90 60
67 5A 3F 79 DD 50 12 C6 17 06 A2 E1 2B 69 FB 2F 30 31 32 33 34 35 36 37 38 39 3A 3B 3C 3D 3E 3F
48.
6C 47 14 96 C4 BB 4A 55 7B F4 3E 52 88 B7 9F A9 0A 0D 19 41 F0 6C 02 D4 F8 04 B5 D5 66 BA 90 60
67 5A 3F 79 DD 50 12 C6 17 06 A2 E1 2B 69 FB C7 30 31 32 33 34 35 36 37 38 39 3A 3B 3C 3D 3E 3F
49.
6C 47 14 96 C4 BB 4A 55 7B F4 3E 52 88 B7 9F A9 0A 0D 19 41 F0 6C 02 D4 F8 04 B5 D5 66 BA 90 60
67 5A 3F 79 DD 50 12 C6 17 06 A2 E1 2B 69 FB C7 3F 31 32 33 34 35 36 37 38 39 3A 3B 3C 3D 3E 3F
50.
6C 47 14 96 C4 BB 4A 55 7B F4 3E 52 88 B7 9F A9 0A 0D 19 41 F0 6C 02 D4 F8 04 B5 D5 66 BA 90 60
67 5A 3F 79 DD 50 12 C6 17 06 A2 E1 2B 69 FB C7 3F D9 32 33 34 35 36 37 38 39 3A 3B 3C 3D 3E 3F
51.
6C 47 14 96 C4 BB 4A 55 7B F4 3E 52 88 B7 9F A9 0A 0D 19 41 F0 6C 02 D4 F8 04 B5 D5 66 BA 90 60
67 5A 3F 79 DD 50 12 C6 17 06 A2 E1 2B 69 FB C7 3F D9 3E 33 34 35 36 37 38 39 3A 3B 3C 3D 3E 3F
52.
6C 47 14 96 C4 BB 4A 55 7B F4 3E 52 88 B7 9F A9 0A 0D 19 41 F0 6C 02 D4 F8 04 B5 D5 66 BA 90 60
67 5A 3F 79 DD 50 12 C6 17 06 A2 E1 2B 69 FB C7 3F D9 3E BC 34 35 36 37 38 39 3A 3B 3C 3D 3E 3F
53.
6C 47 14 96 C4 BB 4A 55 7B F4 3E 52 88 B7 9F A9 0A 0D 19 41 F0 6C 02 D4 F8 04 B5 D5 66 BA 90 60
67 5A 3F 79 DD 50 12 C6 17 06 A2 E1 2B 69 FB C7 3F D9 3E BC 14 35 36 37 38 39 3A 3B 3C 3D 3E 3F
54.
6C 47 14 96 C4 BB 4A 55 7B F4 3E 52 88 B7 9F A9 0A 0D 19 41 F0 6C 02 D4 F8 04 B5 D5 66 BA 90 60
67 5A 3F 79 DD 50 12 C6 17 06 A2 E1 2B 69 FB C7 3F D9 3E BC 14 28 36 37 38 39 3A 3B 3C 3D 3E 3F
55.
6C 47 14 96 C4 BB 4A 55 7B F4 3E 52 88 B7 9F A9 0A 0D 19 41 F0 6C 02 D4 F8 04 B5 D5 66 BA 90 60
67 5A 3F 79 DD 50 12 C6 17 06 A2 E1 2B 69 FB C7 3F D9 3E BC 14 28 03 37 38 39 3A 3B 3C 3D 3E 3F
56.
6C 47 14 96 C4 BB 4A 55 7B F4 3E 52 88 B7 9F A9 0A 0D 19 41 F0 6C 02 D4 F8 04 B5 D5 66 BA 90 60
67 5A 3F 79 DD 50 12 C6 17 06 A2 E1 2B 69 FB C7 3F D9 3E BC 14 28 03 76 38 39 3A 3B 3C 3D 3E 3F
57.
6C 47 14 96 C4 BB 4A 55 7B F4 3E 52 88 B7 9F A9 0A 0D 19 41 F0 6C 02 D4 F8 04 B5 D5 66 BA 90 60
67 5A 3F 79 DD 50 12 C6 17 06 A2 E1 2B 69 FB C7 3F D9 3E BC 14 28 03 76 83 39 3A 3B 3C 3D 3E 3F
58.
6C 47 14 96 C4 BB 4A 55 7B F4 3E 52 88 B7 9F A9 0A 0D 19 41 F0 6C 02 D4 F8 04 B5 D5 66 BA 90 60
67 5A 3F 79 DD 50 12 C6 17 06 A2 E1 2B 69 FB C7 3F D9 3E BC 14 28 03 76 83 3F 3A 3B 3C 3D 3E 3F
59.
6C 47 14 96 C4 BB 4A 55 7B F4 3E 52 88 B7 9F A9 0A 0D 19 41 F0 6C 02 D4 F8 04 B5 D5 66 BA 90 60
67 5A 3F 79 DD 50 12 C6 17 06 A2 E1 2B 69 FB C7 3F D9 3E BC 14 28 03 76 83 3F F8 3B 3C 3D 3E 3F
60.
6C 47 14 96 C4 BB 4A 55 7B F4 3E 52 88 B7 9F A9 0A 0D 19 41 F0 6C 02 D4 F8 04 B5 D5 66 BA 90 60
67 5A 3F 79 DD 50 12 C6 17 06 A2 E1 2B 69 FB C7 3F D9 3E BC 14 28 03 76 83 3F F8 C4 3C 3D 3E 3F
61.
6C 47 14 96 C4 BB 4A 55 7B F4 3E 52 88 B7 9F A9 0A 0D 19 41 F0 6C 02 D4 F8 04 B5 D5 66 BA 90 60
67 5A 3F 79 DD 50 12 C6 17 06 A2 E1 2B 69 FB C7 3F D9 3E BC 14 28 03 76 83 3F F8 C4 C9 3D 3E 3F
62.
6C 47 14 96 C4 BB 4A 55 7B F4 3E 52 88 B7 9F A9 0A 0D 19 41 F0 6C 02 D4 F8 04 B5 D5 66 BA 90 60
67 5A 3F 79 DD 50 12 C6 17 06 A2 E1 2B 69 FB C7 3F D9 3E BC 14 28 03 76 83 3F F8 C4 C9 2F 3E 3F
63.
6C 47 14 96 C4 BB 4A 55 7B F4 3E 52 88 B7 9F A9 0A 0D 19 41 F0 6C 02 D4 F8 04 B5 D5 66 BA 90 60
67 5A 3F 79 DD 50 12 C6 17 06 A2 E1 2B 69 FB C7 3F D9 3E BC 14 28 03 76 83 3F F8 C4 C9 2F 9C 3F
64.
6C 47 14 96 C4 BB 4A 55 7B F4 3E 52 88 B7 9F A9 0A 0D 19 41 F0 6C 02 D4 F8 04 B5 D5 66 BA 90 60
67 5A 3F 79 DD 50 12 C6 17 06 A2 E1 2B 69 FB C7 3F D9 3E BC 14 28 03 76 83 3F F8 C4 C9 2F 9C 47
65.
D2 47 14 96 C4 BB 4A 55 7B F4 3E 52 88 B7 9F A9 0A 0D 19 41 F0 6C 02 D4 F8 04 B5 D5 66 BA 90 60
67 5A 3F 79 DD 50 12 C6 17 06 A2 E1 2B 69 FB C7 3F D9 3E BC 14 28 03 76 83 3F F8 C4 C9 2F 9C 47

Second message digest:
D2 47 14 96 C4 BB 4A 55 7B F4 3E 52 88 B7 9F A9 0A 0D 19 41 F0 6C 02 D4 F8 04 B5 D5 66 BA 90 60
67 5A 3F 79 DD 50 12 C6 17 06 A2 E1 2B 69 FB C7 3F D9 3E BC 14 28 03 76 83 3F F8 C4 C9 2F 9C 47

Final digest:
0E 5F 98 DB D4 F6 BD 12 71 E9 77 84 49 B3 1C 29 DD F3 A9 DD 34 66 90 16 F5 C5 AC 9F 96 AE 4C DC FE 9B 83 DC 6F 57 2A AC 0C C6 2A 13 61 38 4C 48 2D 7B 36 E4 87 CF 57 75 7B D0 E2 C9 AC 1C 99 9A

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

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

Len = 0
Msg = 00
MD = 83FE3B19BE29E41CF2A18CC1CD8BEEF92419F6306509DEDB016E7961

Len = 1
Msg = 00
MD = 71204BF17BA5853B03FA3F70642F9C4C8C0A0ABB135BEF8671363381

Len = 2
Msg = C0
MD = 3C9A735863C47DC5907874662BC3FD6CE36C22B97C3A2B425F96405B

Len = 3
Msg = C0
MD = E6BFBFBC4869C359732CCB99161D162AADEE9868929D65FF92414274

Len = 4
Msg = 80
MD = FE6CE021BE14993850937C58F743689D97A69D91C8525A995891B124

Len = 5
Msg = 48
MD = 78BFEC9A25FBA98D62752A432D52C41A8AAE4619DFC120C0CEEC2A5B

Len = 6
Msg = 50
MD = 969433F7431E18E933D19299EA39DB595919CAE17254E0CFD3EABF0E


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

Len = 2048
Msg =
724627916C50338643E6996F07877EAFD96BDF01DA7E991D4155B9BE1295EA7D21C9391F4C4A41C75F77E5D273
89253393725F1427F57914B273AB862B9E31DABCE506E558720520D33352D119F699E784F9E548FF91BC35CA147
042128709820D69A8287EA3257857615EB0321270E94B84F446942765CE882B191FAEE7E1C87E0F0BD4E0CD8A9
27703524B559B769CA4ECE1F6DBF313FDCF67C572EC4185C1A88E86EC11B6454B371980020F19633B6B95BD280
E4FBCB0161E1A82470320CEC6ECFA25AC73D09F1536F286D3F9DACAFB2CD1D0CE72D64D197F5C7520B3CCB2FD
74EB72664BA93853EF41EABF52F015DD591500D018DD162815CC993595B195
MD = 2BF7955485587A9051A8905849E172FB6BCECDC6BC7647353CBE9497
Len = 2111
Msg =
919FE5E7F35F64A7487649E564771DBBF10AE204ECC2181312D1A79FB579297C94F0DB9EAAE9E009A4F02057AF2
C973C5DAFA7B60154371A5D2C8E992FB6429176F8424B1A866BC1D1BED00438E97FAB42040DCACDEF7CA9FC20
33059B8898BB40CCFB2634B051797BDF3B915C503EC81839AD01E0F4F2F871EFF2008D40011730BE7A47888E79
55A806876BE120CB0F3A139A3620154ECC6482A70F5629F6A9D3341BE6FBBF48E5AA0C53589A04F057DD44268A
FFCABF75ADFC549F73F454264D46A98CCA80E3000C7446853DD5B430C9344E87E3230555B09FB3E7E64B5AD398
9293AC0FEEC0E75F909696F028A5525D26DDEA5D2B2C813FB3613DFF38CE23209285CC77C60860
MD = 0A7F87D03DA97B536ECBFF09F8E09416651D2D503D2F01DFC312DD07
Len = 2174
Msg =
BD687B6D6684949FBD52A8196DF5D5927B403DEE88A47E4E4B52071BDDA6A6284A9EA1EB84950BA17A60277B0
FEA83C930E5619D5A6D232901B9D3A696662C7FD5F1349B494BC166C67B717C06D03E9FB05DB9EE292D4792F4
59E0ACC08369E3D14684CFF388C940F30738FB71D97EFEB51C7DB553CB85B6FC18429815EC71420822151BB8F5
135DD698EFE3D3118963EE194F94682DFA62EC9D3BCB5F826DA790779704DF2AC5C8A9FA2B50A42A87ED2FBAD
F1E1C8E55689531786A9858DE9E88009E56873FD2D431FCFC99B85574342DC7E78406678BDE94B9A06974DFF15
4EAC3BC7977AC7C123EBCDAC0641A69B792058BA373EDD1BA45E3339C2ABC032993B25F4E3BFA3D5FF620C621
D94C40F8
MD = B5F5A2CDED7D84E84A0A4761ADA12DFF6DAD82604434ABEEF0F52239
Len = 2237
Msg =
D13409007A6B3242CBAD4CE01D9AED77EFEF0A7725B96A30097EA092FA1E49A136DE03F3F348464C9BEA033216
F380440C7EC81E284738DCC640D485ED32F5D7DD1CF936C1677CBB3CDD8E0E001783FD5A3F388AE6EF7085FF9
A22FA722C7FCCF4CDC239B200D5D11884B565D01C84E4D563C6623C241C5AE0812CE8F9201BBADE48198378A3
E232EF3E10C03022620A266D0A346A6A22F202333A94D2CEF495DBA102B133B8237449C3350BF80EE51B6EE8A9
72CCFC3ED5FD7790444DA253922EEF6C611180F91DF1B6E58E843D318D94A958A017590B14D383C0F385F9CF25
```

14E8AE1EA749795E10F991E3FB744C6030EF6B02989E8EFFBF8E8BF31FC39B692C517C7C012ECBD0E0785BDEF48
01C4E036C98C6CD0C9328
MD = 1F060B043388B5CFE5779234B33337A1B9CE07F025E0753E02151DBE
Len = 2300
Msg =
68F891C11459B2E9B71774E2B8A2A5C3C9CC36072E3498498496F1C7901684F3E9DACF13A3F1BAE22140DEE525
3732E4D4196B534F675264B53D38659727797F0A18910CCB5B48FE2346C2E998B6537357AF8D15826FCB57BA80
4FE143E765F4680A0B28A9E3716A59ABC60EF253E357A4784FF1BE4680C82D797813CE50355D8FDB3C75936CC3
3E1717B99D9A8ADE9D0EA9172662B708EBCBC31C05064FE67B287C56D01C12411E9B890AD16238B36E192B15C
D86D26F4EFDE5B523D71656F5CEA6CA73BDC04FEB973D303BBAF4C0264761092E23220CEB8359FC91C1D918FB
3F32DBBA92DEAC1C71DA8BC4BE806803F6E7970FA64721C645EED4C2BED7EEFA2B720931FDBD6C67B83756B1C
E51C51F839C250AD900B9D49FE5188FC4A2B5D0
MD = 3532ACFFFB1824C1699CF18D4687891EB7BD564C2912B393690964F6
Len = 2363
Msg =
7D9222C58DC49F14BFD7198A9A1C338D17201C007822A91DCD262860364CA1DA8C0056033EB58E406E36D5A4F
6F7E9D98BE57126C9FE7676B58FDF0F9899432FF78DE2AB65C9000071EBA6967123F97BA3DC1F3825D3C8C5148
EAD7AEF0334F40CB0F6B982CB7C99CA39E1B4B2E3A3541683D1EC5560466F52175518390D38C7461C116DB2D5
6EF913784D2E8B20959BBD6F8F3282C597D94A1EDBFA8F25089E9D2E8DC465EAD90FA23E4388BD6BAFE226327
49B7AAEA53D5CBCF9678227ADC3F4109F1849AC2539B6F2B25B4D8EDAB41E8BFCFC337728DC48A8EA5119115F
C1B133300D68231C96A9D518F6DC3CA51581309C53F49510FE18F608A215069D41F2CFC84E53A9347FD723DFF9
D3F5006F7C0B18441A29BDEF7725920260B1613C6532A0A994B488E0
MD = 210E7FA4212CCEA41932C4CC7DC8729A5DB18EE9FEA25D068900B1EA
Len = 2426
Msg =
FC447A550FC565F964337521DBD6481FF6C4FEC25A2BC946230C0021570E75B0E3D50320AB24C4949CB4EA7ED6
D14D10E1EB9CB4116461A743D49F337597F12D09945285647B249A2AE3EBF69F1FC62A36532B2FC89ECED5B48A
C27A0E18AF8B0F023BE5C00FF0BF8C16F412B34D4AE9ECD2963583FA268ED439B4640FFCC57384EF066362E23D
2F0712F9658CB7B7F56F548C4A3C7DB51D8FF4430D14CE1042221254CAA4BF009B197E6F74B42067E95E42D6C8
F2D37AA5522F5594D61745BA28C8F302E007316282985730FBCB8BDAB0C5A3693BEEC32C0D57AD20D3394B7AC
72831FF5DDFC8208E09057AB9E9EE2FAC208E9FCB6D0B567C4DDED41ED286678DB3860B230C9A52C577867EC3
5A17EF902E258CD8314F36875D97543088679415FD0D7C2A9CB6CAEE76A2A1DC294700
MD = 5FD64AD0FA332260CF00137B86B145C499227284CF8BBDD7962E6DB5

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

Repeat = 16777216
Text = abcdefghbcdefghicdefghijdefghijkefghijklfghijklmghijklmnhijklmno
MD = F7671BACBC5ACA377225968E16C8FEF0A177FA94226C3930D6E88213

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

Seed =
6CD4C0C5CB2CA2A0F1D1AECEBAC03B52E64EA03D1A1654372936545B92BBC5484A59DB74BB60F9C40CEB1A5A
A35A6FAFE80349E14C253A4E8B1D77612DDD81ACE926AE8B0AF6E53176DBFFCC2A6B88C6BD765F939D3D178A9
BDE9EF3AA131C61E31C1E42CDFAF4B4DCDE579A37E150EFBEF5555B4C1CB40439D835A724E2FAE7

j = 0
MD = AA6468D5C2EB9E43806F67EDB493DF0E5E079B2FB71F6AAB61C43DCD

j = 1
MD = 877C7FDE7C8706D52FD00DD33F23695D20DDC67ACC64280DFDF27CEC

j = 2
MD = D03FD26C2D06FE5C4C38257811305A8C669213E91FEAB98E73F7BE3C

j = 3
MD = 5A89B6F050964F8225FCB8B5EDA9C72D7512E725E9810127EC6C9149

j = 4
MD = A062DB201CADC32B454CC14086F9B936435E16C0FE9FE8FA293E549C

j = 5
MD = BC27B75352EE7E01CB13181B65D594C69183A571E6279A7D56C99520

j = 6
MD = 75300DC3495067CD3FE66B4E311CB1575B0282ACE345D96E1C1218D3

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

Len = 0
Msg = 00
MD = 54F3F2ED3B4834468C80CC26F4553B9903962489D1485A2D10FF69177DFEDF09

Len = 1
Msg = 00
MD = 14F32E10073A82FA3A01BCDEE26E93F21620EDD035D72704565AB1B7A3B69D53

Len = 2
Msg = C0
MD = CBF63BB70663A55096D37532B3EFCA4007BC9D1C6985E242AA710B8140DFAA29

Len = 3
Msg = C0
MD = C9CB7416EC83F9C8E13A0AE31CE9D34DE88714CB1B6B2DDFBECFD3D70C9208C2

Len = 4
Msg = 80
MD = F1BC067CAE8206524167B53A1A5C7A8B96FE3B6DDE4EA258FE5F86089E6ED936

Len = 5
Msg = 48
MD = 72C7E18893CEBA631F8E314EDE37BA83355D466F011EF439C0F052A5AD72F8F3

Len = 6
Msg = 50
MD = C0B7146D904CFE90634F580C79EFADD2B1EB1B5E4583CFD5502EA48BDBC515C5

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

Len = 2048
Msg =
724627916C50338643E6996F07877EAFD96BDF01DA7E991D4155B9BE1295EA7D21C9391F4C4A41C75F77E5D273
89253393725F1427F57914B273AB862B9E31DABCE506E558720520D33352D119F699E784F9E548FF91BC35CA147
042128709820D69A8287EA3257857615EB0321270E94B84F446942765CE882B191FAEE7E1C87E0F0BD4E0CD8A9
27703524B559B769CA4ECE1F6DBF313FDCF67C572EC4185C1A88E86EC11B6454B371980020F19633B6B95BD280
E4FBCB0161E1A82470320CEC6ECFA25AC73D09F1536F286D3F9DACAFB2CD1D0CE72D64D197F5C7520B3CCB2FD
74EB72664BA93853EF41EABF52F015DD591500D018DD162815CC993595B195
MD = F339664821409A1E107E6E20BA1E214E32C8DFE9E0544621AC65C5F10E31B93A
Len = 2111
Msg =
919FE5E7F35F64A7487649E564771DBBF10AE204ECC2181312D1A79FB579297C94F0DB9EAAE9E009A4F02057AF2
C973C5DAFA7B60154371A5D2C8E992FB6429176F8424B1A866BC1D1BED00438E97FAB42040DCACDEF7CA9FC20
33059B8898BB40CCFB2634B051797BDF3B915C503EC81839AD01E0F4F2F871EFF2008D40011730BE7A47888E79
55A806876BE120CB0F3A139A3620154ECC6482A70F5629F6A9D3341BE6FBBF48E5AA0C53589A04F057DD44268A
FFCABF75ADFC549F73F454264D46A98CCA80E3000C7446853DD5B430C9344E87E3230555B09FB3E7E64B5AD398
9293AC0FEEC0E75F909696F028A5525D26DDEA5D2B2C813FB3613DFF38CE23209285CC77C60860
MD = 7B32B83036C8D7C19468B4E2E83166FD36D3429FA8AA24ED7737CF1F53923F83
Len = 2174
Msg =
BD687B6D6684949FBD52A8196DF5D5927B403DEE88A47E4E4B52071BDDA6A6284A9EA1EB84950BA17A60277B0
FEA83C930E5619D5A6D232901B9D3A696662C7FD5F1349B494BC166C67B717C06D03E9FB05DB9EE292D4792F4
59E0ACC08369E3D14684CFF388C940F30738FB71D97EFEB51C7DB553CB85B6FC18429815EC71420822151BB8F5
135DD698EFE3D3118963EE194F94682DFA62EC9D3BCB5F826DA790779704DF2AC5C8A9FA2B50A42A87ED2FBAD
F1E1C8E55689531786A9858DE9E88009E56873FD2D431FCFC99B85574342DC7E78406678BDE94B9A06974DFF15
4EAC3BC7977AC7C123EBCDAC0641A69B792058BA373EDD1BA45E3339C2ABC032993B25F4E3BFA3D5FF620C621
D94C40F8
MD = 2029BD997E1C81D06C83354620FF9F7F70181FD8862D778234F7EDFAE902EADC
Len = 2237
Msg =
D13409007A6B3242CBAD4CE01D9AED77EFEF0A7725B96A30097EA092FA1E49A136DE03F3F348464C9BEA033216
F380440C7EC81E284738DCC640D485ED32F5D7DD1CF936C1677CBB3CDD8E0E001783FD5A3F388AE6EF7085FF9
A22FA722C7FCCF4CDC239B200D5D11884B565D01C84E4D563C6623C241C5AE0812CE8F9201BBADE48198378A3
E232EF3E10C03022620A266D0A346A6A22F202333A94D2CEF495DBA102B133B8237449C3350BF80EE51B6EE8A9

72CCFC3ED5FD7790444DA253922EEF6C611180F91DF1B6E58E843D318D94A958A017590B14D383C0F385F9CF25
14E8AE1EA749795E10F991E3FB744C6030EF6B02989E8EFFBF8E8BF31FC39B692C517C7C012ECBD0E0785BDEF48
01C4E036C98C6CD0C9328
MD = E3CE11097071BBC60453EB6CDC4F830FB26E4614879C4AFCA5EFB47ABC732E23
Len = 2300
Msg =
68F891C11459B2E9B71774E2B8A2A5C3C9CC36072E3498498496F1C7901684F3E9DACF13A3F1BAE22140DEE525
3732E4D4196B534F675264B53D38659727797F0A18910CCB5B48FE2346C2E998B6537357AF8D15826FCB57BA80
4FE143E765F4680A0B28A9E3716A59ABC60EF253E357A4784FF1BE4680C82D797813CE50355D8FDB3C75936CC3
3E1717B99D9A8ADE9D0EA9172662B708EBCBC31C05064FE67B287C56D01C12411E9B890AD16238B36E192B15C
D86D26F4EFDE5B523D71656F5CEA6CA73BDC04FEB973D303BBAF4C0264761092E23220CEB8359FC91C1D918FB
3F32DBBA92DEAC1C71DA8BC4BE806803F6E7970FA64721C645EED4C2BED7EEFA2B720931FDBD6C67B83756B1C
E51C51F839C250AD900B9D49FE5188FC4A2B5D0
MD = 0549E30BF3277C5CCBE3EB9684A692B45D03D1FE7119DC2801EC85ADBD29B97C
Len = 2363
Msg =
7D9222C58DC49F14BFD7198A9A1C338D17201C007822A91DCD262860364CA1DA8C0056033EB58E406E36D5A4F
6F7E9D98BE57126C9FE7676B58FDF0F9899432FF78DE2AB65C9000071EBA6967123F97BA3DC1F3825D3C8C5148
EAD7AEF0334F40CB0F6B982CB7C99CA39E1B4B2E3A3541683D1EC5560466F52175518390D38C7461C116DB2D5
6EF913784D2E8B20959BBD6F8F3282C597D94A1EDBFA8F25089E9D2E8DC465EAD90FA23E4388BD6BAFE226327
49B7AAEA53D5CBCF9678227ADC3F4109F1849AC2539B6F2B25B4D8EDAB41E8BFCFC337728DC48A8EA5119115F
C1B133300D68231C96A9D518F6DC3CA51581309C53F49510FE18F608A215069D41F2CFC84E53A9347FD723DFF9
D3F5006F7C0B18441A29BDEF7725920260B1613C6532A0A994B488E0
MD = A3354DAFD4885EB10515D91A301A4DB6370F40A5F5F0C306CB75D6A8EEA31CC8
Len = 2426
Msg =
FC447A550FC565F964337521DBD6481FF6C4FEC25A2BC946230C0021570E75B0E3D50320AB24C4949CB4EA7ED6
D14D10E1EB9CB4116461A743D49F337597F12D09945285647B249A2AE3EBF69F1FC62A36532B2FC89ECED5B48A
C27A0E18AF8B0F023BE5C00FF0BF8C16F412B34D4AE9ECD2963583FA268ED439B4640FFCC57384EF066362E23D
2F0712F9658CB7B7F56F548C4A3C7DB51D8FF4430D14CE1042221254CAA4BF009B197E6F74B42067E95E42D6C8
F2D37AA5522F5594D61745BA28C8F302E007316282985730FBCB8BDAB0C5A3693BEEC32C0D57AD20D3394B7AC
72831FF5DDFC8208E09057AB9E9EE2FAC208E9FCB6D0B567C4DDED41ED286678DB3860B230C9A52C577867EC3
5A17EF902E258CD8314F36875D97543088679415FD0D7C2A9CB6CAEE76A2A1DC294700
MD = 73F04B2A0007DD2EFA6CD48627C34F353F0CAFF0B81B7BED8DC0D1FB1F3D7F41

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

Repeat = 16777216
Text = abcdefghbcdefghicdefghijdefghijkefghijklfghijklmghijklmnhijklmno
MD = 96C28B9279F8B4B9ED2E57293AF6028D8F729F55D36CDD9C6F1DFF8B56E7D9AA

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

Seed =
6CD4C0C5CB2CA2A0F1D1AECEBAC03B52E64EA03D1A1654372936545B92BBC5484A59DB74BB60F9C40CEB1A5A
A35A6FAFE80349E14C253A4E8B1D77612DDD81ACE926AE8B0AF6E53176DBFFCC2A6B88C6BD765F939D3D178A9
BDE9EF3AA131C61E31C1E42CDFAF4B4DCDE579A37E150EFBEF5555B4C1CB40439D835A724E2FAE7

j = 0
MD = 58541DFBADF85E717510DA7BD339D90C762B1C3B19AB5618A75CA8E390D30DB4

j = 1
MD = D25110216724919CD08E502EA7699B3A4C8F3DB299A20E9267395A093A863A7B

j = 2
MD = 13990EAFBB3B833EF4FF8FB5A4905248A496B24ADAAEAAA3ADDB41C7EED47058

j = 3
MD = 66382431E0490092832F6604D05C2A86B0FDB1737063187B5BFDE85F8A6C25B4

j = 4
MD = 1B0DFD6F631A1B5D2D44DB1DC448A9425F1F2B45DC166A33B4B03BEFADD564F0

j = 5
MD = B3D66ACB109A722619896AC720416D557C53EFFC0D1CBA892F164BEDE7E482B9

j = 6
MD = E33821C9F7F747566B5FC13A2863B07013AD5F5130BD8070D8B71D3AC0C0F7B0

ShortMsgKAT_384.txt

Algorithm Name: MCSSHA-8
Principal Submitter: Mikhail Maslennikov

Len = 0
Msg = 00
MD = F6A85903EBE5FCDB7F5CEF1E0A0D42F58776A8A755D7190CAEFD82E3679F8F46455068E790910168128A330B7F6D52F8

Len = 1
Msg = 00
MD = 17A5DC363FACEB0C0BE67672E2F464D32D0A8C5D7285329F6C9F2544642B86A16D2C2ADF84E0345E343413C8CAB944EF

Len = 2
Msg = C0
MD = 7D961BD70663A530B6B315D293AFCAC007DCBD7CA985E2C2AA510B8140FFAAC77ADEBED3D5FEAB5A1520EF8B1181C900

Len = 3
Msg = C0
MD = 33CB4051BBEC9EA7A0095DD7CF8954C769D7A4C573BDAFB301FF0C29BCA5EFFE86930FE172FFA6D86C8D5394DE164C09

Len = 4
Msg = 80
MD = 31E06176AD279944525911F6E422EC40C0139F2C4877CDAACB75EF66C5A7FB92660D503809E09EAB5975DD7AB862972F

Len = 5
Msg = 48
MD = 82FC359FDBA59C3C3F38C771F067F277B0E1EEDA7EBD377A8B5822E0A90AE3139455055BAB0AA78936435AEF65C31CC3

Len = 6
Msg = 50
MD = ED9D117789203D34E4C917D385E0D6BC9690FCC9FB9BBD749CDF9F8BFC4F7D146C3A2D481568236017F258330D28931E

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

Len = 2048
Msg = 724627916C50338643E6996F07877EAFD96BDF01DA7E991D4155B9BE1295EA7D21C9391F4C4A41C75F77E5D27389253393725F1427F57914B273AB862B9E31DABCE506E558720520D33352D119F699E784F9E548FF91BC35CA147042128709820D69A8287EA3257857615EB0321270E94B84F446942765CE882B191FAEE7E1C87E0F0BD4E0CD8A927703524B559B769CA4ECE1F6DBF313FDCF67C572EC4185C1A88E86EC11B6454B371980020F19633B6B95BD280E4FBCB0161E1A82470320CEC6ECFA25AC73D09F1536F286D3F9DACAFB2CD1D0CE72D64D197F5C7520B3CCB2FD74EB72664BA93853EF41EABF52F015DD591500D018DD162815CC993595B195
MD = DD1C8A43198B984F15211F5AD2E2B77A7F3B9E0D1FA4EDC1C1CA14E470802F36013F240989C46C2B50B3A3B4222C51EA
Len = 2111
Msg = 919FE5E7F35F64A7487649E564771DBBF10AE204ECC2181312D1A79FB579297C94F0DB9EAAE9E009A4F02057AF2C973C5DAFA7B60154371A5D2C8E992FB6429176F8424B1A866BC1D1BED00438E97FAB42040DCACDEF7CA9FC2033059B8898BB40CCFB2634B051797BDF3B915C503EC81839AD01E0F4F2F871EFF2008D40011730BE7A47888E7955A806876BE120CB0F3A139A3620154ECC6482A70F5629F6A9D3341BE6FBBF48E5AA0C53589A04F057DD44268AFFCABF75ADFC549F73F454264D46A98CCA80E3000C7446853DD5B430C9344E87E3230555B09FB3E7E64B5AD3989293AC0FEEC0E75F909696F028A5525D26DDEA5D2B2C813FB3613DFF38CE23209285CC77C60860
MD = 68AC02AEDAB06414825BF92BC4EB0C51F83A151ACD47FDD487375ABBF484AEDCC9C56B45E4AD333E2E8439CAEA507CAB
Len = 2174
Msg = BD687B6D6684949FBD52A8196DF5D5927B403DEE88A47E4E4B52071BDDA6A6284A9EA1EB84950BA17A60277B0

FEA83C930E5619D5A6D232901B9D3A696662C7FD5F1349B494BC166C67B717C06D03E9FB05DB9EE292D4792F4
59E0ACC08369E3D14684CFF388C940F30738FB71D97EFEB51C7DB553CB85B6FC18429815EC71420822151BB8F5
135DD698EFE3D3118963EE194F94682DFA62EC9D3BCB5F826DA790779704DF2AC5C8A9FA2B50A42A87ED2FBAD
F1E1C8E55689531786A9858DE9E88009E56873FD2D431FCFC99B85574342DC7E78406678BDE94B9A06974DFF15
4EAC3BC7977AC7C123EBCDAC0641A69B792058BA373EDD1BA45E3339C2ABC032993B25F4E3BFA3D5FF620C621
D94C40F8
MD = 3B5C8A1C37A6D4757DF9BA39B814CDD59DB21EB131DFEF5F05EA4492B05EE7FC5D06D6AF6C96450049296DC9B
395FEDF
Len = 2237
Msg = D13409007A6B3242CBAD4CE01D9AED77EFEF0A7725B96A30097EA092FA1E49A136DE03F3F348464C9BEA033216
F380440C7EC81E284738DCC640D485ED32F5D7DD1CF936C1677CBB3CDD8E0E001783FD5A3F388AE6EF7085FF9
A22FA722C7FCCF4CDC239B200D5D11884B565D01C84E4D563C6623C241C5AE0812CE8F9201BBADE48198378A3
E232EF3E10C03022620A266D0A346A6A22F202333A94D2CEF495DBA102B133B8237449C3350BF80EE51B6EE8A9
72CCFC3ED5FD7790444DA253922EEF6C611180F91DF1B6E58E843D318D94A958A017590B14D383C0F385F9CF25
14E8AE1EA749795E10F991E3FB744C6030EF6B02989E8EFFBF8E8BF31FC39B692C517C7C012ECBD0E0785BDEF48
01C4E036C98C6CD0C9328
MD = 33809F28C93CC1A84E2DE9A551283E02F96E5370C567004DEE1920801633E5FD20CE81E1C344FAE4204BFD5D60
12CF05
Len = 2300
Msg = 68F891C11459B2E9B71774E2B8A2A5C3C9CC36072E3498498496F1C7901684F3E9DACF13A3F1BAE22140DEE525
3732E4D4196B534F675264B53D38659727797F0A18910CCB5B48FE2346C2E998B6537357AF8D15826FCB57BA80
4FE143E765F4680A0B28A9E3716A59ABC60EF253E357A4784FF1BE4680C82D797813CE50355D8FDB3C75936CC3
3E1717B99D9A8ADE9D0EA9172662B708EBCBC31C05064FE67B287C56D01C12411E9B890AD16238B36E192B15C
D86D26F4EFDE5B523D71656F5CEA6CA73BDC04FEB973D303BBAF4C0264761092E23220CEB8359FC91C1D918FB
3F32DBBA92DEAC1C71DA8BC4BE806803F6E7970FA64721C645EED4C2BED7EEFA2B720931FDBD6C67B83756B1C
E51C51F839C250AD900B9D49FE5188FC4A2B5D0
MD = 2A327BD38AA0C053E618E9E04604D88AEA332D3A128261C51AB89E9BA974E56828A8A3FE2F784DE8D4330983B
F74CA30
Len = 2363
Msg = 7D9222C58DC49F14BFD7198A9A1C338D17201C007822A91DCD262860364CA1DA8C0056033EB58E406E36D5A4F
6F7E9D98BE57126C9FE7676B58FDF0F9899432FF78DE2AB65C9000071EBA6967123F97BA3DC1F3825D3C8C5148
EAD7AEF0334F40CB0F6B982CB7C99CA39E1B4B2E3A3541683D1EC5560466F52175518390D38C7461C116DB2D5
6EF913784D2E8B20959BBD6F8F3282C597D94A1EDBFA8F25089E9D2E8DC465EAD90FA23E4388BD6BAFE226327
49B7AAEA53D5CBCF9678227ADC3F4109F1849AC2539B6F2B25B4D8EDAB41E8BFCFC337728DC48A8EA5119115F
C1B133300D68231C96A9D518F6DC3CA51581309C53F49510FE18F608A215069D41F2CFC84E53A9347FD723DFF9
D3F5006F7C0B18441A29BDEF7725920260B1613C6532A0A994B488E0
MD = FD713FF216C5D8343EE489B83A3A86C0A11F1B9D6F15ED424A1A1095E742B6C834DC6F47B72FC75CE480106297
4A1054
Len = 2426
Msg = FC447A550FC565F964337521DBD6481FF6C4FEC25A2BC946230C0021570E75B0E3D50320AB24C4949CB4EA7ED6
D14D10E1EB9CB4116461A743D49F337597F12D09945285647B249A2AE3EBF69F1FC62A36532B2FC89ECED5B48A
C27A0E18AF8B0F023BE5C00FF0BF8C16F412B34D4AE9ECD2963583FA268ED439B4640FFCC57384EF066362E23D
2F0712F9658CB7B7F56F548C4A3C7DB51D8FF4430D14CE1042221254CAA4BF009B197E6F74B42067E95E42D6C8
F2D37AA5522F5594D61745BA28C8F302E00731628298573OFBCB8BDAB0C5A3693BEEC32C0D57AD20D3394B7AC
72831FF5DDFC8208E09057AB9E9EE2FAC208E9FCB6D0B567C4DDED41ED286678DB3860B230C9A52C577867EC3
5A17EF902E258CD8314F36875D97543088679415FD0D7C2A9CB6CAEE76A2A1DC294700
MD = 7E055A996BDF72414D8DF0789DB02897FFAC1AF09062823F3B8A00E28DBC807477F0BB2300DD2CF26203F54DBE
B36CFE

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

Repeat = 16777216
Text = abcdefghbcdefghicdefghijdefghijkefghijklfghijklmghijklmnhijklmno
MD = CE1B921E1FF3E6A143D30A087B6ECE08BD010E34336ABFA3091F90C7B57495653BB513C12333EA9538812E7B41
683452

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

Seed = 6CD4C0C5CB2CA2A0F1D1AECEBAC03B52E64EA03D1A1654372936545B92BBC5484A59DB74BB60F9C40CEB1A5A

A35A6FAFE80349E14C253A4E8B1D77612DDD81ACE926AE8B0AF6E53176DBFFCC2A6B88C6BD765F939D3D178A9
BDE9EF3AA131C61E31C1E42CDFAF4B4DCDE579A37E150EFBEF5555B4C1CB40439D835A724E2FAE7

j = 0
MD = 6DE43F531E46F83FD8D1427AFF147B720737FAFF8F7E6531C548E645C3B63836503EBCCD4163215B6C983CA86D
C3CA3C

j = 1
MD = 91E5F00409052E42EF77F1BEEBE21C3A35AE5429EBD7BB8D7252FACF2CFAAB1F13A8308CFD5C87F347AED8FCEA
FEEA0E

j = 2
MD = 34A0217D4910331140784772EB490EF7E6FFD2F28B00CC2DEBA4138229C71570501821503223 84CDD3844EC4D0
F4BBDD

j = 3
MD = 23C1255A787CDE2C15BD822C23133CEC152A2CD865D5E8AA5E66AD0B8F1F1E3527FF10F6782E0D22E0BA46B0A
987C6AD

j = 4
MD = EBE02E0A1F761B6DD3606791CF1748115F9AC11BAF3D464DD8E2AB7D03915B94D3D516ADAB6A08C4C7860D2B
6D0AC818

j = 5
MD = EB87E49099DA9180513D8F85B45748098ACA7AD00B76964AC4F239DAFE20F4B152B2EF7932E5936D09616A546E
180F13

j = 6
MD = C53AD847A93E049B72FE299A263C24BE55284BCA519D847DD35984A017C7CBEE1FED9A83CB1C0F4CEA916862A
A936DF3

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

Len = 0
Msg = 00
MD = 5C4358517B83BE5E9192DA3995FF415387D22734155936F8AFC62E74122B52949B1F524DAF5CE70A78383AEC16
971CDCA96164A3BC7D5CC8081A2D2C53134431

Len = 1
Msg = 00
MD = 0A336E10077A82BAFA017CDE222E93B21660AD507557E704D6DAF1F7E3769DB86669E6EA93415AB2A88E7BFE17
33EF86E5C0742855FF121286ECFC58F238C198

Len = 2
Msg = C0
MD = 8C8BAEF15897B8682901105315091D788E4D3CD6DC134200A31FCF3CDF3A3919522766721A67E682100E3942A8
D398AB34EC301AE3CBA5C08475DA8227C8E2CA

Len = 3
Msg = C0
MD = 9A40042A0FD6234D4E6ADA6CCBA98ADA8C615F8FF2055AA15E5CFDB4E5E42A45361D8F5AD8A4EE9E44AE1F36C
A462779679427109B853C3E4A27E7A687E33BE7

Len = 4
Msg = 80
MD = 46AF8377D60FC76A1AD647BECBFDF8A32F4BC8725E7561A4B861F8C4917970C0910272A943B8B4147DC95EB38B
0B447C43B79214EA556159429E96483F18D2D6

Len = 5
Msg = 48

MD =
B427DCBFA1856E672A50D416687BB26DC8805F053FCBF28451E2C7740E693CDF277EBF7EFD20442B3E31430210
36C32BC9264238764B3701FF6E09DE9AC2C5C0

Len = 6
Msg = 50
MD =
D670EB610F003F6C86CE554506DDE11F41B3E673BBFAAC3C7D935D1C671D9DF288F564187B415963BFA4D870A
A881F9E998B9B93C4CCD214869FFCB3D41DCB66

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

Len = 2048
Msg =
724627916C50338643E6996F07877EAFD96BDF01DA7E991D4155B9BE1295EA7D21C9391F4C4A41C75F77E5D273
89253393725F1427F57914B273AB862B9E31DABCE506E558720520D33352D119F699E784F9E548FF91BC35CA147
042128709820D69A8287EA3257857615EB0321270E94B84F446942765CE882B191FAEE7E1C87E0F0BD4E0CD8A9
27703524B559B769CA4ECE1F6DBF313FDCF67C572EC4185C1A88E86EC11B6454B371980020F19633B6B95BD280
E4FBCB0161E1A82470320CEC6ECFA25AC73D09F1536F286D3F9DACAFB2CD1D0CE72D64D197F5C7520B3CCB2FD
74EB72664BA93853EF41EABF52F015DD591500D018DD162815CC993595B195
MD =
ED4138E0C52BB1726CDB9A563E6B7E59025D2913056BA1ADB4632061706A8E7C80A0795A4E7C23ACD65A5128B
0FBF98DDCF975EE7CB4ACCD36E9D862A8A47685
Len = 2111
Msg =
919FE5E7F35F64A7487649E564771DBBF10AE204ECC2181312D1A79FB579297C94F0DB9EAAE9E009A4F02057AF2
C973C5DAFA7B60154371A5D2C8E992FB6429176F8424B1A866BC1D1BED00438E97FAB42040DCACDEF7CA9FC20
33059B8898BB40CCFB2634B051797BDF3B915C503EC81839AD01E0F4F2F871EFF2008D40011730BE7A47888E79
55A806876BE120CB0F3A139A3620154ECC6482A70F5629F6A9D3341BE6FBBF48E5AA0C53589A04F057DD44268A
FFCABF75ADFC549F73F454264D46A98CCA80E3000C7446853DD5B430C9344E87E3230555B09FB3E7E64B5AD398
9293AC0FEEC0E75F909696F028A5525D26DDEA5D2B2C813FB3613DFF38CE23209285CC77C60860
MD =
7060A7FFDF85DAA62377F53E681432D89E3587289E0EBE75128EE24146762D45BFE6448FB54233A57B06DBDB59
94752BD4CDCE877B3AF95D06D87C2A1D894130
Len = 2174
Msg =
BD687B6D6684949FBD52A8196DF5D5927B403DEE88A47E4E4B52071BDDA6A6284A9EA1EB84950BA17A60277B0
FEA83C930E5619D5A6D232901B9D3A696662C7FD5F1349B494BC166C67B717C06D03E9FB05DB9EE292D4792F4
59E0ACC08369E3D14684CFF388C940F30738FB71D97EFEB51C7DB553CB85B6FC18429815EC71420822151BB8F5
135DD698EFE3D3118963EE194F94682DFA62EC9D3BCB5F826DA790779704DF2AC5C8A9FA2B50A42A87ED2FBAD
F1E1C8E55689531786A9858DE9E88009E56873FD2D431FCFC99B85574342DC7E78406678BDE94B9A06974DFF15
4EAC3BC7977AC7C123EBCDAC0641A69B792058BA373EDD1BA45E3339C2ABC032993B25F4E3BFA3D5FF620C621
D94C40F8
MD =
FE98ED43485C4927FD48AFB4D7DC78E34CAC450BB0A6153B772484C7A2E0682CADCE604A4B5E42EFBC64DBB24
FAB8FEA93A666119F167E2B1B6E23C31488062E
Len = 2237
Msg =
D13409007A6B3242CBAD4CE01D9AED77EFEF0A7725B96A30097EA092FA1E49A136DE03F3F348464C9BEA033216
F380440C7EC81E284738DCC640D485ED32F5D7DD1CF936C1677CBB3CDD8E0E001783FD5A3F388AE6EF7085FF9
A22FA722C7FCCF4CDC239B200D5D11884B565D01C84E4D563C6623C241C5AE0812CE8F9201BBADE48198378A3
E232EF3E10C03022620A266D0A346A6A22F202333A94D2CEF495DBA102B133B8237449C3350BF80EE51B6EE8A9
72CCFC3ED5FD7790444DA253922EEF6C611180F91DF1B6E58E843D318D94A958A017590B14D383C0F385F9CF25
14E8AE1EA749795E10F991E3FB744C6030EF6B02989E8EFFBF8E8BF31FC39B692C517C7C012ECBD0E0785BDEF48
01C4E036C98C6CD0C9328
MD =
9077C566E83199770F24487CBA6893300666140B46A2D64CB4B16A5515A43E9D2CB3FB3EE6AA32CD879360C8E8
E291BE25A40BA11B691854DF5202560F2B8571
Len = 2300
Msg =
68F891C11459B2E9B71774E2B8A2A5C3C9CC36072E3498498496F1C7901684F3E9DACF13A3F1BAE22140DEE525
3732E4D4196B534F675264B53D38659727797F0A18910CCB5B48FE2346C2E998B6537357AF8D15826FCB57BA80
4FE143E765F4680A0B28A9E3716A59ABC60EF253E357A4784FF1BE4680C82D797813CE50355D8FDB3C75936CC3
3E1717B99D9A8ADE9D0EA9172662B708EBCBC31C05064FE67B287C56D01C12411E9B890AD16238B36E192B15C
D86D26F4EFDE5B523D71656F5CEA6CA73BDC04FEB973D303BBAF4C0264761092E23220CEB8359FC91C1D918FB
3F32DBBA92DEAC1C71DA8BC4BE806803F6E7970FA64721C645EED4C2BED7EEFA2B720931FDBD6C67B83756B1C
E51C51F839C250AD900B9D49FE5188FC4A2B5D0
MD =
918E2430C2CA5FB7B0124EE2E28766564FC74782AE623B557D3FD24A6A08E9F84E1F5BBC283DC3C719E7C0FC8A
ED30E37D98CEDD9E99A7BC6F8FF754B2729716
Len = 2363

Msg =
7D9222C58DC49F14BFD7198A9A1C338D17201C007822A91DCD262860364CA1DA8C0056033EB58E406E36D5A4F
6F7E9D98BE57126C9FE7676B58FDF0F9899432FF78DE2AB65C9000071EBA6967123F97BA3DC1F3825D3C8C5148
EAD7AEF0334F40CB0F6B982CB7C99CA39E1B4B2E3A3541683D1EC5560466F52175518390D38C7461C116DB2D5
6EF913784D2E8B20959BBD6F8F3282C597D94A1EDBFA8F25089E9D2E8DC465EAD90FA23E4388BD6BAFE226327
49B7AAEA53D5CBCF9678227ADC3F4109F1849AC2539B6F2B25B4D8EDAB41E8BFCFC337728DC48A8EA5119115F
C1B133300D68231C96A9D518F6DC3CA51581309C53F49510FE18F608A215069D41F2CFC84E53A9347FD723DFF9
D3F5006F7C0B18441A29BDEF7725920260B1613C6532A0A994B488E0
MD =
BCCFDD080B80FEE5984A0B65EFA5DF407BF3ADBF3110B144573785618F1C10B03DE48BAC418CA3EE028C0F0514
C8E305C82F17380AA2F148A4A30547E3E0FE5D
Len = 2426
Msg =
FC447A550FC565F964337521DBD6481FF6C4FEC25A2BC946230C0021570E75B0E3D50320AB24C4949CB4EA7ED6
D14D10E1EB9CB4116461A743D49F337597F12D09945285647B249A2AE3EBF69F1FC62A36532B2FC89ECED5B48A
C27A0E18AF8B0F023BE5C00FF0BF8C16F412B34D4AE9ECD2963583FA268ED439B4640FFCC57384EF066362E23D
2F0712F9658CB7B7F56F548C4A3C7DB51D8FF4430D14CE1042221254CAA4BF009B197E6F74B42067E95E42D6C8
F2D37AA5522F5594D61745BA28C8F302E007316282985730FBCB8BDAB0C5A3693BEEC32C0D57AD20D3394B7AC
72831FF5DDFC8208E09057AB9E9EE2FAC208E9FCB6D0B567C4DDED41ED286678DB3860B230C9A52C577867EC3
5A17EF902E258CD8314F36875D97543088679415FD0D7C2A9CB6CAEE76A2A1DC294700
MD =
E9B2CDFF2C5002D84FC6E838D11DA1325AEDA3C73B40B24DB1CD41233131247AE983491000FCB82DA2DF492D
4888F2A2635B519FD54BCC5B300EBA562BD3AFC9

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

Repeat = 16777216
Text = abcdefghbcdefghicdefghijdefghijkefghijklfghijklmghijklmnhijklmno
MD =
ED4C83DD82F27EE42F8745EC5A2670F2E4CF28BC0618DA1ABF5D94200FAC1DC575CB45C398D216DE9EA9E988B
1E40529860997D6B48A7D5C4AF946B0981973C1

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

Seed =
6CD4C0C5CB2CA2A0F1D1AECEBAC03B52E64EA03D1A1654372936545B92BBC5484A59DB74BB60F9C40CEB1A5A
A35A6FAFE80349E14C253A4E8B1D77612DDD81ACE926AE8B0AF6E53176DBFFCC2A6B88C6BD765F939D3D178A9
BDE9EF3AA131C61E31C1E42CDFAF4B4DCDE579A37E150EFBEF5555B4C1CB40439D835A724E2FAE7

j = 0
MD =
D940D848902F88510909F470648D74C580D4A413BF98A343C2AE394AFBCD485CC9745D532A620F44E0257F82E0
87FA933BECE894DFF3A4FDEE9CC6298C21CBF9

j = 1
MD =
C2FE025B326CE0AB8B876B5712B8B87E870BA739F147F8EC6EBEB7D501228725CED1DECEC37AED3CDB2663608
2DFECA60839DEB15FB50F481485C5E69500706A

j = 2
MD =
38B1812C995057079AC48DAA0C3CE17BCA72CE2B5A808872DE34BE1E81710F96B415B7E0D1654996FC6D65B7D
1EBD1237A72D7D9F784E3E37E4D7197B75C28D9

j = 3
MD =
382C6FD7D58A2AB8FF13F982915E24A00BC94013FB25A91C680C6027DCECB6E09B36198588F82517D832FA580D
9DA803E6704C08F38A2AAA4C0DEC916DEA6D2B

j = 4
MD =
A69DF80D245E1D6F2585EF69122153A7EC958C2DB29B80111112278116A8E406D66C0E7816F82A25B354E21EDD
2AB733421E406EB37BB5A7C3DC334D06DA3C72

j = 5

MD =
4DA3C8EFCF6CE26D7D96524D24E3FA1B26FBDC825A9F4349EA5C1248D8C76EDD1357B295AF45617C64E321AF1
FEFCC6D953F678BBFFDE929DDB31A43F93528F7

j = 6
MD =
CFABEA9F380310D9A9A640290DE7B3746DE5BF0E4877C8B30FEED082CA481E7578C2EEFDDA8922436095BC7B0
0DD5AC30D12A5394C83D77EF05E7347D10BFEC9