Algorithm: **MCSSHA-6**
Principal submitter: **Mikhail Maslennikov**

Revision: June 08, 2009

SECURE HASH ALGORITHM MCSSHA-6

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 Creating input sequence for stage 1. 9
7.2 Calculating SR state for stage 1. 9
7.3 Creating input sequence for stage 2. 9
7.4 Calculating SR state for stage 2. 10
7.5 Creating input sequence for stage 3. 10
7.6 Calculating SR state for stage 3. 10
8. PARAMETERS OF ALGORITHM MCSSHA-6 FOR DIFFERENT HASH LENGTH 10
9. ESTIMATED COMPUTATIONAL EFFICIENCY AND MEMORY REQUIREMENTS 11
9.1 Memory Requirement 11
9.2 Computation Efficiency 11
10. Appendix A. Calculating hash examples. 14
10.1 Pre-hash computation for hash bit length 224 and 256, delay=3. 14

10.2 Pre-hash computation for hash bit length 384 and 512, delay=3. 15
10.3 Final hash computation for hash bit length 224. 16
10.4 Final hash computation for hash bit length 256. 20
10.5 Final hash computation for hash bit length 384. 24
10.6 Final hash computation for hash bit length 512. 34
11. Appendix B. CAT and MCT tests (delay=3).....45

1. INTRODUCTION

This document specifies secure hash algorithm MCSSHA-6. 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-6 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-6 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-6 algorithm in many respects is similar to previous algorithm MCSSHA-3 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.

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 224, 256, 384 or 512.

Hash byte length (H) Length (in bytes) of the message digest. It may be 28, 32, 48 or 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-6 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. $r = l - 8L$.

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-6 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: $p= (p_4+1)(\text{mod } N)$.
x	Input byte for step.

4. FUNCTIONS AND CONSTANTS

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

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

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 during preprocessing and pre-hash computation doesn't depended from hash length.

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-6 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-6 can't be used as hash function, because in this cases it's possible to find collisions!

7. FINAL HASH COMPUTATION

Final hash computation consist from three stages.

7.1 Creating input sequence for stage 1.

Let's $b_1,b_2,...,b_r$ – remain bits from message M, $a_1,a_2,...,a_n$ – n bits from SR state after pre-hash computation, where n = 8*N. Input sequence Z in bits will be as follow:

$Z = b_1,b_2,...,b_r, a_1,a_2,...,a_{n-r}$

The length in bits of the input sequence is exactly n bits, in bytes – exactly N bytes.

If remain bits absent, then

$Z = a_1,a_2,...,a_n$.

7.2 Calculating SR state for stage 1.

Lets $Z = z_1,z_2,...,z_N$ – input sequence in bytes. Calculating final SR state consist from N steps and for all stages in final hash computation SR length is H – hash length in bytes. For each step i MCSSHA algorithm perform SR step with input byte z_i. Initial SR state is 0,1,2,...,H-1, initial SR points:

$p_1 = 0$;
$p_2 = 1$;
$p_3 = H-4$;
$p_4 = H-1$.

7.3 Creating input sequence for stage 2.

Let's h = 8*H – hash length in bits, $a_{n-r+1},a_{n-r+2},...,a_n$ – remain bits from sequence $a_1,a_2,...,a_n$ after stage 1 and $C'_1,C'_2,...,C'_H$ – H bytes from SR state after stage 1. Let's $C_1,C_2,...,C_H$ – reversed sequence $C'_1,C'_2,...,C'_H$, i.e. $C_1 = C'_H$, $C_2 = C'_{H-1}$, ..., $C_H = C'_1$. Let's $c_1,c_2,...,c_h$ – sequence $C_1,C_2,...,C_H$ in bits. Input sequence Z in bits will be as follow:

$Z = a_{n-r+1},a_{n-r+2},...,a_n, c_1,c_2,...,c_{h-r}$

The length in bits of the input sequence is exactly h bits, in bytes – exactly H bytes.

If remain bits absent, then

$Z = c_1,c_2,...,c_h$

7.4 Calculating SR state for stage 2.

Lets $Z = z_1,z_2,...,z_H$ – input sequence in bytes. Calculating SR state consist from H steps. For each step i MCSSHA algorithm perform SR step with input byte z_i. Starting SR state and SR points are SR state and SR points from stage 1, i.e. stage 2 continue stage 1, change input sequence only.

7.5 Creating input sequence for stage 3.

Let's $c_{h-r+1},c_{h-r+2},...,c_h$ – remain bits from sequence $c_1,c_2,...,c_h$ after stage 2. Input sequence Z in bits will be as follow:

$Z = c_{h-r+1},c_{h-r+2},...,c_h, c_1,c_2,...,c_{h-r}$

The length in bits of the input sequence is exactly h bits, in bytes – exactly H bytes.

If remain bits absent, then

$Z = c_1,c_2,...,c_h$

i.e. input sequence for stage 3 will be same like for stage 2.

7.6 Calculating SR state for stage 3.

Same like for stage 2. Calculating SR state consist from H steps. Starting SR state and SR points are SR state and SR points from stage 2, i.e. stage 3 continue stage 2.

SR state after stage 3 is message digest.

8. PARAMETERS OF ALGORITHM MCSSHA-6 FOR DIFFERENT HASH LENGTH

Hash length in bits (h)	SR length in bytes for pre-hash computation (N)	SR length in bytes for final hash computation (H)
224	64	28
256	64	32
384	128	48
512	128	64

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).

32-bits OS
MS Windows Vista OS, 32-bits, Genuine Intel Core 2 CPU T2500 @ 2.00 GHz 2.00 GHz.

Algorithm	Hash length (in bits)	Text length (in bytes)	Number of tests	Time (sec)
SHA-224	224	1	1000000	1,777
MCSSHA-3	224	1	1000000	2,072
MCSSHA-4 (delay=2)	224	1	1000000	1,766
MCSSHA-4 (delay=3)	224	1	1000000	1,796
MCSSHA-6	224	1	1000000	1,756
Skein	224	1	1000000	2,427
MD6	224	1	1000000	23,332
Essence	224	1	1000000	9,754
Keccak	224	1	1000000	5,164
Groestl	224	1	1000000	9,868
SHAMATA	224	1	1000000	3,768
Blake	224	1	1000000	2,557
Sarmal	224	1	1000000	1,701
Waterfall	224	1	1000000	6,807
Boole	224	1	1000000	4,808

SHA-224	224	100	1000000	3,474
MCSSHA-3	224	100	1000000	5,329
MCSSHA-4 (delay=2)	224	100	1000000	3,91
MCSSHA-4 (delay=3)	224	100	1000000	4,61
MCSSHA-6	224	100	1000000	4,616
Skein	224	100	1000000	5,772
MD6	224	100	1000000	23,552
Essence	224	100	1000000	18,916
Keccak	224	100	1000000	5,34
Groestl	224	100	1000000	13,171
SHAMATA	224	100	1000000	4,554
Blake	224	100	1000000	4,798
Sarmal	224	100	1000000	1,761
Waterfall	224	100	1000000	10,318
Boole	224	100	1000000	6,941
SHA-224	224	100000	1000	2,688
MCSSHA-3	224	100000	1000	3,392
MCSSHA-4 (delay=2)	224	100000	1000	2,285
MCSSHA-4 (delay=3)	224	100000	1000	3,034
MCSSHA-6	224	100000	1000	2,945
Skein	224	100000	1000	3,488
MD6	224	100000	1000	5,727
Essence	224	100000	1000	9,829
Keccak	224	100000	1000	4,002
Groestl	224	100000	1000	5,322
SHAMATA	224	100000	1000	0,902
Blake	224	100000	1000	3,612
Sarmal	224	100000	1000	1,202
Waterfall	224	100000	1000	3,007
Boole	224	100000	1000	2,245
SHA-512	512	1	1000000	6,539
MCSSHA-3	512	1	1000000	3,688
MCSSHA-4 (delay=2)	512	1	1000000	2,856
MCSSHA-4 (delay=3)	512	1	1000000	2,989
MCSSHA-6	512	1	1000000	2,889
Skein	512	1	1000000	4,966
MD6	512	1	1000000	39,144
Essence	512	1	1000000	36,385
Keccak	512	1	1000000	5,201
Groestl	512	1	1000000	14,681
SHAMATA	512	1	1000000	5,115
Blake	512	1	1000000	6,341
Sarmal	512	1	1000000	2,095
Waterfall	512	1	1000000	6,951
Boole	512	1	1000000	5,39

SHA-512	512	100	1000000	6,521
MCSSHA-3	512	100	1000000	6,526
MCSSHA-4 (delay=2)	512	100	1000000	5,05
MCSSHA-4 (delay=3)	512	100	1000000	5,876
MCSSHA-6	512	100	1000000	5,79
Skein	512	100	1000000	7,326
MD6	512	100	1000000	39,27
Essence	512	100	1000000	48,099
Keccak	512	100	1000000	11,593
Groestl	512	100	1000000	14,868
SHAMATA	512	100	1000000	5,96
Blake	512	100	1000000	6,322
Sarmal	512	100	1000000	2,035
Waterfall	512	100	1000000	10,493
Boole	512	100	1000000	7,411
SHA-512	512	100000	1000	4,844
MCSSHA-3	512	100000	1000	2,965
MCSSHA-4 (delay=2)	512	100000	1000	2,298
MCSSHA-4 (delay=3)	512	100000	1000	3,089
MCSSHA-6	512	100000	1000	2,909
Skein	512	100000	1000	3,659
MD6	512	100000	1000	9,649
Essence	512	100000	1000	18,502
Keccak	512	100000	1000	7,738
Groestl	512	100000	1000	6,421
SHAMATA	512	100000	1000	1,012
Blake	512	100000	1000	4,886
Sarmal	512	100000	1000	1,475
Waterfall	512	100000	1000	3,042
Boole	512	100000	1000	2,219

10. Appendix A. Calculating hash examples.

In all this examples message *M* be the 24-bit (l = 24) 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.

Stage 1.

This is SR states for steps in final hash computation. 0 – initial SR state. SR length is 28. Input sequence (from pre-hash computations), 64 bytes:

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

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 for stage 1. Total 64 steps.

1.
2F 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.
2F 64 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.
2F 64 C8 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.
2F 64 C8 66 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.
2F 64 C8 66 9D 05 06 07 08 09 0A 0B 0C 0D 0E 0F 10 11 12 13 14 15 16 17 18 19 1A 1B
6.
2F 64 C8 66 9D ED 06 07 08 09 0A 0B 0C 0D 0E 0F 10 11 12 13 14 15 16 17 18 19 1A 1B
7.
2F 64 C8 66 9D ED C2 07 08 09 0A 0B 0C 0D 0E 0F 10 11 12 13 14 15 16 17 18 19 1A 1B
8.
2F 64 C8 66 9D ED C2 CF 08 09 0A 0B 0C 0D 0E 0F 10 11 12 13 14 15 16 17 18 19 1A 1B
9.
2F 64 C8 66 9D ED C2 CF ED 09 0A 0B 0C 0D 0E 0F 10 11 12 13 14 15 16 17 18 19 1A 1B
10.
2F 64 C8 66 9D ED C2 CF ED E4 0A 0B 0C 0D 0E 0F 10 11 12 13 14 15 16 17 18 19 1A 1B
11.
2F 64 C8 66 9D ED C2 CF ED E4 85 0B 0C 0D 0E 0F 10 11 12 13 14 15 16 17 18 19 1A 1B
12.
2F 64 C8 66 9D ED C2 CF ED E4 85 62 0C 0D 0E 0F 10 11 12 13 14 15 16 17 18 19 1A 1B
13.
2F 64 C8 66 9D ED C2 CF ED E4 85 62 E2 0D 0E 0F 10 11 12 13 14 15 16 17 18 19 1A 1B

14.
2F 64 C8 66 9D ED C2 CF ED E4 85 62 E2 BF 0E 0F 10 11 12 13 14 15 16 17 18 19 1A 1B
15.
2F 64 C8 66 9D ED C2 CF ED E4 85 62 E2 BF 5A 0F 10 11 12 13 14 15 16 17 18 19 1A 1B
16.
2F 64 C8 66 9D ED C2 CF ED E4 85 62 E2 BF 5A 13 10 11 12 13 14 15 16 17 18 19 1A 1B
17.
2F 64 C8 66 9D ED C2 CF ED E4 85 62 E2 BF 5A 13 11 11 12 13 14 15 16 17 18 19 1A 1B
18.
2F 64 C8 66 9D ED C2 CF ED E4 85 62 E2 BF 5A 13 11 61 12 13 14 15 16 17 18 19 1A 1B
19.
2F 64 C8 66 9D ED C2 CF ED E4 85 62 E2 BF 5A 13 11 61 A5 13 14 15 16 17 18 19 1A 1B
20.
2F 64 C8 66 9D ED C2 CF ED E4 85 62 E2 BF 5A 13 11 61 A5 81 14 15 16 17 18 19 1A 1B
21.
2F 64 C8 66 9D ED C2 CF ED E4 85 62 E2 BF 5A 13 11 61 A5 81 F1 15 16 17 18 19 1A 1B
22.
2F 64 C8 66 9D ED C2 CF ED E4 85 62 E2 BF 5A 13 11 61 A5 81 F1 D8 16 17 18 19 1A 1B
23.
2F 64 C8 66 9D ED C2 CF ED E4 85 62 E2 BF 5A 13 11 61 A5 81 F1 D8 93 17 18 19 1A 1B
24.
2F 64 C8 66 9D ED C2 CF ED E4 85 62 E2 BF 5A 13 11 61 A5 81 F1 D8 93 B3 18 19 1A 1B
25.
2F 64 C8 66 9D ED C2 CF ED E4 85 62 E2 BF 5A 13 11 61 A5 81 F1 D8 93 B3 C2 19 1A 1B
26.
2F 64 C8 66 9D ED C2 CF ED E4 85 62 E2 BF 5A 13 11 61 A5 81 F1 D8 93 B3 C2 FF 1A 1B
27.
2F 64 C8 66 9D ED C2 CF ED E4 85 62 E2 BF 5A 13 11 61 A5 81 F1 D8 93 B3 C2 FF E1 1B
28.
2F 64 C8 66 9D ED C2 CF ED E4 85 62 E2 BF 5A 13 11 61 A5 81 F1 D8 93 B3 C2 FF E1 09
29.
3F 64 C8 66 9D ED C2 CF ED E4 85 62 E2 BF 5A 13 11 61 A5 81 F1 D8 93 B3 C2 FF E1 09
30.
3F 32 C8 66 9D ED C2 CF ED E4 85 62 E2 BF 5A 13 11 61 A5 81 F1 D8 93 B3 C2 FF E1 09
31.
3F 32 F7 66 9D ED C2 CF ED E4 85 62 E2 BF 5A 13 11 61 A5 81 F1 D8 93 B3 C2 FF E1 09
32.
3F 32 F7 FF 9D ED C2 CF ED E4 85 62 E2 BF 5A 13 11 61 A5 81 F1 D8 93 B3 C2 FF E1 09
33.
3F 32 F7 FF 92 ED C2 CF ED E4 85 62 E2 BF 5A 13 11 61 A5 81 F1 D8 93 B3 C2 FF E1 09
34.
3F 32 F7 FF 92 CD C2 CF ED E4 85 62 E2 BF 5A 13 11 61 A5 81 F1 D8 93 B3 C2 FF E1 09
35.
3F 32 F7 FF 92 CD 1C CF ED E4 85 62 E2 BF 5A 13 11 61 A5 81 F1 D8 93 B3 C2 FF E1 09
36.
3F 32 F7 FF 92 CD 1C 82 ED E4 85 62 E2 BF 5A 13 11 61 A5 81 F1 D8 93 B3 C2 FF E1 09
37.
3F 32 F7 FF 92 CD 1C 82 42 E4 85 62 E2 BF 5A 13 11 61 A5 81 F1 D8 93 B3 C2 FF E1 09
38.
3F 32 F7 FF 92 CD 1C 82 42 04 85 62 E2 BF 5A 13 11 61 A5 81 F1 D8 93 B3 C2 FF E1 09
39.
3F 32 F7 FF 92 CD 1C 82 42 04 95 62 E2 BF 5A 13 11 61 A5 81 F1 D8 93 B3 C2 FF E1 09
40.
3F 32 F7 FF 92 CD 1C 82 42 04 95 6E E2 BF 5A 13 11 61 A5 81 F1 D8 93 B3 C2 FF E1 09
41.
3F 32 F7 FF 92 CD 1C 82 42 04 95 6E 2E BF 5A 13 11 61 A5 81 F1 D8 93 B3 C2 FF E1 09
42.
3F 32 F7 FF 92 CD 1C 82 42 04 95 6E 2E EC 5A 13 11 61 A5 81 F1 D8 93 B3 C2 FF E1 09
43.
3F 32 F7 FF 92 CD 1C 82 42 04 95 6E 2E EC A3 13 11 61 A5 81 F1 D8 93 B3 C2 FF E1 09
44.
3F 32 F7 FF 92 CD 1C 82 42 04 95 6E 2E EC A3 5C 11 61 A5 81 F1 D8 93 B3 C2 FF E1 09
45.
3F 32 F7 FF 92 CD 1C 82 42 04 95 6E 2E EC A3 5C 61 61 A5 81 F1 D8 93 B3 C2 FF E1 09
46.
3F 32 F7 FF 92 CD 1C 82 42 04 95 6E 2E EC A3 5C 61 82 A5 81 F1 D8 93 B3 C2 FF E1 09
47.
3F 32 F7 FF 92 CD 1C 82 42 04 95 6E 2E EC A3 5C 61 82 E3 81 F1 D8 93 B3 C2 FF E1 09
48.
3F 32 F7 FF 92 CD 1C 82 42 04 95 6E 2E EC A3 5C 61 82 E3 2C F1 D8 93 B3 C2 FF E1 09
49.
3F 32 F7 FF 92 CD 1C 82 42 04 95 6E 2E EC A3 5C 61 82 E3 2C A5 D8 93 B3 C2 FF E1 09
50.
3F 32 F7 FF 92 CD 1C 82 42 04 95 6E 2E EC A3 5C 61 82 E3 2C A5 23 93 B3 C2 FF E1 09

51.
3F 32 F7 FF 92 CD 1C 82 42 04 95 6E 2E EC A3 5C 61 82 E3 2C A5 23 D3 B3 C2 FF E1 09
52.
3F 32 F7 FF 92 CD 1C 82 42 04 95 6E 2E EC A3 5C 61 82 E3 2C A5 23 D3 BD C2 FF E1 09
53.
3F 32 F7 FF 92 CD 1C 82 42 04 95 6E 2E EC A3 5C 61 82 E3 2C A5 23 D3 BD E1 FF E1 09
54.
3F 32 F7 FF 92 CD 1C 82 42 04 95 6E 2E EC A3 5C 61 82 E3 2C A5 23 D3 BD E1 4A E1 09
55.
3F 32 F7 FF 92 CD 1C 82 42 04 95 6E 2E EC A3 5C 61 82 E3 2C A5 23 D3 BD E1 4A 3C 09
56.
3F 32 F7 FF 92 CD 1C 82 42 04 95 6E 2E EC A3 5C 61 82 E3 2C A5 23 D3 BD E1 4A 3C 60
57.
9A 32 F7 FF 92 CD 1C 82 42 04 95 6E 2E EC A3 5C 61 82 E3 2C A5 23 D3 BD E1 4A 3C 60
58.
9A E5 F7 FF 92 CD 1C 82 42 04 95 6E 2E EC A3 5C 61 82 E3 2C A5 23 D3 BD E1 4A 3C 60
59.
9A E5 2F FF 92 CD 1C 82 42 04 95 6E 2E EC A3 5C 61 82 E3 2C A5 23 D3 BD E1 4A 3C 60
60.
9A E5 2F D8 92 CD 1C 82 42 04 95 6E 2E EC A3 5C 61 82 E3 2C A5 23 D3 BD E1 4A 3C 60
61.
9A E5 2F D8 F1 CD 1C 82 42 04 95 6E 2E EC A3 5C 61 82 E3 2C A5 23 D3 BD E1 4A 3C 60
62.
9A E5 2F D8 F1 09 1C 82 42 04 95 6E 2E EC A3 5C 61 82 E3 2C A5 23 D3 BD E1 4A 3C 60
63.
9A E5 2F D8 F1 09 14 82 42 04 95 6E 2E EC A3 5C 61 82 E3 2C A5 23 D3 BD E1 4A 3C 60
64.
9A E5 2F D8 F1 09 14 32 42 04 95 6E 2E EC A3 5C 61 82 E3 2C A5 23 D3 BD E1 4A 3C 60

Stage 2.

Input sequence

32 14 09 F1 D8 2F E5 9A 60 3C 4A E1 BD D3 23 A5 2C E3 82 61 5C A3 EC 2E 6E 95 04 42

Calculating SR state for stage 2. Total 28 steps.

1.
9A E5 2F D8 F1 09 14 32 61 04 95 6E 2E EC A3 5C 61 82 E3 2C A5 23 D3 BD E1 4A 3C 60
2.
9A E5 2F D8 F1 09 14 32 61 27 95 6E 2E EC A3 5C 61 82 E3 2C A5 23 D3 BD E1 4A 3C 60
3.
9A E5 2F D8 F1 09 14 32 61 27 11 6E 2E EC A3 5C 61 82 E3 2C A5 23 D3 BD E1 4A 3C 60
4.
9A E5 2F D8 F1 09 14 32 61 27 11 54 2E EC A3 5C 61 82 E3 2C A5 23 D3 BD E1 4A 3C 60
5.
9A E5 2F D8 F1 09 14 32 61 27 11 54 5B EC A3 5C 61 82 E3 2C A5 23 D3 BD E1 4A 3C 60
6.
9A E5 2F D8 F1 09 14 32 61 27 11 54 5B C6 A3 5C 61 82 E3 2C A5 23 D3 BD E1 4A 3C 60
7.
9A E5 2F D8 F1 09 14 32 61 27 11 54 5B C6 24 5C 61 82 E3 2C A5 23 D3 BD E1 4A 3C 60
8.
9A E5 2F D8 F1 09 14 32 61 27 11 54 5B C6 24 E8 61 82 E3 2C A5 23 D3 BD E1 4A 3C 60
9.
9A E5 2F D8 F1 09 14 32 61 27 11 54 5B C6 24 E8 06 82 E3 2C A5 23 D3 BD E1 4A 3C 60
10.
9A E5 2F D8 F1 09 14 32 61 27 11 54 5B C6 24 E8 06 BB E3 2C A5 23 D3 BD E1 4A 3C 60
11.
9A E5 2F D8 F1 09 14 32 61 27 11 54 5B C6 24 E8 06 BB 90 2C A5 23 D3 BD E1 4A 3C 60
12.
9A E5 2F D8 F1 09 14 32 61 27 11 54 5B C6 24 E8 06 BB 90 17 A5 23 D3 BD E1 4A 3C 60
13.
9A E5 2F D8 F1 09 14 32 61 27 11 54 5B C6 24 E8 06 BB 90 17 04 23 D3 BD E1 4A 3C 60
14.
9A E5 2F D8 F1 09 14 32 61 27 11 54 5B C6 24 E8 06 BB 90 17 04 30 D3 BD E1 4A 3C 60
15.
9A E5 2F D8 F1 09 14 32 61 27 11 54 5B C6 24 E8 06 BB 90 17 04 30 D2 BD E1 4A 3C 60
16.
9A E5 2F D8 F1 09 14 32 61 27 11 54 5B C6 24 E8 06 BB 90 17 04 30 D2 FB E1 4A 3C 60
17.
9A E5 2F D8 F1 09 14 32 61 27 11 54 5B C6 24 E8 06 BB 90 17 04 30 D2 FB A2 4A 3C 60
18.
9A E5 2F D8 F1 09 14 32 61 27 11 54 5B C6 24 E8 06 BB 90 17 04 30 D2 FB A2 E3 3C 60

19.
9A E5 2F D8 F1 09 14 32 61 27 11 54 5B C6 24 E8 06 BB 90 17 04 30 D2 FB A2 E3 F5 60
20.
9A E5 2F D8 F1 09 14 32 61 27 11 54 5B C6 24 E8 06 BB 90 17 04 30 D2 FB A2 E3 F5 D9
21.
9A E5 2F D8 F1 09 14 32 61 27 11 54 5B C6 24 E8 06 BB 90 17 04 30 D2 FB A2 E3 F5 D9
22.
9A 57 2F D8 F1 09 14 32 61 27 11 54 5B C6 24 E8 06 BB 90 17 04 30 D2 FB A2 E3 F5 D9
23.
9A 57 90 D8 F1 09 14 32 61 27 11 54 5B C6 24 E8 06 BB 90 17 04 30 D2 FB A2 E3 F5 D9
24.
9A 57 90 A7 F1 09 14 32 61 27 11 54 5B C6 24 E8 06 BB 90 17 04 30 D2 FB A2 E3 F5 D9
25.
9A 57 90 A7 D2 09 14 32 61 27 11 54 5B C6 24 E8 06 BB 90 17 04 30 D2 FB A2 E3 F5 D9
26.
9A 57 90 A7 D2 07 14 32 61 27 11 54 5B C6 24 E8 06 BB 90 17 04 30 D2 FB A2 E3 F5 D9
27.
9A 57 90 A7 D2 07 37 32 61 27 11 54 5B C6 24 E8 06 BB 90 17 04 30 D2 FB A2 E3 F5 D9
28.
9A 57 90 A7 D2 07 37 AC 61 27 11 54 5B C6 24 E8 06 BB 90 17 04 30 D2 FB A2 E3 F5 D9

Stage 3.

Input sequence

32 14 09 F1 D8 2F E5 9A 60 3C 4A E1 BD D3 23 A5 2C E3 82 61 5C A3 EC 2E 6E 95 04 42

Calculating SR state for stage 3. Total 28 steps.

1.
9A 57 90 A7 D2 07 37 AC 84 27 11 54 5B C6 24 E8 06 BB 90 17 04 30 D2 FB A2 E3 F5 D9
2.
9A 57 90 A7 D2 07 37 AC 84 5B 11 54 5B C6 24 E8 06 BB 90 17 04 30 D2 FB A2 E3 F5 D9
3.
9A 57 90 A7 D2 07 37 AC 84 5B 4D 54 5B C6 24 E8 06 BB 90 17 04 30 D2 FB A2 E3 F5 D9
4.
9A 57 90 A7 D2 07 37 AC 84 5B 4D F4 5B C6 24 E8 06 BB 90 17 04 30 D2 FB A2 E3 F5 D9
5.
9A 57 90 A7 D2 07 37 AC 84 5B 4D F4 C2 C6 24 E8 06 BB 90 17 04 30 D2 FB A2 E3 F5 D9
6.
9A 57 90 A7 D2 07 37 AC 84 5B 4D F4 C2 3C 24 E8 06 BB 90 17 04 30 D2 FB A2 E3 F5 D9
7.
9A 57 90 A7 D2 07 37 AC 84 5B 4D F4 C2 3C C1 E8 06 BB 90 17 04 30 D2 FB A2 E3 F5 D9
8.
9A 57 90 A7 D2 07 37 AC 84 5B 4D F4 C2 3C C1 99 06 BB 90 17 04 30 D2 FB A2 E3 F5 D9
9.
9A 57 90 A7 D2 07 37 AC 84 5B 4D F4 C2 3C C1 99 B7 BB 90 17 04 30 D2 FB A2 E3 F5 D9
10.
9A 57 90 A7 D2 07 37 AC 84 5B 4D F4 C2 3C C1 99 B7 09 90 17 04 30 D2 FB A2 E3 F5 D9
11.
9A 57 90 A7 D2 07 37 AC 84 5B 4D F4 C2 3C C1 99 B7 09 F4 17 04 30 D2 FB A2 E3 F5 D9
12.
9A 57 90 A7 D2 07 37 AC 84 5B 4D F4 C2 3C C1 99 B7 09 F4 7B 04 30 D2 FB A2 E3 F5 D9
13.
9A 57 90 A7 D2 07 37 AC 84 5B 4D F4 C2 3C C1 99 B7 09 F4 7B 47 30 D2 FB A2 E3 F5 D9
14.
9A 57 90 A7 D2 07 37 AC 84 5B 4D F4 C2 3C C1 99 B7 09 F4 7B 47 47 D2 FB A2 E3 F5 D9
15.
9A 57 90 A7 D2 07 37 AC 84 5B 4D F4 C2 3C C1 99 B7 09 F4 7B 47 47 64 FB A2 E3 F5 D9
16.
9A 57 90 A7 D2 07 37 AC 84 5B 4D F4 C2 3C C1 99 B7 09 F4 7B 47 47 64 53 A2 E3 F5 D9
17.
9A 57 90 A7 D2 07 37 AC 84 5B 4D F4 C2 3C C1 99 B7 09 F4 7B 47 47 64 53 7A E3 F5 D9
18.
9A 57 90 A7 D2 07 37 AC 84 5B 4D F4 C2 3C C1 99 B7 09 F4 7B 47 47 64 53 7A 83 F5 D9
19.
9A 57 90 A7 D2 07 37 AC 84 5B 4D F4 C2 3C C1 99 B7 09 F4 7B 47 47 64 53 7A 83 65 D9
20.
9A 57 90 A7 D2 07 37 AC 84 5B 4D F4 C2 3C C1 99 B7 09 F4 7B 47 47 64 53 7A 83 65 B1
21.
A5 57 90 A7 D2 07 37 AC 84 5B 4D F4 C2 3C C1 99 B7 09 F4 7B 47 47 64 53 7A 83 65 B1
22.
A5 89 90 A7 D2 07 37 AC 84 5B 4D F4 C2 3C C1 99 B7 09 F4 7B 47 47 64 53 7A 83 65 B1

23.
A5 89 66 A7 D2 07 37 AC 84 5B 4D F4 C2 3C C1 99 B7 09 F4 7B 47 47 64 53 7A 83 65 B1
24.
A5 89 66 50 D2 07 37 AC 84 5B 4D F4 C2 3C C1 99 B7 09 F4 7B 47 47 64 53 7A 83 65 B1
25.
A5 89 66 50 06 07 37 AC 84 5B 4D F4 C2 3C C1 99 B7 09 F4 7B 47 47 64 53 7A 83 65 B1
26.
A5 89 66 50 06 BB 37 AC 84 5B 4D F4 C2 3C C1 99 B7 09 F4 7B 47 47 64 53 7A 83 65 B1
27.
A5 89 66 50 06 BB 85 AC 84 5B 4D F4 C2 3C C1 99 B7 09 F4 7B 47 47 64 53 7A 83 65 B1
28.
A5 89 66 50 06 BB 85 31 84 5B 4D F4 C2 3C C1 99 B7 09 F4 7B 47 47 64 53 7A 83 65 B1

Final message digest:
A5 89 66 50 06 BB 85 31 84 5B 4D F4 C2 3C C1 99 B7 09 F4 7B 47 47 64 53 7A 83 65 B1

10.4 Final hash computation for hash bit length 256.

Stage 1.

This is SR states for steps in final hash computation. 0 – initial SR state. SR length is 32. Input sequence (from pre-hash computations), 64 bytes:

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

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 for stage 1. Total 64 steps.

1.
2F 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.
2F BE 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.
2F BE A8 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.
2F BE A8 0E 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.
2F BE A8 0E 43 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.
2F BE A8 0E 43 A4 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.
2F BE A8 0E 43 A4 6E 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.
2F BE A8 0E 43 A4 6E 41 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.
2F BE A8 0E 43 A4 6E 41 4A 09 0A 0B 0C 0D 0E 0F 10 11 12 13 14 15 16 17 18 19 1A 1B 1C 1D 1E 1F
10.
2F BE A8 0E 43 A4 6E 41 4A 0C 0A 0B 0C 0D 0E 0F 10 11 12 13 14 15 16 17 18 19 1A 1B 1C 1D 1E 1F
11.
2F BE A8 0E 43 A4 6E 41 4A 0C 3D 0B 0C 0D 0E 0F 10 11 12 13 14 15 16 17 18 19 1A 1B 1C 1D 1E 1F
12.
2F BE A8 0E 43 A4 6E 41 4A 0C 3D E9 0C 0D 0E 0F 10 11 12 13 14 15 16 17 18 19 1A 1B 1C 1D 1E 1F
13.
2F BE A8 0E 43 A4 6E 41 4A 0C 3D E9 85 0D 0E 0F 10 11 12 13 14 15 16 17 18 19 1A 1B 1C 1D 1E 1F
14.
2F BE A8 0E 43 A4 6E 41 4A 0C 3D E9 85 3F 0E 0F 10 11 12 13 14 15 16 17 18 19 1A 1B 1C 1D 1E 1F
15.
2F BE A8 0E 43 A4 6E 41 4A 0C 3D E9 85 3F 6E 0F 10 11 12 13 14 15 16 17 18 19 1A 1B 1C 1D 1E 1F
16.
2F BE A8 0E 43 A4 6E 41 4A 0C 3D E9 85 3F 6E 86 10 11 12 13 14 15 16 17 18 19 1A 1B 1C 1D 1E 1F
17.
2F BE A8 0E 43 A4 6E 41 4A 0C 3D E9 85 3F 6E 86 40 11 12 13 14 15 16 17 18 19 1A 1B 1C 1D 1E 1F
18.

2F BE A8 0E 43 A4 6E 41 4A 0C 3D E9 85 3F 6E 86 40 41 12 13 14 15 16 17 18 19 1A 1B 1C 1D 1E 1F
19.
2F BE A8 0E 43 A4 6E 41 4A 0C 3D E9 85 3F 6E 86 40 41 A6 13 14 15 16 17 18 19 1A 1B 1C 1D 1E 1F
20.
2F BE A8 0E 43 A4 6E 41 4A 0C 3D E9 85 3F 6E 86 40 41 A6 76 14 15 16 17 18 19 1A 1B 1C 1D 1E 1F
21.
2F BE A8 0E 43 A4 6E 41 4A 0C 3D E9 85 3F 6E 86 40 41 A6 76 97 15 16 17 18 19 1A 1B 1C 1D 1E 1F
22.
2F BE A8 0E 43 A4 6E 41 4A 0C 3D E9 85 3F 6E 86 40 41 A6 76 97 A5 16 17 18 19 1A 1B 1C 1D 1E 1F
23.
2F BE A8 0E 43 A4 6E 41 4A 0C 3D E9 85 3F 6E 86 40 41 A6 76 97 A5 7B 17 18 19 1A 1B 1C 1D 1E 1F
24.
2F BE A8 0E 43 A4 6E 41 4A 0C 3D E9 85 3F 6E 86 40 41 A6 76 97 A5 7B 5A 18 19 1A 1B 1C 1D 1E 1F
25.
2F BE A8 0E 43 A4 6E 41 4A 0C 3D E9 85 3F 6E 86 40 41 A6 76 97 A5 7B 5A AD 19 1A 1B 1C 1D 1E 1F
26.
2F BE A8 0E 43 A4 6E 41 4A 0C 3D E9 85 3F 6E 86 40 41 A6 76 97 A5 7B 5A AD 3E 1A 1B 1C 1D 1E 1F
27.
2F BE A8 0E 43 A4 6E 41 4A 0C 3D E9 85 3F 6E 86 40 41 A6 76 97 A5 7B 5A AD 3E AF 1B 1C 1D 1E 1F
28.
2F BE A8 0E 43 A4 6E 41 4A 0C 3D E9 85 3F 6E 86 40 41 A6 76 97 A5 7B 5A AD 3E AF 81 1C 1D 1E 1F
29.
2F BE A8 0E 43 A4 6E 41 4A 0C 3D E9 85 3F 6E 86 40 41 A6 76 97 A5 7B 5A AD 3E AF 81 4A 1D 1E 1F
30.
2F BE A8 0E 43 A4 6E 41 4A 0C 3D E9 85 3F 6E 86 40 41 A6 76 97 A5 7B 5A AD 3E AF 81 4A 8C 1E 1F
31.
2F BE A8 0E 43 A4 6E 41 4A 0C 3D E9 85 3F 6E 86 40 41 A6 76 97 A5 7B 5A AD 3E AF 81 4A 8C 33 1F
32.
2F BE A8 0E 43 A4 6E 41 4A 0C 3D E9 85 3F 6E 86 40 41 A6 76 97 A5 7B 5A AD 3E AF 81 4A 8C 33 29
33.
F0 BE A8 0E 43 A4 6E 41 4A 0C 3D E9 85 3F 6E 86 40 41 A6 76 97 A5 7B 5A AD 3E AF 81 4A 8C 33 29
34.
F0 6A A8 0E 43 A4 6E 41 4A 0C 3D E9 85 3F 6E 86 40 41 A6 76 97 A5 7B 5A AD 3E AF 81 4A 8C 33 29
35.
F0 6A 29 0E 43 A4 6E 41 4A 0C 3D E9 85 3F 6E 86 40 41 A6 76 97 A5 7B 5A AD 3E AF 81 4A 8C 33 29
36.
F0 6A 29 71 43 A4 6E 41 4A 0C 3D E9 85 3F 6E 86 40 41 A6 76 97 A5 7B 5A AD 3E AF 81 4A 8C 33 29
37.
F0 6A 29 71 C5 A4 6E 41 4A 0C 3D E9 85 3F 6E 86 40 41 A6 76 97 A5 7B 5A AD 3E AF 81 4A 8C 33 29
38.
F0 6A 29 71 C5 93 6E 41 4A 0C 3D E9 85 3F 6E 86 40 41 A6 76 97 A5 7B 5A AD 3E AF 81 4A 8C 33 29
39.
F0 6A 29 71 C5 93 7C 41 4A 0C 3D E9 85 3F 6E 86 40 41 A6 76 97 A5 7B 5A AD 3E AF 81 4A 8C 33 29
40.
F0 6A 29 71 C5 93 7C 8E 4A 0C 3D E9 85 3F 6E 86 40 41 A6 76 97 A5 7B 5A AD 3E AF 81 4A 8C 33 29
41.
F0 6A 29 71 C5 93 7C 8E 4D 0C 3D E9 85 3F 6E 86 40 41 A6 76 97 A5 7B 5A AD 3E AF 81 4A 8C 33 29
42.
F0 6A 29 71 C5 93 7C 8E 4D 48 3D E9 85 3F 6E 86 40 41 A6 76 97 A5 7B 5A AD 3E AF 81 4A 8C 33 29
43.
F0 6A 29 71 C5 93 7C 8E 4D 48 CB E9 85 3F 6E 86 40 41 A6 76 97 A5 7B 5A AD 3E AF 81 4A 8C 33 29
44.
F0 6A 29 71 C5 93 7C 8E 4D 48 CB 20 85 3F 6E 86 40 41 A6 76 97 A5 7B 5A AD 3E AF 81 4A 8C 33 29
45.
F0 6A 29 71 C5 93 7C 8E 4D 48 CB 20 C7 3F 6E 86 40 41 A6 76 97 A5 7B 5A AD 3E AF 81 4A 8C 33 29
46.
F0 6A 29 71 C5 93 7C 8E 4D 48 CB 20 C7 FD 6E 86 40 41 A6 76 97 A5 7B 5A AD 3E AF 81 4A 8C 33 29
47.
F0 6A 29 71 C5 93 7C 8E 4D 48 CB 20 C7 FD 1C 86 40 41 A6 76 97 A5 7B 5A AD 3E AF 81 4A 8C 33 29
48.
F0 6A 29 71 C5 93 7C 8E 4D 48 CB 20 C7 FD 1C DD 40 41 A6 76 97 A5 7B 5A AD 3E AF 81 4A 8C 33 29
49.
F0 6A 29 71 C5 93 7C 8E 4D 48 CB 20 C7 FD 1C DD 72 41 A6 76 97 A5 7B 5A AD 3E AF 81 4A 8C 33 29
50.
F0 6A 29 71 C5 93 7C 8E 4D 48 CB 20 C7 FD 1C DD 72 06 A6 76 97 A5 7B 5A AD 3E AF 81 4A 8C 33 29
51.
F0 6A 29 71 C5 93 7C 8E 4D 48 CB 20 C7 FD 1C DD 72 06 20 76 97 A5 7B 5A AD 3E AF 81 4A 8C 33 29
52.
F0 6A 29 71 C5 93 7C 8E 4D 48 CB 20 C7 FD 1C DD 72 06 20 8A 97 A5 7B 5A AD 3E AF 81 4A 8C 33 29
53.
F0 6A 29 71 C5 93 7C 8E 4D 48 CB 20 C7 FD 1C DD 72 06 20 8A 4C A5 7B 5A AD 3E AF 81 4A 8C 33 29
54.
F0 6A 29 71 C5 93 7C 8E 4D 48 CB 20 C7 FD 1C DD 72 06 20 8A 4C A7 7B 5A AD 3E AF 81 4A 8C 33 29
55.

F0 6A 29 71 C5 93 7C 8E 4D 48 CB 20 C7 FD 1C DD 72 06 20 8A 4C A7 C2 5A AD 3E AF 81 4A 8C 33 29
56.
F0 6A 29 71 C5 93 7C 8E 4D 48 CB 20 C7 FD 1C DD 72 06 20 8A 4C A7 C2 B5 AD 3E AF 81 4A 8C 33 29
57.
F0 6A 29 71 C5 93 7C 8E 4D 48 CB 20 C7 FD 1C DD 72 06 20 8A 4C A7 C2 B5 55 3E AF 81 4A 8C 33 29
58.
F0 6A 29 71 C5 93 7C 8E 4D 48 CB 20 C7 FD 1C DD 72 06 20 8A 4C A7 C2 B5 55 FA AF 81 4A 8C 33 29
59.
F0 6A 29 71 C5 93 7C 8E 4D 48 CB 20 C7 FD 1C DD 72 06 20 8A 4C A7 C2 B5 55 FA A3 81 4A 8C 33 29
60.
F0 6A 29 71 C5 93 7C 8E 4D 48 CB 20 C7 FD 1C DD 72 06 20 8A 4C A7 C2 B5 55 FA A3 0D 4A 8C 33 29
61.
F0 6A 29 71 C5 93 7C 8E 4D 48 CB 20 C7 FD 1C DD 72 06 20 8A 4C A7 C2 B5 55 FA A3 0D D4 8C 33 29
62.
F0 6A 29 71 C5 93 7C 8E 4D 48 CB 20 C7 FD 1C DD 72 06 20 8A 4C A7 C2 B5 55 FA A3 0D D4 38 33 29
63.
F0 6A 29 71 C5 93 7C 8E 4D 48 CB 20 C7 FD 1C DD 72 06 20 8A 4C A7 C2 B5 55 FA A3 0D D4 38 47 29
64.
F0 6A 29 71 C5 93 7C 8E 4D 48 CB 20 C7 FD 1C DD 72 06 20 8A 4C A7 C2 B5 55 FA A3 0D D4 38 47 3B

Stage 2.

Input sequence
3B 47 38 D4 0D A3 FA 55 B5 C2 A7 4C 8A 20 06 72 DD 1C FD C7 20 CB 48 4D 8E 7C 93 C5 71 29 6A F0

Calculating SR state for stage 2. Total 32 steps.

1.
AE 6A 29 71 C5 93 7C 8E 4D 48 CB 20 C7 FD 1C DD 72 06 20 8A 4C A7 C2 B5 55 FA A3 0D D4 38 47 3B
2.
AE 27 29 71 C5 93 7C 8E 4D 48 CB 20 C7 FD 1C DD 72 06 20 8A 4C A7 C2 B5 55 FA A3 0D D4 38 47 3B
3.
AE 27 C2 71 C5 93 7C 8E 4D 48 CB 20 C7 FD 1C DD 72 06 20 8A 4C A7 C2 B5 55 FA A3 0D D4 38 47 3B
4.
AE 27 C2 CF C5 93 7C 8E 4D 48 CB 20 C7 FD 1C DD 72 06 20 8A 4C A7 C2 B5 55 FA A3 0D D4 38 47 3B
5.
AE 27 C2 CF CB 93 7C 8E 4D 48 CB 20 C7 FD 1C DD 72 06 20 8A 4C A7 C2 B5 55 FA A3 0D D4 38 47 3B
6.
AE 27 C2 CF CB CE 7C 8E 4D 48 CB 20 C7 FD 1C DD 72 06 20 8A 4C A7 C2 B5 55 FA A3 0D D4 38 47 3B
7.
AE 27 C2 CF CB CE 87 8E 4D 48 CB 20 C7 FD 1C DD 72 06 20 8A 4C A7 C2 B5 55 FA A3 0D D4 38 47 3B
8.
AE 27 C2 CF CB CE 87 73 4D 48 CB 20 C7 FD 1C DD 72 06 20 8A 4C A7 C2 B5 55 FA A3 0D D4 38 47 3B
9.
AE 27 C2 CF CB CE 87 73 20 48 CB 20 C7 FD 1C DD 72 06 20 8A 4C A7 C2 B5 55 FA A3 0D D4 38 47 3B
10.
AE 27 C2 CF CB CE 87 73 20 E6 CB 20 C7 FD 1C DD 72 06 20 8A 4C A7 C2 B5 55 FA A3 0D D4 38 47 3B
11.
AE 27 C2 CF CB CE 87 73 20 E6 BF 20 C7 FD 1C DD 72 06 20 8A 4C A7 C2 B5 55 FA A3 0D D4 38 47 3B
12.
AE 27 C2 CF CB CE 87 73 20 E6 BF D3 C7 FD 1C DD 72 06 20 8A 4C A7 C2 B5 55 FA A3 0D D4 38 47 3B
13.
AE 27 C2 CF CB CE 87 73 20 E6 BF D3 21 FD 1C DD 72 06 20 8A 4C A7 C2 B5 55 FA A3 0D D4 38 47 3B
14.
AE 27 C2 CF CB CE 87 73 20 E6 BF D3 21 B1 1C DD 72 06 20 8A 4C A7 C2 B5 55 FA A3 0D D4 38 47 3B
15.
AE 27 C2 CF CB CE 87 73 20 E6 BF D3 21 B1 5B DD 72 06 20 8A 4C A7 C2 B5 55 FA A3 0D D4 38 47 3B
16.
AE 27 C2 CF CB CE 87 73 20 E6 BF D3 21 B1 5B DF 72 06 20 8A 4C A7 C2 B5 55 FA A3 0D D4 38 47 3B
17.
AE 27 C2 CF CB CE 87 73 20 E6 BF D3 21 B1 5B DF 1E 06 20 8A 4C A7 C2 B5 55 FA A3 0D D4 38 47 3B
18.
AE 27 C2 CF CB CE 87 73 20 E6 BF D3 21 B1 5B DF 1E DA 20 8A 4C A7 C2 B5 55 FA A3 0D D4 38 47 3B
19.
AE 27 C2 CF CB CE 87 73 20 E6 BF D3 21 B1 5B DF 1E DA 3F 8A 4C A7 C2 B5 55 FA A3 0D D4 38 47 3B
20.
AE 27 C2 CF CB CE 87 73 20 E6 BF D3 21 B1 5B DF 1E DA 3F 40 4C A7 C2 B5 55 FA A3 0D D4 38 47 3B
21.
AE 27 C2 CF CB CE 87 73 20 E6 BF D3 21 B1 5B DF 1E DA 3F 40 33 A7 C2 B5 55 FA A3 0D D4 38 47 3B
22.
AE 27 C2 CF CB CE 87 73 20 E6 BF D3 21 B1 5B DF 1E DA 3F 40 33 9E C2 B5 55 FA A3 0D D4 38 47 3B
23.
AE 27 C2 CF CB CE 87 73 20 E6 BF D3 21 B1 5B DF 1E DA 3F 40 33 9E EE B5 55 FA A3 0D D4 38 47 3B

24.
AE 27 C2 CF CB CE 87 73 20 E6 BF D3 21 B1 5B DF 1E DA 3F 40 33 9E EE 4B 55 FA A3 0D D4 38 47 3B
25.
AE 27 C2 CF CB CE 87 73 20 E6 BF D3 21 B1 5B DF 1E DA 3F 40 33 9E EE 4B 8A FA A3 0D D4 38 47 3B
26.
AE 27 C2 CF CB CE 87 73 20 E6 BF D3 21 B1 5B DF 1E DA 3F 40 33 9E EE 4B 8A 8B A3 0D D4 38 47 3B
27.
AE 27 C2 CF CB CE 87 73 20 E6 BF D3 21 B1 5B DF 1E DA 3F 40 33 9E EE 4B 8A 8B 8E 0D D4 38 47 3B
28.
AE 27 C2 CF CB CE 87 73 20 E6 BF D3 21 B1 5B DF 1E DA 3F 40 33 9E EE 4B 8A 8B 8E B8 D4 38 47 3B
29.
AE 27 C2 CF CB CE 87 73 20 E6 BF D3 21 B1 5B DF 1E DA 3F 40 33 9E EE 4B 8A 8B 8E B8 CA 38 47 3B
30.
AE 27 C2 CF CB CE 87 73 20 E6 BF D3 21 B1 5B DF 1E DA 3F 40 33 9E EE 4B 8A 8B 8E B8 CA 2A 47 3B
31.
AE 27 C2 CF CB CE 87 73 20 E6 BF D3 21 B1 5B DF 1E DA 3F 40 33 9E EE 4B 8A 8B 8E B8 CA 2A F6 3B
32.
AE 27 C2 CF CB CE 87 73 20 E6 BF D3 21 B1 5B DF 1E DA 3F 40 33 9E EE 4B 8A 8B 8E B8 CA 2A F6 3E

Stage 3.

Input sequence
3B 47 38 D4 0D A3 FA 55 B5 C2 A7 4C 8A 20 06 72 DD 1C FD C7 20 CB 48 4D 8E 7C 93 C5 71 29 6A F0

Calculating SR state for stage 3. Total 32 steps.

1.
20 27 C2 CF CB CE 87 73 20 E6 BF D3 21 B1 5B DF 1E DA 3F 40 33 9E EE 4B 8A 8B 8E B8 CA 2A F6 3E
2.
20 29 C2 CF CB CE 87 73 20 E6 BF D3 21 B1 5B DF 1E DA 3F 40 33 9E EE 4B 8A 8B 8E B8 CA 2A F6 3E
3.
20 29 24 CF CB CE 87 73 20 E6 BF D3 21 B1 5B DF 1E DA 3F 40 33 9E EE 4B 8A 8B 8E B8 CA 2A F6 3E
4.
20 29 24 B5 CB CE 87 73 20 E6 BF D3 21 B1 5B DF 1E DA 3F 40 33 9E EE 4B 8A 8B 8E B8 CA 2A F6 3E
5.
20 29 24 B5 39 CE 87 73 20 E6 BF D3 21 B1 5B DF 1E DA 3F 40 33 9E EE 4B 8A 8B 8E B8 CA 2A F6 3E
6.
20 29 24 B5 39 C3 87 73 20 E6 BF D3 21 B1 5B DF 1E DA 3F 40 33 9E EE 4B 8A 8B 8E B8 CA 2A F6 3E
7.
20 29 24 B5 39 C3 D3 73 20 E6 BF D3 21 B1 5B DF 1E DA 3F 40 33 9E EE 4B 8A 8B 8E B8 CA 2A F6 3E
8.
20 29 24 B5 39 C3 D3 89 20 E6 BF D3 21 B1 5B DF 1E DA 3F 40 33 9E EE 4B 8A 8B 8E B8 CA 2A F6 3E
9.
20 29 24 B5 39 C3 D3 89 D7 E6 BF D3 21 B1 5B DF 1E DA 3F 40 33 9E EE 4B 8A 8B 8E B8 CA 2A F6 3E
10.
20 29 24 B5 39 C3 D3 89 D7 A5 BF D3 21 B1 5B DF 1E DA 3F 40 33 9E EE 4B 8A 8B 8E B8 CA 2A F6 3E
11.
20 29 24 B5 39 C3 D3 89 D7 A5 13 D3 21 B1 5B DF 1E DA 3F 40 33 9E EE 4B 8A 8B 8E B8 CA 2A F6 3E
12.
20 29 24 B5 39 C3 D3 89 D7 A5 13 E9 21 B1 5B DF 1E DA 3F 40 33 9E EE 4B 8A 8B 8E B8 CA 2A F6 3E
13.
20 29 24 B5 39 C3 D3 89 D7 A5 13 E9 9A B1 5B DF 1E DA 3F 40 33 9E EE 4B 8A 8B 8E B8 CA 2A F6 3E
14.
20 29 24 B5 39 C3 D3 89 D7 A5 13 E9 9A C9 5B DF 1E DA 3F 40 33 9E EE 4B 8A 8B 8E B8 CA 2A F6 3E
15.
20 29 24 B5 39 C3 D3 89 D7 A5 13 E9 9A C9 83 DF 1E DA 3F 40 33 9E EE 4B 8A 8B 8E B8 CA 2A F6 3E
16.
20 29 24 B5 39 C3 D3 89 D7 A5 13 E9 9A C9 83 54 1E DA 3F 40 33 9E EE 4B 8A 8B 8E B8 CA 2A F6 3E
17.
20 29 24 B5 39 C3 D3 89 D7 A5 13 E9 9A C9 83 54 42 DA 3F 40 33 9E EE 4B 8A 8B 8E B8 CA 2A F6 3E
18.
20 29 24 B5 39 C3 D3 89 D7 A5 13 E9 9A C9 83 54 42 6E 3F 40 33 9E EE 4B 8A 8B 8E B8 CA 2A F6 3E
19.
20 29 24 B5 39 C3 D3 89 D7 A5 13 E9 9A C9 83 54 42 6E DE 40 33 9E EE 4B 8A 8B 8E B8 CA 2A F6 3E
20.
20 29 24 B5 39 C3 D3 89 D7 A5 13 E9 9A C9 83 54 42 6E DE 1D 33 9E EE 4B 8A 8B 8E B8 CA 2A F6 3E
21.
20 29 24 B5 39 C3 D3 89 D7 A5 13 E9 9A C9 83 54 42 6E DE 1D 92 9E EE 4B 8A 8B 8E B8 CA 2A F6 3E
22.
20 29 24 B5 39 C3 D3 89 D7 A5 13 E9 9A C9 83 54 42 6E DE 1D 92 AA EE 4B 8A 8B 8E B8 CA 2A F6 3E
23.
20 29 24 B5 39 C3 D3 89 D7 A5 13 E9 9A C9 83 54 42 6E DE 1D 92 AA 25 4B 8A 8B 8E B8 CA 2A F6 3E
24.

20 29 24 B5 39 C3 D3 89 D7 A5 13 E9 9A C9 83 54 42 6E DE 1D 92 AA 25 47 8A 8B 8E B8 CA 2A F6 3E
25.
20 29 24 B5 39 C3 D3 89 D7 A5 13 E9 9A C9 83 54 42 6E DE 1D 92 AA 25 47 7F 8B 8E B8 CA 2A F6 3E
26.
20 29 24 B5 39 C3 D3 89 D7 A5 13 E9 9A C9 83 54 42 6E DE 1D 92 AA 25 47 7F 10 8E B8 CA 2A F6 3E
27.
20 29 24 B5 39 C3 D3 89 D7 A5 13 E9 9A C9 83 54 42 6E DE 1D 92 AA 25 47 7F 10 3D B8 CA 2A F6 3E
28.
20 29 24 B5 39 C3 D3 89 D7 A5 13 E9 9A C9 83 54 42 6E DE 1D 92 AA 25 47 7F 10 3D 3A CA 2A F6 3E
29.
20 29 24 B5 39 C3 D3 89 D7 A5 13 E9 9A C9 83 54 42 6E DE 1D 92 AA 25 47 7F 10 3D 3A 53 2A F6 3E
30.
20 29 24 B5 39 C3 D3 89 D7 A5 13 E9 9A C9 83 54 42 6E DE 1D 92 AA 25 47 7F 10 3D 3A 53 BF F6 3E
31.
20 29 24 B5 39 C3 D3 89 D7 A5 13 E9 9A C9 83 54 42 6E DE 1D 92 AA 25 47 7F 10 3D 3A 53 BF 72 3E
32.
20 29 24 B5 39 C3 D3 89 D7 A5 13 E9 9A C9 83 54 42 6E DE 1D 92 AA 25 47 7F 10 3D 3A 53 BF 72 E4

Final message digest:
20 29 24 B5 39 C3 D3 89 D7 A5 13 E9 9A C9 83 54 42 6E DE 1D 92 AA 25 47 7F 10 3D 3A 53 BF 72 E4

10.5 Final hash computation for hash bit length 384.

Stage 1.

This is SR states for steps in final hash computation. 0 – initial SR state. SR length is 48. Input sequence (from pre-hash computations), 128 bytes:

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

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 for stage 1. Total 128 steps.

1.
2F 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.
2F 59 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.
2F 59 8A 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.
2F 59 8A 21 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.
2F 59 8A 21 5E 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.
2F 59 8A 21 5E 0F 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.
2F 59 8A 21 5E 0F 87 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.
2F 59 8A 21 5E 0F 87 BD 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.
2F 59 8A 21 5E 0F 87 BD ED 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.
2F 59 8A 21 5E 0F 87 BD ED 1E 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.
2F 59 8A 21 5E 0F 87 BD ED 1E 37 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.
2F 59 8A 21 5E 0F 87 BD ED 1E 37 14 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.
2F 59 8A 21 5E 0F 87 BD ED 1E 37 14 F8 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.
2F 59 8A 21 5E 0F 87 BD ED 1E 37 14 F8 57 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.
2F 59 8A 21 5E 0F 87 BD ED 1E 37 14 F8 57 71 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.
2F 59 8A 21 5E 0F 87 BD ED 1E 37 14 F8 57 71 BA 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.
2F 59 8A 21 5E 0F 87 BD ED 1E 37 14 F8 57 71 BA BA 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.
2F 59 8A 21 5E 0F 87 BD ED 1E 37 14 F8 57 71 BA BA EC 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.
2F 59 8A 21 5E 0F 87 BD ED 1E 37 14 F8 57 71 BA BA EC 5B 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.
2F 59 8A 21 5E 0F 87 BD ED 1E 37 14 F8 57 71 BA BA EC 5B EA 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.
2F 59 8A 21 5E 0F 87 BD ED 1E 37 14 F8 57 71 BA BA EC 5B EA 4A 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.
2F 59 8A 21 5E 0F 87 BD ED 1E 37 14 F8 57 71 BA BA EC 5B EA 4A 04 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.
2F 59 8A 21 5E 0F 87 BD ED 1E 37 14 F8 57 71 BA BA EC 5B EA 4A 04 A2 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.
2F 59 8A 21 5E 0F 87 BD ED 1E 37 14 F8 57 71 BA BA EC 5B EA 4A 04 A2 F7 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.
2F 59 8A 21 5E 0F 87 BD ED 1E 37 14 F8 57 71 BA BA EC 5B EA 4A 04 A2 F7 2A 19 1A 1B 1C 1D 1E 1F
20 21 22 23 24 25 26 27 28 29 2A 2B 2C 2D 2E 2F
26.
2F 59 8A 21 5E 0F 87 BD ED 1E 37 14 F8 57 71 BA BA EC 5B EA 4A 04 A2 F7 2A EB 1A 1B 1C 1D 1E 1F
20 21 22 23 24 25 26 27 28 29 2A 2B 2C 2D 2E 2F
27.
2F 59 8A 21 5E 0F 87 BD ED 1E 37 14 F8 57 71 BA BA EC 5B EA 4A 04 A2 F7 2A EB 67 1B 1C 1D 1E 1F
20 21 22 23 24 25 26 27 28 29 2A 2B 2C 2D 2E 2F
28.
2F 59 8A 21 5E 0F 87 BD ED 1E 37 14 F8 57 71 BA BA EC 5B EA 4A 04 A2 F7 2A EB 67 F8 1C 1D 1E 1F
20 21 22 23 24 25 26 27 28 29 2A 2B 2C 2D 2E 2F
29.
2F 59 8A 21 5E 0F 87 BD ED 1E 37 14 F8 57 71 BA BA EC 5B EA 4A 04 A2 F7 2A EB 67 F8 E4 1D 1E 1F
20 21 22 23 24 25 26 27 28 29 2A 2B 2C 2D 2E 2F
30.
2F 59 8A 21 5E 0F 87 BD ED 1E 37 14 F8 57 71 BA BA EC 5B EA 4A 04 A2 F7 2A EB 67 F8 E4 5D 1E 1F
20 21 22 23 24 25 26 27 28 29 2A 2B 2C 2D 2E 2F
31.
2F 59 8A 21 5E 0F 87 BD ED 1E 37 14 F8 57 71 BA BA EC 5B EA 4A 04 A2 F7 2A EB 67 F8 E4 5D 82 1F
20 21 22 23 24 25 26 27 28 29 2A 2B 2C 2D 2E 2F
32.
2F 59 8A 21 5E 0F 87 BD ED 1E 37 14 F8 57 71 BA BA EC 5B EA 4A 04 A2 F7 2A EB 67 F8 E4 5D 82 3E
20 21 22 23 24 25 26 27 28 29 2A 2B 2C 2D 2E 2F
33.
2F 59 8A 21 5E 0F 87 BD ED 1E 37 14 F8 57 71 BA BA EC 5B EA 4A 04 A2 F7 2A EB 67 F8 E4 5D 82 3E
53 21 22 23 24 25 26 27 28 29 2A 2B 2C 2D 2E 2F
34.
2F 59 8A 21 5E 0F 87 BD ED 1E 37 14 F8 57 71 BA BA EC 5B EA 4A 04 A2 F7 2A EB 67 F8 E4 5D 82 3E

53 85 22 23 24 25 26 27 28 29 2A 2B 2C 2D 2E 2F
35.
2F 59 8A 21 5E 0F 87 BD ED 1E 37 14 F8 57 71 BA BA EC 5B EA 4A 04 A2 F7 2A EB 67 F8 E4 5D 82 3E
53 85 89 23 24 25 26 27 28 29 2A 2B 2C 2D 2E 2F
36.
2F 59 8A 21 5E 0F 87 BD ED 1E 37 14 F8 57 71 BA BA EC 5B EA 4A 04 A2 F7 2A EB 67 F8 E4 5D 82 3E
53 85 89 1C 24 25 26 27 28 29 2A 2B 2C 2D 2E 2F
37.
2F 59 8A 21 5E 0F 87 BD ED 1E 37 14 F8 57 71 BA BA EC 5B EA 4A 04 A2 F7 2A EB 67 F8 E4 5D 82 3E
53 85 89 1C AC 25 26 27 28 29 2A 2B 2C 2D 2E 2F
38.
2F 59 8A 21 5E 0F 87 BD ED 1E 37 14 F8 57 71 BA BA EC 5B EA 4A 04 A2 F7 2A EB 67 F8 E4 5D 82 3E
53 85 89 1C AC 11 26 27 28 29 2A 2B 2C 2D 2E 2F
39.
2F 59 8A 21 5E 0F 87 BD ED 1E 37 14 F8 57 71 BA BA EC 5B EA 4A 04 A2 F7 2A EB 67 F8 E4 5D 82 3E
53 85 89 1C AC 11 77 27 28 29 2A 2B 2C 2D 2E 2F
40.
2F 59 8A 21 5E 0F 87 BD ED 1E 37 14 F8 57 71 BA BA EC 5B EA 4A 04 A2 F7 2A EB 67 F8 E4 5D 82 3E
53 85 89 1C AC 11 77 4E 28 29 2A 2B 2C 2D 2E 2F
41.
2F 59 8A 21 5E 0F 87 BD ED 1E 37 14 F8 57 71 BA BA EC 5B EA 4A 04 A2 F7 2A EB 67 F8 E4 5D 82 3E
53 85 89 1C AC 11 77 4E 1D 29 2A 2B 2C 2D 2E 2F
42.
2F 59 8A 21 5E 0F 87 BD ED 1E 37 14 F8 57 71 BA BA EC 5B EA 4A 04 A2 F7 2A EB 67 F8 E4 5D 82 3E
53 85 89 1C AC 11 77 4E 1D 98 2A 2B 2C 2D 2E 2F
43.
2F 59 8A 21 5E 0F 87 BD ED 1E 37 14 F8 57 71 BA BA EC 5B EA 4A 04 A2 F7 2A EB 67 F8 E4 5D 82 3E
53 85 89 1C AC 11 77 4E 1D 98 CB 2B 2C 2D 2E 2F
44.
2F 59 8A 21 5E 0F 87 BD ED 1E 37 14 F8 57 71 BA BA EC 5B EA 4A 04 A2 F7 2A EB 67 F8 E4 5D 82 3E
53 85 89 1C AC 11 77 4E 1D 98 CB 1E 2C 2D 2E 2F
45.
2F 59 8A 21 5E 0F 87 BD ED 1E 37 14 F8 57 71 BA BA EC 5B EA 4A 04 A2 F7 2A EB 67 F8 E4 5D 82 3E
53 85 89 1C AC 11 77 4E 1D 98 CB 1E 5C 2D 2E 2F
46.
2F 59 8A 21 5E 0F 87 BD ED 1E 37 14 F8 57 71 BA BA EC 5B EA 4A 04 A2 F7 2A EB 67 F8 E4 5D 82 3E
53 85 89 1C AC 11 77 4E 1D 98 CB 1E 5C B1 2E 2F
47.
2F 59 8A 21 5E 0F 87 BD ED 1E 37 14 F8 57 71 BA BA EC 5B EA 4A 04 A2 F7 2A EB 67 F8 E4 5D 82 3E
53 85 89 1C AC 11 77 4E 1D 98 CB 1E 5C B1 AC 2F
48.
2F 59 8A 21 5E 0F 87 BD ED 1E 37 14 F8 57 71 BA BA EC 5B EA 4A 04 A2 F7 2A EB 67 F8 E4 5D 82 3E
53 85 89 1C AC 11 77 4E 1D 98 CB 1E 5C B1 AC A5
49.
93 59 8A 21 5E 0F 87 BD ED 1E 37 14 F8 57 71 BA BA EC 5B EA 4A 04 A2 F7 2A EB 67 F8 E4 5D 82 3E
53 85 89 1C AC 11 77 4E 1D 98 CB 1E 5C B1 AC A5
50.
93 E8 8A 21 5E 0F 87 BD ED 1E 37 14 F8 57 71 BA BA EC 5B EA 4A 04 A2 F7 2A EB 67 F8 E4 5D 82 3E
53 85 89 1C AC 11 77 4E 1D 98 CB 1E 5C B1 AC A5
51.
93 E8 B9 21 5E 0F 87 BD ED 1E 37 14 F8 57 71 BA BA EC 5B EA 4A 04 A2 F7 2A EB 67 F8 E4 5D 82 3E
53 85 89 1C AC 11 77 4E 1D 98 CB 1E 5C B1 AC A5
52.
93 E8 B9 D5 5E 0F 87 BD ED 1E 37 14 F8 57 71 BA BA EC 5B EA 4A 04 A2 F7 2A EB 67 F8 E4 5D 82 3E
53 85 89 1C AC 11 77 4E 1D 98 CB 1E 5C B1 AC A5
53.
93 E8 B9 D5 A2 0F 87 BD ED 1E 37 14 F8 57 71 BA BA EC 5B EA 4A 04 A2 F7 2A EB 67 F8 E4 5D 82 3E
53 85 89 1C AC 11 77 4E 1D 98 CB 1E 5C B1 AC A5
54.
93 E8 B9 D5 A2 E3 87 BD ED 1E 37 14 F8 57 71 BA BA EC 5B EA 4A 04 A2 F7 2A EB 67 F8 E4 5D 82 3E
53 85 89 1C AC 11 77 4E 1D 98 CB 1E 5C B1 AC A5
55.
93 E8 B9 D5 A2 E3 52 BD ED 1E 37 14 F8 57 71 BA BA EC 5B EA 4A 04 A2 F7 2A EB 67 F8 E4 5D 82 3E
53 85 89 1C AC 11 77 4E 1D 98 CB 1E 5C B1 AC A5
56.
93 E8 B9 D5 A2 E3 52 5D ED 1E 37 14 F8 57 71 BA BA EC 5B EA 4A 04 A2 F7 2A EB 67 F8 E4 5D 82 3E
53 85 89 1C AC 11 77 4E 1D 98 CB 1E 5C B1 AC A5
57.
93 E8 B9 D5 A2 E3 52 5D 5A 1E 37 14 F8 57 71 BA BA EC 5B EA 4A 04 A2 F7 2A EB 67 F8 E4 5D 82 3E
53 85 89 1C AC 11 77 4E 1D 98 CB 1E 5C B1 AC A5
58.
93 E8 B9 D5 A2 E3 52 5D 5A A1 37 14 F8 57 71 BA BA EC 5B EA 4A 04 A2 F7 2A EB 67 F8 E4 5D 82 3E
53 85 89 1C AC 11 77 4E 1D 98 CB 1E 5C B1 AC A5
59.

93 E8 B9 D5 A2 E3 52 5D 5A A1 22 14 F8 57 71 BA BA EC 5B EA 4A 04 A2 F7 2A EB 67 F8 E4 5D 82 3E
53 85 89 1C AC 11 77 4E 1D 98 CB 1E 5C B1 AC A5
60.
93 E8 B9 D5 A2 E3 52 5D 5A A1 22 7F F8 57 71 BA BA EC 5B EA 4A 04 A2 F7 2A EB 67 F8 E4 5D 82 3E
53 85 89 1C AC 11 77 4E 1D 98 CB 1E 5C B1 AC A5
61.
93 E8 B9 D5 A2 E3 52 5D 5A A1 22 7F 0A 57 71 BA BA EC 5B EA 4A 04 A2 F7 2A EB 67 F8 E4 5D 82 3E
53 85 89 1C AC 11 77 4E 1D 98 CB 1E 5C B1 AC A5
62.
93 E8 B9 D5 A2 E3 52 5D 5A A1 22 7F 0A 43 71 BA BA EC 5B EA 4A 04 A2 F7 2A EB 67 F8 E4 5D 82 3E
53 85 89 1C AC 11 77 4E 1D 98 CB 1E 5C B1 AC A5
63.
93 E8 B9 D5 A2 E3 52 5D 5A A1 22 7F 0A 43 5B BA BA EC 5B EA 4A 04 A2 F7 2A EB 67 F8 E4 5D 82 3E
53 85 89 1C AC 11 77 4E 1D 98 CB 1E 5C B1 AC A5
64.
93 E8 B9 D5 A2 E3 52 5D 5A A1 22 7F 0A 43 5B 54 BA EC 5B EA 4A 04 A2 F7 2A EB 67 F8 E4 5D 82 3E
53 85 89 1C AC 11 77 4E 1D 98 CB 1E 5C B1 AC A5
65.
93 E8 B9 D5 A2 E3 52 5D 5A A1 22 7F 0A 43 5B 54 36 EC 5B EA 4A 04 A2 F7 2A EB 67 F8 E4 5D 82 3E
53 85 89 1C AC 11 77 4E 1D 98 CB 1E 5C B1 AC A5
66.
93 E8 B9 D5 A2 E3 52 5D 5A A1 22 7F 0A 43 5B 54 36 B8 5B EA 4A 04 A2 F7 2A EB 67 F8 E4 5D 82 3E
53 85 89 1C AC 11 77 4E 1D 98 CB 1E 5C B1 AC A5
67.
93 E8 B9 D5 A2 E3 52 5D 5A A1 22 7F 0A 43 5B 54 36 B8 8D EA 4A 04 A2 F7 2A EB 67 F8 E4 5D 82 3E
53 85 89 1C AC 11 77 4E 1D 98 CB 1E 5C B1 AC A5
68.
93 E8 B9 D5 A2 E3 52 5D 5A A1 22 7F 0A 43 5B 54 36 B8 8D 8D 4A 04 A2 F7 2A EB 67 F8 E4 5D 82 3E
53 85 89 1C AC 11 77 4E 1D 98 CB 1E 5C B1 AC A5
69.
93 E8 B9 D5 A2 E3 52 5D 5A A1 22 7F 0A 43 5B 54 36 B8 8D 8D 9C 04 A2 F7 2A EB 67 F8 E4 5D 82 3E
53 85 89 1C AC 11 77 4E 1D 98 CB 1E 5C B1 AC A5
70.
93 E8 B9 D5 A2 E3 52 5D 5A A1 22 7F 0A 43 5B 54 36 B8 8D 8D 9C 9F A2 F7 2A EB 67 F8 E4 5D 82 3E
53 85 89 1C AC 11 77 4E 1D 98 CB 1E 5C B1 AC A5
71.
93 E8 B9 D5 A2 E3 52 5D 5A A1 22 7F 0A 43 5B 54 36 B8 8D 8D 9C 9F 12 F7 2A EB 67 F8 E4 5D 82 3E
53 85 89 1C AC 11 77 4E 1D 98 CB 1E 5C B1 AC A5
72.
93 E8 B9 D5 A2 E3 52 5D 5A A1 22 7F 0A 43 5B 54 36 B8 8D 8D 9C 9F 12 EC 2A EB 67 F8 E4 5D 82 3E
53 85 89 1C AC 11 77 4E 1D 98 CB 1E 5C B1 AC A5
73.
93 E8 B9 D5 A2 E3 52 5D 5A A1 22 7F 0A 43 5B 54 36 B8 8D 8D 9C 9F 12 EC 0B EB 67 F8 E4 5D 82 3E
53 85 89 1C AC 11 77 4E 1D 98 CB 1E 5C B1 AC A5
74.
93 E8 B9 D5 A2 E3 52 5D 5A A1 22 7F 0A 43 5B 54 36 B8 8D 8D 9C 9F 12 EC 0B 0E 67 F8 E4 5D 82 3E
53 85 89 1C AC 11 77 4E 1D 98 CB 1E 5C B1 AC A5
75.
93 E8 B9 D5 A2 E3 52 5D 5A A1 22 7F 0A 43 5B 54 36 B8 8D 8D 9C 9F 12 EC 0B 0E 11 F8 E4 5D 82 3E
53 85 89 1C AC 11 77 4E 1D 98 CB 1E 5C B1 AC A5
76.
93 E8 B9 D5 A2 E3 52 5D 5A A1 22 7F 0A 43 5B 54 36 B8 8D 8D 9C 9F 12 EC 0B 0E 11 97 E4 5D 82 3E
53 85 89 1C AC 11 77 4E 1D 98 CB 1E 5C B1 AC A5
77.
93 E8 B9 D5 A2 E3 52 5D 5A A1 22 7F 0A 43 5B 54 36 B8 8D 8D 9C 9F 12 EC 0B 0E 11 97 D2 5D 82 3E
53 85 89 1C AC 11 77 4E 1D 98 CB 1E 5C B1 AC A5
78.
93 E8 B9 D5 A2 E3 52 5D 5A A1 22 7F 0A 43 5B 54 36 B8 8D 8D 9C 9F 12 EC 0B 0E 11 97 D2 56 82 3E
53 85 89 1C AC 11 77 4E 1D 98 CB 1E 5C B1 AC A5
79.
93 E8 B9 D5 A2 E3 52 5D 5A A1 22 7F 0A 43 5B 54 36 B8 8D 8D 9C 9F 12 EC 0B 0E 11 97 D2 56 6D 3E
53 85 89 1C AC 11 77 4E 1D 98 CB 1E 5C B1 AC A5
80.
93 E8 B9 D5 A2 E3 52 5D 5A A1 22 7F 0A 43 5B 54 36 B8 8D 8D 9C 9F 12 EC 0B 0E 11 97 D2 56 6D F9
53 85 89 1C AC 11 77 4E 1D 98 CB 1E 5C B1 AC A5
81.
93 E8 B9 D5 A2 E3 52 5D 5A A1 22 7F 0A 43 5B 54 36 B8 8D 8D 9C 9F 12 EC 0B 0E 11 97 D2 56 6D F9
B4 85 89 1C AC 11 77 4E 1D 98 CB 1E 5C B1 AC A5
82.
93 E8 B9 D5 A2 E3 52 5D 5A A1 22 7F 0A 43 5B 54 36 B8 8D 8D 9C 9F 12 EC 0B 0E 11 97 D2 56 6D F9
B4 78 89 1C AC 11 77 4E 1D 98 CB 1E 5C B1 AC A5
83.
93 E8 B9 D5 A2 E3 52 5D 5A A1 22 7F 0A 43 5B 54 36 B8 8D 8D 9C 9F 12 EC 0B 0E 11 97 D2 56 6D F9
B4 78 84 1C AC 11 77 4E 1D 98 CB 1E 5C B1 AC A5

84.
93 E8 B9 D5 A2 E3 52 5D 5A A1 22 7F 0A 43 5B 54 36 B8 8D 8D 9C 9F 12 EC 0B 0E 11 97 D2 56 6D F9 B4 78 84 38 AC 11 77 4E 1D 98 CB 1E 5C B1 AC A5
85.
93 E8 B9 D5 A2 E3 52 5D 5A A1 22 7F 0A 43 5B 54 36 B8 8D 8D 9C 9F 12 EC 0B 0E 11 97 D2 56 6D F9 B4 78 84 38 B7 11 77 4E 1D 98 CB 1E 5C B1 AC A5
86.
93 E8 B9 D5 A2 E3 52 5D 5A A1 22 7F 0A 43 5B 54 36 B8 8D 8D 9C 9F 12 EC 0B 0E 11 97 D2 56 6D F9 B4 78 84 38 B7 9F 77 4E 1D 98 CB 1E 5C B1 AC A5
87.
93 E8 B9 D5 A2 E3 52 5D 5A A1 22 7F 0A 43 5B 54 36 B8 8D 8D 9C 9F 12 EC 0B 0E 11 97 D2 56 6D F9 B4 78 84 38 B7 9F 3D 4E 1D 98 CB 1E 5C B1 AC A5
88.
93 E8 B9 D5 A2 E3 52 5D 5A A1 22 7F 0A 43 5B 54 36 B8 8D 8D 9C 9F 12 EC 0B 0E 11 97 D2 56 6D F9 B4 78 84 38 B7 9F 3D E6 1D 98 CB 1E 5C B1 AC A5
89.
93 E8 B9 D5 A2 E3 52 5D 5A A1 22 7F 0A 43 5B 54 36 B8 8D 8D 9C 9F 12 EC 0B 0E 11 97 D2 56 6D F9 B4 78 84 38 B7 9F 3D E6 49 98 CB 1E 5C B1 AC A5
90.
93 E8 B9 D5 A2 E3 52 5D 5A A1 22 7F 0A 43 5B 54 36 B8 8D 8D 9C 9F 12 EC 0B 0E 11 97 D2 56 6D F9 B4 78 84 38 B7 9F 3D E6 49 EF CB 1E 5C B1 AC A5
91.
93 E8 B9 D5 A2 E3 52 5D 5A A1 22 7F 0A 43 5B 54 36 B8 8D 8D 9C 9F 12 EC 0B 0E 11 97 D2 56 6D F9 B4 78 84 38 B7 9F 3D E6 49 EF AE 1E 5C B1 AC A5
92.
93 E8 B9 D5 A2 E3 52 5D 5A A1 22 7F 0A 43 5B 54 36 B8 8D 8D 9C 9F 12 EC 0B 0E 11 97 D2 56 6D F9 B4 78 84 38 B7 9F 3D E6 49 EF AE 7D 5C B1 AC A5
93.
93 E8 B9 D5 A2 E3 52 5D 5A A1 22 7F 0A 43 5B 54 36 B8 8D 8D 9C 9F 12 EC 0B 0E 11 97 D2 56 6D F9 B4 78 84 38 B7 9F 3D E6 49 EF AE 7D DB B1 AC A5
94.
93 E8 B9 D5 A2 E3 52 5D 5A A1 22 7F 0A 43 5B 54 36 B8 8D 8D 9C 9F 12 EC 0B 0E 11 97 D2 56 6D F9 B4 78 84 38 B7 9F 3D E6 49 EF AE 7D DB 04 AC A5
95.
93 E8 B9 D5 A2 E3 52 5D 5A A1 22 7F 0A 43 5B 54 36 B8 8D 8D 9C 9F 12 EC 0B 0E 11 97 D2 56 6D F9 B4 78 84 38 B7 9F 3D E6 49 EF AE 7D DB 04 4D A5
96.
93 E8 B9 D5 A2 E3 52 5D 5A A1 22 7F 0A 43 5B 54 36 B8 8D 8D 9C 9F 12 EC 0B 0E 11 97 D2 56 6D F9 B4 78 84 38 B7 9F 3D E6 49 EF AE 7D DB 04 4D 6B
97.
43 E8 B9 D5 A2 E3 52 5D 5A A1 22 7F 0A 43 5B 54 36 B8 8D 8D 9C 9F 12 EC 0B 0E 11 97 D2 56 6D F9 B4 78 84 38 B7 9F 3D E6 49 EF AE 7D DB 04 4D 6B
98.
43 FB B9 D5 A2 E3 52 5D 5A A1 22 7F 0A 43 5B 54 36 B8 8D 8D 9C 9F 12 EC 0B 0E 11 97 D2 56 6D F9 B4 78 84 38 B7 9F 3D E6 49 EF AE 7D DB 04 4D 6B
99.
43 FB 8E D5 A2 E3 52 5D 5A A1 22 7F 0A 43 5B 54 36 B8 8D 8D 9C 9F 12 EC 0B 0E 11 97 D2 56 6D F9 B4 78 84 38 B7 9F 3D E6 49 EF AE 7D DB 04 4D 6B
100.
43 FB 8E 57 A2 E3 52 5D 5A A1 22 7F 0A 43 5B 54 36 B8 8D 8D 9C 9F 12 EC 0B 0E 11 97 D2 56 6D F9 B4 78 84 38 B7 9F 3D E6 49 EF AE 7D DB 04 4D 6B
101.
43 FB 8E 57 92 E3 52 5D 5A A1 22 7F 0A 43 5B 54 36 B8 8D 8D 9C 9F 12 EC 0B 0E 11 97 D2 56 6D F9 B4 78 84 38 B7 9F 3D E6 49 EF AE 7D DB 04 4D 6B
102.
43 FB 8E 57 92 AA 52 5D 5A A1 22 7F 0A 43 5B 54 36 B8 8D 8D 9C 9F 12 EC 0B 0E 11 97 D2 56 6D F9 B4 78 84 38 B7 9F 3D E6 49 EF AE 7D DB 04 4D 6B
103.
43 FB 8E 57 92 AA 02 5D 5A A1 22 7F 0A 43 5B 54 36 B8 8D 8D 9C 9F 12 EC 0B 0E 11 97 D2 56 6D F9 B4 78 84 38 B7 9F 3D E6 49 EF AE 7D DB 04 4D 6B
104.
43 FB 8E 57 92 AA 02 BA 5A A1 22 7F 0A 43 5B 54 36 B8 8D 8D 9C 9F 12 EC 0B 0E 11 97 D2 56 6D F9 B4 78 84 38 B7 9F 3D E6 49 EF AE 7D DB 04 4D 6B
105.
43 FB 8E 57 92 AA 02 BA AC A1 22 7F 0A 43 5B 54 36 B8 8D 8D 9C 9F 12 EC 0B 0E 11 97 D2 56 6D F9 B4 78 84 38 B7 9F 3D E6 49 EF AE 7D DB 04 4D 6B
106.
43 FB 8E 57 92 AA 02 BA AC 19 22 7F 0A 43 5B 54 36 B8 8D 8D 9C 9F 12 EC 0B 0E 11 97 D2 56 6D F9 B4 78 84 38 B7 9F 3D E6 49 EF AE 7D DB 04 4D 6B
107.
43 FB 8E 57 92 AA 02 BA AC 19 7E 7F 0A 43 5B 54 36 B8 8D 8D 9C 9F 12 EC 0B 0E 11 97 D2 56 6D F9 B4 78 84 38 B7 9F 3D E6 49 EF AE 7D DB 04 4D 6B
108.
43 FB 8E 57 92 AA 02 BA AC 19 7E B7 0A 43 5B 54 36 B8 8D 8D 9C 9F 12 EC 0B 0E 11 97 D2 56 6D F9

B4 78 84 38 B7 9F 3D E6 49 EF AE 7D DB 04 4D 6B
109.
43 FB 8E 57 92 AA 02 BA AC 19 7E B7 00 43 5B 54 36 B8 8D 8D 9C 9F 12 EC 0B 0E 11 97 D2 56 6D F9
B4 78 84 38 B7 9F 3D E6 49 EF AE 7D DB 04 4D 6B
110.
43 FB 8E 57 92 AA 02 BA AC 19 7E B7 00 91 5B 54 36 B8 8D 8D 9C 9F 12 EC 0B 0E 11 97 D2 56 6D F9
B4 78 84 38 B7 9F 3D E6 49 EF AE 7D DB 04 4D 6B
111.
43 FB 8E 57 92 AA 02 BA AC 19 7E B7 00 91 5C 54 36 B8 8D 8D 9C 9F 12 EC 0B 0E 11 97 D2 56 6D F9
B4 78 84 38 B7 9F 3D E6 49 EF AE 7D DB 04 4D 6B
112.
43 FB 8E 57 92 AA 02 BA AC 19 7E B7 00 91 5C F3 36 B8 8D 8D 9C 9F 12 EC 0B 0E 11 97 D2 56 6D F9
B4 78 84 38 B7 9F 3D E6 49 EF AE 7D DB 04 4D 6B
113.
43 FB 8E 57 92 AA 02 BA AC 19 7E B7 00 91 5C F3 A4 B8 8D 8D 9C 9F 12 EC 0B 0E 11 97 D2 56 6D F9
B4 78 84 38 B7 9F 3D E6 49 EF AE 7D DB 04 4D 6B
114.
43 FB 8E 57 92 AA 02 BA AC 19 7E B7 00 91 5C F3 A4 44 8D 8D 9C 9F 12 EC 0B 0E 11 97 D2 56 6D F9
B4 78 84 38 B7 9F 3D E6 49 EF AE 7D DB 04 4D 6B
115.
43 FB 8E 57 92 AA 02 BA AC 19 7E B7 00 91 5C F3 A4 44 50 8D 9C 9F 12 EC 0B 0E 11 97 D2 56 6D F9
B4 78 84 38 B7 9F 3D E6 49 EF AE 7D DB 04 4D 6B
116.
43 FB 8E 57 92 AA 02 BA AC 19 7E B7 00 91 5C F3 A4 44 50 B9 9C 9F 12 EC 0B 0E 11 97 D2 56 6D F9
B4 78 84 38 B7 9F 3D E6 49 EF AE 7D DB 04 4D 6B
117.
43 FB 8E 57 92 AA 02 BA AC 19 7E B7 00 91 5C F3 A4 44 50 B9 97 9F 12 EC 0B 0E 11 97 D2 56 6D F9
B4 78 84 38 B7 9F 3D E6 49 EF AE 7D DB 04 4D 6B
118.
43 FB 8E 57 92 AA 02 BA AC 19 7E B7 00 91 5C F3 A4 44 50 B9 97 F6 12 EC 0B 0E 11 97 D2 56 6D F9
B4 78 84 38 B7 9F 3D E6 49 EF AE 7D DB 04 4D 6B
119.
43 FB 8E 57 92 AA 02 BA AC 19 7E B7 00 91 5C F3 A4 44 50 B9 97 F6 2F EC 0B 0E 11 97 D2 56 6D F9
B4 78 84 38 B7 9F 3D E6 49 EF AE 7D DB 04 4D 6B
120.
43 FB 8E 57 92 AA 02 BA AC 19 7E B7 00 91 5C F3 A4 44 50 B9 97 F6 2F 97 0B 0E 11 97 D2 56 6D F9
B4 78 84 38 B7 9F 3D E6 49 EF AE 7D DB 04 4D 6B
121.
43 FB 8E 57 92 AA 02 BA AC 19 7E B7 00 91 5C F3 A4 44 50 B9 97 F6 2F 97 2A 0E 11 97 D2 56 6D F9
B4 78 84 38 B7 9F 3D E6 49 EF AE 7D DB 04 4D 6B
122.
43 FB 8E 57 92 AA 02 BA AC 19 7E B7 00 91 5C F3 A4 44 50 B9 97 F6 2F 97 2A CE 11 97 D2 56 6D F9
B4 78 84 38 B7 9F 3D E6 49 EF AE 7D DB 04 4D 6B
123.
43 FB 8E 57 92 AA 02 BA AC 19 7E B7 00 91 5C F3 A4 44 50 B9 97 F6 2F 97 2A CE 15 97 D2 56 6D F9
B4 78 84 38 B7 9F 3D E6 49 EF AE 7D DB 04 4D 6B
124.
43 FB 8E 57 92 AA 02 BA AC 19 7E B7 00 91 5C F3 A4 44 50 B9 97 F6 2F 97 2A CE 15 8A D2 56 6D F9
B4 78 84 38 B7 9F 3D E6 49 EF AE 7D DB 04 4D 6B
125.
43 FB 8E 57 92 AA 02 BA AC 19 7E B7 00 91 5C F3 A4 44 50 B9 97 F6 2F 97 2A CE 15 8A 91 56 6D F9
B4 78 84 38 B7 9F 3D E6 49 EF AE 7D DB 04 4D 6B
126.
43 FB 8E 57 92 AA 02 BA AC 19 7E B7 00 91 5C F3 A4 44 50 B9 97 F6 2F 97 2A CE 15 8A 91 8F 6D F9
B4 78 84 38 B7 9F 3D E6 49 EF AE 7D DB 04 4D 6B
127.
43 FB 8E 57 92 AA 02 BA AC 19 7E B7 00 91 5C F3 A4 44 50 B9 97 F6 2F 97 2A CE 15 8A 91 8F 8F F9
B4 78 84 38 B7 9F 3D E6 49 EF AE 7D DB 04 4D 6B
128.
43 FB 8E 57 92 AA 02 BA AC 19 7E B7 00 91 5C F3 A4 44 50 B9 97 F6 2F 97 2A CE 15 8A 91 8F 8F 78
B4 78 84 38 B7 9F 3D E6 49 EF AE 7D DB 04 4D 6B

Stage 2.

Input sequence

78 8F 8F 91 8A 15 CE 2A 97 2F F6 97 B9 50 44 A4 F3 5C 91 00 B7 7E 19 AC BA 02 AA 92 57 8E FB 43
6B 4D 04 DB 7D AE EF 49 E6 3D 9F B7 38 84 78 B4

Calculating SR state for stage 2. Total 48 steps.

1.
43 FB 8E 57 92 AA 02 BA AC 19 7E B7 00 91 5C F3 A4 44 50 B9 97 F6 2F 97 2A CE 15 8A 91 8F 8F 78

B4 78 84 38 B7 9F 3D E6 49 EF AE 7D DB 04 4D 6B
2.
43 FB 8E 57 92 AA 02 BA AC 19 7E B7 00 91 5C F3 A4 44 50 B9 97 F6 2F 97 2A CE 15 8A 91 8F 8F 78
B4 2A 84 38 B7 9F 3D E6 49 EF AE 7D DB 04 4D 6B
3.
43 FB 8E 57 92 AA 02 BA AC 19 7E B7 00 91 5C F3 A4 44 50 B9 97 F6 2F 97 2A CE 15 8A 91 8F 8F 78
B4 2A 11 38 B7 9F 3D E6 49 EF AE 7D DB 04 4D 6B
4.
43 FB 8E 57 92 AA 02 BA AC 19 7E B7 00 91 5C F3 A4 44 50 B9 97 F6 2F 97 2A CE 15 8A 91 8F 8F 78
B4 2A 11 7F B7 9F 3D E6 49 EF AE 7D DB 04 4D 6B
5.
43 FB 8E 57 92 AA 02 BA AC 19 7E B7 00 91 5C F3 A4 44 50 B9 97 F6 2F 97 2A CE 15 8A 91 8F 8F 78
B4 2A 11 7F 29 9F 3D E6 49 EF AE 7D DB 04 4D 6B
6.
43 FB 8E 57 92 AA 02 BA AC 19 7E B7 00 91 5C F3 A4 44 50 B9 97 F6 2F 97 2A CE 15 8A 91 8F 8F 78
B4 2A 11 7F 29 7F 3D E6 49 EF AE 7D DB 04 4D 6B
7.
43 FB 8E 57 92 AA 02 BA AC 19 7E B7 00 91 5C F3 A4 44 50 B9 97 F6 2F 97 2A CE 15 8A 91 8F 8F 78
B4 2A 11 7F 29 7F 76 E6 49 EF AE 7D DB 04 4D 6B
8.
43 FB 8E 57 92 AA 02 BA AC 19 7E B7 00 91 5C F3 A4 44 50 B9 97 F6 2F 97 2A CE 15 8A 91 8F 8F 78
B4 2A 11 7F 29 7F 76 64 49 EF AE 7D DB 04 4D 6B
9.
43 FB 8E 57 92 AA 02 BA AC 19 7E B7 00 91 5C F3 A4 44 50 B9 97 F6 2F 97 2A CE 15 8A 91 8F 8F 78
B4 2A 11 7F 29 7F 76 64 F3 EF AE 7D DB 04 4D 6B
10.
43 FB 8E 57 92 AA 02 BA AC 19 7E B7 00 91 5C F3 A4 44 50 B9 97 F6 2F 97 2A CE 15 8A 91 8F 8F 78
B4 2A 11 7F 29 7F 76 64 F3 8D AE 7D DB 04 4D 6B
11.
43 FB 8E 57 92 AA 02 BA AC 19 7E B7 00 91 5C F3 A4 44 50 B9 97 F6 2F 97 2A CE 15 8A 91 8F 8F 78
B4 2A 11 7F 29 7F 76 64 F3 8D 43 7D DB 04 4D 6B
12.
43 FB 8E 57 92 AA 02 BA AC 19 7E B7 00 91 5C F3 A4 44 50 B9 97 F6 2F 97 2A CE 15 8A 91 8F 8F 78
B4 2A 11 7F 29 7F 76 64 F3 8D 43 47 DB 04 4D 6B
13.
43 FB 8E 57 92 AA 02 BA AC 19 7E B7 00 91 5C F3 A4 44 50 B9 97 F6 2F 97 2A CE 15 8A 91 8F 8F 78
B4 2A 11 7F 29 7F 76 64 F3 8D 43 47 95 04 4D 6B
14.
43 FB 8E 57 92 AA 02 BA AC 19 7E B7 00 91 5C F3 A4 44 50 B9 97 F6 2F 97 2A CE 15 8A 91 8F 8F 78
B4 2A 11 7F 29 7F 76 64 F3 8D 43 47 95 CC 4D 6B
15.
43 FB 8E 57 92 AA 02 BA AC 19 7E B7 00 91 5C F3 A4 44 50 B9 97 F6 2F 97 2A CE 15 8A 91 8F 8F 78
B4 2A 11 7F 29 7F 76 64 F3 8D 43 47 95 CC 0B 6B
16.
43 FB 8E 57 92 AA 02 BA AC 19 7E B7 00 91 5C F3 A4 44 50 B9 97 F6 2F 97 2A CE 15 8A 91 8F 8F 78
B4 2A 11 7F 29 7F 76 64 F3 8D 43 47 95 CC 0B E2
17.
4F FB 8E 57 92 AA 02 BA AC 19 7E B7 00 91 5C F3 A4 44 50 B9 97 F6 2F 97 2A CE 15 8A 91 8F 8F 78
B4 2A 11 7F 29 7F 76 64 F3 8D 43 47 95 CC 0B E2
18.
4F 21 8E 57 92 AA 02 BA AC 19 7E B7 00 91 5C F3 A4 44 50 B9 97 F6 2F 97 2A CE 15 8A 91 8F 8F 78
B4 2A 11 7F 29 7F 76 64 F3 8D 43 47 95 CC 0B E2
19.
4F 21 B7 57 92 AA 02 BA AC 19 7E B7 00 91 5C F3 A4 44 50 B9 97 F6 2F 97 2A CE 15 8A 91 8F 8F 78
B4 2A 11 7F 29 7F 76 64 F3 8D 43 47 95 CC 0B E2
20.
4F 21 B7 03 92 AA 02 BA AC 19 7E B7 00 91 5C F3 A4 44 50 B9 97 F6 2F 97 2A CE 15 8A 91 8F 8F 78
B4 2A 11 7F 29 7F 76 64 F3 8D 43 47 95 CC 0B E2
21.
4F 21 B7 03 2B AA 02 BA AC 19 7E B7 00 91 5C F3 A4 44 50 B9 97 F6 2F 97 2A CE 15 8A 91 8F 8F 78
B4 2A 11 7F 29 7F 76 64 F3 8D 43 47 95 CC 0B E2
22.
4F 21 B7 03 2B 76 02 BA AC 19 7E B7 00 91 5C F3 A4 44 50 B9 97 F6 2F 97 2A CE 15 8A 91 8F 8F 78
B4 2A 11 7F 29 7F 76 64 F3 8D 43 47 95 CC 0B E2
23.
4F 21 B7 03 2B 76 3E BA AC 19 7E B7 00 91 5C F3 A4 44 50 B9 97 F6 2F 97 2A CE 15 8A 91 8F 8F 78
B4 2A 11 7F 29 7F 76 64 F3 8D 43 47 95 CC 0B E2
24.
4F 21 B7 03 2B 76 3E D5 AC 19 7E B7 00 91 5C F3 A4 44 50 B9 97 F6 2F 97 2A CE 15 8A 91 8F 8F 78
B4 2A 11 7F 29 7F 76 64 F3 8D 43 47 95 CC 0B E2
25.
4F 21 B7 03 2B 76 3E D5 7B 19 7E B7 00 91 5C F3 A4 44 50 B9 97 F6 2F 97 2A CE 15 8A 91 8F 8F 78
B4 2A 11 7F 29 7F 76 64 F3 8D 43 47 95 CC 0B E2
26.

4F 21 B7 03 2B 76 3E D5 7B D9 7E B7 00 91 5C F3 A4 44 50 B9 97 F6 2F 97 2A CE 15 8A 91 8F 8F 78
B4 2A 11 7F 29 7F 76 64 F3 8D 43 47 95 CC 0B E2
27.
4F 21 B7 03 2B 76 3E D5 7B D9 85 B7 00 91 5C F3 A4 44 50 B9 97 F6 2F 97 2A CE 15 8A 91 8F 8F 78
B4 2A 11 7F 29 7F 76 64 F3 8D 43 47 95 CC 0B E2
28.
4F 21 B7 03 2B 76 3E D5 7B D9 85 56 00 91 5C F3 A4 44 50 B9 97 F6 2F 97 2A CE 15 8A 91 8F 8F 78
B4 2A 11 7F 29 7F 76 64 F3 8D 43 47 95 CC 0B E2
29.
4F 21 B7 03 2B 76 3E D5 7B D9 85 56 50 91 5C F3 A4 44 50 B9 97 F6 2F 97 2A CE 15 8A 91 8F 8F 78
B4 2A 11 7F 29 7F 76 64 F3 8D 43 47 95 CC 0B E2
30.
4F 21 B7 03 2B 76 3E D5 7B D9 85 56 50 A0 5C F3 A4 44 50 B9 97 F6 2F 97 2A CE 15 8A 91 8F 8F 78
B4 2A 11 7F 29 7F 76 64 F3 8D 43 47 95 CC 0B E2
31.
4F 21 B7 03 2B 76 3E D5 7B D9 85 56 50 A0 72 F3 A4 44 50 B9 97 F6 2F 97 2A CE 15 8A 91 8F 8F 78
B4 2A 11 7F 29 7F 76 64 F3 8D 43 47 95 CC 0B E2
32.
4F 21 B7 03 2B 76 3E D5 7B D9 85 56 50 A0 72 0A A4 44 50 B9 97 F6 2F 97 2A CE 15 8A 91 8F 8F 78
B4 2A 11 7F 29 7F 76 64 F3 8D 43 47 95 CC 0B E2
33.
4F 21 B7 03 2B 76 3E D5 7B D9 85 56 50 A0 72 0A 59 44 50 B9 97 F6 2F 97 2A CE 15 8A 91 8F 8F 78
B4 2A 11 7F 29 7F 76 64 F3 8D 43 47 95 CC 0B E2
34.
4F 21 B7 03 2B 76 3E D5 7B D9 85 56 50 A0 72 0A 59 B8 50 B9 97 F6 2F 97 2A CE 15 8A 91 8F 8F 78
B4 2A 11 7F 29 7F 76 64 F3 8D 43 47 95 CC 0B E2
35.
4F 21 B7 03 2B 76 3E D5 7B D9 85 56 50 A0 72 0A 59 B8 1D B9 97 F6 2F 97 2A CE 15 8A 91 8F 8F 78
B4 2A 11 7F 29 7F 76 64 F3 8D 43 47 95 CC 0B E2
36.
4F 21 B7 03 2B 76 3E D5 7B D9 85 56 50 A0 72 0A 59 B8 1D 5E 97 F6 2F 97 2A CE 15 8A 91 8F 8F 78
B4 2A 11 7F 29 7F 76 64 F3 8D 43 47 95 CC 0B E2
37.
4F 21 B7 03 2B 76 3E D5 7B D9 85 56 50 A0 72 0A 59 B8 1D 5E 4A F6 2F 97 2A CE 15 8A 91 8F 8F 78
B4 2A 11 7F 29 7F 76 64 F3 8D 43 47 95 CC 0B E2
38.
4F 21 B7 03 2B 76 3E D5 7B D9 85 56 50 A0 72 0A 59 B8 1D 5E 4A E1 2F 97 2A CE 15 8A 91 8F 8F 78
B4 2A 11 7F 29 7F 76 64 F3 8D 43 47 95 CC 0B E2
39.
4F 21 B7 03 2B 76 3E D5 7B D9 85 56 50 A0 72 0A 59 B8 1D 5E 4A E1 9A 97 2A CE 15 8A 91 8F 8F 78
B4 2A 11 7F 29 7F 76 64 F3 8D 43 47 95 CC 0B E2
40.
4F 21 B7 03 2B 76 3E D5 7B D9 85 56 50 A0 72 0A 59 B8 1D 5E 4A E1 9A 12 2A CE 15 8A 91 8F 8F 78
B4 2A 11 7F 29 7F 76 64 F3 8D 43 47 95 CC 0B E2
41.
4F 21 B7 03 2B 76 3E D5 7B D9 85 56 50 A0 72 0A 59 B8 1D 5E 4A E1 9A 12 1F CE 15 8A 91 8F 8F 78
B4 2A 11 7F 29 7F 76 64 F3 8D 43 47 95 CC 0B E2
42.
4F 21 B7 03 2B 76 3E D5 7B D9 85 56 50 A0 72 0A 59 B8 1D 5E 4A E1 9A 12 1F 41 15 8A 91 8F 8F 78
B4 2A 11 7F 29 7F 76 64 F3 8D 43 47 95 CC 0B E2
43.
4F 21 B7 03 2B 76 3E D5 7B D9 85 56 50 A0 72 0A 59 B8 1D 5E 4A E1 9A 12 1F 41 1C 8A 91 8F 8F 78
B4 2A 11 7F 29 7F 76 64 F3 8D 43 47 95 CC 0B E2
44.
4F 21 B7 03 2B 76 3E D5 7B D9 85 56 50 A0 72 0A 59 B8 1D 5E 4A E1 9A 12 1F 41 1C 6C 91 8F 8F 78
B4 2A 11 7F 29 7F 76 64 F3 8D 43 47 95 CC 0B E2
45.
4F 21 B7 03 2B 76 3E D5 7B D9 85 56 50 A0 72 0A 59 B8 1D 5E 4A E1 9A 12 1F 41 1C 6C 3E 8F 8F 78
B4 2A 11 7F 29 7F 76 64 F3 8D 43 47 95 CC 0B E2
46.
4F 21 B7 03 2B 76 3E D5 7B D9 85 56 50 A0 72 0A 59 B8 1D 5E 4A E1 9A 12 1F 41 1C 6C 3E 36 8F 78
B4 2A 11 7F 29 7F 76 64 F3 8D 43 47 95 CC 0B E2
47.
4F 21 B7 03 2B 76 3E D5 7B D9 85 56 50 A0 72 0A 59 B8 1D 5E 4A E1 9A 12 1F 41 1C 6C 3E 36 CD 78
B4 2A 11 7F 29 7F 76 64 F3 8D 43 47 95 CC 0B E2
48.
4F 21 B7 03 2B 76 3E D5 7B D9 85 56 50 A0 72 0A 59 B8 1D 5E 4A E1 9A 12 1F 41 1C 6C 3E 36 CD 86
B4 2A 11 7F 29 7F 76 64 F3 8D 43 47 95 CC 0B E2

Stage 3.

Input sequence

78 8F 8F 91 8A 15 CE 2A 97 2F F6 97 B9 50 44 A4 F3 5C 91 00 B7 7E 19 AC BA 02 AA 92 57 8E FB 43 6B 4D 04 DB 7D AE EF 49 E6 3D 9F B7 38 84 78 B4

Calculating SR state for stage 3. Total 48 steps.

1.
4F 21 B7 03 2B 76 3E D5 7B D9 85 56 50 A0 72 0A 59 B8 1D 5E 4A E1 9A 12 1F 41 1C 6C 3E 36 CD 86 0C 2A 11 7F 29 7F 76 64 F3 8D 43 47 95 CC 0B E2
2.
4F 21 B7 03 2B 76 3E D5 7B D9 85 56 50 A0 72 0A 59 B8 1D 5E 4A E1 9A 12 1F 41 1C 6C 3E 36 CD 86 0C 1A 11 7F 29 7F 76 64 F3 8D 43 47 95 CC 0B E2
3.
4F 21 B7 03 2B 76 3E D5 7B D9 85 56 50 A0 72 0A 59 B8 1D 5E 4A E1 9A 12 1F 41 1C 6C 3E 36 CD 86 0C 1A 0E 7F 29 7F 76 64 F3 8D 43 47 95 CC 0B E2
4.
4F 21 B7 03 2B 76 3E D5 7B D9 85 56 50 A0 72 0A 59 B8 1D 5E 4A E1 9A 12 1F 41 1C 6C 3E 36 CD 86 0C 1A 0E C6 29 7F 76 64 F3 8D 43 47 95 CC 0B E2
5.
4F 21 B7 03 2B 76 3E D5 7B D9 85 56 50 A0 72 0A 59 B8 1D 5E 4A E1 9A 12 1F 41 1C 6C 3E 36 CD 86 0C 1A 0E C6 62 7F 76 64 F3 8D 43 47 95 CC 0B E2
6.
4F 21 B7 03 2B 76 3E D5 7B D9 85 56 50 A0 72 0A 59 B8 1D 5E 4A E1 9A 12 1F 41 1C 6C 3E 36 CD 86 0C 1A 0E C6 62 65 76 64 F3 8D 43 47 95 CC 0B E2
7.
4F 21 B7 03 2B 76 3E D5 7B D9 85 56 50 A0 72 0A 59 B8 1D 5E 4A E1 9A 12 1F 41 1C 6C 3E 36 CD 86 0C 1A 0E C6 62 65 8D 64 F3 8D 43 47 95 CC 0B E2
8.
4F 21 B7 03 2B 76 3E D5 7B D9 85 56 50 A0 72 0A 59 B8 1D 5E 4A E1 9A 12 1F 41 1C 6C 3E 36 CD 86 0C 1A 0E C6 62 65 8D EA F3 8D 43 47 95 CC 0B E2
9.
4F 21 B7 03 2B 76 3E D5 7B D9 85 56 50 A0 72 0A 59 B8 1D 5E 4A E1 9A 12 1F 41 1C 6C 3E 36 CD 86 0C 1A 0E C6 62 65 8D EA A8 8D 43 47 95 CC 0B E2
10.
4F 21 B7 03 2B 76 3E D5 7B D9 85 56 50 A0 72 0A 59 B8 1D 5E 4A E1 9A 12 1F 41 1C 6C 3E 36 CD 86 0C 1A 0E C6 62 65 8D EA A8 B8 43 47 95 CC 0B E2
11.
4F 21 B7 03 2B 76 3E D5 7B D9 85 56 50 A0 72 0A 59 B8 1D 5E 4A E1 9A 12 1F 41 1C 6C 3E 36 CD 86 0C 1A 0E C6 62 65 8D EA A8 B8 67 47 95 CC 0B E2
12.
4F 21 B7 03 2B 76 3E D5 7B D9 85 56 50 A0 72 0A 59 B8 1D 5E 4A E1 9A 12 1F 41 1C 6C 3E 36 CD 86 0C 1A 0E C6 62 65 8D EA A8 B8 67 CD 95 CC 0B E2
13.
4F 21 B7 03 2B 76 3E D5 7B D9 85 56 50 A0 72 0A 59 B8 1D 5E 4A E1 9A 12 1F 41 1C 6C 3E 36 CD 86 0C 1A 0E C6 62 65 8D EA A8 B8 67 CD CA CC 0B E2
14.
4F 21 B7 03 2B 76 3E D5 7B D9 85 56 50 A0 72 0A 59 B8 1D 5E 4A E1 9A 12 1F 41 1C 6C 3E 36 CD 86 0C 1A 0E C6 62 65 8D EA A8 B8 67 CD CA 7E 0B E2
15.
4F 21 B7 03 2B 76 3E D5 7B D9 85 56 50 A0 72 0A 59 B8 1D 5E 4A E1 9A 12 1F 41 1C 6C 3E 36 CD 86 0C 1A 0E C6 62 65 8D EA A8 B8 67 CD CA 7E FC E2
16.
4F 21 B7 03 2B 76 3E D5 7B D9 85 56 50 A0 72 0A 59 B8 1D 5E 4A E1 9A 12 1F 41 1C 6C 3E 36 CD 86 0C 1A 0E C6 62 65 8D EA A8 B8 67 CD CA 7E FC 39
17.
4B 21 B7 03 2B 76 3E D5 7B D9 85 56 50 A0 72 0A 59 B8 1D 5E 4A E1 9A 12 1F 41 1C 6C 3E 36 CD 86 0C 1A 0E C6 62 65 8D EA A8 B8 67 CD CA 7E FC 39
18.
4B 8D B7 03 2B 76 3E D5 7B D9 85 56 50 A0 72 0A 59 B8 1D 5E 4A E1 9A 12 1F 41 1C 6C 3E 36 CD 86 0C 1A 0E C6 62 65 8D EA A8 B8 67 CD CA 7E FC 39
19.
4B 8D 01 03 2B 76 3E D5 7B D9 85 56 50 A0 72 0A 59 B8 1D 5E 4A E1 9A 12 1F 41 1C 6C 3E 36 CD 86 0C 1A 0E C6 62 65 8D EA A8 B8 67 CD CA 7E FC 39
20.
4B 8D 01 D7 2B 76 3E D5 7B D9 85 56 50 A0 72 0A 59 B8 1D 5E 4A E1 9A 12 1F 41 1C 6C 3E 36 CD 86 0C 1A 0E C6 62 65 8D EA A8 B8 67 CD CA 7E FC 39
21.
4B 8D 01 D7 74 76 3E D5 7B D9 85 56 50 A0 72 0A 59 B8 1D 5E 4A E1 9A 12 1F 41 1C 6C 3E 36 CD 86 0C 1A 0E C6 62 65 8D EA A8 B8 67 CD CA 7E FC 39
22.
4B 8D 01 D7 74 E1 3E D5 7B D9 85 56 50 A0 72 0A 59 B8 1D 5E 4A E1 9A 12 1F 41 1C 6C 3E 36 CD 86 0C 1A 0E C6 62 65 8D EA A8 B8 67 CD CA 7E FC 39
23.

4B 8D 01 D7 74 E1 42 D5 7B D9 85 56 50 A0 72 0A 59 B8 1D 5E 4A E1 9A 12 1F 41 1C 6C 3E 36 CD 86
0C 1A 0E C6 62 65 8D EA A8 B8 67 CD CA 7E FC 39
24.
4B 8D 01 D7 74 E1 42 54 7B D9 85 56 50 A0 72 0A 59 B8 1D 5E 4A E1 9A 12 1F 41 1C 6C 3E 36 CD 86
0C 1A 0E C6 62 65 8D EA A8 B8 67 CD CA 7E FC 39
25.
4B 8D 01 D7 74 E1 42 54 CA D9 85 56 50 A0 72 0A 59 B8 1D 5E 4A E1 9A 12 1F 41 1C 6C 3E 36 CD 86
0C 1A 0E C6 62 65 8D EA A8 B8 67 CD CA 7E FC 39
26.
4B 8D 01 D7 74 E1 42 54 CA C3 85 56 50 A0 72 0A 59 B8 1D 5E 4A E1 9A 12 1F 41 1C 6C 3E 36 CD 86
0C 1A 0E C6 62 65 8D EA A8 B8 67 CD CA 7E FC 39
27.
4B 8D 01 D7 74 E1 42 54 CA C3 2A 56 50 A0 72 0A 59 B8 1D 5E 4A E1 9A 12 1F 41 1C 6C 3E 36 CD 86
0C 1A 0E C6 62 65 8D EA A8 B8 67 CD CA 7E FC 39
28.
4B 8D 01 D7 74 E1 42 54 CA C3 2A A7 50 A0 72 0A 59 B8 1D 5E 4A E1 9A 12 1F 41 1C 6C 3E 36 CD 86
0C 1A 0E C6 62 65 8D EA A8 B8 67 CD CA 7E FC 39
29.
4B 8D 01 D7 74 E1 42 54 CA C3 2A A7 E0 A0 72 0A 59 B8 1D 5E 4A E1 9A 12 1F 41 1C 6C 3E 36 CD 86
0C 1A 0E C6 62 65 8D EA A8 B8 67 CD CA 7E FC 39
30.
4B 8D 01 D7 74 E1 42 54 CA C3 2A A7 E0 37 72 0A 59 B8 1D 5E 4A E1 9A 12 1F 41 1C 6C 3E 36 CD 86
0C 1A 0E C6 62 65 8D EA A8 B8 67 CD CA 7E FC 39
31.
4B 8D 01 D7 74 E1 42 54 CA C3 2A A7 E0 37 1C 0A 59 B8 1D 5E 4A E1 9A 12 1F 41 1C 6C 3E 36 CD 86
0C 1A 0E C6 62 65 8D EA A8 B8 67 CD CA 7E FC 39
32.
4B 8D 01 D7 74 E1 42 54 CA C3 2A A7 E0 37 1C 2F 59 B8 1D 5E 4A E1 9A 12 1F 41 1C 6C 3E 36 CD 86
0C 1A 0E C6 62 65 8D EA A8 B8 67 CD CA 7E FC 39
33.
4B 8D 01 D7 74 E1 42 54 CA C3 2A A7 E0 37 1C 2F 30 B8 1D 5E 4A E1 9A 12 1F 41 1C 6C 3E 36 CD 86
0C 1A 0E C6 62 65 8D EA A8 B8 67 CD CA 7E FC 39
34.
4B 8D 01 D7 74 E1 42 54 CA C3 2A A7 E0 37 1C 2F 30 87 1D 5E 4A E1 9A 12 1F 41 1C 6C 3E 36 CD 86
0C 1A 0E C6 62 65 8D EA A8 B8 67 CD CA 7E FC 39
35.
4B 8D 01 D7 74 E1 42 54 CA C3 2A A7 E0 37 1C 2F 30 87 45 5E 4A E1 9A 12 1F 41 1C 6C 3E 36 CD 86
0C 1A 0E C6 62 65 8D EA A8 B8 67 CD CA 7E FC 39
36.
4B 8D 01 D7 74 E1 42 54 CA C3 2A A7 E0 37 1C 2F 30 87 45 1C 4A E1 9A 12 1F 41 1C 6C 3E 36 CD 86
0C 1A 0E C6 62 65 8D EA A8 B8 67 CD CA 7E FC 39
37.
4B 8D 01 D7 74 E1 42 54 CA C3 2A A7 E0 37 1C 2F 30 87 45 1C 0D E1 9A 12 1F 41 1C 6C 3E 36 CD 86
0C 1A 0E C6 62 65 8D EA A8 B8 67 CD CA 7E FC 39
38.
4B 8D 01 D7 74 E1 42 54 CA C3 2A A7 E0 37 1C 2F 30 87 45 1C 0D 76 9A 12 1F 41 1C 6C 3E 36 CD 86
0C 1A 0E C6 62 65 8D EA A8 B8 67 CD CA 7E FC 39
39.
4B 8D 01 D7 74 E1 42 54 CA C3 2A A7 E0 37 1C 2F 30 87 45 1C 0D 76 93 12 1F 41 1C 6C 3E 36 CD 86
0C 1A 0E C6 62 65 8D EA A8 B8 67 CD CA 7E FC 39
40.
4B 8D 01 D7 74 E1 42 54 CA C3 2A A7 E0 37 1C 2F 30 87 45 1C 0D 76 93 CE 1F 41 1C 6C 3E 36 CD 86
0C 1A 0E C6 62 65 8D EA A8 B8 67 CD CA 7E FC 39
41.
4B 8D 01 D7 74 E1 42 54 CA C3 2A A7 E0 37 1C 2F 30 87 45 1C 0D 76 93 CE EF 41 1C 6C 3E 36 CD 86
0C 1A 0E C6 62 65 8D EA A8 B8 67 CD CA 7E FC 39
42.
4B 8D 01 D7 74 E1 42 54 CA C3 2A A7 E0 37 1C 2F 30 87 45 1C 0D 76 93 CE EF B6 1C 6C 3E 36 CD 86
0C 1A 0E C6 62 65 8D EA A8 B8 67 CD CA 7E FC 39
43.
4B 8D 01 D7 74 E1 42 54 CA C3 2A A7 E0 37 1C 2F 30 87 45 1C 0D 76 93 CE EF B6 CD 6C 3E 36 CD 86
0C 1A 0E C6 62 65 8D EA A8 B8 67 CD CA 7E FC 39
44.
4B 8D 01 D7 74 E1 42 54 CA C3 2A A7 E0 37 1C 2F 30 87 45 1C 0D 76 93 CE EF B6 CD 12 3E 36 CD 86
0C 1A 0E C6 62 65 8D EA A8 B8 67 CD CA 7E FC 39
45.
4B 8D 01 D7 74 E1 42 54 CA C3 2A A7 E0 37 1C 2F 30 87 45 1C 0D 76 93 CE EF B6 CD 12 14 36 CD 86
0C 1A 0E C6 62 65 8D EA A8 B8 67 CD CA 7E FC 39
46.
4B 8D 01 D7 74 E1 42 54 CA C3 2A A7 E0 37 1C 2F 30 87 45 1C 0D 76 93 CE EF B6 CD 12 14 97 CD 86
0C 1A 0E C6 62 65 8D EA A8 B8 67 CD CA 7E FC 39
47.
4B 8D 01 D7 74 E1 42 54 CA C3 2A A7 E0 37 1C 2F 30 87 45 1C 0D 76 93 CE EF B6 CD 12 14 97 14 86
0C 1A 0E C6 62 65 8D EA A8 B8 67 CD CA 7E FC 39

48.
4B 8D 01 D7 74 E1 42 54 CA C3 2A A7 E0 37 1C 2F 30 87 45 1C 0D 76 93 CE EF B6 CD 12 14 97 14 A7
0C 1A 0E C6 62 65 8D EA A8 B8 67 CD CA 7E FC 39

Final message digest:
4B 8D 01 D7 74 E1 42 54 CA C3 2A A7 E0 37 1C 2F 30 87 45 1C 0D 76 93 CE EF B6 CD 12 14 97 14 A7
0C 1A 0E C6 62 65 8D EA A8 B8 67 CD CA 7E FC 39

10.6 Final hash computation for hash bit length 512.

Stage 1.

This is SR states for steps in final hash computation. 0 – initial SR state. SR length is 48. Input sequence (from pre-hash computations), 128 bytes:

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

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 for stage 1. Total 128 steps.

1.
2F 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.
2F A0 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.
2F A0 B3 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.
2F A0 B3 F6 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.
2F A0 B3 F6 85 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.
2F A0 B3 F6 85 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 30 31 32 33 34 35 36 37 38 39 3A 3B 3C 3D 3E 3F
7.
2F A0 B3 F6 85 41 99 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.
2F A0 B3 F6 85 41 99 4C 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.
2F A0 B3 F6 85 41 99 4C 53 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.
2F A0 B3 F6 85 41 99 4C 53 A1 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.
2F A0 B3 F6 85 41 99 4C 53 A1 41 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.
2F A0 B3 F6 85 41 99 4C 53 A1 41 66 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.
2F A0 B3 F6 85 41 99 4C 53 A1 41 66 2F 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.
2F A0 B3 F6 85 41 99 4C 53 A1 41 66 2F 96 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.
2F A0 B3 F6 85 41 99 4C 53 A1 41 66 2F 96 74 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.
2F A0 B3 F6 85 41 99 4C 53 A1 41 66 2F 96 74 89 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.
2F A0 B3 F6 85 41 99 4C 53 A1 41 66 2F 96 74 89 43 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.
2F A0 B3 F6 85 41 99 4C 53 A1 41 66 2F 96 74 89 43 23 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.
2F A0 B3 F6 85 41 99 4C 53 A1 41 66 2F 96 74 89 43 23 65 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.
2F A0 B3 F6 85 41 99 4C 53 A1 41 66 2F 96 74 89 43 23 65 C0 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.
2F A0 B3 F6 85 41 99 4C 53 A1 41 66 2F 96 74 89 43 23 65 C0 07 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.
2F A0 B3 F6 85 41 99 4C 53 A1 41 66 2F 96 74 89 43 23 65 C0 07 B4 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.
2F A0 B3 F6 85 41 99 4C 53 A1 41 66 2F 96 74 89 43 23 65 C0 07 B4 5C 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.
2F A0 B3 F6 85 41 99 4C 53 A1 41 66 2F 96 74 89 43 23 65 C0 07 B4 5C 2D 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.
2F A0 B3 F6 85 41 99 4C 53 A1 41 66 2F 96 74 89 43 23 65 C0 07 B4 5C 2D EA 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.
2F A0 B3 F6 85 41 99 4C 53 A1 41 66 2F 96 74 89 43 23 65 C0 07 B4 5C 2D EA 9C 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.
2F A0 B3 F6 85 41 99 4C 53 A1 41 66 2F 96 74 89 43 23 65 C0 07 B4 5C 2D EA 9C 03 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.
2F A0 B3 F6 85 41 99 4C 53 A1 41 66 2F 96 74 89 43 23 65 C0 07 B4 5C 2D EA 9C 03 CC 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.
2F A0 B3 F6 85 41 99 4C 53 A1 41 66 2F 96 74 89 43 23 65 C0 07 B4 5C 2D EA 9C 03 CC 60 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.
2F A0 B3 F6 85 41 99 4C 53 A1 41 66 2F 96 74 89 43 23 65 C0 07 B4 5C 2D EA 9C 03 CC 60 A1 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.
2F A0 B3 F6 85 41 99 4C 53 A1 41 66 2F 96 74 89 43 23 65 C0 07 B4 5C 2D EA 9C 03 CC 60 A1 76 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.
2F A0 B3 F6 85 41 99 4C 53 A1 41 66 2F 96 74 89 43 23 65 C0 07 B4 5C 2D EA 9C 03 CC 60 A1 76 E8
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.
2F A0 B3 F6 85 41 99 4C 53 A1 41 66 2F 96 74 89 43 23 65 C0 07 B4 5C 2D EA 9C 03 CC 60 A1 76 E8
71 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.
2F A0 B3 F6 85 41 99 4C 53 A1 41 66 2F 96 74 89 43 23 65 C0 07 B4 5C 2D EA 9C 03 CC 60 A1 76 E8
71 45 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.
2F A0 B3 F6 85 41 99 4C 53 A1 41 66 2F 96 74 89 43 23 65 C0 07 B4 5C 2D EA 9C 03 CC 60 A1 76 E8
71 45 6D 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.
2F A0 B3 F6 85 41 99 4C 53 A1 41 66 2F 96 74 89 43 23 65 C0 07 B4 5C 2D EA 9C 03 CC 60 A1 76 E8
71 45 6D 9A 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.
2F A0 B3 F6 85 41 99 4C 53 A1 41 66 2F 96 74 89 43 23 65 C0 07 B4 5C 2D EA 9C 03 CC 60 A1 76 E8
71 45 6D 9A 69 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.

2F A0 B3 F6 85 41 99 4C 53 A1 41 66 2F 96 74 89 43 23 65 C0 07 B4 5C 2D EA 9C 03 CC 60 A1 76 E8
71 45 6D 9A 69 61 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.
2F A0 B3 F6 85 41 99 4C 53 A1 41 66 2F 96 74 89 43 23 65 C0 07 B4 5C 2D EA 9C 03 CC 60 A1 76 E8
71 45 6D 9A 69 61 93 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.
2F A0 B3 F6 85 41 99 4C 53 A1 41 66 2F 96 74 89 43 23 65 C0 07 B4 5C 2D EA 9C 03 CC 60 A1 76 E8
71 45 6D 9A 69 61 93 67 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.
2F A0 B3 F6 85 41 99 4C 53 A1 41 66 2F 96 74 89 43 23 65 C0 07 B4 5C 2D EA 9C 03 CC 60 A1 76 E8
71 45 6D 9A 69 61 93 67 DA 29 2A 2B 2C 2D 2E 2F 30 31 32 33 34 35 36 37 38 39 3A 3B 3C 3D 3E 3F
42.
2F A0 B3 F6 85 41 99 4C 53 A1 41 66 2F 96 74 89 43 23 65 C0 07 B4 5C 2D EA 9C 03 CC 60 A1 76 E8
71 45 6D 9A 69 61 93 67 DA 5B 2A 2B 2C 2D 2E 2F 30 31 32 33 34 35 36 37 38 39 3A 3B 3C 3D 3E 3F
43.
2F A0 B3 F6 85 41 99 4C 53 A1 41 66 2F 96 74 89 43 23 65 C0 07 B4 5C 2D EA 9C 03 CC 60 A1 76 E8
71 45 6D 9A 69 61 93 67 DA 5B 3D 2B 2C 2D 2E 2F 30 31 32 33 34 35 36 37 38 39 3A 3B 3C 3D 3E 3F
44.
2F A0 B3 F6 85 41 99 4C 53 A1 41 66 2F 96 74 89 43 23 65 C0 07 B4 5C 2D EA 9C 03 CC 60 A1 76 E8
71 45 6D 9A 69 61 93 67 DA 5B 3D DC 2C 2D 2E 2F 30 31 32 33 34 35 36 37 38 39 3A 3B 3C 3D 3E 3F
45.
2F A0 B3 F6 85 41 99 4C 53 A1 41 66 2F 96 74 89 43 23 65 C0 07 B4 5C 2D EA 9C 03 CC 60 A1 76 E8
71 45 6D 9A 69 61 93 67 DA 5B 3D DC 8C 2D 2E 2F 30 31 32 33 34 35 36 37 38 39 3A 3B 3C 3D 3E 3F
46.
2F A0 B3 F6 85 41 99 4C 53 A1 41 66 2F 96 74 89 43 23 65 C0 07 B4 5C 2D EA 9C 03 CC 60 A1 76 E8
71 45 6D 9A 69 61 93 67 DA 5B 3D DC 8C 2E 2E 2F 30 31 32 33 34 35 36 37 38 39 3A 3B 3C 3D 3E 3F
47.
2F A0 B3 F6 85 41 99 4C 53 A1 41 66 2F 96 74 89 43 23 65 C0 07 B4 5C 2D EA 9C 03 CC 60 A1 76 E8
71 45 6D 9A 69 61 93 67 DA 5B 3D DC 8C 2E F3 2F 30 31 32 33 34 35 36 37 38 39 3A 3B 3C 3D 3E 3F
48.
2F A0 B3 F6 85 41 99 4C 53 A1 41 66 2F 96 74 89 43 23 65 C0 07 B4 5C 2D EA 9C 03 CC 60 A1 76 E8
71 45 6D 9A 69 61 93 67 DA 5B 3D DC 8C 2E F3 26 30 31 32 33 34 35 36 37 38 39 3A 3B 3C 3D 3E 3F
49.
2F A0 B3 F6 85 41 99 4C 53 A1 41 66 2F 96 74 89 43 23 65 C0 07 B4 5C 2D EA 9C 03 CC 60 A1 76 E8
71 45 6D 9A 69 61 93 67 DA 5B 3D DC 8C 2E F3 26 8D 31 32 33 34 35 36 37 38 39 3A 3B 3C 3D 3E 3F
50.
2F A0 B3 F6 85 41 99 4C 53 A1 41 66 2F 96 74 89 43 23 65 C0 07 B4 5C 2D EA 9C 03 CC 60 A1 76 E8
71 45 6D 9A 69 61 93 67 DA 5B 3D DC 8C 2E F3 26 8D 99 32 33 34 35 36 37 38 39 3A 3B 3C 3D 3E 3F
51.
2F A0 B3 F6 85 41 99 4C 53 A1 41 66 2F 96 74 89 43 23 65 C0 07 B4 5C 2D EA 9C 03 CC 60 A1 76 E8
71 45 6D 9A 69 61 93 67 DA 5B 3D DC 8C 2E F3 26 8D 99 B9 33 34 35 36 37 38 39 3A 3B 3C 3D 3E 3F
52.
2F A0 B3 F6 85 41 99 4C 53 A1 41 66 2F 96 74 89 43 23 65 C0 07 B4 5C 2D EA 9C 03 CC 60 A1 76 E8
71 45 6D 9A 69 61 93 67 DA 5B 3D DC 8C 2E F3 26 8D 99 B9 5F 34 35 36 37 38 39 3A 3B 3C 3D 3E 3F
53.
2F A0 B3 F6 85 41 99 4C 53 A1 41 66 2F 96 74 89 43 23 65 C0 07 B4 5C 2D EA 9C 03 CC 60 A1 76 E8
71 45 6D 9A 69 61 93 67 DA 5B 3D DC 8C 2E F3 26 8D 99 B9 5F 3B 35 36 37 38 39 3A 3B 3C 3D 3E 3F
54.
2F A0 B3 F6 85 41 99 4C 53 A1 41 66 2F 96 74 89 43 23 65 C0 07 B4 5C 2D EA 9C 03 CC 60 A1 76 E8
71 45 6D 9A 69 61 93 67 DA 5B 3D DC 8C 2E F3 26 8D 99 B9 5F 3B 2A 36 37 38 39 3A 3B 3C 3D 3E 3F
55.
2F A0 B3 F6 85 41 99 4C 53 A1 41 66 2F 96 74 89 43 23 65 C0 07 B4 5C 2D EA 9C 03 CC 60 A1 76 E8
71 45 6D 9A 69 61 93 67 DA 5B 3D DC 8C 2E F3 26 8D 99 B9 5F 3B 2A A8 37 38 39 3A 3B 3C 3D 3E 3F
56.
2F A0 B3 F6 85 41 99 4C 53 A1 41 66 2F 96 74 89 43 23 65 C0 07 B4 5C 2D EA 9C 03 CC 60 A1 76 E8
71 45 6D 9A 69 61 93 67 DA 5B 3D DC 8C 2E F3 26 8D 99 B9 5F 3B 2A A8 84 38 39 3A 3B 3C 3D 3E 3F
57.
2F A0 B3 F6 85 41 99 4C 53 A1 41 66 2F 96 74 89 43 23 65 C0 07 B4 5C 2D EA 9C 03 CC 60 A1 76 E8
71 45 6D 9A 69 61 93 67 DA 5B 3D DC 8C 2E F3 26 8D 99 B9 5F 3B 2A A8 84 85 39 3A 3B 3C 3D 3E 3F
58.
2F A0 B3 F6 85 41 99 4C 53 A1 41 66 2F 96 74 89 43 23 65 C0 07 B4 5C 2D EA 9C 03 CC 60 A1 76 E8
71 45 6D 9A 69 61 93 67 DA 5B 3D DC 8C 2E F3 26 8D 99 B9 5F 3B 2A A8 84 85 60 3A 3B 3C 3D 3E 3F
59.
2F A0 B3 F6 85 41 99 4C 53 A1 41 66 2F 96 74 89 43 23 65 C0 07 B4 5C 2D EA 9C 03 CC 60 A1 76 E8
71 45 6D 9A 69 61 93 67 DA 5B 3D DC 8C 2E F3 26 8D 99 B9 5F 3B 2A A8 84 85 60 1A 3B 3C 3D 3E 3F
60.
2F A0 B3 F6 85 41 99 4C 53 A1 41 66 2F 96 74 89 43 23 65 C0 07 B4 5C 2D EA 9C 03 CC 60 A1 76 E8
71 45 6D 9A 69 61 93 67 DA 5B 3D DC 8C 2E F3 26 8D 99 B9 5F 3B 2A A8 84 85 60 1A 97 3C 3D 3E 3F
61.
2F A0 B3 F6 85 41 99 4C 53 A1 41 66 2F 96 74 89 43 23 65 C0 07 B4 5C 2D EA 9C 03 CC 60 A1 76 E8
71 45 6D 9A 69 61 93 67 DA 5B 3D DC 8C 2E F3 26 8D 99 B9 5F 3B 2A A8 84 85 60 1A 97 D8 3D 3E 3F
62.
2F A0 B3 F6 85 41 99 4C 53 A1 41 66 2F 96 74 89 43 23 65 C0 07 B4 5C 2D EA 9C 03 CC 60 A1 76 E8
71 45 6D 9A 69 61 93 67 DA 5B 3D DC 8C 2E F3 26 8D 99 B9 5F 3B 2A A8 84 85 60 1A 97 D8 D3 3E 3F

63.
2F A0 B3 F6 85 41 99 4C 53 A1 41 66 2F 96 74 89 43 23 65 C0 07 B4 5C 2D EA 9C 03 CC 60 A1 76 E8
71 45 6D 9A 69 61 93 67 DA 5B 3D DC 8C 2E F3 26 8D 99 B9 5F 3B 2A A8 84 85 60 1A 97 D8 D3 43 3F
64.
2F A0 B3 F6 85 41 99 4C 53 A1 41 66 2F 96 74 89 43 23 65 C0 07 B4 5C 2D EA 9C 03 CC 60 A1 76 E8
71 45 6D 9A 69 61 93 67 DA 5B 3D DC 8C 2E F3 26 8D 99 B9 5F 3B 2A A8 84 85 60 1A 97 D8 D3 43 E2
65.
9D A0 B3 F6 85 41 99 4C 53 A1 41 66 2F 96 74 89 43 23 65 C0 07 B4 5C 2D EA 9C 03 CC 60 A1 76 E8
71 45 6D 9A 69 61 93 67 DA 5B 3D DC 8C 2E F3 26 8D 99 B9 5F 3B 2A A8 84 85 60 1A 97 D8 D3 43 E2
66.
9D 21 B3 F6 85 41 99 4C 53 A1 41 66 2F 96 74 89 43 23 65 C0 07 B4 5C 2D EA 9C 03 CC 60 A1 76 E8
71 45 6D 9A 69 61 93 67 DA 5B 3D DC 8C 2E F3 26 8D 99 B9 5F 3B 2A A8 84 85 60 1A 97 D8 D3 43 E2
67.
9D 21 58 F6 85 41 99 4C 53 A1 41 66 2F 96 74 89 43 23 65 C0 07 B4 5C 2D EA 9C 03 CC 60 A1 76 E8
71 45 6D 9A 69 61 93 67 DA 5B 3D DC 8C 2E F3 26 8D 99 B9 5F 3B 2A A8 84 85 60 1A 97 D8 D3 43 E2
68.
9D 21 58 C5 85 41 99 4C 53 A1 41 66 2F 96 74 89 43 23 65 C0 07 B4 5C 2D EA 9C 03 CC 60 A1 76 E8
71 45 6D 9A 69 61 93 67 DA 5B 3D DC 8C 2E F3 26 8D 99 B9 5F 3B 2A A8 84 85 60 1A 97 D8 D3 43 E2
69.
9D 21 58 C5 EA 41 99 4C 53 A1 41 66 2F 96 74 89 43 23 65 C0 07 B4 5C 2D EA 9C 03 CC 60 A1 76 E8
71 45 6D 9A 69 61 93 67 DA 5B 3D DC 8C 2E F3 26 8D 99 B9 5F 3B 2A A8 84 85 60 1A 97 D8 D3 43 E2
70.
9D 21 58 C5 EA 79 99 4C 53 A1 41 66 2F 96 74 89 43 23 65 C0 07 B4 5C 2D EA 9C 03 CC 60 A1 76 E8
71 45 6D 9A 69 61 93 67 DA 5B 3D DC 8C 2E F3 26 8D 99 B9 5F 3B 2A A8 84 85 60 1A 97 D8 D3 43 E2
71.
9D 21 58 C5 EA 79 E0 4C 53 A1 41 66 2F 96 74 89 43 23 65 C0 07 B4 5C 2D EA 9C 03 CC 60 A1 76 E8
71 45 6D 9A 69 61 93 67 DA 5B 3D DC 8C 2E F3 26 8D 99 B9 5F 3B 2A A8 84 85 60 1A 97 D8 D3 43 E2
72.
9D 21 58 C5 EA 79 E0 99 53 A1 41 66 2F 96 74 89 43 23 65 C0 07 B4 5C 2D EA 9C 03 CC 60 A1 76 E8
71 45 6D 9A 69 61 93 67 DA 5B 3D DC 8C 2E F3 26 8D 99 B9 5F 3B 2A A8 84 85 60 1A 97 D8 D3 43 E2
73.
9D 21 58 C5 EA 79 E0 99 B2 A1 41 66 2F 96 74 89 43 23 65 C0 07 B4 5C 2D EA 9C 03 CC 60 A1 76 E8
71 45 6D 9A 69 61 93 67 DA 5B 3D DC 8C 2E F3 26 8D 99 B9 5F 3B 2A A8 84 85 60 1A 97 D8 D3 43 E2
74.
9D 21 58 C5 EA 79 E0 99 B2 A6 41 66 2F 96 74 89 43 23 65 C0 07 B4 5C 2D EA 9C 03 CC 60 A1 76 E8
71 45 6D 9A 69 61 93 67 DA 5B 3D DC 8C 2E F3 26 8D 99 B9 5F 3B 2A A8 84 85 60 1A 97 D8 D3 43 E2
75.
9D 21 58 C5 EA 79 E0 99 B2 A6 3F 66 2F 96 74 89 43 23 65 C0 07 B4 5C 2D EA 9C 03 CC 60 A1 76 E8
71 45 6D 9A 69 61 93 67 DA 5B 3D DC 8C 2E F3 26 8D 99 B9 5F 3B 2A A8 84 85 60 1A 97 D8 D3 43 E2
76.
9D 21 58 C5 EA 79 E0 99 B2 A6 3F 64 2F 96 74 89 43 23 65 C0 07 B4 5C 2D EA 9C 03 CC 60 A1 76 E8
71 45 6D 9A 69 61 93 67 DA 5B 3D DC 8C 2E F3 26 8D 99 B9 5F 3B 2A A8 84 85 60 1A 97 D8 D3 43 E2
77.
9D 21 58 C5 EA 79 E0 99 B2 A6 3F 64 F5 96 74 89 43 23 65 C0 07 B4 5C 2D EA 9C 03 CC 60 A1 76 E8
71 45 6D 9A 69 61 93 67 DA 5B 3D DC 8C 2E F3 26 8D 99 B9 5F 3B 2A A8 84 85 60 1A 97 D8 D3 43 E2
78.
9D 21 58 C5 EA 79 E0 99 B2 A6 3F 64 F5 81 74 89 43 23 65 C0 07 B4 5C 2D EA 9C 03 CC 60 A1 76 E8
71 45 6D 9A 69 61 93 67 DA 5B 3D DC 8C 2E F3 26 8D 99 B9 5F 3B 2A A8 84 85 60 1A 97 D8 D3 43 E2
79.
9D 21 58 C5 EA 79 E0 99 B2 A6 3F 64 F5 81 A9 89 43 23 65 C0 07 B4 5C 2D EA 9C 03 CC 60 A1 76 E8
71 45 6D 9A 69 61 93 67 DA 5B 3D DC 8C 2E F3 26 8D 99 B9 5F 3B 2A A8 84 85 60 1A 97 D8 D3 43 E2
80.
9D 21 58 C5 EA 79 E0 99 B2 A6 3F 64 F5 81 A9 FB 43 23 65 C0 07 B4 5C 2D EA 9C 03 CC 60 A1 76 E8
71 45 6D 9A 69 61 93 67 DA 5B 3D DC 8C 2E F3 26 8D 99 B9 5F 3B 2A A8 84 85 60 1A 97 D8 D3 43 E2
81.
9D 21 58 C5 EA 79 E0 99 B2 A6 3F 64 F5 81 A9 FB 3C 23 65 C0 07 B4 5C 2D EA 9C 03 CC 60 A1 76 E8
71 45 6D 9A 69 61 93 67 DA 5B 3D DC 8C 2E F3 26 8D 99 B9 5F 3B 2A A8 84 85 60 1A 97 D8 D3 43 E2
82.
9D 21 58 C5 EA 79 E0 99 B2 A6 3F 64 F5 81 A9 FB 3C 1B 65 C0 07 B4 5C 2D EA 9C 03 CC 60 A1 76 E8
71 45 6D 9A 69 61 93 67 DA 5B 3D DC 8C 2E F3 26 8D 99 B9 5F 3B 2A A8 84 85 60 1A 97 D8 D3 43 E2
83.
9D 21 58 C5 EA 79 E0 99 B2 A6 3F 64 F5 81 A9 FB 3C 1B 4F C0 07 B4 5C 2D EA 9C 03 CC 60 A1 76 E8
71 45 6D 9A 69 61 93 67 DA 5B 3D DC 8C 2E F3 26 8D 99 B9 5F 3B 2A A8 84 85 60 1A 97 D8 D3 43 E2
84.
9D 21 58 C5 EA 79 E0 99 B2 A6 3F 64 F5 81 A9 FB 3C 1B 4F CD 07 B4 5C 2D EA 9C 03 CC 60 A1 76 E8
71 45 6D 9A 69 61 93 67 DA 5B 3D DC 8C 2E F3 26 8D 99 B9 5F 3B 2A A8 84 85 60 1A 97 D8 D3 43 E2
85.
9D 21 58 C5 EA 79 E0 99 B2 A6 3F 64 F5 81 A9 FB 3C 1B 4F CD C9 B4 5C 2D EA 9C 03 CC 60 A1 76 E8
71 45 6D 9A 69 61 93 67 DA 5B 3D DC 8C 2E F3 26 8D 99 B9 5F 3B 2A A8 84 85 60 1A 97 D8 D3 43 E2
86.
9D 21 58 C5 EA 79 E0 99 B2 A6 3F 64 F5 81 A9 FB 3C 1B 4F CD C9 E8 5C 2D EA 9C 03 CC 60 A1 76 E8
71 45 6D 9A 69 61 93 67 DA 5B 3D DC 8C 2E F3 26 8D 99 B9 5F 3B 2A A8 84 85 60 1A 97 D8 D3 43 E2
87.
9D 21 58 C5 EA 79 E0 99 B2 A6 3F 64 F5 81 A9 FB 3C 1B 4F CD C9 E8 DE 2D EA 9C 03 CC 60 A1 76 E8

71 45 6D 9A 69 61 93 67 DA 5B 3D DC 8C 2E F3 26 8D 99 B9 5F 3B 2A A8 84 85 60 1A 97 D8 D3 43 E2
88.
9D 21 58 C5 EA 79 E0 99 B2 A6 3F 64 F5 81 A9 FB 3C 1B 4F CD C9 E8 DE BD EA 9C 03 CC 60 A1 76 E8
71 45 6D 9A 69 61 93 67 DA 5B 3D DC 8C 2E F3 26 8D 99 B9 5F 3B 2A A8 84 85 60 1A 97 D8 D3 43 E2
89.
9D 21 58 C5 EA 79 E0 99 B2 A6 3F 64 F5 81 A9 FB 3C 1B 4F CD C9 E8 DE BD 06 9C 03 CC 60 A1 76 E8
71 45 6D 9A 69 61 93 67 DA 5B 3D DC 8C 2E F3 26 8D 99 B9 5F 3B 2A A8 84 85 60 1A 97 D8 D3 43 E2
90.
9D 21 58 C5 EA 79 E0 99 B2 A6 3F 64 F5 81 A9 FB 3C 1B 4F CD C9 E8 DE BD 06 39 03 CC 60 A1 76 E8
71 45 6D 9A 69 61 93 67 DA 5B 3D DC 8C 2E F3 26 8D 99 B9 5F 3B 2A A8 84 85 60 1A 97 D8 D3 43 E2
91.
9D 21 58 C5 EA 79 E0 99 B2 A6 3F 64 F5 81 A9 FB 3C 1B 4F CD C9 E8 DE BD 06 39 86 CC 60 A1 76 E8
71 45 6D 9A 69 61 93 67 DA 5B 3D DC 8C 2E F3 26 8D 99 B9 5F 3B 2A A8 84 85 60 1A 97 D8 D3 43 E2
92.
9D 21 58 C5 EA 79 E0 99 B2 A6 3F 64 F5 81 A9 FB 3C 1B 4F CD C9 E8 DE BD 06 39 86 DE 60 A1 76 E8
71 45 6D 9A 69 61 93 67 DA 5B 3D DC 8C 2E F3 26 8D 99 B9 5F 3B 2A A8 84 85 60 1A 97 D8 D3 43 E2
93.
9D 21 58 C5 EA 79 E0 99 B2 A6 3F 64 F5 81 A9 FB 3C 1B 4F CD C9 E8 DE BD 06 39 86 DE B2 A1 76 E8
71 45 6D 9A 69 61 93 67 DA 5B 3D DC 8C 2E F3 26 8D 99 B9 5F 3B 2A A8 84 85 60 1A 97 D8 D3 43 E2
94.
9D 21 58 C5 EA 79 E0 99 B2 A6 3F 64 F5 81 A9 FB 3C 1B 4F CD C9 E8 DE BD 06 39 86 DE B2 AC 76 E8
71 45 6D 9A 69 61 93 67 DA 5B 3D DC 8C 2E F3 26 8D 99 B9 5F 3B 2A A8 84 85 60 1A 97 D8 D3 43 E2
95.
9D 21 58 C5 EA 79 E0 99 B2 A6 3F 64 F5 81 A9 FB 3C 1B 4F CD C9 E8 DE BD 06 39 86 DE B2 AC 4F E8
71 45 6D 9A 69 61 93 67 DA 5B 3D DC 8C 2E F3 26 8D 99 B9 5F 3B 2A A8 84 85 60 1A 97 D8 D3 43 E2
96.
9D 21 58 C5 EA 79 E0 99 B2 A6 3F 64 F5 81 A9 FB 3C 1B 4F CD C9 E8 DE BD 06 39 86 DE B2 AC 4F 3D
71 45 6D 9A 69 61 93 67 DA 5B 3D DC 8C 2E F3 26 8D 99 B9 5F 3B 2A A8 84 85 60 1A 97 D8 D3 43 E2
97.
9D 21 58 C5 EA 79 E0 99 B2 A6 3F 64 F5 81 A9 FB 3C 1B 4F CD C9 E8 DE BD 06 39 86 DE B2 AC 4F 3D
40 45 6D 9A 69 61 93 67 DA 5B 3D DC 8C 2E F3 26 8D 99 B9 5F 3B 2A A8 84 85 60 1A 97 D8 D3 43 E2
98.
9D 21 58 C5 EA 79 E0 99 B2 A6 3F 64 F5 81 A9 FB 3C 1B 4F CD C9 E8 DE BD 06 39 86 DE B2 AC 4F 3D
40 07 6D 9A 69 61 93 67 DA 5B 3D DC 8C 2E F3 26 8D 99 B9 5F 3B 2A A8 84 85 60 1A 97 D8 D3 43 E2
99.
9D 21 58 C5 EA 79 E0 99 B2 A6 3F 64 F5 81 A9 FB 3C 1B 4F CD C9 E8 DE BD 06 39 86 DE B2 AC 4F 3D
40 07 0E 9A 69 61 93 67 DA 5B 3D DC 8C 2E F3 26 8D 99 B9 5F 3B 2A A8 84 85 60 1A 97 D8 D3 43 E2
100.
9D 21 58 C5 EA 79 E0 99 B2 A6 3F 64 F5 81 A9 FB 3C 1B 4F CD C9 E8 DE BD 06 39 86 DE B2 AC 4F 3D
40 07 0E CA 69 61 93 67 DA 5B 3D DC 8C 2E F3 26 8D 99 B9 5F 3B 2A A8 84 85 60 1A 97 D8 D3 43 E2
101.
9D 21 58 C5 EA 79 E0 99 B2 A6 3F 64 F5 81 A9 FB 3C 1B 4F CD C9 E8 DE BD 06 39 86 DE B2 AC 4F 3D
40 07 0E CA 90 61 93 67 DA 5B 3D DC 8C 2E F3 26 8D 99 B9 5F 3B 2A A8 84 85 60 1A 97 D8 D3 43 E2
102.
9D 21 58 C5 EA 79 E0 99 B2 A6 3F 64 F5 81 A9 FB 3C 1B 4F CD C9 E8 DE BD 06 39 86 DE B2 AC 4F 3D
40 07 0E CA 90 85 93 67 DA 5B 3D DC 8C 2E F3 26 8D 99 B9 5F 3B 2A A8 84 85 60 1A 97 D8 D3 43 E2
103.
9D 21 58 C5 EA 79 E0 99 B2 A6 3F 64 F5 81 A9 FB 3C 1B 4F CD C9 E8 DE BD 06 39 86 DE B2 AC 4F 3D
40 07 0E CA 90 85 F8 67 DA 5B 3D DC 8C 2E F3 26 8D 99 B9 5F 3B 2A A8 84 85 60 1A 97 D8 D3 43 E2
104.
9D 21 58 C5 EA 79 E0 99 B2 A6 3F 64 F5 81 A9 FB 3C 1B 4F CD C9 E8 DE BD 06 39 86 DE B2 AC 4F 3D
40 07 0E CA 90 85 F8 92 DA 5B 3D DC 8C 2E F3 26 8D 99 B9 5F 3B 2A A8 84 85 60 1A 97 D8 D3 43 E2
105.
9D 21 58 C5 EA 79 E0 99 B2 A6 3F 64 F5 81 A9 FB 3C 1B 4F CD C9 E8 DE BD 06 39 86 DE B2 AC 4F 3D
40 07 0E CA 90 85 F8 92 18 5B 3D DC 8C 2E F3 26 8D 99 B9 5F 3B 2A A8 84 85 60 1A 97 D8 D3 43 E2
106.
9D 21 58 C5 EA 79 E0 99 B2 A6 3F 64 F5 81 A9 FB 3C 1B 4F CD C9 E8 DE BD 06 39 86 DE B2 AC 4F 3D
40 07 0E CA 90 85 F8 92 18 20 3D DC 8C 2E F3 26 8D 99 B9 5F 3B 2A A8 84 85 60 1A 97 D8 D3 43 E2
107.
9D 21 58 C5 EA 79 E0 99 B2 A6 3F 64 F5 81 A9 FB 3C 1B 4F CD C9 E8 DE BD 06 39 86 DE B2 AC 4F 3D
40 07 0E CA 90 85 F8 92 18 20 89 DC 8C 2E F3 26 8D 99 B9 5F 3B 2A A8 84 85 60 1A 97 D8 D3 43 E2
108.
9D 21 58 C5 EA 79 E0 99 B2 A6 3F 64 F5 81 A9 FB 3C 1B 4F CD C9 E8 DE BD 06 39 86 DE B2 AC 4F 3D
40 07 0E CA 90 85 F8 92 18 20 89 56 8C 2E F3 26 8D 99 B9 5F 3B 2A A8 84 85 60 1A 97 D8 D3 43 E2
109.
9D 21 58 C5 EA 79 E0 99 B2 A6 3F 64 F5 81 A9 FB 3C 1B 4F CD C9 E8 DE BD 06 39 86 DE B2 AC 4F 3D
40 07 0E CA 90 85 F8 92 18 20 89 56 E0 2E F3 26 8D 99 B9 5F 3B 2A A8 84 85 60 1A 97 D8 D3 43 E2
110.
9D 21 58 C5 EA 79 E0 99 B2 A6 3F 64 F5 81 A9 FB 3C 1B 4F CD C9 E8 DE BD 06 39 86 DE B2 AC 4F 3D
40 07 0E CA 90 85 F8 92 18 20 89 56 E0 52 F3 26 8D 99 B9 5F 3B 2A A8 84 85 60 1A 97 D8 D3 43 E2
111.
9D 21 58 C5 EA 79 E0 99 B2 A6 3F 64 F5 81 A9 FB 3C 1B 4F CD C9 E8 DE BD 06 39 86 DE B2 AC 4F 3D
40 07 0E CA 90 85 F8 92 18 20 89 56 E0 52 89 26 8D 99 B9 5F 3B 2A A8 84 85 60 1A 97 D8 D3 43 E2
112.

9D 21 58 C5 EA 79 E0 99 B2 A6 3F 64 F5 81 A9 FB 3C 1B 4F CD C9 E8 DE BD 06 39 86 DE B2 AC 4F 3D 40 07 0E CA 90 85 F8 92 18 20 89 56 E0 52 89 28 8D 99 B9 5F 3B 2A A8 84 85 60 1A 97 D8 D3 43 E2
113.
9D 21 58 C5 EA 79 E0 99 B2 A6 3F 64 F5 81 A9 FB 3C 1B 4F CD C9 E8 DE BD 06 39 86 DE B2 AC 4F 3D 40 07 0E CA 90 85 F8 92 18 20 89 56 E0 52 89 28 0D 99 B9 5F 3B 2A A8 84 85 60 1A 97 D8 D3 43 E2
114.
9D 21 58 C5 EA 79 E0 99 B2 A6 3F 64 F5 81 A9 FB 3C 1B 4F CD C9 E8 DE BD 06 39 86 DE B2 AC 4F 3D 40 07 0E CA 90 85 F8 92 18 20 89 56 E0 52 89 28 0D 87 B9 5F 3B 2A A8 84 85 60 1A 97 D8 D3 43 E2
115.
9D 21 58 C5 EA 79 E0 99 B2 A6 3F 64 F5 81 A9 FB 3C 1B 4F CD C9 E8 DE BD 06 39 86 DE B2 AC 4F 3D 40 07 0E CA 90 85 F8 92 18 20 89 56 E0 52 89 28 0D 87 56 5F 3B 2A A8 84 85 60 1A 97 D8 D3 43 E2
116.
9D 21 58 C5 EA 79 E0 99 B2 A6 3F 64 F5 81 A9 FB 3C 1B 4F CD C9 E8 DE BD 06 39 86 DE B2 AC 4F 3D 40 07 0E CA 90 85 F8 92 18 20 89 56 E0 52 89 28 0D 87 56 18 3B 2A A8 84 85 60 1A 97 D8 D3 43 E2
117.
9D 21 58 C5 EA 79 E0 99 B2 A6 3F 64 F5 81 A9 FB 3C 1B 4F CD C9 E8 DE BD 06 39 86 DE B2 AC 4F 3D 40 07 0E CA 90 85 F8 92 18 20 89 56 E0 52 89 28 0D 87 56 18 05 2A A8 84 85 60 1A 97 D8 D3 43 E2
118.
9D 21 58 C5 EA 79 E0 99 B2 A6 3F 64 F5 81 A9 FB 3C 1B 4F CD C9 E8 DE BD 06 39 86 DE B2 AC 4F 3D 40 07 0E CA 90 85 F8 92 18 20 89 56 E0 52 89 28 0D 87 56 18 05 A5 A8 84 85 60 1A 97 D8 D3 43 E2
119.
9D 21 58 C5 EA 79 E0 99 B2 A6 3F 64 F5 81 A9 FB 3C 1B 4F CD C9 E8 DE BD 06 39 86 DE B2 AC 4F 3D 40 07 0E CA 90 85 F8 92 18 20 89 56 E0 52 89 28 0D 87 56 18 05 A5 72 84 85 60 1A 97 D8 D3 43 E2
120.
9D 21 58 C5 EA 79 E0 99 B2 A6 3F 64 F5 81 A9 FB 3C 1B 4F CD C9 E8 DE BD 06 39 86 DE B2 AC 4F 3D 40 07 0E CA 90 85 F8 92 18 20 89 56 E0 52 89 28 0D 87 56 18 05 A5 72 AA 85 60 1A 97 D8 D3 43 E2
121.
9D 21 58 C5 EA 79 E0 99 B2 A6 3F 64 F5 81 A9 FB 3C 1B 4F CD C9 E8 DE BD 06 39 86 DE B2 AC 4F 3D 40 07 0E CA 90 85 F8 92 18 20 89 56 E0 52 89 28 0D 87 56 18 05 A5 72 AA D1 60 1A 97 D8 D3 43 E2
122.
9D 21 58 C5 EA 79 E0 99 B2 A6 3F 64 F5 81 A9 FB 3C 1B 4F CD C9 E8 DE BD 06 39 86 DE B2 AC 4F 3D 40 07 0E CA 90 85 F8 92 18 20 89 56 E0 52 89 28 0D 87 56 18 05 A5 72 AA D1 61 1A 97 D8 D3 43 E2
123.
9D 21 58 C5 EA 79 E0 99 B2 A6 3F 64 F5 81 A9 FB 3C 1B 4F CD C9 E8 DE BD 06 39 86 DE B2 AC 4F 3D 40 07 0E CA 90 85 F8 92 18 20 89 56 E0 52 89 28 0D 87 56 18 05 A5 72 AA D1 61 62 97 D8 D3 43 E2
124.
9D 21 58 C5 EA 79 E0 99 B2 A6 3F 64 F5 81 A9 FB 3C 1B 4F CD C9 E8 DE BD 06 39 86 DE B2 AC 4F 3D 40 07 0E CA 90 85 F8 92 18 20 89 56 E0 52 89 28 0D 87 56 18 05 A5 72 AA D1 61 62 11 D8 D3 43 E2
125.
9D 21 58 C5 EA 79 E0 99 B2 A6 3F 64 F5 81 A9 FB 3C 1B 4F CD C9 E8 DE BD 06 39 86 DE B2 AC 4F 3D 40 07 0E CA 90 85 F8 92 18 20 89 56 E0 52 89 28 0D 87 56 18 05 A5 72 AA D1 61 62 11 EC D3 43 E2
126.
9D 21 58 C5 EA 79 E0 99 B2 A6 3F 64 F5 81 A9 FB 3C 1B 4F CD C9 E8 DE BD 06 39 86 DE B2 AC 4F 3D 40 07 0E CA 90 85 F8 92 18 20 89 56 E0 52 89 28 0D 87 56 18 05 A5 72 AA D1 61 62 11 EC 16 43 E2
127.
9D 21 58 C5 EA 79 E0 99 B2 A6 3F 64 F5 81 A9 FB 3C 1B 4F CD C9 E8 DE BD 06 39 86 DE B2 AC 4F 3D 40 07 0E CA 90 85 F8 92 18 20 89 56 E0 52 89 28 0D 87 56 18 05 A5 72 AA D1 61 62 11 EC 16 C0 E2
128.
9D 21 58 C5 EA 79 E0 99 B2 A6 3F 64 F5 81 A9 FB 3C 1B 4F CD C9 E8 DE BD 06 39 86 DE B2 AC 4F 3D 40 07 0E CA 90 85 F8 92 18 20 89 56 E0 52 89 28 0D 87 56 18 05 A5 72 AA D1 61 62 11 EC 16 C0 9B

Stage 2.

Input sequence

9B C0 16 EC 11 62 61 D1 AA 72 A5 05 18 56 87 0D 28 89 52 E0 56 89 20 18 92 F8 85 90 CA 0E 07 40 3D 4F AC B2 DE 86 39 06 BD DE E8 C9 CD 4F 1B 3C FB A9 81 F5 64 3F A6 B2 99 E0 79 EA C5 58 21 9D

Calculating SR state for stage 2. Total 64 steps.

1.
77 21 58 C5 EA 79 E0 99 B2 A6 3F 64 F5 81 A9 FB 3C 1B 4F CD C9 E8 DE BD 06 39 86 DE B2 AC 4F 3D 40 07 0E CA 90 85 F8 92 18 20 89 56 E0 52 89 28 0D 87 56 18 05 A5 72 AA D1 61 62 11 EC 16 C0 9B
2.
77 01 58 C5 EA 79 E0 99 B2 A6 3F 64 F5 81 A9 FB 3C 1B 4F CD C9 E8 DE BD 06 39 86 DE B2 AC 4F 3D 40 07 0E CA 90 85 F8 92 18 20 89 56 E0 52 89 28 0D 87 56 18 05 A5 72 AA D1 61 62 11 EC 16 C0 9B
3.
77 01 F5 C5 EA 79 E0 99 B2 A6 3F 64 F5 81 A9 FB 3C 1B 4F CD C9 E8 DE BD 06 39 86 DE B2 AC 4F 3D 40 07 0E CA 90 85 F8 92 18 20 89 56 E0 52 89 28 0D 87 56 18 05 A5 72 AA D1 61 62 11 EC 16 C0 9B
4.
77 01 F5 6F EA 79 E0 99 B2 A6 3F 64 F5 81 A9 FB 3C 1B 4F CD C9 E8 DE BD 06 39 86 DE B2 AC 4F 3D 40 07 0E CA 90 85 F8 92 18 20 89 56 E0 52 89 28 0D 87 56 18 05 A5 72 AA D1 61 62 11 EC 16 C0 9B
5.

77 01 F5 6F D0 79 E0 99 B2 A6 3F 64 F5 81 A9 FB 3C 1B 4F CD C9 E8 DE BD 06 39 86 DE B2 AC 4F 3D
40 07 0E CA 90 85 F8 92 18 20 89 56 E0 52 89 28 0D 87 56 18 05 A5 72 AA D1 61 62 11 EC 16 C0 9B
6.
77 01 F5 6F D0 54 E0 99 B2 A6 3F 64 F5 81 A9 FB 3C 1B 4F CD C9 E8 DE BD 06 39 86 DE B2 AC 4F 3D
40 07 0E CA 90 85 F8 92 18 20 89 56 E0 52 89 28 0D 87 56 18 05 A5 72 AA D1 61 62 11 EC 16 C0 9B
7.
77 01 F5 6F D0 54 2E 99 B2 A6 3F 64 F5 81 A9 FB 3C 1B 4F CD C9 E8 DE BD 06 39 86 DE B2 AC 4F 3D
40 07 0E CA 90 85 F8 92 18 20 89 56 E0 52 89 28 0D 87 56 18 05 A5 72 AA D1 61 62 11 EC 16 C0 9B
8.
77 01 F5 6F D0 54 2E 9E B2 A6 3F 64 F5 81 A9 FB 3C 1B 4F CD C9 E8 DE BD 06 39 86 DE B2 AC 4F 3D
40 07 0E CA 90 85 F8 92 18 20 89 56 E0 52 89 28 0D 87 56 18 05 A5 72 AA D1 61 62 11 EC 16 C0 9B
9.
77 01 F5 6F D0 54 2E 9E 70 A6 3F 64 F5 81 A9 FB 3C 1B 4F CD C9 E8 DE BD 06 39 86 DE B2 AC 4F 3D
40 07 0E CA 90 85 F8 92 18 20 89 56 E0 52 89 28 0D 87 56 18 05 A5 72 AA D1 61 62 11 EC 16 C0 9B
10.
77 01 F5 6F D0 54 2E 9E 70 8C 3F 64 F5 81 A9 FB 3C 1B 4F CD C9 E8 DE BD 06 39 86 DE B2 AC 4F 3D
40 07 0E CA 90 85 F8 92 18 20 89 56 E0 52 89 28 0D 87 56 18 05 A5 72 AA D1 61 62 11 EC 16 C0 9B
11.
77 01 F5 6F D0 54 2E 9E 70 8C F1 64 F5 81 A9 FB 3C 1B 4F CD C9 E8 DE BD 06 39 86 DE B2 AC 4F 3D
40 07 0E CA 90 85 F8 92 18 20 89 56 E0 52 89 28 0D 87 56 18 05 A5 72 AA D1 61 62 11 EC 16 C0 9B
12.
77 01 F5 6F D0 54 2E 9E 70 8C F1 9A F5 81 A9 FB 3C 1B 4F CD C9 E8 DE BD 06 39 86 DE B2 AC 4F 3D
40 07 0E CA 90 85 F8 92 18 20 89 56 E0 52 89 28 0D 87 56 18 05 A5 72 AA D1 61 62 11 EC 16 C0 9B
13.
77 01 F5 6F D0 54 2E 9E 70 8C F1 9A 91 81 A9 FB 3C 1B 4F CD C9 E8 DE BD 06 39 86 DE B2 AC 4F 3D
40 07 0E CA 90 85 F8 92 18 20 89 56 E0 52 89 28 0D 87 56 18 05 A5 72 AA D1 61 62 11 EC 16 C0 9B
14.
77 01 F5 6F D0 54 2E 9E 70 8C F1 9A 91 6F A9 FB 3C 1B 4F CD C9 E8 DE BD 06 39 86 DE B2 AC 4F 3D
40 07 0E CA 90 85 F8 92 18 20 89 56 E0 52 89 28 0D 87 56 18 05 A5 72 AA D1 61 62 11 EC 16 C0 9B
15.
77 01 F5 6F D0 54 2E 9E 70 8C F1 9A 91 6F 92 FB 3C 1B 4F CD C9 E8 DE BD 06 39 86 DE B2 AC 4F 3D
40 07 0E CA 90 85 F8 92 18 20 89 56 E0 52 89 28 0D 87 56 18 05 A5 72 AA D1 61 62 11 EC 16 C0 9B
16.
77 01 F5 6F D0 54 2E 9E 70 8C F1 9A 91 6F 92 ED 3C 1B 4F CD C9 E8 DE BD 06 39 86 DE B2 AC 4F 3D
40 07 0E CA 90 85 F8 92 18 20 89 56 E0 52 89 28 0D 87 56 18 05 A5 72 AA D1 61 62 11 EC 16 C0 9B
17.
77 01 F5 6F D0 54 2E 9E 70 8C F1 9A 91 6F 92 ED BF 1B 4F CD C9 E8 DE BD 06 39 86 DE B2 AC 4F 3D
40 07 0E CA 90 85 F8 92 18 20 89 56 E0 52 89 28 0D 87 56 18 05 A5 72 AA D1 61 62 11 EC 16 C0 9B
18.
77 01 F5 6F D0 54 2E 9E 70 8C F1 9A 91 6F 92 ED BF 1A 4F CD C9 E8 DE BD 06 39 86 DE B2 AC 4F 3D
40 07 0E CA 90 85 F8 92 18 20 89 56 E0 52 89 28 0D 87 56 18 05 A5 72 AA D1 61 62 11 EC 16 C0 9B
19.
77 01 F5 6F D0 54 2E 9E 70 8C F1 9A 91 6F 92 ED BF 1A 6A CD C9 E8 DE BD 06 39 86 DE B2 AC 4F 3D
40 07 0E CA 90 85 F8 92 18 20 89 56 E0 52 89 28 0D 87 56 18 05 A5 72 AA D1 61 62 11 EC 16 C0 9B
20.
77 01 F5 6F D0 54 2E 9E 70 8C F1 9A 91 6F 92 ED BF 1A 6A 90 C9 E8 DE BD 06 39 86 DE B2 AC 4F 3D
40 07 0E CA 90 85 F8 92 18 20 89 56 E0 52 89 28 0D 87 56 18 05 A5 72 AA D1 61 62 11 EC 16 C0 9B
21.
77 01 F5 6F D0 54 2E 9E 70 8C F1 9A 91 6F 92 ED BF 1A 6A 90 4E E8 DE BD 06 39 86 DE B2 AC 4F 3D
40 07 0E CA 90 85 F8 92 18 20 89 56 E0 52 89 28 0D 87 56 18 05 A5 72 AA D1 61 62 11 EC 16 C0 9B
22.
77 01 F5 6F D0 54 2E 9E 70 8C F1 9A 91 6F 92 ED BF 1A 6A 90 4E 5C DE BD 06 39 86 DE B2 AC 4F 3D
40 07 0E CA 90 85 F8 92 18 20 89 56 E0 52 89 28 0D 87 56 18 05 A5 72 AA D1 61 62 11 EC 16 C0 9B
23.
77 01 F5 6F D0 54 2E 9E 70 8C F1 9A 91 6F 92 ED BF 1A 6A 90 4E 5C A6 BD 06 39 86 DE B2 AC 4F 3D
40 07 0E CA 90 85 F8 92 18 20 89 56 E0 52 89 28 0D 87 56 18 05 A5 72 AA D1 61 62 11 EC 16 C0 9B
24.
77 01 F5 6F D0 54 2E 9E 70 8C F1 9A 91 6F 92 ED BF 1A 6A 90 4E 5C A6 E0 06 39 86 DE B2 AC 4F 3D
40 07 0E CA 90 85 F8 92 18 20 89 56 E0 52 89 28 0D 87 56 18 05 A5 72 AA D1 61 62 11 EC 16 C0 9B
25.
77 01 F5 6F D0 54 2E 9E 70 8C F1 9A 91 6F 92 ED BF 1A 6A 90 4E 5C A6 E0 E6 39 86 DE B2 AC 4F 3D
40 07 0E CA 90 85 F8 92 18 20 89 56 E0 52 89 28 0D 87 56 18 05 A5 72 AA D1 61 62 11 EC 16 C0 9B
26.
77 01 F5 6F D0 54 2E 9E 70 8C F1 9A 91 6F 92 ED BF 1A 6A 90 4E 5C A6 E0 E6 B9 86 DE B2 AC 4F 3D
40 07 0E CA 90 85 F8 92 18 20 89 56 E0 52 89 28 0D 87 56 18 05 A5 72 AA D1 61 62 11 EC 16 C0 9B
27.
77 01 F5 6F D0 54 2E 9E 70 8C F1 9A 91 6F 92 ED BF 1A 6A 90 4E 5C A6 E0 E6 B9 B0 DE B2 AC 4F 3D
40 07 0E CA 90 85 F8 92 18 20 89 56 E0 52 89 28 0D 87 56 18 05 A5 72 AA D1 61 62 11 EC 16 C0 9B
28.
77 01 F5 6F D0 54 2E 9E 70 8C F1 9A 91 6F 92 ED BF 1A 6A 90 4E 5C A6 E0 E6 B9 B0 CF B2 AC 4F 3D
40 07 0E CA 90 85 F8 92 18 20 89 56 E0 52 89 28 0D 87 56 18 05 A5 72 AA D1 61 62 11 EC 16 C0 9B
29.
77 01 F5 6F D0 54 2E 9E 70 8C F1 9A 91 6F 92 ED BF 1A 6A 90 4E 5C A6 E0 E6 B9 B0 CF 55 AC 4F 3D
40 07 0E CA 90 85 F8 92 18 20 89 56 E0 52 89 28 0D 87 56 18 05 A5 72 AA D1 61 62 11 EC 16 C0 9B

30.
77 01 F5 6F D0 54 2E 9E 70 8C F1 9A 91 6F 92 ED BF 1A 6A 90 4E 5C A6 E0 E6 B9 B0 CF 55 2C 4F 3D
40 07 0E CA 90 85 F8 92 18 20 89 56 E0 52 89 28 0D 87 56 18 05 A5 72 AA D1 61 62 11 EC 16 C0 9B
31.
77 01 F5 6F D0 54 2E 9E 70 8C F1 9A 91 6F 92 ED BF 1A 6A 90 4E 5C A6 E0 E6 B9 B0 CF 55 2C 7D 3D
40 07 0E CA 90 85 F8 92 18 20 89 56 E0 52 89 28 0D 87 56 18 05 A5 72 AA D1 61 62 11 EC 16 C0 9B
32.
77 01 F5 6F D0 54 2E 9E 70 8C F1 9A 91 6F 92 ED BF 1A 6A 90 4E 5C A6 E0 E6 B9 B0 CF 55 2C 7D 7B
40 07 0E CA 90 85 F8 92 18 20 89 56 E0 52 89 28 0D 87 56 18 05 A5 72 AA D1 61 62 11 EC 16 C0 9B
33.
77 01 F5 6F D0 54 2E 9E 70 8C F1 9A 91 6F 92 ED BF 1A 6A 90 4E 5C A6 E0 E6 B9 B0 CF 55 2C 7D 7B
91 07 0E CA 90 85 F8 92 18 20 89 56 E0 52 89 28 0D 87 56 18 05 A5 72 AA D1 61 62 11 EC 16 C0 9B
34.
77 01 F5 6F D0 54 2E 9E 70 8C F1 9A 91 6F 92 ED BF 1A 6A 90 4E 5C A6 E0 E6 B9 B0 CF 55 2C 7D 7B
91 B7 0E CA 90 85 F8 92 18 20 89 56 E0 52 89 28 0D 87 56 18 05 A5 72 AA D1 61 62 11 EC 16 C0 9B
35.
77 01 F5 6F D0 54 2E 9E 70 8C F1 9A 91 6F 92 ED BF 1A 6A 90 4E 5C A6 E0 E6 B9 B0 CF 55 2C 7D 7B
91 B7 3A CA 90 85 F8 92 18 20 89 56 E0 52 89 28 0D 87 56 18 05 A5 72 AA D1 61 62 11 EC 16 C0 9B
36.
77 01 F5 6F D0 54 2E 9E 70 8C F1 9A 91 6F 92 ED BF 1A 6A 90 4E 5C A6 E0 E6 B9 B0 CF 55 2C 7D 7B
91 B7 3A D0 90 85 F8 92 18 20 89 56 E0 52 89 28 0D 87 56 18 05 A5 72 AA D1 61 62 11 EC 16 C0 9B
37.
77 01 F5 6F D0 54 2E 9E 70 8C F1 9A 91 6F 92 ED BF 1A 6A 90 4E 5C A6 E0 E6 B9 B0 CF 55 2C 7D 7B
91 B7 3A D0 D7 85 F8 92 18 20 89 56 E0 52 89 28 0D 87 56 18 05 A5 72 AA D1 61 62 11 EC 16 C0 9B
38.
77 01 F5 6F D0 54 2E 9E 70 8C F1 9A 91 6F 92 ED BF 1A 6A 90 4E 5C A6 E0 E6 B9 B0 CF 55 2C 7D 7B
91 B7 3A D0 D7 F1 F8 92 18 20 89 56 E0 52 89 28 0D 87 56 18 05 A5 72 AA D1 61 62 11 EC 16 C0 9B
39.
77 01 F5 6F D0 54 2E 9E 70 8C F1 9A 91 6F 92 ED BF 1A 6A 90 4E 5C A6 E0 E6 B9 B0 CF 55 2C 7D 7B
91 B7 3A D0 D7 F1 F5 92 18 20 89 56 E0 52 89 28 0D 87 56 18 05 A5 72 AA D1 61 62 11 EC 16 C0 9B
40.
77 01 F5 6F D0 54 2E 9E 70 8C F1 9A 91 6F 92 ED BF 1A 6A 90 4E 5C A6 E0 E6 B9 B0 CF 55 2C 7D 7B
91 B7 3A D0 D7 F1 F5 0F 18 20 89 56 E0 52 89 28 0D 87 56 18 05 A5 72 AA D1 61 62 11 EC 16 C0 9B
41.
77 01 F5 6F D0 54 2E 9E 70 8C F1 9A 91 6F 92 ED BF 1A 6A 90 4E 5C A6 E0 E6 B9 B0 CF 55 2C 7D 7B
91 B7 3A D0 D7 F1 F5 0F BE 20 89 56 E0 52 89 28 0D 87 56 18 05 A5 72 AA D1 61 62 11 EC 16 C0 9B
42.
77 01 F5 6F D0 54 2E 9E 70 8C F1 9A 91 6F 92 ED BF 1A 6A 90 4E 5C A6 E0 E6 B9 B0 CF 55 2C 7D 7B
91 B7 3A D0 D7 F1 F5 0F BE B6 89 56 E0 52 89 28 0D 87 56 18 05 A5 72 AA D1 61 62 11 EC 16 C0 9B
43.
77 01 F5 6F D0 54 2E 9E 70 8C F1 9A 91 6F 92 ED BF 1A 6A 90 4E 5C A6 E0 E6 B9 B0 CF 55 2C 7D 7B
91 B7 3A D0 D7 F1 F5 0F BE B6 04 56 E0 52 89 28 0D 87 56 18 05 A5 72 AA D1 61 62 11 EC 16 C0 9B
44.
77 01 F5 6F D0 54 2E 9E 70 8C F1 9A 91 6F 92 ED BF 1A 6A 90 4E 5C A6 E0 E6 B9 B0 CF 55 2C 7D 7B
91 B7 3A D0 D7 F1 F5 0F BE B6 04 90 E0 52 89 28 0D 87 56 18 05 A5 72 AA D1 61 62 11 EC 16 C0 9B
45.
77 01 F5 6F D0 54 2E 9E 70 8C F1 9A 91 6F 92 ED BF 1A 6A 90 4E 5C A6 E0 E6 B9 B0 CF 55 2C 7D 7B
91 B7 3A D0 D7 F1 F5 0F BE B6 04 90 04 52 89 28 0D 87 56 18 05 A5 72 AA D1 61 62 11 EC 16 C0 9B
46.
77 01 F5 6F D0 54 2E 9E 70 8C F1 9A 91 6F 92 ED BF 1A 6A 90 4E 5C A6 E0 E6 B9 B0 CF 55 2C 7D 7B
91 B7 3A D0 D7 F1 F5 0F BE B6 04 90 04 4C 89 28 0D 87 56 18 05 A5 72 AA D1 61 62 11 EC 16 C0 9B
47.
77 01 F5 6F D0 54 2E 9E 70 8C F1 9A 91 6F 92 ED BF 1A 6A 90 4E 5C A6 E0 E6 B9 B0 CF 55 2C 7D 7B
91 B7 3A D0 D7 F1 F5 0F BE B6 04 90 04 4C E4 28 0D 87 56 18 05 A5 72 AA D1 61 62 11 EC 16 C0 9B
48.
77 01 F5 6F D0 54 2E 9E 70 8C F1 9A 91 6F 92 ED BF 1A 6A 90 4E 5C A6 E0 E6 B9 B0 CF 55 2C 7D 7B
91 B7 3A D0 D7 F1 F5 0F BE B6 04 90 04 4C E4 19 0D 87 56 18 05 A5 72 AA D1 61 62 11 EC 16 C0 9B
49.
77 01 F5 6F D0 54 2E 9E 70 8C F1 9A 91 6F 92 ED BF 1A 6A 90 4E 5C A6 E0 E6 B9 B0 CF 55 2C 7D 7B
91 B7 3A D0 D7 F1 F5 0F BE B6 04 90 04 4C E4 19 11 87 56 18 05 A5 72 AA D1 61 62 11 EC 16 C0 9B
50.
77 01 F5 6F D0 54 2E 9E 70 8C F1 9A 91 6F 92 ED BF 1A 6A 90 4E 5C A6 E0 E6 B9 B0 CF 55 2C 7D 7B
91 B7 3A D0 D7 F1 F5 0F BE B6 04 90 04 4C E4 19 11 B7 56 18 05 A5 72 AA D1 61 62 11 EC 16 C0 9B
51.
77 01 F5 6F D0 54 2E 9E 70 8C F1 9A 91 6F 92 ED BF 1A 6A 90 4E 5C A6 E0 E6 B9 B0 CF 55 2C 7D 7B
91 B7 3A D0 D7 F1 F5 0F BE B6 04 90 04 4C E4 19 11 B7 1D 18 05 A5 72 AA D1 61 62 11 EC 16 C0 9B
52.
77 01 F5 6F D0 54 2E 9E 70 8C F1 9A 91 6F 92 ED BF 1A 6A 90 4E 5C A6 E0 E6 B9 B0 CF 55 2C 7D 7B
91 B7 3A D0 D7 F1 F5 0F BE B6 04 90 04 4C E4 19 11 B7 1D F2 05 A5 72 AA D1 61 62 11 EC 16 C0 9B
53.
77 01 F5 6F D0 54 2E 9E 70 8C F1 9A 91 6F 92 ED BF 1A 6A 90 4E 5C A6 E0 E6 B9 B0 CF 55 2C 7D 7B
91 B7 3A D0 D7 F1 F5 0F BE B6 04 90 04 4C E4 19 11 B7 1D F2 21 A5 72 AA D1 61 62 11 EC 16 C0 9B
54.
77 01 F5 6F D0 54 2E 9E 70 8C F1 9A 91 6F 92 ED BF 1A 6A 90 4E 5C A6 E0 E6 B9 B0 CF 55 2C 7D 7B

91 B7 3A D0 D7 F1 F5 0F BE B6 04 90 04 4C E4 19 11 B7 1D F2 21 97 72 AA D1 61 62 11 EC 16 C0 9B
55.
77 01 F5 6F D0 54 2E 9E 70 8C F1 9A 91 6F 92 ED BF 1A 6A 90 4E 5C A6 E0 E6 B9 B0 CF 55 2C 7D 7B
91 B7 3A D0 D7 F1 F5 0F BE B6 04 90 04 4C E4 19 11 B7 1D F2 21 97 54 AA D1 61 62 11 EC 16 C0 9B
56.
77 01 F5 6F D0 54 2E 9E 70 8C F1 9A 91 6F 92 ED BF 1A 6A 90 4E 5C A6 E0 E6 B9 B0 CF 55 2C 7D 7B
91 B7 3A D0 D7 F1 F5 0F BE B6 04 90 04 4C E4 19 11 B7 1D F2 21 97 54 95 D1 61 62 11 EC 16 C0 9B
57.
77 01 F5 6F D0 54 2E 9E 70 8C F1 9A 91 6F 92 ED BF 1A 6A 90 4E 5C A6 E0 E6 B9 B0 CF 55 2C 7D 7B
91 B7 3A D0 D7 F1 F5 0F BE B6 04 90 04 4C E4 19 11 B7 1D F2 21 97 54 95 0E 61 62 11 EC 16 C0 9B
58.
77 01 F5 6F D0 54 2E 9E 70 8C F1 9A 91 6F 92 ED BF 1A 6A 90 4E 5C A6 E0 E6 B9 B0 CF 55 2C 7D 7B
91 B7 3A D0 D7 F1 F5 0F BE B6 04 90 04 4C E4 19 11 B7 1D F2 21 97 54 95 0E 78 62 11 EC 16 C0 9B
59.
77 01 F5 6F D0 54 2E 9E 70 8C F1 9A 91 6F 92 ED BF 1A 6A 90 4E 5C A6 E0 E6 B9 B0 CF 55 2C 7D 7B
91 B7 3A D0 D7 F1 F5 0F BE B6 04 90 04 4C E4 19 11 B7 1D F2 21 97 54 95 0E 78 9A 11 EC 16 C0 9B
60.
77 01 F5 6F D0 54 2E 9E 70 8C F1 9A 91 6F 92 ED BF 1A 6A 90 4E 5C A6 E0 E6 B9 B0 CF 55 2C 7D 7B
91 B7 3A D0 D7 F1 F5 0F BE B6 04 90 04 4C E4 19 11 B7 1D F2 21 97 54 95 0E 78 9A 2B EC 16 C0 9B
61.
77 01 F5 6F D0 54 2E 9E 70 8C F1 9A 91 6F 92 ED BF 1A 6A 90 4E 5C A6 E0 E6 B9 B0 CF 55 2C 7D 7B
91 B7 3A D0 D7 F1 F5 0F BE B6 04 90 04 4C E4 19 11 B7 1D F2 21 97 54 95 0E 78 9A 2B 32 16 C0 9B
62.
77 01 F5 6F D0 54 2E 9E 70 8C F1 9A 91 6F 92 ED BF 1A 6A 90 4E 5C A6 E0 E6 B9 B0 CF 55 2C 7D 7B
91 B7 3A D0 D7 F1 F5 0F BE B6 04 90 04 4C E4 19 11 B7 1D F2 21 97 54 95 0E 78 9A 2B 32 2D C0 9B
63.
77 01 F5 6F D0 54 2E 9E 70 8C F1 9A 91 6F 92 ED BF 1A 6A 90 4E 5C A6 E0 E6 B9 B0 CF 55 2C 7D 7B
91 B7 3A D0 D7 F1 F5 0F BE B6 04 90 04 4C E4 19 11 B7 1D F2 21 97 54 95 0E 78 9A 2B 32 2D 26 9B
64.
77 01 F5 6F D0 54 2E 9E 70 8C F1 9A 91 6F 92 ED BF 1A 6A 90 4E 5C A6 E0 E6 B9 B0 CF 55 2C 7D 7B
91 B7 3A D0 D7 F1 F5 0F BE B6 04 90 04 4C E4 19 11 B7 1D F2 21 97 54 95 0E 78 9A 2B 32 2D 26 00

Stage 3.

Input sequence

9B C0 16 EC 11 62 61 D1 AA 72 A5 05 18 56 87 0D 28 89 52 E0 56 89 20 18 92 F8 85 90 CA 0E 07 40
3D 4F AC B2 DE 86 39 06 BD DE E8 C9 CD 4F 1B 3C FB A9 81 F5 64 3F A6 B2 99 E0 79 EA C5 58 21 9D

Calculating SR state for stage 3. Total 64 steps.

1.
82 01 F5 6F D0 54 2E 9E 70 8C F1 9A 91 6F 92 ED BF 1A 6A 90 4E 5C A6 E0 E6 B9 B0 CF 55 2C 7D 7B
91 B7 3A D0 D7 F1 F5 0F BE B6 04 90 04 4C E4 19 11 B7 1D F2 21 97 54 95 0E 78 9A 2B 32 2D 26 00
2.
82 2A F5 6F D0 54 2E 9E 70 8C F1 9A 91 6F 92 ED BF 1A 6A 90 4E 5C A6 E0 E6 B9 B0 CF 55 2C 7D 7B
91 B7 3A D0 D7 F1 F5 0F BE B6 04 90 04 4C E4 19 11 B7 1D F2 21 97 54 95 0E 78 9A 2B 32 2D 26 00
3.
82 2A 38 6F D0 54 2E 9E 70 8C F1 9A 91 6F 92 ED BF 1A 6A 90 4E 5C A6 E0 E6 B9 B0 CF 55 2C 7D 7B
91 B7 3A D0 D7 F1 F5 0F BE B6 04 90 04 4C E4 19 11 B7 1D F2 21 97 54 95 0E 78 9A 2B 32 2D 26 00
4.
82 2A 38 8E D0 54 2E 9E 70 8C F1 9A 91 6F 92 ED BF 1A 6A 90 4E 5C A6 E0 E6 B9 B0 CF 55 2C 7D 7B
91 B7 3A D0 D7 F1 F5 0F BE B6 04 90 04 4C E4 19 11 B7 1D F2 21 97 54 95 0E 78 9A 2B 32 2D 26 00
5.
82 2A 38 8E CB 54 2E 9E 70 8C F1 9A 91 6F 92 ED BF 1A 6A 90 4E 5C A6 E0 E6 B9 B0 CF 55 2C 7D 7B
91 B7 3A D0 D7 F1 F5 0F BE B6 04 90 04 4C E4 19 11 B7 1D F2 21 97 54 95 0E 78 9A 2B 32 2D 26 00
6.
82 2A 38 8E CB 75 2E 9E 70 8C F1 9A 91 6F 92 ED BF 1A 6A 90 4E 5C A6 E0 E6 B9 B0 CF 55 2C 7D 7B
91 B7 3A D0 D7 F1 F5 0F BE B6 04 90 04 4C E4 19 11 B7 1D F2 21 97 54 95 0E 78 9A 2B 32 2D 26 00
7.
82 2A 38 8E CB 75 29 9E 70 8C F1 9A 91 6F 92 ED BF 1A 6A 90 4E 5C A6 E0 E6 B9 B0 CF 55 2C 7D 7B
91 B7 3A D0 D7 F1 F5 0F BE B6 04 90 04 4C E4 19 11 B7 1D F2 21 97 54 95 0E 78 9A 2B 32 2D 26 00
8.
82 2A 38 8E CB 75 29 CB 70 8C F1 9A 91 6F 92 ED BF 1A 6A 90 4E 5C A6 E0 E6 B9 B0 CF 55 2C 7D 7B
91 B7 3A D0 D7 F1 F5 0F BE B6 04 90 04 4C E4 19 11 B7 1D F2 21 97 54 95 0E 78 9A 2B 32 2D 26 00
9.
82 2A 38 8E CB 75 29 CB 1F 8C F1 9A 91 6F 92 ED BF 1A 6A 90 4E 5C A6 E0 E6 B9 B0 CF 55 2C 7D 7B
91 B7 3A D0 D7 F1 F5 0F BE B6 04 90 04 4C E4 19 11 B7 1D F2 21 97 54 95 0E 78 9A 2B 32 2D 26 00
10.
82 2A 38 8E CB 75 29 CB 1F E2 F1 9A 91 6F 92 ED BF 1A 6A 90 4E 5C A6 E0 E6 B9 B0 CF 55 2C 7D 7B
91 B7 3A D0 D7 F1 F5 0F BE B6 04 90 04 4C E4 19 11 B7 1D F2 21 97 54 95 0E 78 9A 2B 32 2D 26 00
11.
82 2A 38 8E CB 75 29 CB 1F E2 7A 9A 91 6F 92 ED BF 1A 6A 90 4E 5C A6 E0 E6 B9 B0 CF 55 2C 7D 7B

91 B7 3A D0 D7 F1 F5 0F BE B6 04 90 04 4C E4 19 11 B7 1D F2 21 97 54 95 0E 78 9A 2B 32 2D 26 00
12.
82 2A 38 8E CB 75 29 CB 1F E2 7A 0A 91 6F 92 ED BF 1A 6A 90 4E 5C A6 E0 E6 B9 B0 CF 55 2C 7D 7B
91 B7 3A D0 D7 F1 F5 0F BE B6 04 90 04 4C E4 19 11 B7 1D F2 21 97 54 95 0E 78 9A 2B 32 2D 26 00
13.
82 2A 38 8E CB 75 29 CB 1F E2 7A 0A 92 6F 92 ED BF 1A 6A 90 4E 5C A6 E0 E6 B9 B0 CF 55 2C 7D 7B
91 B7 3A D0 D7 F1 F5 0F BE B6 04 90 04 4C E4 19 11 B7 1D F2 21 97 54 95 0E 78 9A 2B 32 2D 26 00
14.
82 2A 38 8E CB 75 29 CB 1F E2 7A 0A 92 DF 92 ED BF 1A 6A 90 4E 5C A6 E0 E6 B9 B0 CF 55 2C 7D 7B
91 B7 3A D0 D7 F1 F5 0F BE B6 04 90 04 4C E4 19 11 B7 1D F2 21 97 54 95 0E 78 9A 2B 32 2D 26 00
15.
82 2A 38 8E CB 75 29 CB 1F E2 7A 0A 92 DF 9F ED BF 1A 6A 90 4E 5C A6 E0 E6 B9 B0 CF 55 2C 7D 7B
91 B7 3A D0 D7 F1 F5 0F BE B6 04 90 04 4C E4 19 11 B7 1D F2 21 97 54 95 0E 78 9A 2B 32 2D 26 00
16.
82 2A 38 8E CB 75 29 CB 1F E2 7A 0A 92 DF 9F 91 BF 1A 6A 90 4E 5C A6 E0 E6 B9 B0 CF 55 2C 7D 7B
91 B7 3A D0 D7 F1 F5 0F BE B6 04 90 04 4C E4 19 11 B7 1D F2 21 97 54 95 0E 78 9A 2B 32 2D 26 00
17.
82 2A 38 8E CB 75 29 CB 1F E2 7A 0A 92 DF 9F 91 77 1A 6A 90 4E 5C A6 E0 E6 B9 B0 CF 55 2C 7D 7B
91 B7 3A D0 D7 F1 F5 0F BE B6 04 90 04 4C E4 19 11 B7 1D F2 21 97 54 95 0E 78 9A 2B 32 2D 26 00
18.
82 2A 38 8E CB 75 29 CB 1F E2 7A 0A 92 DF 9F 91 77 D6 6A 90 4E 5C A6 E0 E6 B9 B0 CF 55 2C 7D 7B
91 B7 3A D0 D7 F1 F5 0F BE B6 04 90 04 4C E4 19 11 B7 1D F2 21 97 54 95 0E 78 9A 2B 32 2D 26 00
19.
82 2A 38 8E CB 75 29 CB 1F E2 7A 0A 92 DF 9F 91 77 D6 EE 90 4E 5C A6 E0 E6 B9 B0 CF 55 2C 7D 7B
91 B7 3A D0 D7 F1 F5 0F BE B6 04 90 04 4C E4 19 11 B7 1D F2 21 97 54 95 0E 78 9A 2B 32 2D 26 00
20.
82 2A 38 8E CB 75 29 CB 1F E2 7A 0A 92 DF 9F 91 77 D6 EE E9 4E 5C A6 E0 E6 B9 B0 CF 55 2C 7D 7B
91 B7 3A D0 D7 F1 F5 0F BE B6 04 90 04 4C E4 19 11 B7 1D F2 21 97 54 95 0E 78 9A 2B 32 2D 26 00
21.
82 2A 38 8E CB 75 29 CB 1F E2 7A 0A 92 DF 9F 91 77 D6 EE E9 2E 5C A6 E0 E6 B9 B0 CF 55 2C 7D 7B
91 B7 3A D0 D7 F1 F5 0F BE B6 04 90 04 4C E4 19 11 B7 1D F2 21 97 54 95 0E 78 9A 2B 32 2D 26 00
22.
82 2A 38 8E CB 75 29 CB 1F E2 7A 0A 92 DF 9F 91 77 D6 EE E9 2E 87 A6 E0 E6 B9 B0 CF 55 2C 7D 7B
91 B7 3A D0 D7 F1 F5 0F BE B6 04 90 04 4C E4 19 11 B7 1D F2 21 97 54 95 0E 78 9A 2B 32 2D 26 00
23.
82 2A 38 8E CB 75 29 CB 1F E2 7A 0A 92 DF 9F 91 77 D6 EE E9 2E 87 74 E0 E6 B9 B0 CF 55 2C 7D 7B
91 B7 3A D0 D7 F1 F5 0F BE B6 04 90 04 4C E4 19 11 B7 1D F2 21 97 54 95 0E 78 9A 2B 32 2D 26 00
24.
82 2A 38 8E CB 75 29 CB 1F E2 7A 0A 92 DF 9F 91 77 D6 EE E9 2E 87 74 50 E6 B9 B0 CF 55 2C 7D 7B
91 B7 3A D0 D7 F1 F5 0F BE B6 04 90 04 4C E4 19 11 B7 1D F2 21 97 54 95 0E 78 9A 2B 32 2D 26 00
25.
82 2A 38 8E CB 75 29 CB 1F E2 7A 0A 92 DF 9F 91 77 D6 EE E9 2E 87 74 50 98 B9 B0 CF 55 2C 7D 7B
91 B7 3A D0 D7 F1 F5 0F BE B6 04 90 04 4C E4 19 11 B7 1D F2 21 97 54 95 0E 78 9A 2B 32 2D 26 00
26.
82 2A 38 8E CB 75 29 CB 1F E2 7A 0A 92 DF 9F 91 77 D6 EE E9 2E 87 74 50 98 E6 B0 CF 55 2C 7D 7B
91 B7 3A D0 D7 F1 F5 0F BE B6 04 90 04 4C E4 19 11 B7 1D F2 21 97 54 95 0E 78 9A 2B 32 2D 26 00
27.
82 2A 38 8E CB 75 29 CB 1F E2 7A 0A 92 DF 9F 91 77 D6 EE E9 2E 87 74 50 98 E6 43 CF 55 2C 7D 7B
91 B7 3A D0 D7 F1 F5 0F BE B6 04 90 04 4C E4 19 11 B7 1D F2 21 97 54 95 0E 78 9A 2B 32 2D 26 00
28.
82 2A 38 8E CB 75 29 CB 1F E2 7A 0A 92 DF 9F 91 77 D6 EE E9 2E 87 74 50 98 E6 43 44 55 2C 7D 7B
91 B7 3A D0 D7 F1 F5 0F BE B6 04 90 04 4C E4 19 11 B7 1D F2 21 97 54 95 0E 78 9A 2B 32 2D 26 00
29.
82 2A 38 8E CB 75 29 CB 1F E2 7A 0A 92 DF 9F 91 77 D6 EE E9 2E 87 74 50 98 E6 43 44 7B 2C 7D 7B
91 B7 3A D0 D7 F1 F5 0F BE B6 04 90 04 4C E4 19 11 B7 1D F2 21 97 54 95 0E 78 9A 2B 32 2D 26 00
30.
82 2A 38 8E CB 75 29 CB 1F E2 7A 0A 92 DF 9F 91 77 D6 EE E9 2E 87 74 50 98 E6 43 44 7B F5 7D 7B
91 B7 3A D0 D7 F1 F5 0F BE B6 04 90 04 4C E4 19 11 B7 1D F2 21 97 54 95 0E 78 9A 2B 32 2D 26 00
31.
82 2A 38 8E CB 75 29 CB 1F E2 7A 0A 92 DF 9F 91 77 D6 EE E9 2E 87 74 50 98 E6 43 44 7B F5 F8 7B
91 B7 3A D0 D7 F1 F5 0F BE B6 04 90 04 4C E4 19 11 B7 1D F2 21 97 54 95 0E 78 9A 2B 32 2D 26 00
32.
82 2A 38 8E CB 75 29 CB 1F E2 7A 0A 92 DF 9F 91 77 D6 EE E9 2E 87 74 50 98 E6 43 44 7B F5 F8 B9
91 B7 3A D0 D7 F1 F5 0F BE B6 04 90 04 4C E4 19 11 B7 1D F2 21 97 54 95 0E 78 9A 2B 32 2D 26 00
33.
82 2A 38 8E CB 75 29 CB 1F E2 7A 0A 92 DF 9F 91 77 D6 EE E9 2E 87 74 50 98 E6 43 44 7B F5 F8 B9
33 B7 3A D0 D7 F1 F5 0F BE B6 04 90 04 4C E4 19 11 B7 1D F2 21 97 54 95 0E 78 9A 2B 32 2D 26 00
34.
82 2A 38 8E CB 75 29 CB 1F E2 7A 0A 92 DF 9F 91 77 D6 EE E9 2E 87 74 50 98 E6 43 44 7B F5 F8 B9
33 7A 3A D0 D7 F1 F5 0F BE B6 04 90 04 4C E4 19 11 B7 1D F2 21 97 54 95 0E 78 9A 2B 32 2D 26 00
35.
82 2A 38 8E CB 75 29 CB 1F E2 7A 0A 92 DF 9F 91 77 D6 EE E9 2E 87 74 50 98 E6 43 44 7B F5 F8 B9
33 7A EA D0 D7 F1 F5 0F BE B6 04 90 04 4C E4 19 11 B7 1D F2 21 97 54 95 0E 78 9A 2B 32 2D 26 00
36.

82 2A 38 8E CB 75 29 CB 1F E2 7A 0A 92 DF 9F 91 77 D6 EE E9 2E 87 74 50 98 E6 43 44 7B F5 F8 B9
33 7A EA F3 D7 F1 F5 0F BE B6 04 90 04 4C E4 19 11 B7 1D F2 21 97 54 95 0E 78 9A 2B 32 2D 26 00
37.
82 2A 38 8E CB 75 29 CB 1F E2 7A 0A 92 DF 9F 91 77 D6 EE E9 2E 87 74 50 98 E6 43 44 7B F5 F8 B9
33 7A EA F3 AB F1 F5 0F BE B6 04 90 04 4C E4 19 11 B7 1D F2 21 97 54 95 0E 78 9A 2B 32 2D 26 00
38.
82 2A 38 8E CB 75 29 CB 1F E2 7A 0A 92 DF 9F 91 77 D6 EE E9 2E 87 74 50 98 E6 43 44 7B F5 F8 B9
33 7A EA F3 AB E1 F5 0F BE B6 04 90 04 4C E4 19 11 B7 1D F2 21 97 54 95 0E 78 9A 2B 32 2D 26 00
39.
82 2A 38 8E CB 75 29 CB 1F E2 7A 0A 92 DF 9F 91 77 D6 EE E9 2E 87 74 50 98 E6 43 44 7B F5 F8 B9
33 7A EA F3 AB E1 52 0F BE B6 04 90 04 4C E4 19 11 B7 1D F2 21 97 54 95 0E 78 9A 2B 32 2D 26 00
40.
82 2A 38 8E CB 75 29 CB 1F E2 7A 0A 92 DF 9F 91 77 D6 EE E9 2E 87 74 50 98 E6 43 44 7B F5 F8 B9
33 7A EA F3 AB E1 52 86 BE B6 04 90 04 4C E4 19 11 B7 1D F2 21 97 54 95 0E 78 9A 2B 32 2D 26 00
41.
82 2A 38 8E CB 75 29 CB 1F E2 7A 0A 92 DF 9F 91 77 D6 EE E9 2E 87 74 50 98 E6 43 44 7B F5 F8 B9
33 7A EA F3 AB E1 52 86 5C B6 04 90 04 4C E4 19 11 B7 1D F2 21 97 54 95 0E 78 9A 2B 32 2D 26 00
42.
82 2A 38 8E CB 75 29 CB 1F E2 7A 0A 92 DF 9F 91 77 D6 EE E9 2E 87 74 50 98 E6 43 44 7B F5 F8 B9
33 7A EA F3 AB E1 52 86 5C 39 04 90 04 4C E4 19 11 B7 1D F2 21 97 54 95 0E 78 9A 2B 32 2D 26 00
43.
82 2A 38 8E CB 75 29 CB 1F E2 7A 0A 92 DF 9F 91 77 D6 EE E9 2E 87 74 50 98 E6 43 44 7B F5 F8 B9
33 7A EA F3 AB E1 52 86 5C 39 CA 90 04 4C E4 19 11 B7 1D F2 21 97 54 95 0E 78 9A 2B 32 2D 26 00
44.
82 2A 38 8E CB 75 29 CB 1F E2 7A 0A 92 DF 9F 91 77 D6 EE E9 2E 87 74 50 98 E6 43 44 7B F5 F8 B9
33 7A EA F3 AB E1 52 86 5C 39 CA 9A 04 4C E4 19 11 B7 1D F2 21 97 54 95 0E 78 9A 2B 32 2D 26 00
45.
82 2A 38 8E CB 75 29 CB 1F E2 7A 0A 92 DF 9F 91 77 D6 EE E9 2E 87 74 50 98 E6 43 44 7B F5 F8 B9
33 7A EA F3 AB E1 52 86 5C 39 CA 9A DB 4C E4 19 11 B7 1D F2 21 97 54 95 0E 78 9A 2B 32 2D 26 00
46.
82 2A 38 8E CB 75 29 CB 1F E2 7A 0A 92 DF 9F 91 77 D6 EE E9 2E 87 74 50 98 E6 43 44 7B F5 F8 B9
33 7A EA F3 AB E1 52 86 5C 39 CA 9A DB 67 E4 19 11 B7 1D F2 21 97 54 95 0E 78 9A 2B 32 2D 26 00
47.
82 2A 38 8E CB 75 29 CB 1F E2 7A 0A 92 DF 9F 91 77 D6 EE E9 2E 87 74 50 98 E6 43 44 7B F5 F8 B9
33 7A EA F3 AB E1 52 86 5C 39 CA 9A DB 67 0D 19 11 B7 1D F2 21 97 54 95 0E 78 9A 2B 32 2D 26 00
48.
82 2A 38 8E CB 75 29 CB 1F E2 7A 0A 92 DF 9F 91 77 D6 EE E9 2E 87 74 50 98 E6 43 44 7B F5 F8 B9
33 7A EA F3 AB E1 52 86 5C 39 CA 9A DB 67 0D EF 11 B7 1D F2 21 97 54 95 0E 78 9A 2B 32 2D 26 00
49.
82 2A 38 8E CB 75 29 CB 1F E2 7A 0A 92 DF 9F 91 77 D6 EE E9 2E 87 74 50 98 E6 43 44 7B F5 F8 B9
33 7A EA F3 AB E1 52 86 5C 39 CA 9A DB 67 0D EF 95 B7 1D F2 21 97 54 95 0E 78 9A 2B 32 2D 26 00
50.
82 2A 38 8E CB 75 29 CB 1F E2 7A 0A 92 DF 9F 91 77 D6 EE E9 2E 87 74 50 98 E6 43 44 7B F5 F8 B9
33 7A EA F3 AB E1 52 86 5C 39 CA 9A DB 67 0D EF 95 31 1D F2 21 97 54 95 0E 78 9A 2B 32 2D 26 00
51.
82 2A 38 8E CB 75 29 CB 1F E2 7A 0A 92 DF 9F 91 77 D6 EE E9 2E 87 74 50 98 E6 43 44 7B F5 F8 B9
33 7A EA F3 AB E1 52 86 5C 39 CA 9A DB 67 0D EF 95 31 87 F2 21 97 54 95 0E 78 9A 2B 32 2D 26 00
52.
82 2A 38 8E CB 75 29 CB 1F E2 7A 0A 92 DF 9F 91 77 D6 EE E9 2E 87 74 50 98 E6 43 44 7B F5 F8 B9
33 7A EA F3 AB E1 52 86 5C 39 CA 9A DB 67 0D EF 95 31 87 B4 21 97 54 95 0E 78 9A 2B 32 2D 26 00
53.
82 2A 38 8E CB 75 29 CB 1F E2 7A 0A 92 DF 9F 91 77 D6 EE E9 2E 87 74 50 98 E6 43 44 7B F5 F8 B9
33 7A EA F3 AB E1 52 86 5C 39 CA 9A DB 67 0D EF 95 31 87 B4 2D 97 54 95 0E 78 9A 2B 32 2D 26 00
54.
82 2A 38 8E CB 75 29 CB 1F E2 7A 0A 92 DF 9F 91 77 D6 EE E9 2E 87 74 50 98 E6 43 44 7B F5 F8 B9
33 7A EA F3 AB E1 52 86 5C 39 CA 9A DB 67 0D EF 95 31 87 B4 2D 28 54 95 0E 78 9A 2B 32 2D 26 00
55.
82 2A 38 8E CB 75 29 CB 1F E2 7A 0A 92 DF 9F 91 77 D6 EE E9 2E 87 74 50 98 E6 43 44 7B F5 F8 B9
33 7A EA F3 AB E1 52 86 5C 39 CA 9A DB 67 0D EF 95 31 87 B4 2D 28 DD 95 0E 78 9A 2B 32 2D 26 00
56.
82 2A 38 8E CB 75 29 CB 1F E2 7A 0A 92 DF 9F 91 77 D6 EE E9 2E 87 74 50 98 E6 43 44 7B F5 F8 B9
33 7A EA F3 AB E1 52 86 5C 39 CA 9A DB 67 0D EF 95 31 87 B4 2D 28 DD 32 0E 78 9A 2B 32 2D 26 00
57.
82 2A 38 8E CB 75 29 CB 1F E2 7A 0A 92 DF 9F 91 77 D6 EE E9 2E 87 74 50 98 E6 43 44 7B F5 F8 B9
33 7A EA F3 AB E1 52 86 5C 39 CA 9A DB 67 0D EF 95 31 87 B4 2D 28 DD 32 AF 78 9A 2B 32 2D 26 00
58.
82 2A 38 8E CB 75 29 CB 1F E2 7A 0A 92 DF 9F 91 77 D6 EE E9 2E 87 74 50 98 E6 43 44 7B F5 F8 B9
33 7A EA F3 AB E1 52 86 5C 39 CA 9A DB 67 0D EF 95 31 87 B4 2D 28 DD 32 AF 5B 9A 2B 32 2D 26 00
59.
82 2A 38 8E CB 75 29 CB 1F E2 7A 0A 92 DF 9F 91 77 D6 EE E9 2E 87 74 50 98 E6 43 44 7B F5 F8 B9
33 7A EA F3 AB E1 52 86 5C 39 CA 9A DB 67 0D EF 95 31 87 B4 2D 28 DD 32 AF 5B EC 2B 32 2D 26 00
60.
82 2A 38 8E CB 75 29 CB 1F E2 7A 0A 92 DF 9F 91 77 D6 EE E9 2E 87 74 50 98 E6 43 44 7B F5 F8 B9
33 7A EA F3 AB E1 52 86 5C 39 CA 9A DB 67 0D EF 95 31 87 B4 2D 28 DD 32 AF 5B EC C3 32 2D 26 00

61.
82 2A 38 8E CB 75 29 CB 1F E2 7A 0A 92 DF 9F 91 77 D6 EE E9 2E 87 74 50 98 E6 43 44 7B F5 F8 B9
33 7A EA F3 AB E1 52 86 5C 39 CA 9A DB 67 0D EF 95 31 87 B4 2D 28 DD 32 AF 5B EC C3 60 2D 26 00
62.
82 2A 38 8E CB 75 29 CB 1F E2 7A 0A 92 DF 9F 91 77 D6 EE E9 2E 87 74 50 98 E6 43 44 7B F5 F8 B9
33 7A EA F3 AB E1 52 86 5C 39 CA 9A DB 67 0D EF 95 31 87 B4 2D 28 DD 32 AF 5B EC C3 60 80 26 00
63.
82 2A 38 8E CB 75 29 CB 1F E2 7A 0A 92 DF 9F 91 77 D6 EE E9 2E 87 74 50 98 E6 43 44 7B F5 F8 B9
33 7A EA F3 AB E1 52 86 5C 39 CA 9A DB 67 0D EF 95 31 87 B4 2D 28 DD 32 AF 5B EC C3 60 80 35 00
64.
82 2A 38 8E CB 75 29 CB 1F E2 7A 0A 92 DF 9F 91 77 D6 EE E9 2E 87 74 50 98 E6 43 44 7B F5 F8 B9
33 7A EA F3 AB E1 52 86 5C 39 CA 9A DB 67 0D EF 95 31 87 B4 2D 28 DD 32 AF 5B EC C3 60 80 35 62

Final message digest:
82 2A 38 8E CB 75 29 CB 1F E2 7A 0A 92 DF 9F 91 77 D6 EE E9 2E 87 74 50 98 E6 43 44 7B F5 F8 B9
33 7A EA F3 AB E1 52 86 5C 39 CA 9A DB 67 0D EF 95 31 87 B4 2D 28 DD 32 AF 5B EC C3 60 80 35 62

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

ShortMsgKAT_224.txt
Algorithm Name: MCSSHA-6
Principal Submitter: Mikhail Maslennikov

Len = 0
Msg = 00
MD = F9A7B5623D984F6EF85F1E86E9E59CF4194B843B64C94299B683AF1C

Len = 1
Msg = 00
MD = 3CB878981C3DFC4F0A449CADE1AF8268C242E3C2730AE7E94BCA2941

Len = 2
Msg = C0
MD = E4644C944C100A73A988F473DA89F25BF31048D04E524FA4EA72B1A2

Len = 3
Msg = C0
MD = CC1D85606A650E930CDCE1C7DD0C2C01C27A8553AAE004CEA96E62A6

Len = 4
Msg = 80
MD = AB9300F1E87BC45792001D147B1C1C0C90F600F68D84A865AD59B8A8

Len = 5
Msg = 48
MD = 116E4ABAF5CD01381EC8B0F70B33B5DFF6A3382F664ACDFA7468740E

Len = 6
Msg = 50
MD = 17451D7EDA5ECED868FA5E9B0F7E61E6ADD2BA05350F53D54F4856C2

LongMsgKAT_224.txt
Algorithm Name: MCSSHA-6
Principal Submitter: Mikhail Maslennikov

Len = 2048
Msg =
724627916C50338643E6996F07877EAFD96BDF01DA7E991D4155B9BE1295EA7D21C9391F4C4A41C75F77E5D273
89253393725F1427F57914B273AB862B9E31DABCE506E558720520D33352D119F699E784F9E548FF91BC35CA147
042128709820D69A8287EA3257857615EB0321270E94B84F446942765CE882B191FAEE7E1C87E0F0BD4E0CD8A9
27703524B559B769CA4ECE1F6DBF313FDCF67C572EC4185C1A88E86EC11B6454B371980020F19633B6B95BD280
E4FBCB0161E1A82470320CEC6ECFA25AC73D09F1536F286D3F9DACAFB2CD1D0CE72D64D197F5C7520B3CCB2FD
74EB72664BA93853EF41EABF52F015DD591500D018DD162815CC993595B195
MD = C9129DEDC461E59C4ABDA3484E40728676EA109C86FB6A2A4A42A26F
Len = 2111
Msg =
919FE5E7F35F64A7487649E564771DBBF10AE204ECC2181312D1A79FB579297C94F0DB9EAAE9E009A4F02057AF2
C973C5DAFA7B60154371A5D2C8E992FB6429176F8424B1A866BC1D1BED00438E97FAB42040DCACDEF7CA9FC20

33059B8898BB40CCFB2634B051797BDF3B915C503EC81839AD01E0F4F2F871EFF2008D40011730BE7A47888E79
55A806876BE120CB0F3A139A3620154ECC6482A70F5629F6A9D3341BE6FBBF48E5AA0C53589A04F057DD44268A
FFCABF75ADFC549F73F454264D46A98CCA80E3000C7446853DD5B430C9344E87E3230555B09FB3E7E64B5AD398
9293AC0FEEC0E75F909696F028A5525D26DDEA5D2B2C813FB3613DFF38CE23209285CC77C60860
MD = 0CC87D30F62118786DA95A17D703E6ADD9C6159E859005AF10C8F923
Len = 2174
Msg =
BD687B6D6684949FBD52A8196DF5D5927B403DEE88A47E4E4B52071BDDA6A6284A9EA1EB84950BA17A60277B0
FEA83C930E5619D5A6D232901B9D3A696662C7FD5F1349B494BC166C67B717C06D03E9FB05DB9EE292D4792F4
59E0ACC08369E3D14684CFF388C940F30738FB71D97EFEB51C7DB553CB85B6FC18429815EC71420822151BB8F5
135DD698EFE3D3118963EE194F94682DFA62EC9D3BCB5F826DA790779704DF2AC5C8A9FA2B50A42A87ED2FBAD
F1E1C8E55689531786A9858DE9E88009E56873FD2D431FCFC99B85574342DC7E78406678BDE94B9A06974DFF15
4EAC3BC7977AC7C123EBCDAC0641A69B792058BA373EDD1BA45E3339C2ABC032993B25F4E3BFA3D5FF620C621
D94C40F8
MD = FB5C3988398A98D9B4979F848F8F82176216F4E4BCA4636709679861
Len = 2237
Msg =
D13409007A6B3242CBAD4CE01D9AED77EFEF0A7725B96A30097EA092FA1E49A136DE03F3F348464C9BEA033216
F380440C7EC81E284738DCC640D485ED32F5D7DD1CF936C1677CBB3CDD8E0E001783FD5A3F388AE6EF7085FF9
A22FA722C7FCCF4CDC239B200D5D11884B565D01C84E4D563C6623C241C5AE0812CE8F9201BBADE48198378A3
E232EF3E10C03022620A266D0A346A6A22F202333A94D2CEF495DBA102B133B8237449C3350BF80EE51B6EE8A9
72CCFC3ED5FD7790444DA253922EEF6C611180F91DF1B6E58E843D318D94A958A017590B14D383C0F385F9CF25
14E8AE1EA749795E10F991E3FB744C6030EF6B02989E8EFFBF8E8BF31FC39B692C517C7C012ECBD0E0785BDEF48
01C4E036C98C6CD0C9328
MD = 3FFCD9C22AF06FC25A45F18F9A8E441D933C839E9B4B7982A3261E98
Len = 2300
Msg =
68F891C11459B2E9B71774E2B8A2A5C3C9CC36072E3498498496F1C7901684F3E9DACF13A3F1BAE22140DEE525
3732E4D4196B534F675264B53D38659727797F0A18910CCB5B48FE2346C2E998B6537357AF8D15826FCB57BA80
4FE143E765F4680A0B28A9E3716A59ABC60EF253E357A4784FF1BE4680C82D797813CE50355D8FDB3C75936CC3
3E1717B99D9A8ADE9D0EA9172662B708EBCBC31C05064FE67B287C56D01C12411E9B890AD16238B36E192B15C
D86D26F4EFDE5B523D71656F5CEA6CA73BDC04FEB973D303BBAF4C0264761092E23220CEB8359FC91C1D918FB
3F32DBBA92DEAC1C71DA8BC4BE806803F6E7970FA64721C645EED4C2BED7EEFA2B720931FDBD6C67B83756B1C
E51C51F839C250AD900B9D49FE5188FC4A2B5D0
MD = 7934EF30DAD347D1CD4CF68F70CE5748926D3753EA4FB76CCD9E2684
Len = 2363
Msg =
7D9222C58DC49F14BFD7198A9A1C338D17201C007822A91DCD262860364CA1DA8C0056033EB58E406E36D5A4F
6F7E9D98BE57126C9FE7676B58FDF0F9899432FF78DE2AB65C9000071EBA6967123F97BA3DC1F3825D3C8C5148
EAD7AEF0334F40CB0F6B982CB7C99CA39E1B4B2E3A3541683D1EC5560466F52175518390D38C7461C116DB2D5
6EF913784D2E8B20959BBD6F8F3282C597D94A1EDBFA8F25089E9D2E8DC465EAD90FA23E4388BD6BAFE226327
49B7AAEA53D5CBCF9678227ADC3F4109F1849AC2539B6F2B25B4D8EDAB41E8BFCFC337728DC48A8EA5119115F
C1B133300D68231C96A9D518F6DC3CA51581309C53F49510FE18F608A215069D41F2CFC84E53A9347FD723DFF9
D3F5006F7C0B18441A29BDEF7725920260B1613C6532A0A994B488E0
MD = B829F29742C4A496E196D0A222AB9A1F502A43AC6AA892ADCBAED423
Len = 2426
Msg =
FC447A550FC565F964337521DBD6481FF6C4FEC25A2BC946230C0021570E75B0E3D50320AB24C4949CB4EA7ED6
D14D10E1EB9CB4116461A743D49F337597F12D09945285647B249A2AE3EBF69F1FC62A36532B2FC89ECED5B48A
C27A0E18AF8B0F023BE5C00FF0BF8C16F412B34D4AE9ECD2963583FA268ED439B4640FFCC57384EF066362E23D
2F0712F9658CB7B7F56F548C4A3C7DB51D8FF4430D14CE1042221254CAA4BF009B197E6F74B42067E95E42D6C8
F2D37AA5522F5594D61745BA28C8F302E00731628298573OFBCB8BDAB0C5A3693BEEC32C0D57AD20D3394B7AC
72831FF5DDFC8208E09057AB9E9EE2FAC208E9FCB6D0B567C4DDED41ED286678DB3860B230C9A52C577867EC3
5A17EF902E258CD8314F36875D97543088679415FD0D7C2A9CB6CAEE76A2A1DC294700
MD = 373FA60E3DE9E7178AF8967C4BD374063A14B12530C14E99DB157D20

ExtremelyLongMsgKAT_224.txt
Algorithm Name: MCSSHA-6
Principal Submitter: Mikhail Maslennikov

Repeat = 16777216
Text = abcdefghbcdefghicdefghijdefghijkefghijklfghijklmghijklmnhijklmno
MD = E32E88B4F8BCD0C1610A8B57FDAFA7F7E52A5BF74092FC93CFA8305C

MonteCarlo_224.txt

Algorithm Name: MCSSHA-6
Principal Submitter: Mikhail Maslennikov

Seed =
6CD4C0C5CB2CA2A0F1D1AECEBAC03B52E64EA03D1A1654372936545B92BBC5484A59DB74BB60F9C40CEB1A5A
A35A6FAFE80349E14C253A4E8B1D77612DDD81ACE926AE8B0AF6E53176DBFFCC2A6B88C6BD765F939D3D178A9
BDE9EF3AA131C61E31C1E42CDFAF4B4DCDE579A37E150EFBEF5555B4C1CB40439D835A724E2FAE7

j = 0
MD = F6D9648C4280CD707890A3A01121D87509499DCC2091240B433E5632

j = 1
MD = 9E0536C34A884738F1B89E4992BE7B203BB14352A2E57F64085F0532

j = 2
MD = 2915537A7926587FE30919D3162F220D819E8FC5A4802ED905C56DED

j = 3
MD = 3ECCF163419D5557065DDD5A578811702A871F9C7E38BBAFF4236C0C

j = 4
MD = EA275F9F661A084974C532326C3BCB64BE49FF0FAEF8DF8CF9CFA4BA

j = 5
MD = 114ED1EAE3A6848B409A65B8A13D68CD1E5F13A17A9210DB4F87FB9F

j = 6
MD = 6D90C75B6B8777B77F5020B595B4626FC4B9C53825CB106B475890BB

ShortMsgKAT_256.txt
Algorithm Name: MCSSHA-6
Principal Submitter: Mikhail Maslennikov

Len = 0
Msg = 00
MD = 2D09073A0E7E3D2C414E344DFD5A653FE716961BC0229AB667730F953A9E186E

Len = 1
Msg = 00
MD = 5C525A301FF8A4EAD5A79C1C0FAD507D6EF7C4451C57E528238BA8D6990093B5

Len = 2
Msg = C0
MD = B364C81967A70925A17EC4460AF20BD5C57D8BE652C50A10D5E4A0D65639CB12

Len = 3
Msg = C0
MD = 9544509330BC5463D778A2666324367C4D5360DAC5F6B5532731F429F4396949

Len = 4
Msg = 80
MD = 587DD24C34541F851D29D1DE8DE84911E60C7631EDF3BAF2ABC011D2040C83BA

Len = 5
Msg = 48
MD = 215A7CC651C255A590A46C5AD884DFB7822BD8A76477233F97178FE52F2BFA6B

Len = 6
Msg = 50
MD = 03507636ECBAE4E088DC154258A2D323ED4A2E8F3E2A6861D827E1FD5C07E0E7

LongMsgKAT_256.txt
Algorithm Name: MCSSHA-6
Principal Submitter: Mikhail Maslennikov

Len = 2048

Msg =
724627916C50338643E6996F07877EAFD96BDF01DA7E991D4155B9BE1295EA7D21C9391F4C4A41C75F77E5D273
89253393725F1427F57914B273AB862B9E31DABCE506E558720520D33352D119F699E784F9E548FF91BC35CA147
042128709820D69A8287EA3257857615EB0321270E94B84F446942765CE882B191FAEE7E1C87E0F0BD4E0CD8A9
27703524B559B769CA4ECE1F6DBF313FDCF67C572EC4185C1A88E86EC11B6454B371980020F19633B6B95BD280
E4FBCB0161E1A82470320CEC6ECFA25AC73D09F1536F286D3F9DACAFB2CD1D0CE72D64D197F5C7520B3CCB2FD
74EB72664BA93853EF41EABF52F015DD591500D018DD162815CC993595B195
MD = A9F03127531733E72AC76A499044F492070DC3950E5880E88DDF6879D016EE9A
Len = 2111
Msg =
919FE5E7F35F64A7487649E564771DBBF10AE204ECC2181312D1A79FB579297C94F0DB9EAAE9E009A4F02057AF2
C973C5DAFA7B60154371A5D2C8E992FB6429176F8424B1A866BC1D1BED00438E97FAB42040DCACDEF7CA9FC20
33059B8898BB40CCFB2634B051797BDF3B915C503EC81839AD01E0F4F2F871EFF2008D40011730BE7A47888E79
55A806876BE120CB0F3A139A3620154ECC6482A70F5629F6A9D3341BE6FBBF48E5AA0C53589A04F057DD44268A
FFCABF75ADFC549F73F454264D46A98CCA80E3000C7446853DD5B430C9344E87E3230555B09FB3E7E64B5AD398
9293AC0FEEC0E75F909696F028A5525D26DDEA5D2B2C813FB3613DFF38CE23209285CC77C60860
MD = F66D0C29209126D12FFBA5EA87497D4634B3F0A1412A9E5FAD3BD1417A9D52FA
Len = 2174
Msg =
BD687B6D6684949FBD52A8196DF5D5927B403DEE88A47E4E4B52071BDDA6A6284A9EA1EB84950BA17A60277B0
FEA83C930E5619D5A6D232901B9D3A696662C7FD5F1349B494BC166C67B717C06D03E9FB05DB9EE292D4792F4
59E0ACC08369E3D14684CFF388C940F30738FB71D97EFEB51C7DB553CB85B6FC18429815EC71420822151BB8F5
135DD698EFE3D3118963EE194F94682DFA62EC9D3BCB5F826DA790779704DF2AC5C8A9FA2B50A42A87ED2FBAD
F1E1C8E55689531786A9858DE9E88009E56873FD2D431FCFC99B85574342DC7E78406678BDE94B9A06974DFF15
4EAC3BC7977AC7C123EBCDAC0641A69B792058BA373EDD1BA45E3339C2ABC032993B25F4E3BFA3D5FF620C621
D94C40F8
MD = 91958FC3721B907CBD282064F1DD57FA8293F374DF7C4E9A6F82115019165363
Len = 2237
Msg =
D13409007A6B3242CBAD4CE01D9AED77EFEF0A7725B96A30097EA092FA1E49A136DE03F3F348464C9BEA033216
F380440C7EC81E284738DCC640D485ED32F5D7DD1CF936C1677CBB3CDD8E0E001783FD5A3F388AE6EF7085FF9
A22FA722C7FCCF4CDC239B200D5D11884B565D01C84E4D563C6623C241C5AE0812CE8F9201BBADE48198378A3
E232EF3E10C03022620A266D0A346A6A22F202333A94D2CEF495DBA102B133B8237449C3350BF80EE51B6EE8A9
72CCFC3ED5FD7790444DA253922EEF6C611180F91DF1B6E58E843D318D94A958A017590B14D383C0F385F9CF25
14E8AE1EA749795E10F991E3FB744C6030EF6B02989E8EFFBF8E8BF31FC39B692C517C7C012ECBD0E0785BDEF48
01C4E036C98C6CD0C9328
MD = 24791E042FBFF39FBBB8DF981E928B02991B0DDC2F059568CAD5FC71DD9D541A
Len = 2300
Msg =
68F891C11459B2E9B71774E2B8A2A5C3C9CC36072E3498498496F1C7901684F3E9DACF13A3F1BAE22140DEE525
3732E4D4196B534F675264B53D38659727797F0A18910CCB5B48FE2346C2E998B6537357AF8D15826FCB57BA80
4FE143E765F4680A0B28A9E3716A59ABC60EF253E357A4784FF1BE4680C82D797813CE50355D8FDB3C75936CC3
3E1717B99D9A8ADE9D0EA9172662B708EBCBC31C05064FE67B287C56D01C12411E9B890AD16238B36E192B15C
D86D26F4EFDE5B523D71656F5CEA6CA73BDC04FEB973D303BBAF4C0264761092E23220CEB8359FC91C1D918FB
3F32DBBA92DEAC1C71DA8BC4BE806803F6E7970FA64721C645EED4C2BED7EEFA2B720931FDBD6C67B83756B1C
E51C51F839C250AD900B9D49FE5188FC4A2B5D0
MD = C7FB73CA2656E7E5CB638EDB32E7F148BAA46BBD4C2AAB38D3CA42B353431678
Len = 2363
Msg =
7D9222C58DC49F14BFD7198A9A1C338D17201C007822A91DCD262860364CA1DA8C0056033EB58E406E36D5A4F
6F7E9D98BE57126C9FE7676B58FDF0F9899432FF78DE2AB65C9000071EBA6967123F97BA3DC1F3825D3C8C5148
EAD7AEF0334F40CB0F6B982CB7C99CA39E1B4B2E3A3541683D1EC5560466F52175518390D38C7461C116DB2D5
6EF913784D2E8B20959BBD6F8F3282C597D94A1EDBFA8F25089E9D2E8DC465EAD90FA23E4388BD6BAFE226327
49B7AAEA53D5CBCF9678227ADC3F4109F1849AC2539B6F2B25B4D8EDAB41E8BFCFC337728DC48A8EA5119115F
C1B133300D68231C96A9D518F6DC3CA51581309C53F49510FE18F608A215069D41F2CFC84E53A9347FD723DFF9
D3F5006F7C0B18441A29BDEF7725920260B1613C6532A0A994B488E0
MD = CB4FA8FB773C8FFA5DE8850F6EFA86D4D18CBF1777D770E590DB50590DEC7A0F
Len = 2426
Msg =
FC447A550FC565F964337521DBD6481FF6C4FEC25A2BC946230C0021570E75B0E3D50320AB24C4949CB4EA7ED6
D14D10E1EB9CB4116461A743D49F337597F12D09945285647B249A2AE3EBF69F1FC62A36532B2FC89ECED5B48A
C27A0E18AF8B0F023BE5C00FF0BF8C16F412B34D4AE9ECD2963583FA268ED439B4640FFCC57384EF066362E23D
2F0712F9658CB7B7F56F548C4A3C7DB51D8FF4430D14CE1042221254CAA4BF009B197E6F74B42067E95E42D6C8
F2D37AA5522F5594D61745BA28C8F302E007316282985730FBCB8BDAB0C5A3693BEEC32C0D57AD20D3394B7AC
72831FF5DDFC8208E09057AB9E9EE2FAC208E9FCB6D0B567C4DDED41ED286678DB3860B230C9A52C577867EC3
5A17EF902E258CD8314F36875D97543088679415FD0D7C2A9CB6CAEE76A2A1DC294700
MD = F9FD11A7D2F0A7AB64DA86B7499874A886E3B59C443F1138C1F430B8AD74D831

ExtremelyLongMsgKAT_256.txt
Algorithm Name: MCSSHA-6
Principal Submitter: Mikhail Maslennikov

Repeat = 16777216
Text = abcdefghbcdefghicdefghijdefghijkefghijklfghijklmghijklmnhijklmno
MD = 217F6213F9E1A966B5B0D90264AE27DD5D5BAB8B1F9298FC7AEA9F95DECF4F4C

MonteCarlo_256.txt
Algorithm Name: MCSSHA-6
Principal Submitter: Mikhail Maslennikov

Seed = 6CD4C0C5CB2CA2A0F1D1AECEBAC03B52E64EA03D1A1654372936545B92BBC5484A59DB74BB60F9C40CEB1A5A A35A6FAFE80349E14C253A4E8B1D77612DDD81ACE926AE8B0AF6E53176DBFFCC2A6B88C6BD765F939D3D178A9 BDE9EF3AA131C61E31C1E42CDFAF4B4DCDE579A37E150EFBEF5555B4C1CB40439D835A724E2FAE7

j = 0
MD = 5F489DB92DD35AC621F8D7F8035FFC52B7C1F48A4585CE29AF6E64E4D0033869

j = 1
MD = 02C7FFB4C092C233FA4B64DF2549E0808D3384A33B9EAC2279A22BDFDD3400CA

j = 2
MD = 29855BB739105514BEA5B3119F180AEA1CB97CA6149E47E36BAAFDAFEB4A31BE

j = 3
MD = C0B71879258E1C44AA2468567F1F4CC92DD2DF9DC17831EC8CFBDAE53A48A2FC

j = 4
MD = 4333071CD91562DA2D179BF70D68DAF134AEEB1D49CC2BAF21229AD0049D6E6C

j = 5
MD = 4D95FD9A2248C54726E1B1700826EB12CAEBB13C07765AD3BF1A4EF6FAB1C5AC

j = 6
MD = 4DAEB3BA0CE27355BE8103954B37179CC85CDCBA61E910118FFE91D61C64137C

ShortMsgKAT_384.txt
Algorithm Name: MCSSHA-6
Principal Submitter: Mikhail Maslennikov

Len = 0
Msg = 00
MD = 0E79D37990809C8C1A2272E12B2AB5A4749F53E5691FDEEC42FF0881804C84015C06E0647A3B7B8BA562F660B3 E71D2A

Len = 1
Msg = 00
MD = 18DBFBD19C65E78A93D876D03A6A3779639B9E21D77E6B1E04027CE0F78B37572E48904F3F6A9F8397761BD692 D90028

Len = 2
Msg = C0
MD = 30BE22F3D03E107B2604FDA79ABB8B79B7C44D7AD622FC27ECE68DECEA63B7DFF3289A389DECF7FD18BB8CF32 E08FD7A

Len = 3
Msg = C0
MD = F6EE37D59ABE14A14EF11B4EA360E2E9CC81A15B86CCBB1608486FB3485E88716347A6B1503DA00F7B9A604E39 D4900D

Len = 4
Msg = 80
MD = 94CAC5C69A68C8E0293849C5A7E6C652179646F78ED618BA25CFF10DE754DC7F3BE396C0EC495C7B342B4FED5 65171A4

Len = 5
Msg = 48
MD =
49AE5D2D5A553627141E4C3D82C3ED935A30362DD9687C693B6EE7C61490AF9AFA05F3DFB96F8DFBF257B5FF291DC709

Len = 6
Msg = 50
MD =
96766419A490A99E09E5EAB59EE068A4806AC01CE7D07BF6EFB267A6D29C257D6C72BFF8B4BF0BB286E82CFAAA683CCB

LongMsgKAT_384.txt
Algorithm Name: MCSSHA-6
Principal Submitter: Mikhail Maslennikov

Len = 2048
Msg =
724627916C50338643E6996F07877EAFD96BDF01DA7E991D4155B9BE1295EA7D21C9391F4C4A41C75F77E5D27389253393725F1427F57914B273AB862B9E31DABCE506E558720520D33352D119F699E784F9E548FF91BC35CA147042128709820D69A8287EA3257857615EB0321270E94B84F446942765CE882B191FAEE7E1C87E0F0BD4E0CD8A927703524B559B769CA4ECE1F6DBF313FDCF67C572EC4185C1A88E86EC11B6454B371980020F19633B6B95BD280E4FBCB0161E1A82470320CEC6ECFA25AC73D09F1536F286D3F9DACAFB2CD1D0CE72D64D197F5C7520B3CCB2FD74EB72664BA93853EF41EABF52F015DD591500D018DD162815CC993595B195
MD =
65BE187FD5F1004A5E05191B3D7751955388FAA7E0E1E058EBF54EAF5A9B8788F5457689D1D7617096BBF18214325930
Len = 2111
Msg =
919FE5E7F35F64A7487649E564771DBBF10AE204ECC2181312D1A79FB579297C94F0DB9EAAE9E009A4F02057AF2C973C5DAFA7B60154371A5D2C8E992FB6429176F8424B1A866BC1D1BED00438E97FAB42040DCACDEF7CA9FC2033059B8898BB40CCFB2634B051797BDF3B915C503EC81839AD01E0F4F2F871EFF2008D40011730BE7A47888E7955A806876BE120CB0F3A139A3620154ECC6482A70F5629F6A9D3341BE6FBBF48E5AA0C53589A04F057DD44268AFFCABF75ADFC549F73F454264D46A98CCA80E3000C7446853DD5B430C9344E87E3230555B09FB3E7E64B5AD3989293AC0FEEC0E75F909696F028A5525D26DDEA5D2B2C813FB3613DFF38CE23209285CC77C60860
MD =
55965A05A5693C77CE9ADD2017B97CEF8860B0B9D25198AE5FD33B3FDF2BB7D09454875B1E36D973F1C5397E6389BC9F
Len = 2174
Msg =
BD687B6D6684949FBD52A8196DF5D5927B403DEE88A47E4E4B52071BDDA6A6284A9EA1EB84950BA17A60277B0FEA83C930E5619D5A6D232901B9D3A696662C7FD5F1349B494BC166C67B717C06D03E9FB05DB9EE292D4792F459E0ACC08369E3D14684CFF388C940F30738FB71D97EFEB51C7DB553CB85B6FC18429815EC71420822151BB8F5135DD698EFE3D3118963EE194F94682DFA62EC9D3BCB5F826DA790779704DF2AC5C8A9FA2B50A42A87ED2FBADF1E1C8E55689531786A9858DE9E88009E56873FD2D431FCFC99B85574342DC7E78406678BDE94B9A06974DFF154EAC3BC7977AC7C123EBCDAC0641A69B792058BA373EDD1BA45E3339C2ABC032993B25F4E3BFA3D5FF620C621D94C40F8
MD =
518D72159B028545D300D02A831DF9D24B7FFA9E17E5966E3F0B2E20902D6948941995D22183B11DCB80C3D070A11AB0
Len = 2237
Msg =
D13409007A6B3242CBAD4CE01D9AED77EFEF0A7725B96A30097EA092FA1E49A136DE03F3F348464C9BEA033216F380440C7EC81E284738DCC640D485ED32F5D7DD1CF936C1677CBB3CDD8E0E001783FD5A3F388AE6EF7085FF9A22FA722C7FCCF4CDC239B200D5D11884B565D01C84E4D563C6623C241C5AE0812CE8F9201BBADE48198378A3E232EF3E10C03022620A266D0A346A6A22F202333A94D2CEF495DBA102B133B8237449C3350BF80EE51B6EE8A972CCFC3ED5FD7790444DA253922EEF6C611180F91DF1B6E58E843D318D94A958A017590B14D383C0F385F9CF2514E8AE1EA749795E10F991E3FB744C6030EF6B02989E8EFFBF8E8BF31FC39B692C517C7C012ECBD0E0785BDEF4801C4E036C98C6CD0C9328
MD =
EC421AC02769BB920ACA7F57429C4251F62D1AF7A34B52E3D2FB7229A9EADD7271D94609D3E38C39FEBFFC7A1253B5A4
Len = 2300
Msg =
68F891C11459B2E9B71774E2B8A2A5C3C9CC36072E3498498496F1C7901684F3E9DACF13A3F1BAE22140DEE5253732E4D4196B534F675264B53D38659727797F0A18910CCB5B48FE2346C2E998B6537357AF8D15826FCB57BA804FE143E765F4680A0B28A9E3716A59ABC60EF253E357A4784FF1BE4680C82D797813CE50355D8FDB3C75936CC33E1717B99D9A8ADE9D0EA9172662B708EBCBC31C05064FE67B287C56D01C12411E9B890AD16238B36E192B15CD86D26F4EFDE5B523D71656F5CEA6CA73BDC04FEB973D303BBAF4C0264761092E23220CEB8359FC91C1D918FB

3F32DBBA92DEAC1C71DA8BC4BE806803F6E7970FA64721C645EED4C2BED7EEFA2B720931FDBD6C67B83756B1C
E51C51F839C250AD900B9D49FE5188FC4A2B5D0
MD =
7AAC6B0F03E40A202D78B149620D61008DE334F4EF8C2CF8BDAB12746E2E6A94E7B60E9900E333138D25537F66
A83EF7
Len = 2363
Msg =
7D9222C58DC49F14BFD7198A9A1C338D17201C007822A91DCD262860364CA1DA8C0056033EB58E406E36D5A4F
6F7E9D98BE57126C9FE7676B58FDF0F9899432FF78DE2AB65C9000071EBA6967123F97BA3DC1F3825D3C8C5148
EAD7AEF0334F40CB0F6B982CB7C99CA39E1B4B2E3A3541683D1EC5560466F52175518390D38C7461C116DB2D5
6EF913784D2E8B20959BBD6F8F3282C597D94A1EDBFA8F25089E9D2E8DC465EAD90FA23E4388BD6BAFE226327
49B7AAEA53D5CBCF9678227ADC3F4109F1849AC2539B6F2B25B4D8EDAB41E8BFCFC337728DC48A8EA5119115F
C1B133300D68231C96A9D518F6DC3CA51581309C53F49510FE18F608A215069D41F2CFC84E53A9347FD723DFF9
D3F5006F7C0B18441A29BDEF7725920260B1613C6532A0A994B488E0
MD =
637FB7A83F32756863741EACA4627F7A872A9D21AEFAE9940C317AA8ACF9F371EE76398D4CBECB73A98C28B086
63BDA0
Len = 2426
Msg =
FC447A550FC565F964337521DBD6481FF6C4FEC25A2BC946230C0021570E75B0E3D50320AB24C4949CB4EA7ED6
D14D10E1EB9CB4116461A743D49F337597F12D09945285647B249A2AE3EBF69F1FC62A36532B2FC89ECED5B48A
C27A0E18AF8B0F023BE5C00FF0BF8C16F412B34D4AE9ECD2963583FA268ED439B4640FFCC57384EF066362E23D
2F0712F9658CB7B7F56F548C4A3C7DB51D8FF4430D14CE1042221254CAA4BF009B197E6F74B42067E95E42D6C8
F2D37AA5522F5594D61745BA28C8F302E007316282985730FBCB8BDAB0C5A3693BEEC32C0D57AD20D3394B7AC
72831FF5DDFC8208E09057AB9E9EE2FAC208E9FCB6D0B567C4DDED41ED286678DB3860B230C9A52C577867EC3
5A17EF902E258CD8314F36875D97543088679415FD0D7C2A9CB6CAEE76A2A1DC294700
MD =
B50851428F08E9BB269F4B517AD8B3B281A271AA34E30EBD9AD1435BD0B58A6D7BB73103C1180B87B8D987382
CDA660E

ExtremelyLongMsgKAT_384.txt
Algorithm Name: MCSSHA-6
Principal Submitter: Mikhail Maslennikov

Repeat = 16777216
Text = abcdefghbcdefghicdefghijdefghijkefghijklfghijklmghijklmnhijklmno
MD =
2B3914FAD1D79489AD42F34718652526E6E8E4FF26B62B4F6769170FF83E01A71BE17DD2806D8E7A027B2F8929
FDEFD4

MonteCarlo_384.txt
Algorithm Name: MCSSHA-6
Principal Submitter: Mikhail Maslennikov

Seed =
6CD4C0C5CB2CA2A0F1D1AECEBAC03B52E64EA03D1A1654372936545B92BBC5484A59DB74BB60F9C40CEB1A5A
A35A6FAFE80349E14C253A4E8B1D77612DDD81ACE926AE8B0AF6E53176DBFFCC2A6B88C6BD765F939D3D178A9
BDE9EF3AA131C61E31C1E42CDFAF4B4DCDE579A37E150EFBEF5555B4C1CB40439D835A724E2FAE7

j = 0
MD =
5D5D736181254B25A8225AF7698E8F438F812FBDE1B220225CA9CAEB38D04C5D81915AFCCC2A0344EFF58A39AE
0D593A

j = 1
MD =
33605DE6D31ACE06DC47F4AC21F1B75A34E8E056EB1D11766C1C74F05E6A51D5EEEB52F79C2A1A9C613332A86
A910E75

j = 2
MD =
3C5D2B0FFC165AF8E641A97592362C0B18EF836C2640F12CF217BC96013209FCEA5A94BF413C9B50B2C4007DCD
11AD67

j = 3
MD =
B94A206492F2EA7C49E381E51EA9F7EE6AC90AE2D43DFA6EE72B2342E2D01B00DBC0A70A2B5CA9034EFA578094
8F7869

j = 4
MD = 0F20BB8D57FF73BAD7F3B7220C14A6767FA842A773C5B1CB4ABD6D28FDFB15A453C120CA1CC095F99DF6FF91F24D9341

j = 5
MD = 6B19C4E2B01C12B69C373BCFA3A661C341E8DD82C9954FCA0552FCDD6C178F881A6FFF5C97A6335EF97B958B69D7F93E

j = 6
MD = 5F2A62270DEEE110378EEE61FEFC681380543CAE7F8B11CBCE96D2D24A4264628CC4DC2E3130263C3D6988B03F5CE082

ShortMsgKAT_512.txt
Algorithm Name: MCSSHA-6
Principal Submitter: Mikhail Maslennikov

Len = 0
Msg = 00
MD = 5A7EDA6899953478F342BC8ECAB719C2906EA8EB219C6B6868A473F1EC909766D189FD59DC8DF0412643A60A34C9D688DC6AF988D2BA6EB32A4EFF35C499FDC7

Len = 1
Msg = 00
MD = FA05EF5FA986BC5A61B5559C63A11889714B0BF9C570ECBE0EA8606AE9F868318B09B686AE8885F370BF5003CDA112EB755ABB25AEC2E8CD86F4D8FDA67AEA77

Len = 2
Msg = C0
MD = 73D7FDD383A344E3860DC638487757A52FF0EC6F79C2B48D44275663150DDD1721E03FFF826317C1291ED41674AF0BEFE8C3D037E5A6F73958E78F506369B2FF

Len = 3
Msg = C0
MD = 38352FB6C35BAC6A6C4645AB8A158F734B04AB6514CB4FADAD5F2CC4AE4462B8F0EB3B9B2613DC59C49DCCE40DC9605781D9F0DA98BC321FB125D0A84E8862EA

Len = 4
Msg = 80
MD = FB9E1901820E62066A029726ECD6D435E9E33884010E1804EE2BCA9DEBAE723FB82F0AB58734FD6E07543B4A35D833B424832B4501D358D37C848611AB6BDAF9

Len = 5
Msg = 48
MD = 1BCB886035BDDC202C9971AE64601B22E9ADD18182F5FE966CBFBAB57ADCF15D34F8A87B03435BDC9969A5A2F110460B105E7A6EE2C0DD98BCDE17B3C6D4C333

Len = 6
Msg = 50
MD = 723E5160E2B6F306669554F3819ED0974A5172939DA707C5F954E08EE964E950F22894D17989E47F9B417916AA740301EDF92A3B6908DAF399032CD0C19A7E3D

LongMsgKAT_512.txt
Algorithm Name: MCSSHA-6
Principal Submitter: Mikhail Maslennikov

Len = 2048

Msg =
724627916C50338643E6996F07877EAFD96BDF01DA7E991D4155B9BE1295EA7D21C9391F4C4A41C75F77E5D273
89253393725F1427F57914B273AB862B9E31DABCE506E558720520D33352D119F699E784F9E548FF91BC35CA147
042128709820D69A8287EA3257857615EB0321270E94B84F446942765CE882B191FAEE7E1C87E0F0BD4E0CD8A9
27703524B559B769CA4ECE1F6DBF313FDCF67C572EC4185C1A88E86EC11B6454B371980020F19633B6B95BD280
E4FBCB0161E1A82470320CEC6ECFA25AC73D09F1536F286D3F9DACAFB2CD1D0CE72D64D197F5C7520B3CCB2FD
74EB72664BA93853EF41EABF52F015DD591500D018DD162815CC993595B195
MD =
C9EFB6D39596DAEDC41E09C7523FF0439FCE05E6D5BCCDB096C7D5BB1DC6AB87C4FAF70C9D69B56F3BF03F497
6DDD81DFD5522C85B8FF05B336B0A3DF7D21C5D
Len = 2111
Msg =
919FE5E7F35F64A7487649E564771DBBF10AE204ECC2181312D1A79FB579297C94F0DB9EAAE9E009A4F02057AF2
C973C5DAFA7B60154371A5D2C8E992FB6429176F8424B1A866BC1D1BED00438E97FAB42040DCACDEF7CA9FC20
33059B8898BB40CCFB2634B051797BDF3B915C503EC81839AD01E0F4F2F871EFF2008D40011730BE7A47888E79
55A806876BE120CB0F3A139A3620154ECC6482A70F5629F6A9D3341BE6FBBF48E5AA0C53589A04F057DD44268A
FFCABF75ADFC549F73F454264D46A98CCA80E3000C7446853DD5B430C9344E87E3230555B09FB3E7E64B5AD398
9293AC0FEEC0E75F909696F028A5525D26DDEA5D2B2C813FB3613DFF38CE23209285CC77C60860
MD =
171881590F726C38A100716EFA49BAE42E3DE696BD3B0C5EF5142904B4066C09E327AD61E87F5F908613606619F
2FB51D8F2F2AACD17796DE6EEA1F596EBD3FC
Len = 2174
Msg =
BD687B6D6684949FBD52A8196DF5D5927B403DEE88A47E4E4B52071BDDA6A6284A9EA1EB84950BA17A60277B0
FEA83C930E5619D5A6D232901B9D3A696662C7FD5F1349B494BC166C67B717C06D03E9FB05DB9EE292D4792F4
59E0ACC08369E3D14684CFF388C940F30738FB71D97EFEB51C7DB553CB85B6FC18429815EC71420822151BB8F5
135DD698EFE3D3118963EE194F94682DFA62EC9D3BCB5F826DA790779704DF2AC5C8A9FA2B50A42A87ED2FBAD
F1E1C8E55689531786A9858DE9E88009E56873FD2D431FCFC99B85574342DC7E78406678BDE94B9A06974DFF15
4EAC3BC7977AC7C123EBCDAC0641A69B792058BA373EDD1BA45E3339C2ABC032993B25F4E3BFA3D5FF620C621
D94C40F8
MD =
7164A1C734E8333D4BD391B8674E2A66B8FCA846AAF37572644B391F1655ABA63042D00B4F3A6AF3C5228D6062
BE222B4502B726D4E1D3082409BBE0A3BBE489
Len = 2237
Msg =
D13409007A6B3242CBAD4CE01D9AED77EFEF0A7725B96A30097EA092FA1E49A136DE03F3F348464C9BEA033216
F380440C7EC81E284738DCC640D485ED32F5D7DD1CF936C1677CBB3CDD8E0E001783FD5A3F388AE6EF7085FF9
A22FA722C7FCCF4CDC239B200D5D11884B565D01C84E4D563C6623C241C5AE0812CE8F9201BBADE48198378A3
E232EF3E10C03022620A266D0A346A6A22F202333A94D2CEF495DBA102B133B8237449C3350BF80EE51B6EE8A9
72CCFC3ED5FD7790444DA253922EEF6C611180F91DF1B6E58E843D318D94A958A017590B14D383C0F385F9CF25
14E8AE1EA749795E10F991E3FB744C6030EF6B02989E8EFFBF8E8BF31FC39B692C517C7C012ECBD0E0785BDEF48
01C4E036C98C6CD0C9328
MD =
277E91B36C48CAA1F1F5AB7398971A5888BDE23BEA92BB788633E467D454EF970521548AFFDE438FF8FE653B3E
ED97B552912E110F59EEE367AF734722B2EF95
Len = 2300
Msg =
68F891C11459B2E9B71774E2B8A2A5C3C9CC36072E3498498496F1C7901684F3E9DACF13A3F1BAE22140DEE525
3732E4D4196B534F675264B53D38659727797F0A18910CCB5B48FE2346C2E998B6537357AF8D15826FCB57BA80
4FE143E765F4680A0B28A9E3716A59ABC60EF253E357A4784FF1BE4680C82D797813CE50355D8FDB3C75936CC3
3E1717B99D9A8ADE9D0EA9172662B708EBCBC31C05064FE67B287C56D01C12411E9B890AD16238B36E192B15C
D86D26F4EFDE5B523D71656F5CEA6CA73BDC04FEB973D303BBAF4C0264761092E23220CEB8359FC91C1D918FB
3F32DBBA92DEAC1C71DA8BC4BE806803F6E7970FA64721C645EED4C2BED7EEFA2B720931FDBD6C67B83756B1C
E51C51F839C250AD900B9D49FE5188FC4A2B5D0
MD =
B377E917C58450437F3EB93EB062329175C3C11C81F8EADDAC9897487079CAAEBC137E69AE784C450D7A56BAD
B34E89AE8FF3F388FCCF471573757F70E30292F
Len = 2363
Msg =
7D9222C58DC49F14BFD7198A9A1C338D17201C007822A91DCD262860364CA1DA8C0056033EB58E406E36D5A4F
6F7E9D98BE57126C9FE7676B58FDF0F9899432FF78DE2AB65C9000071EBA6967123F97BA3DC1F3825D3C8C5148
EAD7AEF0334F40CB0F6B982CB7C99CA39E1B4B2E3A3541683D1EC5560466F52175518390D38C7461C116DB2D5
6EF913784D2E8B20959BBD6F8F3282C597D94A1EDBFA8F25089E9D2E8DC465EAD90FA23E4388BD6BAFE226327
49B7AAEA53D5CBCF9678227ADC3F4109F1849AC2539B6F2B25B4D8EDAB41E8BFCFC337728DC48A8EA5119115F
C1B133300D68231C96A9D518F6DC3CA51581309C53F49510FE18F608A215069D41F2CFC84E53A9347FD723DFF9
D3F5006F7C0B18441A29BDEF7725920260B1613C6532A0A994B488E0
MD =
5177359CC5AC87F3CBB0A01277AED4C060EA31397F0E484675CD11BC981881507FE3515E96DC86468F2092C1B0
33499D5B43D312604B829DFBA3886ABFD8C4C1
Len = 2426
Msg =
FC447A550FC565F964337521DBD6481FF6C4FEC25A2BC946230C0021570E75B0E3D50320AB24C4949CB4EA7ED6
D14D10E1EB9CB4116461A743D49F337597F12D09945285647B249A2AE3EBF69F1FC62A36532B2FC89ECED5B48A
C27A0E18AF8B0F023BE5C00FF0BF8C16F412B34D4AE9ECD2963583FA268ED439B4640FFCC57384EF066362E23D

2F0712F9658CB7B7F56F548C4A3C7DB51D8FF4430D14CE1042221254CAA4BF009B197E6F74B42067E95E42D6C8
F2D37AA5522F5594D61745BA28C8F302E007316282985730FBCB8BDAB0C5A3693BEEC32C0D57AD20D3394B7AC
72831FF5DDFC8208E09057AB9E9EE2FAC208E9FCB6D0B567C4DDED41ED286678DB3860B230C9A52C577867EC3
5A17EF902E258CD8314F36875D97543088679415FD0D7C2A9CB6CAEE76A2A1DC294700
MD = 2E678B5664102BCC2238B3D04E1C17CA13BAC1B4B60BE38632827FF02C6D7F6629902DC97270A1553ABD1F50B
97B0B1E7FC7C90ECFC80184A613C2CD8C66D6C0

ExtremelyLongMsgKAT_512.txt
Algorithm Name: MCSSHA-6
Principal Submitter: Mikhail Maslennikov

Repeat = 16777216
Text = abcdefghbcdefghicdefghijdefghijkefghijklfghijklmghijklmnhijklmno
MD = AEC8AD70591A2E437419A2B8C6BDB9E5EB3B2B25CE1C00999160CB6DB3FA8ED22CEBFA28A55FDA4D62F0B7D0
6BCC66EAB3E2BDD6FBD9350634040A88D28FC674

MonteCarlo_512.txt
Algorithm Name: MCSSHA-6
Principal Submitter: Mikhail Maslennikov

Seed = 6CD4C0C5CB2CA2A0F1D1AECEBAC03B52E64EA03D1A1654372936545B92BBC5484A59DB74BB60F9C40CEB1A5A
A35A6FAFE80349E14C253A4E8B1D77612DDD81ACE926AE8B0AF6E53176DBFFCC2A6B88C6BD765F939D3D178A9
BDE9EF3AA131C61E31C1E42CDFAF4B4DCDE579A37E150EFBEF5555B4C1CB40439D835A724E2FAE7

j = 0
MD = C2FFE416B211E26021618EA1E9270CAE4220CE586EF4E06651FF921F90B4C2B0F1EB20B8E509EFA9BCBF24490B8
AEC5EEFE2609DC30690DAA13C1BE1C3863F7E

j = 1
MD = 87FD27F4408953A2FE58EC4E6C20C0605D32CED4EAFFEDD1D2F45D3561FF64E2E267E5E4E3853095C01173495A
1A6788EAEAB35B70F614E4D63C0C796CC77E05

j = 2
MD = C952D16029899FA9B228F390F1131E9DE22525D26C8F5CF9FED4A1AC852780CF521B992E0F0475B20A6058DEBB
0A2E0B010BA69DC2D058AC4684FE3066C09551

j = 3
MD = 6FE3D6C2A605A3304728C55D9FDC13E4250C8A567B7D9E0CA33D70F7756BB4D1D0474C0BF83DB18F3B46A119A
D9238516E58B6ADA0CB8DA46BBD1FA7AC26BACF

j = 4
MD = 8A9DEFD74FEEEAD1839C8ED9857F7C385F7CCF6EAEADD76747CBAFF9B25D95D4C4298C825C00168B00CD9E85A
D56CC06A9F171ED822880BC13C481B4071056B0

j = 5
MD = F1016B5A301E345E6DEFF4FE9B08186882B4682232CFD3BC80A875012D363BDC9D839431F015BB9272F8486622
32432B1E6997119ACC1310E67E5FED2C9469A0

j = 6
MD = 5ED0F13146AF33138C94FB0468C7EDB2318DC89EDEE94112575249A65C85D2370F35E3AACF2AAF5A47E0D71F1A
6B610C7B0957E41DEDB238F18305A114D27FF5