

Algorithm: **MCSSHA-4**

Principal submitter: **Mikhail Maslennikov**

Revision: January 08, 2009

SECURE HASH ALGORITHM MCSSHA-4

Оглавление

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	9
7.2 Calculating final SR state	9
8. PARAMETERS OF ALGORITHM MCSSHA-4 FOR DIFFERENT HASH LENGTH.....	9
9. ESTIMATED COMPUTATIONAL EFFICIENCY AND MEMORY REQUIREMENTS ...	10
9.1 Memory Requirement.....	10
9.2 Computation Efficiency.....	10
10. Appendix A. Calculating hash examples.....	15
10.1 Hash bit length 224, delay=2.....	15
10.2 Hash bit length 256, delay=2.....	21
10.3 Hash bit length 384, delay=2.....	26
10.4 Hash bit length 512, delay=2.....	41
11. Appendix B. CAT and MCT tests (delay=2).....	56

1. INTRODUCTION

This document specifies secure hash algorithm MCSSHA-4. This algorithm 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-4 algorithm can be described in three stages: preprocessing, pre-hash computation and final hash computation. Each stage changes *Shift Registry state* (SR-state) and final SR-state is message digest.

Preprocessing sets initial SR-state to be used in the hash computation. Initial SR-state is not dependent on message and padding is not used in MCSSHA-4 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-4 algorithm in many respects is similar to previous algorithm MCSSHA-3 of the 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 the final stage.

2. DEFINITIONS

2.1 Glossary of Terms and Acronyms

<i>Bit</i>	A binary digit having a value of 0 or 1.
<i>Byte</i>	A group of eight bits.
<i>Hash bit length (h)</i>	Length (in bits) of the message digest. It may be 224, 256, 384 or 512.
<i>Hash byte length (H)</i>	Length (in bytes) of the message digest. It may be 28, 32, 48 or 64.
<i>Shift Registry length (N)</i>	Integer value.
<i>Shift Registry state (SR state)</i>	A group of N bytes.
<i>Initial SR state</i>	SR state before pre-hash computation.
<i>Shift Registry point (SR point)</i>	Digit from 0 to N-1.
<i>SR points</i>	A group of four SR points
<i>Initial SR points</i>	SR points before pre-hash computation.
<i>Shift Registry Substitution</i>	A group of 256 bytes where all values are various.
<i>Shift Registry step (SR step)</i>	Transformation of a SR state during one step.
<i>Input byte for SR step</i>	Byte that use SR step.
<i>Message</i>	A group of bits.
<i>Message length in bits</i>	Number of bits in message.
<i>Message length in bytes</i>	Number of full bytes in message.
<i>Message remain bits</i>	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-4 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 .

$M = m_1, m_2, \dots, m_L$ 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-4 algorithm specifications.

$+$ Addition on the module 256.

$-$ Subtraction on the module 256.

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

$a(\text{mod } N)$ 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 $\{00, 01, \dots, 09, 0A, \dots, 0F, 10, \dots, FF\}$.

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

3.2 Shift Registry Steps

The following terminology related to SR steps will be used.

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

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

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

x Input byte for step.

4. FUNCTIONS AND CONSTANTS

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

4.1 Constants

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

```

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

```

4.2 Functions

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

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

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

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

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

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-4 algorithm is 2.

Thus, as default pre-hash computation for message M and length in bytes L consist from $3L$ steps.

It's possible to change this parameter for more security. As one possible variant value Δ may be 3.

WARNING!

For values Δ below 2 (0 or 1) algorithm MCSSHA-4 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 two stages: creating final input sequence Z and calculating final SR state using final input sequence.

7.1 Creating input sequence

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

$$Z = b_1, b_2, \dots, b_r, a_1, a_2, \dots, a_n, a_1, a_2, \dots, a_n. \quad (7.1)$$

The length in bits of the input sequence if exactly $2n$ bits, in bytes – exactly $2N$ bytes.

If remain bits absent, then

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

7.2 Calculating final SR state

Lets $Z = z_1, z_2, \dots, z_{2N}$ – input sequence in bytes. Calculating final SR state consist from $2N$ steps and for 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 $0, 1, 2, \dots, H-1$, initial SR points:

$$\begin{aligned} p_1 &= 0; \\ p_2 &= 1; \\ p_3 &= H-4; \\ p_4 &= H-1. \end{aligned}$$

Final SR state is message digest.

8. PARAMETERS OF ALGORITHM MCSSHA-4 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-4 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).

1) 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
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
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
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
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
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
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

2) 64-bits OS

MS Windows Server 2003 R2, Enterprise x64 Edition, Service Pack 1, AMD Athlon 64 Processor, 3200+, 2.01 GHz.

Algorithm	Hash length (in bits)	Text length (in bytes)	Number of tests	Time (sec)
SHA-224	224	1	1000000	1.437
MCSSHA-3	224	1	1000000	2.172
MCSSHA-4 (delay=2)	224	1	1000000	2.157
MCSSHA-4 (delay=3)	224	1	1000000	2.156
Skein	224	1	1000000	1.609
MD6	224	1	1000000	19.219
Essence	224	1	1000000	7.625
Keccak	224	1	1000000	4
Groestl	224	1	1000000	11.203

SHAMATA	224	1	1000000	4.891
Blake	224	1	1000000	2.25
Sarmal	224	1	1000000	1.735
Waterfall	224	1	1000000	6.719
Boole	224	1	1000000	4.234
SHA-224	224	100	1000000	3
MCSSHA-3	224	100	1000000	6.921
MCSSHA-4 (delay=2)	224	100	1000000	5.484
MCSSHA-4 (delay=3)	224	100	1000000	6.907
Skein	224	100	1000000	3.672
MD6	224	100	1000000	19.188
Essence	224	100	1000000	15.047
Keccak	224	100	1000000	4.094
Groestl	224	100	1000000	17.469
SHAMATA	224	100	1000000	5.906
Blake	224	100	1000000	4.203
Sarmal	224	100	1000000	1.672
Waterfall	224	100	1000000	9.093
Boole	224	100	1000000	6.109
SHA-224	224	100000	1000	2.406
MCSSHA-3	224	100000	1000	4.797
MCSSHA-4 (delay=2)	224	100000	1000	3.36
MCSSHA-4 (delay=3)	224	100000	1000	4.797
Skein	224	100000	1000	2.172
MD6	224	100000	1000	4.656
Essence	224	100000	1000	7.672
Keccak	224	100000	1000	3.031
Groestl	224	100000	1000	9.891
SHAMATA	224	100000	1000	1.094
Blake	224	100000	1000	3.125
Sarmal	224	100000	1000	1.172
Waterfall	224	100000	1000	3.406
Boole	224	100000	1000	1.953
SHA-512	512	1	1000000	4.765
MCSSHA-3	512	1	1000000	4.657
MCSSHA-4 (delay=2)	512	1	1000000	3.797
MCSSHA-4 (delay=3)	512	1	1000000	3.797
Skein	512	1	1000000	3.344
MD6	512	1	1000000	31.625
Essence	512	1	1000000	27.875
Keccak	512	1	1000000	4
Groestl	512	1	1000000	27.015
SHAMATA	512	1	1000000	6.172
Blake	512	1	1000000	5.141
Sarmal	512	1	1000000	2.062
Waterfall	512	1	1000000	6.765

Boole	512	1	1000000	4.719
SHA-512	512	100	1000000	4.766
MCSSHA-3	512	100	1000000	8.812
MCSSHA-4 (delay=2)	512	100	1000000	7.14
MCSSHA-4 (delay=3)	512	100	1000000	8,546
Skein	512	100	1000000	4.921
MD6	512	100	1000000	31.735
Essence	512	100	1000000	37.204
Keccak	512	100	1000000	7.922
Groestl	512	100	1000000	26.968
SHAMATA	512	100	1000000	7.329
Blake	512	100	1000000	5.156
Sarmal	512	100	1000000	2
Waterfall	512	100	1000000	9.125
Boole	512	100	1000000	6.625
SHA-512	512	100000	1000	3.563
MCSSHA-3	512	100000	1000	4.188
MCSSHA-4 (delay=2)	512	100000	1000	3.36
MCSSHA-4 (delay=3)	512	100000	1000	4,782
Skein	512	100000	1000	2.438
MD6	512	100000	1000	7.829
Essence	512	100000	1000	14.437
Keccak	512	100000	1000	6.031
Groestl	512	100000	1000	12.906
SHAMATA	512	100000	1000	1.234
Blake	512	100000	1000	3.813
Sarmal	512	100000	1000	1.438
Waterfall	512	100000	1000	3.391
Boole	512	100000	1000	1.969

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 Hash bit length 224, delay=2.

For this message digest calculation consist from:

- 9 steps for pre-hash computation;
- 128 steps for final hash computation.

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

Stage 1. Preprocessing

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 – 9 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

Input byte 62

4.

C8 22 9F B6 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.

C8 22 9F B6 73 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 B6 73 D0 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 63

7.

C8 22 9F B6 73 D0 64 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 B6 73 D0 64 6B 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.

C8 22 9F B6 73 D0 64 6B 04 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 3. Final hash computation – 128 steps

This is SR states for steps in final hash computation. SR length is 28.

10.

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

11.

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

12.

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

13.

2F 64 C8 C8 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F 10 11 12 13 14 15 16 17 18 19 1A 1B

14.

2F 64 C8 C8 FD 05 06 07 08 09 0A 0B 0C 0D 0E 0F 10 11 12 13 14 15 16 17 18 19 1A 1B

15.

2F 64 C8 C8 FD 5A 06 07 08 09 0A 0B 0C 0D 0E 0F 10 11 12 13 14 15 16 17 18 19 1A 1B

16.

2F 64 C8 C8 FD 5A D2 07 08 09 0A 0B 0C 0D 0E 0F 10 11 12 13 14 15 16 17 18 19 1A 1B

17.

2F 64 C8 C8 FD 5A D2 78 08 09 0A 0B 0C 0D 0E 0F 10 11 12 13 14 15 16 17 18 19 1A 1B

18.

2F 64 C8 C8 FD 5A D2 78 4D 09 0A 0B 0C 0D 0E 0F 10 11 12 13 14 15 16 17 18 19 1A 1B

19.

2F 64 C8 C8 FD 5A D2 78 4D F9 0A 0B 0C 0D 0E 0F 10 11 12 13 14 15 16 17 18 19 1A 1B

20.

2F 64 C8 C8 FD 5A D2 78 4D F9 F6 0B 0C 0D 0E 0F 10 11 12 13 14 15 16 17 18 19 1A 1B

21.

2F 64 C8 C8 FD 5A D2 78 4D F9 F6 A2 0C 0D 0E 0F 10 11 12 13 14 15 16 17 18 19 1A 1B

22.

2F 64 C8 C8 FD 5A D2 78 4D F9 F6 A2 72 0D 0E 0F 10 11 12 13 14 15 16 17 18 19 1A 1B

23.

2F 64 C8 C8 FD 5A D2 78 4D F9 F6 A2 72 3F 0E 0F 10 11 12 13 14 15 16 17 18 19 1A 1B

24.

2F 64 C8 C8 FD 5A D2 78 4D F9 F6 A2 72 3F 5B 0F 10 11 12 13 14 15 16 17 18 19 1A 1B

25.

2F 64 C8 C8 FD 5A D2 78 4D F9 F6 A2 72 3F 5B 14 10 11 12 13 14 15 16 17 18 19 1A 1B

26.

2F 64 C8 C8 FD 5A D2 78 4D F9 F6 A2 72 3F 5B 14 05 11 12 13 14 15 16 17 18 19 1A 1B

27.

2F 64 C8 C8 FD 5A D2 78 4D F9 F6 A2 72 3F 5B 14 05 B9 12 13 14 15 16 17 18 19 1A 1B

28.

2F 64 C8 C8 FD 5A D2 78 4D F9 F6 A2 72 3F 5B 14 05 B9 01 13 14 15 16 17 18 19 1A 1B

29.

2F 64 C8 C8 FD 5A D2 78 4D F9 F6 A2 72 3F 5B 14 05 B9 01 51 14 15 16 17 18 19 1A 1B

30.

2F 64 C8 C8 FD 5A D2 78 4D F9 F6 A2 72 3F 5B 14 05 B9 01 51 BD 15 16 17 18 19 1A 1B

31.

2F 64 C8 C8 FD 5A D2 78 4D F9 F6 A2 72 3F 5B 14 05 B9 01 51 BD CA 16 17 18 19 1A 1B

32.

2F 64 C8 C8 FD 5A D2 78 4D F9 F6 A2 72 3F 5B 14 05 B9 01 51 BD CA 9E 17 18 19 1A 1B

33.
2F 64 C8 C8 FD 5A D2 78 4D F9 F6 A2 72 3F 5B 14 05 B9 01 51 BD CA 9E 54 18 19 1A 1B

34.
2F 64 C8 C8 FD 5A D2 78 4D F9 F6 A2 72 3F 5B 14 05 B9 01 51 BD CA 9E 54 33 19 1A 1B

35.
2F 64 C8 C8 FD 5A D2 78 4D F9 F6 A2 72 3F 5B 14 05 B9 01 51 BD CA 9E 54 33 0B 1A 1B

36.
2F 64 C8 C8 FD 5A D2 78 4D F9 F6 A2 72 3F 5B 14 05 B9 01 51 BD CA 9E 54 33 0B C0 1B

37.
2F 64 C8 C8 FD 5A D2 78 4D F9 F6 A2 72 3F 5B 14 05 B9 01 51 BD CA 9E 54 33 0B C0 FF

38.
72 64 C8 C8 FD 5A D2 78 4D F9 F6 A2 72 3F 5B 14 05 B9 01 51 BD CA 9E 54 33 0B C0 FF

39.
72 D2 C8 C8 FD 5A D2 78 4D F9 F6 A2 72 3F 5B 14 05 B9 01 51 BD CA 9E 54 33 0B C0 FF

40.
72 D2 41 C8 FD 5A D2 78 4D F9 F6 A2 72 3F 5B 14 05 B9 01 51 BD CA 9E 54 33 0B C0 FF

41.
72 D2 41 99 FD 5A D2 78 4D F9 F6 A2 72 3F 5B 14 05 B9 01 51 BD CA 9E 54 33 0B C0 FF

42.
72 D2 41 99 79 5A D2 78 4D F9 F6 A2 72 3F 5B 14 05 B9 01 51 BD CA 9E 54 33 0B C0 FF

43.
72 D2 41 99 79 57 D2 78 4D F9 F6 A2 72 3F 5B 14 05 B9 01 51 BD CA 9E 54 33 0B C0 FF

44.
72 D2 41 99 79 57 94 78 4D F9 F6 A2 72 3F 5B 14 05 B9 01 51 BD CA 9E 54 33 0B C0 FF

45.
72 D2 41 99 79 57 94 0F 4D F9 F6 A2 72 3F 5B 14 05 B9 01 51 BD CA 9E 54 33 0B C0 FF

46.
72 D2 41 99 79 57 94 0F 05 F9 F6 A2 72 3F 5B 14 05 B9 01 51 BD CA 9E 54 33 0B C0 FF

47.
72 D2 41 99 79 57 94 0F 05 DC F6 A2 72 3F 5B 14 05 B9 01 51 BD CA 9E 54 33 0B C0 FF

48.
72 D2 41 99 79 57 94 0F 05 DC 9A A2 72 3F 5B 14 05 B9 01 51 BD CA 9E 54 33 0B C0 FF

49.
72 D2 41 99 79 57 94 0F 05 DC 9A 52 72 3F 5B 14 05 B9 01 51 BD CA 9E 54 33 0B C0 FF

50.
72 D2 41 99 79 57 94 0F 05 DC 9A 52 28 3F 5B 14 05 B9 01 51 BD CA 9E 54 33 0B C0 FF

51.
72 D2 41 99 79 57 94 0F 05 DC 9A 52 28 2A 5B 14 05 B9 01 51 BD CA 9E 54 33 0B C0 FF

52.
72 D2 41 99 79 57 94 0F 05 DC 9A 52 28 2A CC 14 05 B9 01 51 BD CA 9E 54 33 0B C0 FF

53.
72 D2 41 99 79 57 94 0F 05 DC 9A 52 28 2A CC 4A 05 B9 01 51 BD CA 9E 54 33 0B C0 FF

54.
72 D2 41 99 79 57 94 0F 05 DC 9A 52 28 2A CC 4A C6 B9 01 51 BD CA 9E 54 33 0B C0 FF

55.
72 D2 41 99 79 57 94 0F 05 DC 9A 52 28 2A CC 4A C6 93 01 51 BD CA 9E 54 33 0B C0 FF

56.
72 D2 41 99 79 57 94 0F 05 DC 9A 52 28 2A CC 4A C6 93 C4 51 BD CA 9E 54 33 0B C0 FF

57.
72 D2 41 99 79 57 94 0F 05 DC 9A 52 28 2A CC 4A C6 93 C4 2D BD CA 9E 54 33 0B C0 FF

58.
72 D2 41 99 79 57 94 0F 05 DC 9A 52 28 2A CC 4A C6 93 C4 2D 57 CA 9E 54 33 0B C0 FF
59.
72 D2 41 99 79 57 94 0F 05 DC 9A 52 28 2A CC 4A C6 93 C4 2D 57 F6 9E 54 33 0B C0 FF
60.
72 D2 41 99 79 57 94 0F 05 DC 9A 52 28 2A CC 4A C6 93 C4 2D 57 F6 25 54 33 0B C0 FF
61.
72 D2 41 99 79 57 94 0F 05 DC 9A 52 28 2A CC 4A C6 93 C4 2D 57 F6 25 CE 33 0B C0 FF
62.
72 D2 41 99 79 57 94 0F 05 DC 9A 52 28 2A CC 4A C6 93 C4 2D 57 F6 25 CE 3D 0B C0 FF
63.
72 D2 41 99 79 57 94 0F 05 DC 9A 52 28 2A CC 4A C6 93 C4 2D 57 F6 25 CE 3D 61 C0 FF
64.
72 D2 41 99 79 57 94 0F 05 DC 9A 52 28 2A CC 4A C6 93 C4 2D 57 F6 25 CE 3D 61 E8 FF
65.
72 D2 41 99 79 57 94 0F 05 DC 9A 52 28 2A CC 4A C6 93 C4 2D 57 F6 25 CE 3D 61 E8 11
66.
0E D2 41 99 79 57 94 0F 05 DC 9A 52 28 2A CC 4A C6 93 C4 2D 57 F6 25 CE 3D 61 E8 11
67.
0E 0C 41 99 79 57 94 0F 05 DC 9A 52 28 2A CC 4A C6 93 C4 2D 57 F6 25 CE 3D 61 E8 11
68.
0E 0C F3 99 79 57 94 0F 05 DC 9A 52 28 2A CC 4A C6 93 C4 2D 57 F6 25 CE 3D 61 E8 11
69.
0E 0C F3 A2 79 57 94 0F 05 DC 9A 52 28 2A CC 4A C6 93 C4 2D 57 F6 25 CE 3D 61 E8 11
70.
0E 0C F3 A2 EB 57 94 0F 05 DC 9A 52 28 2A CC 4A C6 93 C4 2D 57 F6 25 CE 3D 61 E8 11
71.
0E 0C F3 A2 EB 47 94 0F 05 DC 9A 52 28 2A CC 4A C6 93 C4 2D 57 F6 25 CE 3D 61 E8 11
72.
0E 0C F3 A2 EB 47 88 0F 05 DC 9A 52 28 2A CC 4A C6 93 C4 2D 57 F6 25 CE 3D 61 E8 11
73.
0E 0C F3 A2 EB 47 88 04 05 DC 9A 52 28 2A CC 4A C6 93 C4 2D 57 F6 25 CE 3D 61 E8 11
74.
0E 0C F3 A2 EB 47 88 04 76 DC 9A 52 28 2A CC 4A C6 93 C4 2D 57 F6 25 CE 3D 61 E8 11
75.
0E 0C F3 A2 EB 47 88 04 76 56 9A 52 28 2A CC 4A C6 93 C4 2D 57 F6 25 CE 3D 61 E8 11
76.
0E 0C F3 A2 EB 47 88 04 76 56 96 52 28 2A CC 4A C6 93 C4 2D 57 F6 25 CE 3D 61 E8 11
77.
0E 0C F3 A2 EB 47 88 04 76 56 96 59 28 2A CC 4A C6 93 C4 2D 57 F6 25 CE 3D 61 E8 11
78.
0E 0C F3 A2 EB 47 88 04 76 56 96 59 B7 2A CC 4A C6 93 C4 2D 57 F6 25 CE 3D 61 E8 11
79.
0E 0C F3 A2 EB 47 88 04 76 56 96 59 B7 4C CC 4A C6 93 C4 2D 57 F6 25 CE 3D 61 E8 11
80.
0E 0C F3 A2 EB 47 88 04 76 56 96 59 B7 4C 24 4A C6 93 C4 2D 57 F6 25 CE 3D 61 E8 11
81.
0E 0C F3 A2 EB 47 88 04 76 56 96 59 B7 4C 24 71 C6 93 C4 2D 57 F6 25 CE 3D 61 E8 11
- 82.

0E 0C F3 A2 EB 47 88 04 76 56 96 59 B7 4C 24 71 77 93 C4 2D 57 F6 25 CE 3D 61 E8 11

83.
0E 0C F3 A2 EB 47 88 04 76 56 96 59 B7 4C 24 71 77 96 C4 2D 57 F6 25 CE 3D 61 E8 11

84.
0E 0C F3 A2 EB 47 88 04 76 56 96 59 B7 4C 24 71 77 96 17 2D 57 F6 25 CE 3D 61 E8 11

85.
0E 0C F3 A2 EB 47 88 04 76 56 96 59 B7 4C 24 71 77 96 17 FE 57 F6 25 CE 3D 61 E8 11

86.
0E 0C F3 A2 EB 47 88 04 76 56 96 59 B7 4C 24 71 77 96 17 FE EA F6 25 CE 3D 61 E8 11

87.
0E 0C F3 A2 EB 47 88 04 76 56 96 59 B7 4C 24 71 77 96 17 FE EA DF 25 CE 3D 61 E8 11

88.
0E 0C F3 A2 EB 47 88 04 76 56 96 59 B7 4C 24 71 77 96 17 FE EA DF 71 CE 3D 61 E8 11

89.
0E 0C F3 A2 EB 47 88 04 76 56 96 59 B7 4C 24 71 77 96 17 FE EA DF 71 52 3D 61 E8 11

90.
0E 0C F3 A2 EB 47 88 04 76 56 96 59 B7 4C 24 71 77 96 17 FE EA DF 71 52 F7 61 E8 11

91.
0E 0C F3 A2 EB 47 88 04 76 56 96 59 B7 4C 24 71 77 96 17 FE EA DF 71 52 F7 7F E8 11

92.
0E 0C F3 A2 EB 47 88 04 76 56 96 59 B7 4C 24 71 77 96 17 FE EA DF 71 52 F7 7F 90 11

93.
0E 0C F3 A2 EB 47 88 04 76 56 96 59 B7 4C 24 71 77 96 17 FE EA DF 71 52 F7 7F 90 D0

94.
C1 0C F3 A2 EB 47 88 04 76 56 96 59 B7 4C 24 71 77 96 17 FE EA DF 71 52 F7 7F 90 D0

95.
C1 F7 F3 A2 EB 47 88 04 76 56 96 59 B7 4C 24 71 77 96 17 FE EA DF 71 52 F7 7F 90 D0

96.
C1 F7 1B A2 EB 47 88 04 76 56 96 59 B7 4C 24 71 77 96 17 FE EA DF 71 52 F7 7F 90 D0

97.
C1 F7 1B 7E EB 47 88 04 76 56 96 59 B7 4C 24 71 77 96 17 FE EA DF 71 52 F7 7F 90 D0

98.
C1 F7 1B 7E 82 47 88 04 76 56 96 59 B7 4C 24 71 77 96 17 FE EA DF 71 52 F7 7F 90 D0

99.
C1 F7 1B 7E 82 12 88 04 76 56 96 59 B7 4C 24 71 77 96 17 FE EA DF 71 52 F7 7F 90 D0

100.
C1 F7 1B 7E 82 12 CD 04 76 56 96 59 B7 4C 24 71 77 96 17 FE EA DF 71 52 F7 7F 90 D0

101.
C1 F7 1B 7E 82 12 CD 34 76 56 96 59 B7 4C 24 71 77 96 17 FE EA DF 71 52 F7 7F 90 D0

102.
C1 F7 1B 7E 82 12 CD 34 B0 56 96 59 B7 4C 24 71 77 96 17 FE EA DF 71 52 F7 7F 90 D0

103.
C1 F7 1B 7E 82 12 CD 34 B0 85 96 59 B7 4C 24 71 77 96 17 FE EA DF 71 52 F7 7F 90 D0

104.
C1 F7 1B 7E 82 12 CD 34 B0 85 82 59 B7 4C 24 71 77 96 17 FE EA DF 71 52 F7 7F 90 D0

105.
C1 F7 1B 7E 82 12 CD 34 B0 85 82 E4 B7 4C 24 71 77 96 17 FE EA DF 71 52 F7 7F 90 D0

106.
C1 F7 1B 7E 82 12 CD 34 B0 85 82 E4 29 4C 24 71 77 96 17 FE EA DF 71 52 F7 7F 90 D0

107.
C1 F7 1B 7E 82 12 CD 34 B0 85 82 E4 29 DA 24 71 77 96 17 FE EA DF 71 52 F7 7F 90 D0

108.
C1 F7 1B 7E 82 12 CD 34 B0 85 82 E4 29 DA 91 71 77 96 17 FE EA DF 71 52 F7 7F 90 D0

109.
C1 F7 1B 7E 82 12 CD 34 B0 85 82 E4 29 DA 91 FD 77 96 17 FE EA DF 71 52 F7 7F 90 D0

110.
C1 F7 1B 7E 82 12 CD 34 B0 85 82 E4 29 DA 91 FD 82 96 17 FE EA DF 71 52 F7 7F 90 D0

111.
C1 F7 1B 7E 82 12 CD 34 B0 85 82 E4 29 DA 91 FD 82 96 17 FE EA DF 71 52 F7 7F 90 D0

112.
C1 F7 1B 7E 82 12 CD 34 B0 85 82 E4 29 DA 91 FD 82 96 50 FE EA DF 71 52 F7 7F 90 D0

113.
C1 F7 1B 7E 82 12 CD 34 B0 85 82 E4 29 DA 91 FD 82 96 50 EB EA DF 71 52 F7 7F 90 D0

114.
C1 F7 1B 7E 82 12 CD 34 B0 85 82 E4 29 DA 91 FD 82 96 50 EB FE DF 71 52 F7 7F 90 D0

115.
C1 F7 1B 7E 82 12 CD 34 B0 85 82 E4 29 DA 91 FD 82 96 50 EB FE 40 71 52 F7 7F 90 D0

116.
C1 F7 1B 7E 82 12 CD 34 B0 85 82 E4 29 DA 91 FD 82 96 50 EB FE 40 E0 52 F7 7F 90 D0

117.
C1 F7 1B 7E 82 12 CD 34 B0 85 82 E4 29 DA 91 FD 82 96 50 EB FE 40 E0 FB F7 7F 90 D0

118.
C1 F7 1B 7E 82 12 CD 34 B0 85 82 E4 29 DA 91 FD 82 96 50 EB FE 40 E0 FB 4D 7F 90 D0

119.
C1 F7 1B 7E 82 12 CD 34 B0 85 82 E4 29 DA 91 FD 82 96 50 EB FE 40 E0 FB 4D 6C 90 D0

120.
C1 F7 1B 7E 82 12 CD 34 B0 85 82 E4 29 DA 91 FD 82 96 50 EB FE 40 E0 FB 4D 6C 6B D0

121.
C1 F7 1B 7E 82 12 CD 34 B0 85 82 E4 29 DA 91 FD 82 96 50 EB FE 40 E0 FB 4D 6C 6B 5E

122.
DD F7 1B 7E 82 12 CD 34 B0 85 82 E4 29 DA 91 FD 82 96 50 EB FE 40 E0 FB 4D 6C 6B 5E

123.
DD 57 1B 7E 82 12 CD 34 B0 85 82 E4 29 DA 91 FD 82 96 50 EB FE 40 E0 FB 4D 6C 6B 5E

124.
DD 57 51 7E 82 12 CD 34 B0 85 82 E4 29 DA 91 FD 82 96 50 EB FE 40 E0 FB 4D 6C 6B 5E

125.
DD 57 51 BE 82 12 CD 34 B0 85 82 E4 29 DA 91 FD 82 96 50 EB FE 40 E0 FB 4D 6C 6B 5E

126.
DD 57 51 BE 84 12 CD 34 B0 85 82 E4 29 DA 91 FD 82 96 50 EB FE 40 E0 FB 4D 6C 6B 5E

127.
DD 57 51 BE 84 1D CD 34 B0 85 82 E4 29 DA 91 FD 82 96 50 EB FE 40 E0 FB 4D 6C 6B 5E

128.
DD 57 51 BE 84 1D B1 34 B0 85 82 E4 29 DA 91 FD 82 96 50 EB FE 40 E0 FB 4D 6C 6B 5E

129.
DD 57 51 BE 84 1D B1 CD B0 85 82 E4 29 DA 91 FD 82 96 50 EB FE 40 E0 FB 4D 6C 6B 5E

130.
DD 57 51 BE 84 1D B1 CD 0E 85 82 E4 29 DA 91 FD 82 96 50 EB FE 40 E0 FB 4D 6C 6B 5E

131.
DD 57 51 BE 84 1D B1 CD 0E 55 82 E4 29 DA 91 FD 82 96 50 EB FE 40 E0 FB 4D 6C 6B 5E

132.
DD 57 51 BE 84 1D B1 CD 0E 55 E8 E4 29 DA 91 FD 82 96 50 EB FE 40 E0 FB 4D 6C 6B 5E

133.
DD 57 51 BE 84 1D B1 CD 0E 55 E8 52 29 DA 91 FD 82 96 50 EB FE 40 E0 FB 4D 6C 6B 5E

134.
DD 57 51 BE 84 1D B1 CD 0E 55 E8 52 83 DA 91 FD 82 96 50 EB FE 40 E0 FB 4D 6C 6B 5E

135.
DD 57 51 BE 84 1D B1 CD 0E 55 E8 52 83 D3 91 FD 82 96 50 EB FE 40 E0 FB 4D 6C 6B 5E

136.
DD 57 51 BE 84 1D B1 CD 0E 55 E8 52 83 D3 6D FD 82 96 50 EB FE 40 E0 FB 4D 6C 6B 5E

137.
DD 57 51 BE 84 1D B1 CD 0E 55 E8 52 83 D3 6D 5A 82 96 50 EB FE 40 E0 FB 4D 6C 6B 5E

Message digest: DD 57 51 BE 84 1D B1 CD 0E 55 E8 52 83 D3 6D 5A 82 96 50 EB FE 40 E0 FB 4D 6C 6B 5E

10.2 Hash bit length 256, delay=2.

For this message digest calculation consist from:

9 steps for pre-hash computation – same like for 224 hashbitlen;
128 steps for final hash computation.

Stage 1-2 – same like 10.1.

Stage 3. Final hash computation – 128 steps

This is SR states for steps in final hash computation. SR length is 32.

10.
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

11.
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

12.
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

13.
2F BE A8 70 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

14.
2F BE A8 70 2B 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

15.
2F BE A8 70 2B 76 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

16.
2F BE A8 70 2B 76 2C 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

17.
2F BE A8 70 2B 76 2C 96 08 09 0A 0B 0C 0D 0E 0F 10 11 12 13 14 15 16 17 18 19 1A 1B 1C 1D 1E 1F

18.
2F BE A8 70 2B 76 2C 96 89 09 0A 0B 0C 0D 0E 0F 10 11 12 13 14 15 16 17 18 19 1A 1B 1C 1D 1E 1F

19.
2F BE A8 70 2B 76 2C 96 89 2C 0A 0B 0C 0D 0E 0F 10 11 12 13 14 15 16 17 18 19 1A 1B 1C 1D 1E 1F

20.
2F BE A8 70 2B 76 2C 96 89 2C 69 0B 0C 0D 0E 0F 10 11 12 13 14 15 16 17 18 19 1A 1B 1C 1D 1E 1F

21.

2F BE A8 70 2B 76 2C 96 89 2C 69 9F 0C 0D 0E 0F 10 11 12 13 14 15 16 17 18 19 1A 1B 1C 1D 1E 1F

22.
2F BE A8 70 2B 76 2C 96 89 2C 69 9F 4E 0D 0E 0F 10 11 12 13 14 15 16 17 18 19 1A 1B 1C 1D 1E 1F

23.
2F BE A8 70 2B 76 2C 96 89 2C 69 9F 4E AD 0E 0F 10 11 12 13 14 15 16 17 18 19 1A 1B 1C 1D 1E 1F

24.
2F BE A8 70 2B 76 2C 96 89 2C 69 9F 4E AD 1D 0F 10 11 12 13 14 15 16 17 18 19 1A 1B 1C 1D 1E 1F

25.
2F BE A8 70 2B 76 2C 96 89 2C 69 9F 4E AD 1D A6 10 11 12 13 14 15 16 17 18 19 1A 1B 1C 1D 1E 1F

26.
2F BE A8 70 2B 76 2C 96 89 2C 69 9F 4E AD 1D A6 30 11 12 13 14 15 16 17 18 19 1A 1B 1C 1D 1E 1F

27.
2F BE A8 70 2B 76 2C 96 89 2C 69 9F 4E AD 1D A6 30 21 12 13 14 15 16 17 18 19 1A 1B 1C 1D 1E 1F

28.
2F BE A8 70 2B 76 2C 96 89 2C 69 9F 4E AD 1D A6 30 21 C7 13 14 15 16 17 18 19 1A 1B 1C 1D 1E 1F

29.
2F BE A8 70 2B 76 2C 96 89 2C 69 9F 4E AD 1D A6 30 21 C7 B4 14 15 16 17 18 19 1A 1B 1C 1D 1E 1F

30.
2F BE A8 70 2B 76 2C 96 89 2C 69 9F 4E AD 1D A6 30 21 C7 B4 2E 15 16 17 18 19 1A 1B 1C 1D 1E 1F

31.
2F BE A8 70 2B 76 2C 96 89 2C 69 9F 4E AD 1D A6 30 21 C7 B4 2E 3D 16 17 18 19 1A 1B 1C 1D 1E 1F

32.
2F BE A8 70 2B 76 2C 96 89 2C 69 9F 4E AD 1D A6 30 21 C7 B4 2E 3D 37 17 18 19 1A 1B 1C 1D 1E 1F

33.
2F BE A8 70 2B 76 2C 96 89 2C 69 9F 4E AD 1D A6 30 21 C7 B4 2E 3D 37 27 18 19 1A 1B 1C 1D 1E 1F

34.
2F BE A8 70 2B 76 2C 96 89 2C 69 9F 4E AD 1D A6 30 21 C7 B4 2E 3D 37 27 58 19 1A 1B 1C 1D 1E 1F

35.
2F BE A8 70 2B 76 2C 96 89 2C 69 9F 4E AD 1D A6 30 21 C7 B4 2E 3D 37 27 58 07 1A 1B 1C 1D 1E 1F

36.
2F BE A8 70 2B 76 2C 96 89 2C 69 9F 4E AD 1D A6 30 21 C7 B4 2E 3D 37 27 58 07 3E 1B 1C 1D 1E 1F

37.
2F BE A8 70 2B 76 2C 96 89 2C 69 9F 4E AD 1D A6 30 21 C7 B4 2E 3D 37 27 58 07 3E 12 1C 1D 1E 1F

38.
2F BE A8 70 2B 76 2C 96 89 2C 69 9F 4E AD 1D A6 30 21 C7 B4 2E 3D 37 27 58 07 3E 12 C0 1D 1E 1F

39.
2F BE A8 70 2B 76 2C 96 89 2C 69 9F 4E AD 1D A6 30 21 C7 B4 2E 3D 37 27 58 07 3E 12 C0 22 1E 1F

40.
2F BE A8 70 2B 76 2C 96 89 2C 69 9F 4E AD 1D A6 30 21 C7 B4 2E 3D 37 27 58 07 3E 12 C0 22 BD 1F

41.
2F BE A8 70 2B 76 2C 96 89 2C 69 9F 4E AD 1D A6 30 21 C7 B4 2E 3D 37 27 58 07 3E 12 C0 22 BD 35

42.
F4 BE A8 70 2B 76 2C 96 89 2C 69 9F 4E AD 1D A6 30 21 C7 B4 2E 3D 37 27 58 07 3E 12 C0 22 BD 35

43.
F4 FF A8 70 2B 76 2C 96 89 2C 69 9F 4E AD 1D A6 30 21 C7 B4 2E 3D 37 27 58 07 3E 12 C0 22 BD 35

44.
F4 FF 6B 70 2B 76 2C 96 89 2C 69 9F 4E AD 1D A6 30 21 C7 B4 2E 3D 37 27 58 07 3E 12 C0 22 BD 35

45.
F4 FF 6B D6 2B 76 2C 96 89 2C 69 9F 4E AD 1D A6 30 21 C7 B4 2E 3D 37 27 58 07 3E 12 C0 22 BD 35

46.
F4 FF 6B D6 7A 76 2C 96 89 2C 69 9F 4E AD 1D A6 30 21 C7 B4 2E 3D 37 27 58 07 3E 12 C0 22 BD 35

47.
F4 FF 6B D6 7A CD 2C 96 89 2C 69 9F 4E AD 1D A6 30 21 C7 B4 2E 3D 37 27 58 07 3E 12 C0 22 BD 35

48.
F4 FF 6B D6 7A CD 66 96 89 2C 69 9F 4E AD 1D A6 30 21 C7 B4 2E 3D 37 27 58 07 3E 12 C0 22 BD 35

49.
F4 FF 6B D6 7A CD 66 7F 89 2C 69 9F 4E AD 1D A6 30 21 C7 B4 2E 3D 37 27 58 07 3E 12 C0 22 BD 35

50.
F4 FF 6B D6 7A CD 66 7F 03 2C 69 9F 4E AD 1D A6 30 21 C7 B4 2E 3D 37 27 58 07 3E 12 C0 22 BD 35

51.
F4 FF 6B D6 7A CD 66 7F 03 47 69 9F 4E AD 1D A6 30 21 C7 B4 2E 3D 37 27 58 07 3E 12 C0 22 BD 35

52.
F4 FF 6B D6 7A CD 66 7F 03 47 65 9F 4E AD 1D A6 30 21 C7 B4 2E 3D 37 27 58 07 3E 12 C0 22 BD 35

53.
F4 FF 6B D6 7A CD 66 7F 03 47 65 5C 4E AD 1D A6 30 21 C7 B4 2E 3D 37 27 58 07 3E 12 C0 22 BD 35

54.
F4 FF 6B D6 7A CD 66 7F 03 47 65 5C B9 AD 1D A6 30 21 C7 B4 2E 3D 37 27 58 07 3E 12 C0 22 BD 35

55.
F4 FF 6B D6 7A CD 66 7F 03 47 65 5C B9 94 1D A6 30 21 C7 B4 2E 3D 37 27 58 07 3E 12 C0 22 BD 35

56.
F4 FF 6B D6 7A CD 66 7F 03 47 65 5C B9 94 FB A6 30 21 C7 B4 2E 3D 37 27 58 07 3E 12 C0 22 BD 35

57.
F4 FF 6B D6 7A CD 66 7F 03 47 65 5C B9 94 FB 71 30 21 C7 B4 2E 3D 37 27 58 07 3E 12 C0 22 BD 35

58.
F4 FF 6B D6 7A CD 66 7F 03 47 65 5C B9 94 FB 71 43 21 C7 B4 2E 3D 37 27 58 07 3E 12 C0 22 BD 35

59.
F4 FF 6B D6 7A CD 66 7F 03 47 65 5C B9 94 FB 71 43 3E C7 B4 2E 3D 37 27 58 07 3E 12 C0 22 BD 35

60.
F4 FF 6B D6 7A CD 66 7F 03 47 65 5C B9 94 FB 71 43 3E 26 B4 2E 3D 37 27 58 07 3E 12 C0 22 BD 35

61.
F4 FF 6B D6 7A CD 66 7F 03 47 65 5C B9 94 FB 71 43 3E 26 16 2E 3D 37 27 58 07 3E 12 C0 22 BD 35

62.
F4 FF 6B D6 7A CD 66 7F 03 47 65 5C B9 94 FB 71 43 3E 26 16 95 3D 37 27 58 07 3E 12 C0 22 BD 35

63.
F4 FF 6B D6 7A CD 66 7F 03 47 65 5C B9 94 FB 71 43 3E 26 16 95 24 37 27 58 07 3E 12 C0 22 BD 35

64.
F4 FF 6B D6 7A CD 66 7F 03 47 65 5C B9 94 FB 71 43 3E 26 16 95 24 34 27 58 07 3E 12 C0 22 BD 35

65.
F4 FF 6B D6 7A CD 66 7F 03 47 65 5C B9 94 FB 71 43 3E 26 16 95 24 34 AA 58 07 3E 12 C0 22 BD 35

66.
F4 FF 6B D6 7A CD 66 7F 03 47 65 5C B9 94 FB 71 43 3E 26 16 95 24 34 AA A1 07 3E 12 C0 22 BD 35

67.
F4 FF 6B D6 7A CD 66 7F 03 47 65 5C B9 94 FB 71 43 3E 26 16 95 24 34 AA A1 93 3E 12 C0 22 BD 35

68.
F4 FF 6B D6 7A CD 66 7F 03 47 65 5C B9 94 FB 71 43 3E 26 16 95 24 34 AA A1 93 E6 12 C0 22 BD 35

69.
F4 FF 6B D6 7A CD 66 7F 03 47 65 5C B9 94 FB 71 43 3E 26 16 95 24 34 AA A1 93 E6 B1 C0 22 BD 35

70.
F4 FF 6B D6 7A CD 66 7F 03 47 65 5C B9 94 FB 71 43 3E 26 16 95 24 34 AA A1 93 E6 B1 8F 22 BD 35

71.
F4 FF 6B D6 7A CD 66 7F 03 47 65 5C B9 94 FB 71 43 3E 26 16 95 24 34 AA A1 93 E6 B1 8F A7 BD 35
72.
F4 FF 6B D6 7A CD 66 7F 03 47 65 5C B9 94 FB 71 43 3E 26 16 95 24 34 AA A1 93 E6 B1 8F A7 67 35
73.
F4 FF 6B D6 7A CD 66 7F 03 47 65 5C B9 94 FB 71 43 3E 26 16 95 24 34 AA A1 93 E6 B1 8F A7 67 43
74.
91 FF 6B D6 7A CD 66 7F 03 47 65 5C B9 94 FB 71 43 3E 26 16 95 24 34 AA A1 93 E6 B1 8F A7 67 43
75.
91 B0 6B D6 7A CD 66 7F 03 47 65 5C B9 94 FB 71 43 3E 26 16 95 24 34 AA A1 93 E6 B1 8F A7 67 43
76.
91 B0 D4 D6 7A CD 66 7F 03 47 65 5C B9 94 FB 71 43 3E 26 16 95 24 34 AA A1 93 E6 B1 8F A7 67 43
77.
91 B0 D4 29 7A CD 66 7F 03 47 65 5C B9 94 FB 71 43 3E 26 16 95 24 34 AA A1 93 E6 B1 8F A7 67 43
78.
91 B0 D4 29 E3 CD 66 7F 03 47 65 5C B9 94 FB 71 43 3E 26 16 95 24 34 AA A1 93 E6 B1 8F A7 67 43
79.
91 B0 D4 29 E3 D3 66 7F 03 47 65 5C B9 94 FB 71 43 3E 26 16 95 24 34 AA A1 93 E6 B1 8F A7 67 43
80.
91 B0 D4 29 E3 D3 38 7F 03 47 65 5C B9 94 FB 71 43 3E 26 16 95 24 34 AA A1 93 E6 B1 8F A7 67 43
81.
91 B0 D4 29 E3 D3 38 17 03 47 65 5C B9 94 FB 71 43 3E 26 16 95 24 34 AA A1 93 E6 B1 8F A7 67 43
82.
91 B0 D4 29 E3 D3 38 17 C9 47 65 5C B9 94 FB 71 43 3E 26 16 95 24 34 AA A1 93 E6 B1 8F A7 67 43
83.
91 B0 D4 29 E3 D3 38 17 C9 26 65 5C B9 94 FB 71 43 3E 26 16 95 24 34 AA A1 93 E6 B1 8F A7 67 43
84.
91 B0 D4 29 E3 D3 38 17 C9 26 0E 5C B9 94 FB 71 43 3E 26 16 95 24 34 AA A1 93 E6 B1 8F A7 67 43
85.
91 B0 D4 29 E3 D3 38 17 C9 26 0E 0E B9 94 FB 71 43 3E 26 16 95 24 34 AA A1 93 E6 B1 8F A7 67 43
86.
91 B0 D4 29 E3 D3 38 17 C9 26 0E 0E 91 94 FB 71 43 3E 26 16 95 24 34 AA A1 93 E6 B1 8F A7 67 43
87.
91 B0 D4 29 E3 D3 38 17 C9 26 0E 0E 91 50 FB 71 43 3E 26 16 95 24 34 AA A1 93 E6 B1 8F A7 67 43
88.
91 B0 D4 29 E3 D3 38 17 C9 26 0E 0E 91 50 C7 71 43 3E 26 16 95 24 34 AA A1 93 E6 B1 8F A7 67 43
89.
91 B0 D4 29 E3 D3 38 17 C9 26 0E 0E 91 50 C7 91 43 3E 26 16 95 24 34 AA A1 93 E6 B1 8F A7 67 43
90.
91 B0 D4 29 E3 D3 38 17 C9 26 0E 0E 91 50 C7 91 FA 3E 26 16 95 24 34 AA A1 93 E6 B1 8F A7 67 43
91.
91 B0 D4 29 E3 D3 38 17 C9 26 0E 0E 91 50 C7 91 FA A6 26 16 95 24 34 AA A1 93 E6 B1 8F A7 67 43
92.
91 B0 D4 29 E3 D3 38 17 C9 26 0E 0E 91 50 C7 91 FA A6 9D 16 95 24 34 AA A1 93 E6 B1 8F A7 67 43
93.
91 B0 D4 29 E3 D3 38 17 C9 26 0E 0E 91 50 C7 91 FA A6 9D 9C 95 24 34 AA A1 93 E6 B1 8F A7 67 43
94.
91 B0 D4 29 E3 D3 38 17 C9 26 0E 0E 91 50 C7 91 FA A6 9D 9C 9A 24 34 AA A1 93 E6 B1 8F A7 67 43
- 95.

91 B0 D4 29 E3 D3 38 17 C9 26 0E 0E 91 50 C7 91 FA A6 9D 9C 9A 8A 34 AA A1 93 E6 B1 8F A7 67 43

96.
91 B0 D4 29 E3 D3 38 17 C9 26 0E 0E 91 50 C7 91 FA A6 9D 9C 9A 8A AC AA A1 93 E6 B1 8F A7 67 43

97.
91 B0 D4 29 E3 D3 38 17 C9 26 0E 0E 91 50 C7 91 FA A6 9D 9C 9A 8A AC B2 A1 93 E6 B1 8F A7 67 43

98.
91 B0 D4 29 E3 D3 38 17 C9 26 0E 0E 91 50 C7 91 FA A6 9D 9C 9A 8A AC B2 04 93 E6 B1 8F A7 67 43

99.
91 B0 D4 29 E3 D3 38 17 C9 26 0E 0E 91 50 C7 91 FA A6 9D 9C 9A 8A AC B2 04 8A E6 B1 8F A7 67 43

100.
91 B0 D4 29 E3 D3 38 17 C9 26 0E 0E 91 50 C7 91 FA A6 9D 9C 9A 8A AC B2 04 8A A0 B1 8F A7 67 43

101.
91 B0 D4 29 E3 D3 38 17 C9 26 0E 0E 91 50 C7 91 FA A6 9D 9C 9A 8A AC B2 04 8A A0 F0 8F A7 67 43

102.
91 B0 D4 29 E3 D3 38 17 C9 26 0E 0E 91 50 C7 91 FA A6 9D 9C 9A 8A AC B2 04 8A A0 F0 FB A7 67 43

103.
91 B0 D4 29 E3 D3 38 17 C9 26 0E 0E 91 50 C7 91 FA A6 9D 9C 9A 8A AC B2 04 8A A0 F0 FB D4 67 43

104.
91 B0 D4 29 E3 D3 38 17 C9 26 0E 0E 91 50 C7 91 FA A6 9D 9C 9A 8A AC B2 04 8A A0 F0 FB D4 02 43

105.
91 B0 D4 29 E3 D3 38 17 C9 26 0E 0E 91 50 C7 91 FA A6 9D 9C 9A 8A AC B2 04 8A A0 F0 FB D4 02 80

106.
89 B0 D4 29 E3 D3 38 17 C9 26 0E 0E 91 50 C7 91 FA A6 9D 9C 9A 8A AC B2 04 8A A0 F0 FB D4 02 80

107.
89 8F D4 29 E3 D3 38 17 C9 26 0E 0E 91 50 C7 91 FA A6 9D 9C 9A 8A AC B2 04 8A A0 F0 FB D4 02 80

108.
89 8F E2 29 E3 D3 38 17 C9 26 0E 0E 91 50 C7 91 FA A6 9D 9C 9A 8A AC B2 04 8A A0 F0 FB D4 02 80

109.
89 8F E2 AF E3 D3 38 17 C9 26 0E 0E 91 50 C7 91 FA A6 9D 9C 9A 8A AC B2 04 8A A0 F0 FB D4 02 80

110.
89 8F E2 AF B3 D3 38 17 C9 26 0E 0E 91 50 C7 91 FA A6 9D 9C 9A 8A AC B2 04 8A A0 F0 FB D4 02 80

111.
89 8F E2 AF B3 A1 38 17 C9 26 0E 0E 91 50 C7 91 FA A6 9D 9C 9A 8A AC B2 04 8A A0 F0 FB D4 02 80

112.
89 8F E2 AF B3 A1 A7 17 C9 26 0E 0E 91 50 C7 91 FA A6 9D 9C 9A 8A AC B2 04 8A A0 F0 FB D4 02 80

113.
89 8F E2 AF B3 A1 A7 81 C9 26 0E 0E 91 50 C7 91 FA A6 9D 9C 9A 8A AC B2 04 8A A0 F0 FB D4 02 80

114.
89 8F E2 AF B3 A1 A7 81 5C 26 0E 0E 91 50 C7 91 FA A6 9D 9C 9A 8A AC B2 04 8A A0 F0 FB D4 02 80

115.
89 8F E2 AF B3 A1 A7 81 5C 57 0E 0E 91 50 C7 91 FA A6 9D 9C 9A 8A AC B2 04 8A A0 F0 FB D4 02 80

116.
89 8F E2 AF B3 A1 A7 81 5C 57 AA 0E 91 50 C7 91 FA A6 9D 9C 9A 8A AC B2 04 8A A0 F0 FB D4 02 80

117.
89 8F E2 AF B3 A1 A7 81 5C 57 AA F8 91 50 C7 91 FA A6 9D 9C 9A 8A AC B2 04 8A A0 F0 FB D4 02 80

118.
89 8F E2 AF B3 A1 A7 81 5C 57 AA F8 45 50 C7 91 FA A6 9D 9C 9A 8A AC B2 04 8A A0 F0 FB D4 02 80

119.
89 8F E2 AF B3 A1 A7 81 5C 57 AA F8 45 C3 C7 91 FA A6 9D 9C 9A 8A AC B2 04 8A A0 F0 FB D4 02 80

120.
89 8F E2 AF B3 A1 A7 81 5C 57 AA F8 45 C3 34 91 FA A6 9D 9C 9A 8A AC B2 04 8A A0 F0 FB D4 02 80

121.
89 8F E2 AF B3 A1 A7 81 5C 57 AA F8 45 C3 34 5D FA A6 9D 9C 9A 8A AC B2 04 8A A0 F0 FB D4 02 80

122.
89 8F E2 AF B3 A1 A7 81 5C 57 AA F8 45 C3 34 5D D6 A6 9D 9C 9A 8A AC B2 04 8A A0 F0 FB D4 02 80

123.
89 8F E2 AF B3 A1 A7 81 5C 57 AA F8 45 C3 34 5D D6 C2 9D 9C 9A 8A AC B2 04 8A A0 F0 FB D4 02 80

124.
89 8F E2 AF B3 A1 A7 81 5C 57 AA F8 45 C3 34 5D D6 C2 F5 9C 9A 8A AC B2 04 8A A0 F0 FB D4 02 80

125.
89 8F E2 AF B3 A1 A7 81 5C 57 AA F8 45 C3 34 5D D6 C2 F5 36 9A 8A AC B2 04 8A A0 F0 FB D4 02 80

126.
89 8F E2 AF B3 A1 A7 81 5C 57 AA F8 45 C3 34 5D D6 C2 F5 36 A6 8A AC B2 04 8A A0 F0 FB D4 02 80

127.
89 8F E2 AF B3 A1 A7 81 5C 57 AA F8 45 C3 34 5D D6 C2 F5 36 A6 CA AC B2 04 8A A0 F0 FB D4 02 80

128.
89 8F E2 AF B3 A1 A7 81 5C 57 AA F8 45 C3 34 5D D6 C2 F5 36 A6 CA 5A B2 04 8A A0 F0 FB D4 02 80

129.
89 8F E2 AF B3 A1 A7 81 5C 57 AA F8 45 C3 34 5D D6 C2 F5 36 A6 CA 5A CB 04 8A A0 F0 FB D4 02 80

130.
89 8F E2 AF B3 A1 A7 81 5C 57 AA F8 45 C3 34 5D D6 C2 F5 36 A6 CA 5A CB 41 8A A0 F0 FB D4 02 80

131.
89 8F E2 AF B3 A1 A7 81 5C 57 AA F8 45 C3 34 5D D6 C2 F5 36 A6 CA 5A CB 41 A3 A0 F0 FB D4 02 80

132.
89 8F E2 AF B3 A1 A7 81 5C 57 AA F8 45 C3 34 5D D6 C2 F5 36 A6 CA 5A CB 41 A3 58 F0 FB D4 02 80

133.
89 8F E2 AF B3 A1 A7 81 5C 57 AA F8 45 C3 34 5D D6 C2 F5 36 A6 CA 5A CB 41 A3 58 4B FB D4 02 80

134.
89 8F E2 AF B3 A1 A7 81 5C 57 AA F8 45 C3 34 5D D6 C2 F5 36 A6 CA 5A CB 41 A3 58 4B 91 D4 02 80

135.
89 8F E2 AF B3 A1 A7 81 5C 57 AA F8 45 C3 34 5D D6 C2 F5 36 A6 CA 5A CB 41 A3 58 4B 91 B5 02 80

136.
89 8F E2 AF B3 A1 A7 81 5C 57 AA F8 45 C3 34 5D D6 C2 F5 36 A6 CA 5A CB 41 A3 58 4B 91 B5 BD 80

137.
89 8F E2 AF B3 A1 A7 81 5C 57 AA F8 45 C3 34 5D D6 C2 F5 36 A6 CA 5A CB 41 A3 58 4B 91 B5 BD FE

Message digest:

89 8F E2 AF B3 A1 A7 81 5C 57 AA F8 45 C3 34 5D D6 C2 F5 36 A6 CA 5A CB 41 A3 58 4B 91 B5 BD FE

10.3 Hash bit length 384, delay=2.

For this message digest calculation consist from:

- 9 steps for pre-hash computation;
- 256 steps for final hash computation.

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

Stage 1. Preprocessing

29.
2F 59 8A 83 05 61 8F 08 B7 99 17 09 5C A2 30 FB 89 E5 03 38 14 15 16 17 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.
2F 59 8A 83 05 61 8F 08 B7 99 17 09 5C A2 30 FB 89 E5 03 38 67 15 16 17 18 19 1A 1B 1C 1D 1E 1F 20 21 22 23
24 25 26 27 28 29 2A 2B 2C 2D 2E 2F
31.
2F 59 8A 83 05 61 8F 08 B7 99 17 09 5C A2 30 FB 89 E5 03 38 67 C5 16 17 18 19 1A 1B 1C 1D 1E 1F 20 21 22 23
24 25 26 27 28 29 2A 2B 2C 2D 2E 2F
32.
2F 59 8A 83 05 61 8F 08 B7 99 17 09 5C A2 30 FB 89 E5 03 38 67 C5 C0 17 18 19 1A 1B 1C 1D 1E 1F 20 21 22
23 24 25 26 27 28 29 2A 2B 2C 2D 2E 2F
33.
2F 59 8A 83 05 61 8F 08 B7 99 17 09 5C A2 30 FB 89 E5 03 38 67 C5 C0 68 18 19 1A 1B 1C 1D 1E 1F 20 21 22
23 24 25 26 27 28 29 2A 2B 2C 2D 2E 2F
34.
2F 59 8A 83 05 61 8F 08 B7 99 17 09 5C A2 30 FB 89 E5 03 38 67 C5 C0 68 48 19 1A 1B 1C 1D 1E 1F 20 21 22
23 24 25 26 27 28 29 2A 2B 2C 2D 2E 2F
35.
2F 59 8A 83 05 61 8F 08 B7 99 17 09 5C A2 30 FB 89 E5 03 38 67 C5 C0 68 48 29 1A 1B 1C 1D 1E 1F 20 21 22
23 24 25 26 27 28 29 2A 2B 2C 2D 2E 2F
36.
2F 59 8A 83 05 61 8F 08 B7 99 17 09 5C A2 30 FB 89 E5 03 38 67 C5 C0 68 48 29 0C 1B 1C 1D 1E 1F 20 21 22
23 24 25 26 27 28 29 2A 2B 2C 2D 2E 2F
37.
2F 59 8A 83 05 61 8F 08 B7 99 17 09 5C A2 30 FB 89 E5 03 38 67 C5 C0 68 48 29 0C AD 1C 1D 1E 1F 20 21 22
23 24 25 26 27 28 29 2A 2B 2C 2D 2E 2F
38.
2F 59 8A 83 05 61 8F 08 B7 99 17 09 5C A2 30 FB 89 E5 03 38 67 C5 C0 68 48 29 0C AD F4 1D 1E 1F 20 21 22
23 24 25 26 27 28 29 2A 2B 2C 2D 2E 2F
39.
2F 59 8A 83 05 61 8F 08 B7 99 17 09 5C A2 30 FB 89 E5 03 38 67 C5 C0 68 48 29 0C AD F4 76 1E 1F 20 21 22 23
24 25 26 27 28 29 2A 2B 2C 2D 2E 2F
40.
2F 59 8A 83 05 61 8F 08 B7 99 17 09 5C A2 30 FB 89 E5 03 38 67 C5 C0 68 48 29 0C AD F4 76 DD 1F 20 21 22
23 24 25 26 27 28 29 2A 2B 2C 2D 2E 2F
41.
2F 59 8A 83 05 61 8F 08 B7 99 17 09 5C A2 30 FB 89 E5 03 38 67 C5 C0 68 48 29 0C AD F4 76 DD 55 20 21 22
23 24 25 26 27 28 29 2A 2B 2C 2D 2E 2F
42.
2F 59 8A 83 05 61 8F 08 B7 99 17 09 5C A2 30 FB 89 E5 03 38 67 C5 C0 68 48 29 0C AD F4 76 DD 55 57 21 22
23 24 25 26 27 28 29 2A 2B 2C 2D 2E 2F
43.
2F 59 8A 83 05 61 8F 08 B7 99 17 09 5C A2 30 FB 89 E5 03 38 67 C5 C0 68 48 29 0C AD F4 76 DD 55 57 A2 22
23 24 25 26 27 28 29 2A 2B 2C 2D 2E 2F
44.
2F 59 8A 83 05 61 8F 08 B7 99 17 09 5C A2 30 FB 89 E5 03 38 67 C5 C0 68 48 29 0C AD F4 76 DD 55 57 A2 83
23 24 25 26 27 28 29 2A 2B 2C 2D 2E 2F
45.
2F 59 8A 83 05 61 8F 08 B7 99 17 09 5C A2 30 FB 89 E5 03 38 67 C5 C0 68 48 29 0C AD F4 76 DD 55 57 A2 83
7E 24 25 26 27 28 29 2A 2B 2C 2D 2E 2F
46.
2F 59 8A 83 05 61 8F 08 B7 99 17 09 5C A2 30 FB 89 E5 03 38 67 C5 C0 68 48 29 0C AD F4 76 DD 55 57 A2 83
7E 10 25 26 27 28 29 2A 2B 2C 2D 2E 2F
- 47.

66.
76 12 54 CF E6 02 B9 1A DD 99 17 09 5C A2 30 FB 89 E5 03 38 67 C5 C0 68 48 29 0C AD F4 76 DD 55 57 A2 83
7E 10 D9 B6 58 13 75 96 EC 49 5B 8F C1
67.
76 12 54 CF E6 02 B9 1A DD 28 17 09 5C A2 30 FB 89 E5 03 38 67 C5 C0 68 48 29 0C AD F4 76 DD 55 57 A2 83
7E 10 D9 B6 58 13 75 96 EC 49 5B 8F C1
68.
76 12 54 CF E6 02 B9 1A DD 28 D1 09 5C A2 30 FB 89 E5 03 38 67 C5 C0 68 48 29 0C AD F4 76 DD 55 57 A2 83
7E 10 D9 B6 58 13 75 96 EC 49 5B 8F C1
69.
76 12 54 CF E6 02 B9 1A DD 28 D1 13 5C A2 30 FB 89 E5 03 38 67 C5 C0 68 48 29 0C AD F4 76 DD 55 57 A2 83
7E 10 D9 B6 58 13 75 96 EC 49 5B 8F C1
70.
76 12 54 CF E6 02 B9 1A DD 28 D1 13 01 A2 30 FB 89 E5 03 38 67 C5 C0 68 48 29 0C AD F4 76 DD 55 57 A2 83
7E 10 D9 B6 58 13 75 96 EC 49 5B 8F C1
71.
76 12 54 CF E6 02 B9 1A DD 28 D1 13 01 E6 30 FB 89 E5 03 38 67 C5 C0 68 48 29 0C AD F4 76 DD 55 57 A2 83
7E 10 D9 B6 58 13 75 96 EC 49 5B 8F C1
72.
76 12 54 CF E6 02 B9 1A DD 28 D1 13 01 E6 37 FB 89 E5 03 38 67 C5 C0 68 48 29 0C AD F4 76 DD 55 57 A2 83
7E 10 D9 B6 58 13 75 96 EC 49 5B 8F C1
73.
76 12 54 CF E6 02 B9 1A DD 28 D1 13 01 E6 37 5A 89 E5 03 38 67 C5 C0 68 48 29 0C AD F4 76 DD 55 57 A2 83
7E 10 D9 B6 58 13 75 96 EC 49 5B 8F C1
74.
76 12 54 CF E6 02 B9 1A DD 28 D1 13 01 E6 37 5A F2 E5 03 38 67 C5 C0 68 48 29 0C AD F4 76 DD 55 57 A2 83
7E 10 D9 B6 58 13 75 96 EC 49 5B 8F C1
75.
76 12 54 CF E6 02 B9 1A DD 28 D1 13 01 E6 37 5A F2 52 03 38 67 C5 C0 68 48 29 0C AD F4 76 DD 55 57 A2 83
7E 10 D9 B6 58 13 75 96 EC 49 5B 8F C1
76.
76 12 54 CF E6 02 B9 1A DD 28 D1 13 01 E6 37 5A F2 52 16 38 67 C5 C0 68 48 29 0C AD F4 76 DD 55 57 A2 83
7E 10 D9 B6 58 13 75 96 EC 49 5B 8F C1
77.
76 12 54 CF E6 02 B9 1A DD 28 D1 13 01 E6 37 5A F2 52 16 CC 67 C5 C0 68 48 29 0C AD F4 76 DD 55 57 A2 83
7E 10 D9 B6 58 13 75 96 EC 49 5B 8F C1
78.
76 12 54 CF E6 02 B9 1A DD 28 D1 13 01 E6 37 5A F2 52 16 CC 37 C5 C0 68 48 29 0C AD F4 76 DD 55 57 A2 83
7E 10 D9 B6 58 13 75 96 EC 49 5B 8F C1
79.
76 12 54 CF E6 02 B9 1A DD 28 D1 13 01 E6 37 5A F2 52 16 CC 37 26 C0 68 48 29 0C AD F4 76 DD 55 57 A2 83
7E 10 D9 B6 58 13 75 96 EC 49 5B 8F C1
80.
76 12 54 CF E6 02 B9 1A DD 28 D1 13 01 E6 37 5A F2 52 16 CC 37 26 38 68 48 29 0C AD F4 76 DD 55 57 A2 83
7E 10 D9 B6 58 13 75 96 EC 49 5B 8F C1
81.
76 12 54 CF E6 02 B9 1A DD 28 D1 13 01 E6 37 5A F2 52 16 CC 37 26 38 A9 48 29 0C AD F4 76 DD 55 57 A2 83
7E 10 D9 B6 58 13 75 96 EC 49 5B 8F C1
82.
76 12 54 CF E6 02 B9 1A DD 28 D1 13 01 E6 37 5A F2 52 16 CC 37 26 38 A9 B6 29 0C AD F4 76 DD 55 57 A2 83
7E 10 D9 B6 58 13 75 96 EC 49 5B 8F C1
83.
76 12 54 CF E6 02 B9 1A DD 28 D1 13 01 E6 37 5A F2 52 16 CC 37 26 38 A9 B6 B4 0C AD F4 76 DD 55 57 A2 83
7E 10 D9 B6 58 13 75 96 EC 49 5B 8F C1
- 84.

76 12 54 CF E6 02 B9 1A DD 28 D1 13 01 E6 37 5A F2 52 16 CC 37 26 38 A9 B6 B4 F7 AD F4 76 DD 55 57 A2 83
7E 10 D9 B6 58 13 75 96 EC 49 5B 8F C1

85.
76 12 54 CF E6 02 B9 1A DD 28 D1 13 01 E6 37 5A F2 52 16 CC 37 26 38 A9 B6 B4 F7 70 F4 76 DD 55 57 A2 83
7E 10 D9 B6 58 13 75 96 EC 49 5B 8F C1

86.
76 12 54 CF E6 02 B9 1A DD 28 D1 13 01 E6 37 5A F2 52 16 CC 37 26 38 A9 B6 B4 F7 70 0C 76 DD 55 57 A2 83
7E 10 D9 B6 58 13 75 96 EC 49 5B 8F C1

87.
76 12 54 CF E6 02 B9 1A DD 28 D1 13 01 E6 37 5A F2 52 16 CC 37 26 38 A9 B6 B4 F7 70 0C F4 DD 55 57 A2 83
7E 10 D9 B6 58 13 75 96 EC 49 5B 8F C1

88.
76 12 54 CF E6 02 B9 1A DD 28 D1 13 01 E6 37 5A F2 52 16 CC 37 26 38 A9 B6 B4 F7 70 0C F4 86 55 57 A2 83
7E 10 D9 B6 58 13 75 96 EC 49 5B 8F C1

89.
76 12 54 CF E6 02 B9 1A DD 28 D1 13 01 E6 37 5A F2 52 16 CC 37 26 38 A9 B6 B4 F7 70 0C F4 86 A1 57 A2 83
7E 10 D9 B6 58 13 75 96 EC 49 5B 8F C1

90.
76 12 54 CF E6 02 B9 1A DD 28 D1 13 01 E6 37 5A F2 52 16 CC 37 26 38 A9 B6 B4 F7 70 0C F4 86 A1 49 A2 83
7E 10 D9 B6 58 13 75 96 EC 49 5B 8F C1

91.
76 12 54 CF E6 02 B9 1A DD 28 D1 13 01 E6 37 5A F2 52 16 CC 37 26 38 A9 B6 B4 F7 70 0C F4 86 A1 49 27 83
7E 10 D9 B6 58 13 75 96 EC 49 5B 8F C1

92.
76 12 54 CF E6 02 B9 1A DD 28 D1 13 01 E6 37 5A F2 52 16 CC 37 26 38 A9 B6 B4 F7 70 0C F4 86 A1 49 27 1F
7E 10 D9 B6 58 13 75 96 EC 49 5B 8F C1

93.
76 12 54 CF E6 02 B9 1A DD 28 D1 13 01 E6 37 5A F2 52 16 CC 37 26 38 A9 B6 B4 F7 70 0C F4 86 A1 49 27 1F
91 10 D9 B6 58 13 75 96 EC 49 5B 8F C1

94.
76 12 54 CF E6 02 B9 1A DD 28 D1 13 01 E6 37 5A F2 52 16 CC 37 26 38 A9 B6 B4 F7 70 0C F4 86 A1 49 27 1F
91 83 D9 B6 58 13 75 96 EC 49 5B 8F C1

95.
76 12 54 CF E6 02 B9 1A DD 28 D1 13 01 E6 37 5A F2 52 16 CC 37 26 38 A9 B6 B4 F7 70 0C F4 86 A1 49 27 1F
91 83 84 B6 58 13 75 96 EC 49 5B 8F C1

96.
76 12 54 CF E6 02 B9 1A DD 28 D1 13 01 E6 37 5A F2 52 16 CC 37 26 38 A9 B6 B4 F7 70 0C F4 86 A1 49 27 1F
91 83 84 DA 58 13 75 96 EC 49 5B 8F C1

97.
76 12 54 CF E6 02 B9 1A DD 28 D1 13 01 E6 37 5A F2 52 16 CC 37 26 38 A9 B6 B4 F7 70 0C F4 86 A1 49 27 1F
91 83 84 DA CD 13 75 96 EC 49 5B 8F C1

98.
76 12 54 CF E6 02 B9 1A DD 28 D1 13 01 E6 37 5A F2 52 16 CC 37 26 38 A9 B6 B4 F7 70 0C F4 86 A1 49 27 1F
91 83 84 DA CD 36 75 96 EC 49 5B 8F C1

99.
76 12 54 CF E6 02 B9 1A DD 28 D1 13 01 E6 37 5A F2 52 16 CC 37 26 38 A9 B6 B4 F7 70 0C F4 86 A1 49 27 1F
91 83 84 DA CD 36 C7 96 EC 49 5B 8F C1

100.
76 12 54 CF E6 02 B9 1A DD 28 D1 13 01 E6 37 5A F2 52 16 CC 37 26 38 A9 B6 B4 F7 70 0C F4 86 A1 49 27 1F
91 83 84 DA CD 36 C7 B0 EC 49 5B 8F C1

101.
76 12 54 CF E6 02 B9 1A DD 28 D1 13 01 E6 37 5A F2 52 16 CC 37 26 38 A9 B6 B4 F7 70 0C F4 86 A1 49 27 1F
91 83 84 DA CD 36 C7 B0 2A 49 5B 8F C1

102.
76 12 54 CF E6 02 B9 1A DD 28 D1 13 01 E6 37 5A F2 52 16 CC 37 26 38 A9 B6 B4 F7 70 0C F4 86 A1 49 27 1F
91 83 84 DA CD 36 C7 B0 2A 68 5B 8F C1

103.

76 12 54 CF E6 02 B9 1A DD 28 D1 13 01 E6 37 5A F2 52 16 CC 37 26 38 A9 B6 B4 F7 70 0C F4 86 A1 49 27 1F
91 83 84 DA CD 36 C7 B0 2A 68 11 8F C1

104.

76 12 54 CF E6 02 B9 1A DD 28 D1 13 01 E6 37 5A F2 52 16 CC 37 26 38 A9 B6 B4 F7 70 0C F4 86 A1 49 27 1F
91 83 84 DA CD 36 C7 B0 2A 68 11 94 C1

105.

76 12 54 CF E6 02 B9 1A DD 28 D1 13 01 E6 37 5A F2 52 16 CC 37 26 38 A9 B6 B4 F7 70 0C F4 86 A1 49 27 1F
91 83 84 DA CD 36 C7 B0 2A 68 11 94 BD

106.

04 12 54 CF E6 02 B9 1A DD 28 D1 13 01 E6 37 5A F2 52 16 CC 37 26 38 A9 B6 B4 F7 70 0C F4 86 A1 49 27 1F
91 83 84 DA CD 36 C7 B0 2A 68 11 94 BD

107.

04 18 54 CF E6 02 B9 1A DD 28 D1 13 01 E6 37 5A F2 52 16 CC 37 26 38 A9 B6 B4 F7 70 0C F4 86 A1 49 27 1F
91 83 84 DA CD 36 C7 B0 2A 68 11 94 BD

108.

04 18 6F CF E6 02 B9 1A DD 28 D1 13 01 E6 37 5A F2 52 16 CC 37 26 38 A9 B6 B4 F7 70 0C F4 86 A1 49 27 1F
91 83 84 DA CD 36 C7 B0 2A 68 11 94 BD

109.

04 18 6F 79 E6 02 B9 1A DD 28 D1 13 01 E6 37 5A F2 52 16 CC 37 26 38 A9 B6 B4 F7 70 0C F4 86 A1 49 27 1F
91 83 84 DA CD 36 C7 B0 2A 68 11 94 BD

110.

04 18 6F 79 97 02 B9 1A DD 28 D1 13 01 E6 37 5A F2 52 16 CC 37 26 38 A9 B6 B4 F7 70 0C F4 86 A1 49 27 1F
91 83 84 DA CD 36 C7 B0 2A 68 11 94 BD

111.

04 18 6F 79 97 ED B9 1A DD 28 D1 13 01 E6 37 5A F2 52 16 CC 37 26 38 A9 B6 B4 F7 70 0C F4 86 A1 49 27 1F
91 83 84 DA CD 36 C7 B0 2A 68 11 94 BD

112.

04 18 6F 79 97 ED 22 1A DD 28 D1 13 01 E6 37 5A F2 52 16 CC 37 26 38 A9 B6 B4 F7 70 0C F4 86 A1 49 27 1F
91 83 84 DA CD 36 C7 B0 2A 68 11 94 BD

113.

04 18 6F 79 97 ED 22 3B DD 28 D1 13 01 E6 37 5A F2 52 16 CC 37 26 38 A9 B6 B4 F7 70 0C F4 86 A1 49 27 1F
91 83 84 DA CD 36 C7 B0 2A 68 11 94 BD

114.

04 18 6F 79 97 ED 22 3B 9B 28 D1 13 01 E6 37 5A F2 52 16 CC 37 26 38 A9 B6 B4 F7 70 0C F4 86 A1 49 27 1F
91 83 84 DA CD 36 C7 B0 2A 68 11 94 BD

115.

04 18 6F 79 97 ED 22 3B 9B 53 D1 13 01 E6 37 5A F2 52 16 CC 37 26 38 A9 B6 B4 F7 70 0C F4 86 A1 49 27 1F
91 83 84 DA CD 36 C7 B0 2A 68 11 94 BD

116.

04 18 6F 79 97 ED 22 3B 9B 53 F5 13 01 E6 37 5A F2 52 16 CC 37 26 38 A9 B6 B4 F7 70 0C F4 86 A1 49 27 1F 91
83 84 DA CD 36 C7 B0 2A 68 11 94 BD

117.

04 18 6F 79 97 ED 22 3B 9B 53 F5 24 01 E6 37 5A F2 52 16 CC 37 26 38 A9 B6 B4 F7 70 0C F4 86 A1 49 27 1F 91
83 84 DA CD 36 C7 B0 2A 68 11 94 BD

118.

04 18 6F 79 97 ED 22 3B 9B 53 F5 24 BB E6 37 5A F2 52 16 CC 37 26 38 A9 B6 B4 F7 70 0C F4 86 A1 49 27 1F
91 83 84 DA CD 36 C7 B0 2A 68 11 94 BD

119.

04 18 6F 79 97 ED 22 3B 9B 53 F5 24 BB 6A 37 5A F2 52 16 CC 37 26 38 A9 B6 B4 F7 70 0C F4 86 A1 49 27 1F
91 83 84 DA CD 36 C7 B0 2A 68 11 94 BD

120.

04 18 6F 79 97 ED 22 3B 9B 53 F5 24 BB 6A 13 5A F2 52 16 CC 37 26 38 A9 B6 B4 F7 70 0C F4 86 A1 49 27 1F
91 83 84 DA CD 36 C7 B0 2A 68 11 94 BD

121.

04 18 6F 79 97 ED 22 3B 9B 53 F5 24 BB 6A 13 8F F2 52 16 CC 37 26 38 A9 B6 B4 F7 70 0C F4 86 A1 49 27 1F 91
83 84 DA CD 36 C7 B0 2A 68 11 94 BD

122.
04 18 6F 79 97 ED 22 3B 9B 53 F5 24 BB 6A 13 8F 46 52 16 CC 37 26 38 A9 B6 B4 F7 70 0C F4 86 A1 49 27 1F
91 83 84 DA CD 36 C7 B0 2A 68 11 94 BD

123.
04 18 6F 79 97 ED 22 3B 9B 53 F5 24 BB 6A 13 8F 46 67 16 CC 37 26 38 A9 B6 B4 F7 70 0C F4 86 A1 49 27 1F
91 83 84 DA CD 36 C7 B0 2A 68 11 94 BD

124.
04 18 6F 79 97 ED 22 3B 9B 53 F5 24 BB 6A 13 8F 46 67 EB CC 37 26 38 A9 B6 B4 F7 70 0C F4 86 A1 49 27 1F
91 83 84 DA CD 36 C7 B0 2A 68 11 94 BD

125.
04 18 6F 79 97 ED 22 3B 9B 53 F5 24 BB 6A 13 8F 46 67 EB 1A 37 26 38 A9 B6 B4 F7 70 0C F4 86 A1 49 27 1F 91
83 84 DA CD 36 C7 B0 2A 68 11 94 BD

126.
04 18 6F 79 97 ED 22 3B 9B 53 F5 24 BB 6A 13 8F 46 67 EB 1A F2 26 38 A9 B6 B4 F7 70 0C F4 86 A1 49 27 1F 91
83 84 DA CD 36 C7 B0 2A 68 11 94 BD

127.
04 18 6F 79 97 ED 22 3B 9B 53 F5 24 BB 6A 13 8F 46 67 EB 1A F2 3F 38 A9 B6 B4 F7 70 0C F4 86 A1 49 27 1F 91
83 84 DA CD 36 C7 B0 2A 68 11 94 BD

128.
04 18 6F 79 97 ED 22 3B 9B 53 F5 24 BB 6A 13 8F 46 67 EB 1A F2 3F 15 A9 B6 B4 F7 70 0C F4 86 A1 49 27 1F 91
83 84 DA CD 36 C7 B0 2A 68 11 94 BD

129.
04 18 6F 79 97 ED 22 3B 9B 53 F5 24 BB 6A 13 8F 46 67 EB 1A F2 3F 15 88 B6 B4 F7 70 0C F4 86 A1 49 27 1F 91
83 84 DA CD 36 C7 B0 2A 68 11 94 BD

130.
04 18 6F 79 97 ED 22 3B 9B 53 F5 24 BB 6A 13 8F 46 67 EB 1A F2 3F 15 88 02 B4 F7 70 0C F4 86 A1 49 27 1F 91
83 84 DA CD 36 C7 B0 2A 68 11 94 BD

131.
04 18 6F 79 97 ED 22 3B 9B 53 F5 24 BB 6A 13 8F 46 67 EB 1A F2 3F 15 88 02 79 F7 70 0C F4 86 A1 49 27 1F 91
83 84 DA CD 36 C7 B0 2A 68 11 94 BD

132.
04 18 6F 79 97 ED 22 3B 9B 53 F5 24 BB 6A 13 8F 46 67 EB 1A F2 3F 15 88 02 79 A7 70 0C F4 86 A1 49 27 1F 91
83 84 DA CD 36 C7 B0 2A 68 11 94 BD

133.
04 18 6F 79 97 ED 22 3B 9B 53 F5 24 BB 6A 13 8F 46 67 EB 1A F2 3F 15 88 02 79 A7 95 0C F4 86 A1 49 27 1F 91
83 84 DA CD 36 C7 B0 2A 68 11 94 BD

134.
04 18 6F 79 97 ED 22 3B 9B 53 F5 24 BB 6A 13 8F 46 67 EB 1A F2 3F 15 88 02 79 A7 95 B7 F4 86 A1 49 27 1F 91
83 84 DA CD 36 C7 B0 2A 68 11 94 BD

135.
04 18 6F 79 97 ED 22 3B 9B 53 F5 24 BB 6A 13 8F 46 67 EB 1A F2 3F 15 88 02 79 A7 95 B7 8F 86 A1 49 27 1F 91
83 84 DA CD 36 C7 B0 2A 68 11 94 BD

136.
04 18 6F 79 97 ED 22 3B 9B 53 F5 24 BB 6A 13 8F 46 67 EB 1A F2 3F 15 88 02 79 A7 95 B7 8F 46 A1 49 27 1F 91
83 84 DA CD 36 C7 B0 2A 68 11 94 BD

137.
04 18 6F 79 97 ED 22 3B 9B 53 F5 24 BB 6A 13 8F 46 67 EB 1A F2 3F 15 88 02 79 A7 95 B7 8F 46 8C 49 27 1F 91
83 84 DA CD 36 C7 B0 2A 68 11 94 BD

138.
04 18 6F 79 97 ED 22 3B 9B 53 F5 24 BB 6A 13 8F 46 67 EB 1A F2 3F 15 88 02 79 A7 95 B7 8F 46 8C CC 27 1F 91
83 84 DA CD 36 C7 B0 2A 68 11 94 BD

139.
04 18 6F 79 97 ED 22 3B 9B 53 F5 24 BB 6A 13 8F 46 67 EB 1A F2 3F 15 88 02 79 A7 95 B7 8F 46 8C CC 69 1F 91
83 84 DA CD 36 C7 B0 2A 68 11 94 BD

140.

04 18 6F 79 97 ED 22 3B 9B 53 F5 24 BB 6A 13 8F 46 67 EB 1A F2 3F 15 88 02 79 A7 95 B7 8F 46 8C CC 69 00
91 83 84 DA CD 36 C7 B0 2A 68 11 94 BD

141.

04 18 6F 79 97 ED 22 3B 9B 53 F5 24 BB 6A 13 8F 46 67 EB 1A F2 3F 15 88 02 79 A7 95 B7 8F 46 8C CC 69 00
6C 83 84 DA CD 36 C7 B0 2A 68 11 94 BD

142.

04 18 6F 79 97 ED 22 3B 9B 53 F5 24 BB 6A 13 8F 46 67 EB 1A F2 3F 15 88 02 79 A7 95 B7 8F 46 8C CC 69 00
6C 50 84 DA CD 36 C7 B0 2A 68 11 94 BD

143.

04 18 6F 79 97 ED 22 3B 9B 53 F5 24 BB 6A 13 8F 46 67 EB 1A F2 3F 15 88 02 79 A7 95 B7 8F 46 8C CC 69 00
6C 50 94 DA CD 36 C7 B0 2A 68 11 94 BD

144.

04 18 6F 79 97 ED 22 3B 9B 53 F5 24 BB 6A 13 8F 46 67 EB 1A F2 3F 15 88 02 79 A7 95 B7 8F 46 8C CC 69 00
6C 50 94 6D CD 36 C7 B0 2A 68 11 94 BD

145.

04 18 6F 79 97 ED 22 3B 9B 53 F5 24 BB 6A 13 8F 46 67 EB 1A F2 3F 15 88 02 79 A7 95 B7 8F 46 8C CC 69 00
6C 50 94 6D 23 36 C7 B0 2A 68 11 94 BD

146.

04 18 6F 79 97 ED 22 3B 9B 53 F5 24 BB 6A 13 8F 46 67 EB 1A F2 3F 15 88 02 79 A7 95 B7 8F 46 8C CC 69 00
6C 50 94 6D 23 FE C7 B0 2A 68 11 94 BD

147.

04 18 6F 79 97 ED 22 3B 9B 53 F5 24 BB 6A 13 8F 46 67 EB 1A F2 3F 15 88 02 79 A7 95 B7 8F 46 8C CC 69 00
6C 50 94 6D 23 FE B9 B0 2A 68 11 94 BD

148.

04 18 6F 79 97 ED 22 3B 9B 53 F5 24 BB 6A 13 8F 46 67 EB 1A F2 3F 15 88 02 79 A7 95 B7 8F 46 8C CC 69 00
6C 50 94 6D 23 FE B9 9E 2A 68 11 94 BD

149.

04 18 6F 79 97 ED 22 3B 9B 53 F5 24 BB 6A 13 8F 46 67 EB 1A F2 3F 15 88 02 79 A7 95 B7 8F 46 8C CC 69 00
6C 50 94 6D 23 FE B9 9E CC 68 11 94 BD

150.

04 18 6F 79 97 ED 22 3B 9B 53 F5 24 BB 6A 13 8F 46 67 EB 1A F2 3F 15 88 02 79 A7 95 B7 8F 46 8C CC 69 00
6C 50 94 6D 23 FE B9 9E CC DE 11 94 BD

151.

04 18 6F 79 97 ED 22 3B 9B 53 F5 24 BB 6A 13 8F 46 67 EB 1A F2 3F 15 88 02 79 A7 95 B7 8F 46 8C CC 69 00
6C 50 94 6D 23 FE B9 9E CC DE 17 94 BD

152.

04 18 6F 79 97 ED 22 3B 9B 53 F5 24 BB 6A 13 8F 46 67 EB 1A F2 3F 15 88 02 79 A7 95 B7 8F 46 8C CC 69 00
6C 50 94 6D 23 FE B9 9E CC DE 17 DE BD

153.

04 18 6F 79 97 ED 22 3B 9B 53 F5 24 BB 6A 13 8F 46 67 EB 1A F2 3F 15 88 02 79 A7 95 B7 8F 46 8C CC 69 00
6C 50 94 6D 23 FE B9 9E CC DE 17 DE 5D

154.

D7 18 6F 79 97 ED 22 3B 9B 53 F5 24 BB 6A 13 8F 46 67 EB 1A F2 3F 15 88 02 79 A7 95 B7 8F 46 8C CC 69 00
6C 50 94 6D 23 FE B9 9E CC DE 17 DE 5D

155.

D7 D0 6F 79 97 ED 22 3B 9B 53 F5 24 BB 6A 13 8F 46 67 EB 1A F2 3F 15 88 02 79 A7 95 B7 8F 46 8C CC 69 00
6C 50 94 6D 23 FE B9 9E CC DE 17 DE 5D

156.

D7 D0 F0 79 97 ED 22 3B 9B 53 F5 24 BB 6A 13 8F 46 67 EB 1A F2 3F 15 88 02 79 A7 95 B7 8F 46 8C CC 69 00
6C 50 94 6D 23 FE B9 9E CC DE 17 DE 5D

157.

D7 D0 F0 34 97 ED 22 3B 9B 53 F5 24 BB 6A 13 8F 46 67 EB 1A F2 3F 15 88 02 79 A7 95 B7 8F 46 8C CC 69 00
6C 50 94 6D 23 FE B9 9E CC DE 17 DE 5D

158.

177.

D7 D0 F0 34 39 02 34 EE CA 05 24 24 57 E6 78 77 7F 63 C5 BB AF BD 5E F2 02 79 A7 95 B7 8F 46 8C CC 69 00
6C 50 94 6D 23 FE B9 9E CC DE 17 DE 5D

178.

D7 D0 F0 34 39 02 34 EE CA 05 24 24 57 E6 78 77 7F 63 C5 BB AF BD 5E F2 E1 79 A7 95 B7 8F 46 8C CC 69 00
6C 50 94 6D 23 FE B9 9E CC DE 17 DE 5D

179.

D7 D0 F0 34 39 02 34 EE CA 05 24 24 57 E6 78 77 7F 63 C5 BB AF BD 5E F2 E1 37 A7 95 B7 8F 46 8C CC 69 00
6C 50 94 6D 23 FE B9 9E CC DE 17 DE 5D

180.

D7 D0 F0 34 39 02 34 EE CA 05 24 24 57 E6 78 77 7F 63 C5 BB AF BD 5E F2 E1 37 57 95 B7 8F 46 8C CC 69 00
6C 50 94 6D 23 FE B9 9E CC DE 17 DE 5D

181.

D7 D0 F0 34 39 02 34 EE CA 05 24 24 57 E6 78 77 7F 63 C5 BB AF BD 5E F2 E1 37 57 3A B7 8F 46 8C CC 69 00
6C 50 94 6D 23 FE B9 9E CC DE 17 DE 5D

182.

D7 D0 F0 34 39 02 34 EE CA 05 24 24 57 E6 78 77 7F 63 C5 BB AF BD 5E F2 E1 37 57 3A DC 8F 46 8C CC 69 00
6C 50 94 6D 23 FE B9 9E CC DE 17 DE 5D

183.

D7 D0 F0 34 39 02 34 EE CA 05 24 24 57 E6 78 77 7F 63 C5 BB AF BD 5E F2 E1 37 57 3A DC 3E 46 8C CC 69 00
6C 50 94 6D 23 FE B9 9E CC DE 17 DE 5D

184.

D7 D0 F0 34 39 02 34 EE CA 05 24 24 57 E6 78 77 7F 63 C5 BB AF BD 5E F2 E1 37 57 3A DC 3E 23 8C CC 69 00
6C 50 94 6D 23 FE B9 9E CC DE 17 DE 5D

185.

D7 D0 F0 34 39 02 34 EE CA 05 24 24 57 E6 78 77 7F 63 C5 BB AF BD 5E F2 E1 37 57 3A DC 3E 23 F8 CC 69 00
6C 50 94 6D 23 FE B9 9E CC DE 17 DE 5D

186.

D7 D0 F0 34 39 02 34 EE CA 05 24 24 57 E6 78 77 7F 63 C5 BB AF BD 5E F2 E1 37 57 3A DC 3E 23 F8 5F 69 00
6C 50 94 6D 23 FE B9 9E CC DE 17 DE 5D

187.

D7 D0 F0 34 39 02 34 EE CA 05 24 24 57 E6 78 77 7F 63 C5 BB AF BD 5E F2 E1 37 57 3A DC 3E 23 F8 5F 53 00
6C 50 94 6D 23 FE B9 9E CC DE 17 DE 5D

188.

D7 D0 F0 34 39 02 34 EE CA 05 24 24 57 E6 78 77 7F 63 C5 BB AF BD 5E F2 E1 37 57 3A DC 3E 23 F8 5F 53 93
6C 50 94 6D 23 FE B9 9E CC DE 17 DE 5D

189.

D7 D0 F0 34 39 02 34 EE CA 05 24 24 57 E6 78 77 7F 63 C5 BB AF BD 5E F2 E1 37 57 3A DC 3E 23 F8 5F 53 93
13 50 94 6D 23 FE B9 9E CC DE 17 DE 5D

190.

D7 D0 F0 34 39 02 34 EE CA 05 24 24 57 E6 78 77 7F 63 C5 BB AF BD 5E F2 E1 37 57 3A DC 3E 23 F8 5F 53 93
13 A6 94 6D 23 FE B9 9E CC DE 17 DE 5D

191.

D7 D0 F0 34 39 02 34 EE CA 05 24 24 57 E6 78 77 7F 63 C5 BB AF BD 5E F2 E1 37 57 3A DC 3E 23 F8 5F 53 93
13 A6 7E 6D 23 FE B9 9E CC DE 17 DE 5D

192.

D7 D0 F0 34 39 02 34 EE CA 05 24 24 57 E6 78 77 7F 63 C5 BB AF BD 5E F2 E1 37 57 3A DC 3E 23 F8 5F 53 93
13 A6 7E B9 23 FE B9 9E CC DE 17 DE 5D

193.

D7 D0 F0 34 39 02 34 EE CA 05 24 24 57 E6 78 77 7F 63 C5 BB AF BD 5E F2 E1 37 57 3A DC 3E 23 F8 5F 53 93
13 A6 7E B9 85 FE B9 9E CC DE 17 DE 5D

194.

D7 D0 F0 34 39 02 34 EE CA 05 24 24 57 E6 78 77 7F 63 C5 BB AF BD 5E F2 E1 37 57 3A DC 3E 23 F8 5F 53 93
13 A6 7E B9 85 71 B9 9E CC DE 17 DE 5D

195.

214.

24 32 9A 72 7C 3B C8 90 92 09 07 32 E8 E6 78 77 7F 63 C5 BB AF BD 5E F2 E1 37 57 3A DC 3E 23 F8 5F 53 93
13 A6 7E B9 85 71 37 0A 37 C5 50 51 16

215.

24 32 9A 72 7C 3B C8 90 92 09 07 32 E8 73 78 77 7F 63 C5 BB AF BD 5E F2 E1 37 57 3A DC 3E 23 F8 5F 53 93
13 A6 7E B9 85 71 37 0A 37 C5 50 51 16

216.

24 32 9A 72 7C 3B C8 90 92 09 07 32 E8 73 02 77 7F 63 C5 BB AF BD 5E F2 E1 37 57 3A DC 3E 23 F8 5F 53 93
13 A6 7E B9 85 71 37 0A 37 C5 50 51 16

217.

24 32 9A 72 7C 3B C8 90 92 09 07 32 E8 73 02 D7 7F 63 C5 BB AF BD 5E F2 E1 37 57 3A DC 3E 23 F8 5F 53 93
13 A6 7E B9 85 71 37 0A 37 C5 50 51 16

218.

24 32 9A 72 7C 3B C8 90 92 09 07 32 E8 73 02 D7 BF 63 C5 BB AF BD 5E F2 E1 37 57 3A DC 3E 23 F8 5F 53 93
13 A6 7E B9 85 71 37 0A 37 C5 50 51 16

219.

24 32 9A 72 7C 3B C8 90 92 09 07 32 E8 73 02 D7 BF 32 C5 BB AF BD 5E F2 E1 37 57 3A DC 3E 23 F8 5F 53 93
13 A6 7E B9 85 71 37 0A 37 C5 50 51 16

220.

24 32 9A 72 7C 3B C8 90 92 09 07 32 E8 73 02 D7 BF 32 5A BB AF BD 5E F2 E1 37 57 3A DC 3E 23 F8 5F 53 93
13 A6 7E B9 85 71 37 0A 37 C5 50 51 16

221.

24 32 9A 72 7C 3B C8 90 92 09 07 32 E8 73 02 D7 BF 32 5A 16 AF BD 5E F2 E1 37 57 3A DC 3E 23 F8 5F 53 93
13 A6 7E B9 85 71 37 0A 37 C5 50 51 16

222.

24 32 9A 72 7C 3B C8 90 92 09 07 32 E8 73 02 D7 BF 32 5A 16 7D BD 5E F2 E1 37 57 3A DC 3E 23 F8 5F 53 93
13 A6 7E B9 85 71 37 0A 37 C5 50 51 16

223.

24 32 9A 72 7C 3B C8 90 92 09 07 32 E8 73 02 D7 BF 32 5A 16 7D F3 5E F2 E1 37 57 3A DC 3E 23 F8 5F 53 93
13 A6 7E B9 85 71 37 0A 37 C5 50 51 16

224.

24 32 9A 72 7C 3B C8 90 92 09 07 32 E8 73 02 D7 BF 32 5A 16 7D F3 40 F2 E1 37 57 3A DC 3E 23 F8 5F 53 93
13 A6 7E B9 85 71 37 0A 37 C5 50 51 16

225.

24 32 9A 72 7C 3B C8 90 92 09 07 32 E8 73 02 D7 BF 32 5A 16 7D F3 40 3A E1 37 57 3A DC 3E 23 F8 5F 53 93
13 A6 7E B9 85 71 37 0A 37 C5 50 51 16

226.

24 32 9A 72 7C 3B C8 90 92 09 07 32 E8 73 02 D7 BF 32 5A 16 7D F3 40 3A 1C 37 57 3A DC 3E 23 F8 5F 53 93
13 A6 7E B9 85 71 37 0A 37 C5 50 51 16

227.

24 32 9A 72 7C 3B C8 90 92 09 07 32 E8 73 02 D7 BF 32 5A 16 7D F3 40 3A 1C 66 57 3A DC 3E 23 F8 5F 53 93
13 A6 7E B9 85 71 37 0A 37 C5 50 51 16

228.

24 32 9A 72 7C 3B C8 90 92 09 07 32 E8 73 02 D7 BF 32 5A 16 7D F3 40 3A 1C 66 69 3A DC 3E 23 F8 5F 53 93
13 A6 7E B9 85 71 37 0A 37 C5 50 51 16

229.

24 32 9A 72 7C 3B C8 90 92 09 07 32 E8 73 02 D7 BF 32 5A 16 7D F3 40 3A 1C 66 69 E4 DC 3E 23 F8 5F 53 93
13 A6 7E B9 85 71 37 0A 37 C5 50 51 16

230.

24 32 9A 72 7C 3B C8 90 92 09 07 32 E8 73 02 D7 BF 32 5A 16 7D F3 40 3A 1C 66 69 E4 C5 3E 23 F8 5F 53 93
13 A6 7E B9 85 71 37 0A 37 C5 50 51 16

231.

24 32 9A 72 7C 3B C8 90 92 09 07 32 E8 73 02 D7 BF 32 5A 16 7D F3 40 3A 1C 66 69 E4 C5 A6 23 F8 5F 53 93
13 A6 7E B9 85 71 37 0A 37 C5 50 51 16

232.

251.

08 B9 9A 72 7C 3B C8 90 92 09 07 32 E8 73 02 D7 BF 32 5A 16 7D F3 40 3A 1C 66 69 E4 C5 A6 50 49 62 54 D9
15 11 75 37 F6 CB 83 CD 94 3F 98 01 C3

252.

08 B9 F3 72 7C 3B C8 90 92 09 07 32 E8 73 02 D7 BF 32 5A 16 7D F3 40 3A 1C 66 69 E4 C5 A6 50 49 62 54 D9
15 11 75 37 F6 CB 83 CD 94 3F 98 01 C3

253.

08 B9 F3 5F 7C 3B C8 90 92 09 07 32 E8 73 02 D7 BF 32 5A 16 7D F3 40 3A 1C 66 69 E4 C5 A6 50 49 62 54 D9
15 11 75 37 F6 CB 83 CD 94 3F 98 01 C3

254.

08 B9 F3 5F FE 3B C8 90 92 09 07 32 E8 73 02 D7 BF 32 5A 16 7D F3 40 3A 1C 66 69 E4 C5 A6 50 49 62 54 D9
15 11 75 37 F6 CB 83 CD 94 3F 98 01 C3

255.

08 B9 F3 5F FE 7A C8 90 92 09 07 32 E8 73 02 D7 BF 32 5A 16 7D F3 40 3A 1C 66 69 E4 C5 A6 50 49 62 54 D9
15 11 75 37 F6 CB 83 CD 94 3F 98 01 C3

256.

08 B9 F3 5F FE 7A F2 90 92 09 07 32 E8 73 02 D7 BF 32 5A 16 7D F3 40 3A 1C 66 69 E4 C5 A6 50 49 62 54 D9
15 11 75 37 F6 CB 83 CD 94 3F 98 01 C3

257.

08 B9 F3 5F FE 7A F2 E5 92 09 07 32 E8 73 02 D7 BF 32 5A 16 7D F3 40 3A 1C 66 69 E4 C5 A6 50 49 62 54 D9
15 11 75 37 F6 CB 83 CD 94 3F 98 01 C3

258.

08 B9 F3 5F FE 7A F2 E5 EA 09 07 32 E8 73 02 D7 BF 32 5A 16 7D F3 40 3A 1C 66 69 E4 C5 A6 50 49 62 54 D9
15 11 75 37 F6 CB 83 CD 94 3F 98 01 C3

259.

08 B9 F3 5F FE 7A F2 E5 EA 61 07 32 E8 73 02 D7 BF 32 5A 16 7D F3 40 3A 1C 66 69 E4 C5 A6 50 49 62 54 D9
15 11 75 37 F6 CB 83 CD 94 3F 98 01 C3

260.

08 B9 F3 5F FE 7A F2 E5 EA 61 61 32 E8 73 02 D7 BF 32 5A 16 7D F3 40 3A 1C 66 69 E4 C5 A6 50 49 62 54 D9
15 11 75 37 F6 CB 83 CD 94 3F 98 01 C3

261.

08 B9 F3 5F FE 7A F2 E5 EA 61 61 49 E8 73 02 D7 BF 32 5A 16 7D F3 40 3A 1C 66 69 E4 C5 A6 50 49 62 54 D9
15 11 75 37 F6 CB 83 CD 94 3F 98 01 C3

262.

08 B9 F3 5F FE 7A F2 E5 EA 61 61 49 5B 73 02 D7 BF 32 5A 16 7D F3 40 3A 1C 66 69 E4 C5 A6 50 49 62 54 D9
15 11 75 37 F6 CB 83 CD 94 3F 98 01 C3

263.

08 B9 F3 5F FE 7A F2 E5 EA 61 61 49 5B 44 02 D7 BF 32 5A 16 7D F3 40 3A 1C 66 69 E4 C5 A6 50 49 62 54 D9
15 11 75 37 F6 CB 83 CD 94 3F 98 01 C3

264.

08 B9 F3 5F FE 7A F2 E5 EA 61 61 49 5B 44 7C D7 BF 32 5A 16 7D F3 40 3A 1C 66 69 E4 C5 A6 50 49 62 54 D9
15 11 75 37 F6 CB 83 CD 94 3F 98 01 C3

265.

08 B9 F3 5F FE 7A F2 E5 EA 61 61 49 5B 44 7C 28 BF 32 5A 16 7D F3 40 3A 1C 66 69 E4 C5 A6 50 49 62 54 D9
15 11 75 37 F6 CB 83 CD 94 3F 98 01 C3

Message digest:

08 B9 F3 5F FE 7A F2 E5 EA 61 61 49 5B 44 7C 28 BF 32 5A 16 7D F3 40 3A 1C 66 69 E4 C5 A6 50 49 62 54 D9
15 11 75 37 F6 CB 83 CD 94 3F 98 01 C3

10.4 Hash bit length 512, delay=2.

For this message digest calculation consist from:

9 steps for pre-hash computation – same like for 384 hashbitlen;
256 steps for final hash computation.

Stage 1-2 – same like 10.3.

Stage 3. Final hash computation – 256 steps

This is SR states for steps in final hash computation. SR length is 64.

10.

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

11.

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

12.

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

13.

2F A0 B3 58 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

14.

2F A0 B3 58 8C 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

15.

2F A0 B3 58 8C 53 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

16.

2F A0 B3 58 8C 53 81 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

17.

2F A0 B3 58 8C 53 81 DE 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

18.

2F A0 B3 58 8C 53 81 DE A0 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

19.

2F A0 B3 58 8C 53 81 DE A0 46 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

20.

2F A0 B3 58 8C 53 81 DE A0 46 6B 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

21.

2F A0 B3 58 8C 53 81 DE A0 46 6B 6D 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

22.

2F A0 B3 58 8C 53 81 DE A0 46 6B 6D C5 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

23.

2F A0 B3 58 8C 53 81 DE A0 46 6B 6D C5 9B 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

24.

2F A0 B3 58 8C 53 81 DE A0 46 6B 6D C5 9B 44 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

25.

2F A0 B3 58 8C 53 81 DE A0 46 6B 6D C5 9B 44 26 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

26.

Message digest:

84 A0 65 CA 25 FC 5D 9A 1E 53 BF 05 5B 62 9C 7F 88 18 E6 A2 D2 56 DD 5F 1F CB D5 8F 62 57 96 8A 24 64 33
A3 8F 87 4B 8E E8 94 8C A4 69 98 54 5A 9A 13 D0 B3 6E F2 29 F3 C7 A6 51 9F B8 52 4D 82

11. Appendix B. CAT and MCT tests (delay=2).

ShortMsgKAT_224.txt
Algorithm Name: MCSSHA-4
Principal Submitter: Mikhail Maslennikov

Len = 0
Msg = 00
MD = F54C8D343DD0E646FC6EBE20AD2D18E7B369A8F07ECD13377E79601F

Len = 1
Msg = 00
MD = E9653B9705C51F32D777CA436AF8D04DCAE3D352CF75CD7E9297491D

Len = 2
Msg = C0
MD = C8FC8A6BF6391024874EEC47397225F52686C2B2E5A45038B3851C09

Len = 3
Msg = C0
MD = A7AE2ECBE47EEBE774F6A671B403558797C0C59F1B78F82723C0580

Len = 4
Msg = 80
MD = 0AB24535875B579F8DC68DE85148AB5FDD00F9D715222D9DEE429DAE

Len = 5
Msg = 48
MD = 20A021AAA4DB120BC15372B0834EB81E4B1754234B4365FB67D1F8FB

Len = 6
Msg = 50
MD = FAC75EEC8A0534E1DAD657321476A5BF7E988E52B35BF1BE94C4BF4B

LongMsgKAT_224.txt
Algorithm Name: MCSSHA-4
Principal Submitter: Mikhail Maslennikov

Len = 2048
Msg =
724627916C50338643E6996F07877EAFD96BDF01DA7E991D4155B9BE1295EA7D21C9391F4C4A41C75F77E5D273
89253393725F1427F57914B273AB862B9E31DABCE506E558720520D33352D119F699E784F9E548FF91BC35CA147
042128709820D69A8287EA3257857615EB0321270E94B84F446942765CE882B191FAEE7E1C87E0F0BD4E0CD8A9
27703524B559B769CA4ECE1F6DBF313FDC67C572EC4185C1A88E86EC11B6454B371980020F19633B6B95BD280
E4FBCB0161E1A82470320CEC6ECFA25AC73D09F1536F286D3F9DACAFB2CD1D0CE72D64D197F5C7520B3CCB2FD
74EB72664BA93853EF41EABF52F015DD591500D018DD162815CC993595B195
MD = 227EBE01E161FE9A9280B9A4DC35C87366BFE3DE809805BA7B99043

Len = 2111
Msg =
919FE5E7F35F64A7487649E564771DBBF10AE204ECC2181312D1A79FB579297C94F0DB9EAAE9E009A4F02057AF2
C973C5DAFA7B60154371A5D2C8E992FB6429176F8424B1A866BC1D1BED00438E97FAB42040DCACDEF7CA9FC20
33059B8898BB40CCFB2634B051797BDF3B915C503EC81839AD01E0F4F2F871EFF2008D40011730BE7A47888E79
55A806876BE120CB0F3A139A3620154ECC6482A70F5629F6A9D3341BE6FBBF48E5AA0C53589A04F057DD44268A
FFCABF75ADFC549F73F454264D46A98CCA80E3000C7446853DD5B430C9344E87E3230555B09FB3E7E64B5AD398
9293AC0FEEC0E75F909696F028A5525D26DDEA5D2B2C813FB3613DFF38CE23209285CC77C60860
MD = 3B6CD67BD13A83C60F7A9E4608396C515CB302EDD09CEB7ED4C47A6D

Len = 2174
Msg =
BD687B6D6684949FBD52A8196DF5D5927B403DEE88A47E4E4B52071BDDA6A6284A9EA1EB84950BA17A60277B0
FEA83C930E5619D5A6D232901B9D3A696662C7FD5F1349B494BC166C67B717C06D03E9FB05DB9EE292D4792F4
59E0ACC08369E3D14684CFF388C940F30738FB71D97EFEB51C7DB553CB85B6FC18429815EC71420822151BB8F5
135DD698EFE3D3118963EE194F94682DFA62EC9D3BCB5F826DA790779704DF2AC5C8A9FA2B50A42A87ED2FBAD
F1E1C8E55689531786A9858DE9E88009E56873FD2D431FCFC99B85574342DC7E78406678BDE94B9A06974DFF15
4EAC3BC7977AC7C123EBCDAC0641A69B792058BA373EDD1BA45E3339C2ABC032993B25F4E3BFA3D5FF620C621
D94C40F8

MD = C03FA4248768E06FEBCAFD874E3525F893D4DCD1946BFCDBD8EE99ED

Len = 2237

Msg

D13409007A6B3242CBAD4CE01D9AED77EFEF0A7725B96A30097EA092FA1E49A136DE03F3F348464C9BEA033216
F380440C7EC81E284738DCC640D485ED32F5D7DD1CF936C1677CBB3CDD8E0E001783FD5A3F388AE6EF7085FF9
A22FA722C7FCCF4CDC239B200D5D11884B565D01C84E4D563C6623C241C5AE0812CE8F9201BBAD4E8198378A3
E232EF3E10C03022620A266D0A346A6A22F202333A94D2CEF495DBA102B133B8237449C3350BF80EE51B6EE8A9
72CCFC3ED5FD7790444DA253922EEF6C611180F91DF1B6E58E843D318D94A958A017590B14D383C0F385F9CF25
14E8AE1EA749795E10F991E3FB744C6030EF6B02989E8EFFB8E8BF31FC39B692C517C7C012ECBD0E0785BDEF48
01C4E036C98C6CD0C9328

MD = 23C1D9112A30D300671D1020D82501CE5535EC5E1184F3C0F55162AC

Len = 2300

Msg

68F891C11459B2E9B71774E2B8A2A5C3C9CC36072E3498498496F1C7901684F3E9DACF13A3F1BAE22140DEE525
3732E4D4196B534F675264B53D38659727797F0A18910CCB5B48FE2346C2E998B6537357AF8D15826FCB57BA80
4FE143E765F4680A0B28A9E3716A59ABC60EF253E357A4784FF1BE4680C82D797813CE50355D8FDB3C75936CC3
3E1717B99D9A8ADE9D0EA9172662B708EBCBC31C05064FE67B287C56D01C12411E9B890AD16238B36E192B15C
D86D26F4EFDE5B523D71656F5CEA6CA73BDC04FEB973D303BBAF4C0264761092E23220CEB8359FC91C1D918FB
3F32DBBA92DEAC1C71DA8BC4BE806803F6E7970FA64721C645EED4C2BED7EEFA2B720931FDBD6C67B83756B1C
E51C51F839C250AD900B9D49FE5188FC4A2B5D0

MD = 27C275E70ABA22196389B6E86F57B79C019BDF8BF29087414FD8FA9

Len = 2363

Msg

7D9222C58DC49F14BFD7198A9A1C338D17201C007822A91DCD262860364CA1DA8C0056033EB58E406E36D5A4F
6F7E9D98BE57126C9FE7676B58FDF0F9899432FF78DE2AB65C9000071EBA6967123F97BA3DC1F3825D3C8C5148
EAD7AEF0334F40CB0F6B982CB7C99CA39E1B4B2E3A3541683D1EC5560466F52175518390D38C7461C116DB2D5
6EF913784D2E8B20959BBD6F8F3282C597D94A1EDBFA8F25089E9D2E8DC465EAD90FA23E4388BD6BAFE226327
49B7AAEA53D5CBCF9678227ADC3F4109F1849AC2539B6F2B25B4D8EDAB41E8BFCFC337728DC48A8EA5119115F
C1B133300D68231C96A9D518F6DC3CA51581309C53F49510FE18F608A215069D41F2CFC84E53A9347FD723DFF9
D3F5006F7C0B18441A29BDEF7725920260B1613C6532A0A994B488E0

MD = 723823C189A05291A4ADE5381B1729AF23BB7B77B3B6248A2B74B140

ExtremelyLongMsgKAT_224.txt

Algorithm Name: MCSSHA-4

Principal Submitter: Mikhail Maslennikov

Repeat = 16777216

Text = abcdefghbcdefghicdefghijdefghijkefghijklfghijklmghijklmnhijklmno

MD = 803AE511DE94D9514CA5C9C6A90DC2B33A8E0656130435895608CA82

MonteCarlo_224.txt

Algorithm Name: MCSSHA-4

Principal Submitter: Mikhail Maslennikov

Seed

6CD4C0C5CB2CA2A0F1D1AECEBAC03B52E64EA03D1A1654372936545B92BBC5484A59DB74BB60F9C40CEB1A5A
A35A6FAFE80349E14C253A4E8B1D77612DDD81ACE926AE8B0AF6E53176DBFFCC2A6B88C6BD765F939D3D178A9
BDE9EF3AA131C61E31C1E42CDFAF4B4DCDE579A37E150EFBEF5555B4C1CB40439D835A724E2FAE7

j = 0

MD = B1F051D8A776517FC0E138CF96AFA2D3D875C49214057515929701C8

j = 1

MD = 603F4F03CFD372C2DC75D69593A40B1665F97CA5BA1E6410BCD83786

j = 2

MD = B10317B896E97E9AC1E2FF4FC152F80785769A6B3BE75403544A69F7

j = 3

MD = B0CFEAD74DF1B09784CFBD07940025ABC823842A07113D866DA0D33

j = 4

MD = 467AF8AC2074DF2D605B2BFF1B5CDDC9FB4DAD6F31FD07A6938C84C6

j = 5

MD = 11B4B731C1C1A9D4A00DED99C37EA4A05CE904A25448E0EF2B04CFBC

ShortMsgKAT_256.txt

Algorithm Name: MCSSHA-4

Principal Submitter: Mikhail Maslennikov

Len = 0
Msg = 00
MD = 3CAF23728BACBBE20EDB09A9185745BAF42EAA3AFC85A31EF93D49853EC9404A

Len = 1
Msg = 00
MD = EA61D6E3240592FDCC4C5147C5835256977974D5C6114761BD5AB067DF50AB20

Len = 2
Msg = C0
MD = D112E6E43DCCF69A83B302950569426636F9717C2943738A7C09F3A6B38CD5B1

Len = 3
Msg = C0
MD = 7D048AA2290F55D03D90415E58AB2BE0232F8090D2B0D603242BAA2684A973C3

Len = 4
Msg = 80
MD = 924B12E5E7FF88ABFFF6F5354E00CA00CC8C5CE787B44EB2051C51BCEA9B5CDF

Len = 5
Msg = 48
MD = F4F94D77B0A10A8E07D320E7A5A892710DB534894720323F60D6BF59CFA86011

LongMsgKAT_256.txt
Algorithm Name: MCSSHA-4
Principal Submitter: Mikhail Maslennikov

Len = 2048
Msg =
724627916C50338643E6996F07877EAFD96BDF01DA7E991D4155B9BE1295EA7D21C9391F4C4A41C75F77E5D273
89253393725F1427F57914B273AB862B9E31DABCE506E558720520D33352D119F699E784F9E548FF91BC35CA147
042128709820D69A8287EA3257857615EB0321270E94B84F446942765CE882B191FAEE7E1C87E0F0BD4E0CD8A9
27703524B559B769CA4ECE1F6DBF313FDCF67C572EC4185C1A88E86EC11B6454B371980020F19633B6B95BD280
E4FBCB0161E1A82470320CEC6ECFA25AC73D09F1536F286D3F9DACAFB2CD1D0CE72D64D197F5C7520B3CCB2FD
74EB72664BA93853EF41EABF52F015DD591500D018DD162815CC993595B195
MD = BAAF19AEE3F2EF645C69CDFAAABDCD312F7AEA7CAFEE9F8F275517C38A55BC0FD

Len = 2111
Msg =
919FE5E7F35F64A7487649E564771DBBF10AE204ECC2181312D1A79FB579297C94F0DB9EAAE9E009A4F02057AF2
C973C5DAFA7B60154371A5D2C8E992FB6429176F8424B1A866BC1D1BED00438E97FAB42040DCACDEF7CA9FC20
33059B8898BB40CCFB2634B051797BDF3B915C503EC81839AD01E0F4F2F871EFF2008D40011730BE7A47888E79
55A806876BE120CB0F3A139A3620154ECC6482A70F5629F6A9D3341BE6FBBF48E5AA0C53589A04F057DD44268A
FFCABF75ADFC549F73F454264D46A98CCA80E3000C7446853DD5B430C9344E87E3230555B09FB3E7E64B5AD398
9293AC0FEEC0E75F909696F028A5525D26DDEA5D2B2C813FB3613DFF38CE23209285CC77C60860
MD = 7EDE0C3061FBBEBBD2EA6213DD4FD792AF09950CC19E330AAA6B075E28A65ED5

Len = 2174
Msg =
BD687B6D6684949FBD52A8196DF5D5927B403DEE88A47E4E4B52071BDDA6A6284A9EA1EB84950BA17A60277B0
FEA83C930E5619D5A6D232901B9D3A696662C7FD5F1349B494BC166C67B717C06D03E9FB05DB9EE292D4792F4
59E0ACC08369E3D14684CFF388C940F30738FB71D97EFEB51C7DB553CB85B6FC18429815EC71420822151BB8F5
135DD698EFE3D3118963EE194F94682DFA62EC9D3BCB5F826DA790779704DF2AC5C8A9FA2B50A42A87ED2FBAD
F1E1C8E55689531786A9858DE9E88009E56873FD2D431FCFC99B85574342DC7E78406678BDE94B9A06974DFF15
4EAC3BC7977AC7C123EBCDAC0641A69B792058BA373EDD1BA45E3339C2ABC032993B25F4E3BFA3D5FF620C621
D94C40F8
MD = 5641A35F2E2E99D869D538B3AB4A2D9F01276C6EECE388BEC74458580038AED2

Len = 2237
Msg =
D13409007A6B324CBAD4CE01D9AED77EFEF0A7725B96A30097EA092FA1E49A136DE03F3F348464C9BEA033216
F380440C7EC81E284738DCC640D485ED32F5D7DD1CF936C1677CBB3CDD8E0E001783FD5A3F388AE6EF7085FF9
A22FA722C7FCCF4CDC239B200D5D11884B565D01C84E4D563C6623C241C5AE0812CE8F9201BBAD48198378A3
E232EF3E10C03022620A266D0A346A6A22F202333A94D2CEF495DBA102B133B8237449C3350BF80EE51B6EE8A9
72CCFC3ED5FD7790444DA253922EEF6C611180F91DF1B6E58E843D318D94A958A017590B14D383C0F385F9CF25
14E8AE1EA749795E10F991E3FB744C6030EF6B02989E8EFFBF8E8BF31FC39B692C517C7C012ECBD0E0785BDEF48
01C4E036C98C6CD0C9328
MD = F84AFE1256E218F9DF41BFA12FCF98F938068E2EE867AAAB7B02EA1B216652C7

Len = 2300

Msg =
68F891C11459B2E9B71774E2B8A2A5C3C9CC36072E3498498496F1C7901684F3E9DACF13A3F1BAE22140DEE525
3732E4D4196B534F675264B53D38659727797F0A18910CCB5B48FE2346C2E998B6537357AF8D15826FCB57BA80
4FE143E765F4680A0B28A9E3716A59ABC60EF253E357A4784FF1BE4680C82D797813CE50355D8FDB3C75936CC3
3E1717B99D9A8ADE9D0EA9172662B708EBCBC31C05064FE67B287C56D01C12411E9B890AD16238B36E192B15C
D86D26F4EFDE5B523D71656F5CEA6CA73BDC04FEB973D303BBAF4C0264761092E23220CEB8359FC91C1D918FB
3F32DBBA92DEAC1C71DA8BC4BE806803F6E7970FA64721C645EED4C2BED7EEFA2B720931FDBD6C67B83756B1C
E51C51F839C250AD900B9D49FE5188FC4A2B5D0
MD = EA258FBB85041F9A5313905459197D512710A4662CAB64756724A3E7EA55AC7D
Len = 2363

Msg =
7D9222C58DC49F14BFD7198A9A1C338D17201C007822A91DCD262860364CA1DA8C0056033EB58E406E36D5A4F
6F7E9D98BE57126C9FE7676B58FDF0F9899432FF78DE2AB65C9000071EBA6967123F97BA3DC1F3825D3C8C5148
EAD7AEF0334F40CB0F6B982CB7C99CA39E1B4B2E3A3541683D1EC5560466F52175518390D38C7461C116DB2D5
6EF913784D2E8B20959BBD6F8F3282C597D94A1EDBFA8F25089E9D2E8DC465EAD90FA23E4388BD6BAFE226327
49B7AAEA53D5CBCF9678227ADC3F4109F1849AC2539B6F2B25B4D8EDAB41E8BFCFC337728DC48A8EA5119115F
C1B133300D68231C96A9D518F6DC3CA51581309C53F49510FE18F608A215069D41F2CFC84E53A9347FD723DFF9
D3F5006F7C0B18441A29BDEF7725920260B1613C6532A0A994B488E0
MD = FD7310A0A22FC5A4114622B52B157B401CF2D2AC8EA38C87A50793184D80E35A

ExtremelyLongMsgKAT_256.txt
Algorithm Name: MCSSHA-4
Principal Submitter: Mikhail Maslennikov

Repeat = 16777216
Text = abcdefghbcdefghicdefghijdefghijkefghijklfghijklmghijklmnhijklmno
MD = B69ED91298B5CD9BA91D66040777E06B4736BB8ADB8E09111BED0C6CD3F0196F

MonteCarlo_256.txt
Algorithm Name: MCSSHA-4
Principal Submitter: Mikhail Maslennikov

Seed =
6CD4C0C5CB2CA2A0F1D1AECEBAC03B52E64EA03D1A1654372936545B92BBC5484A59DB74BB60F9C40CEB1A5A
A35A6FAFE80349E14C253A4E8B1D77612DDD81ACE926AE8B0AF6E53176DBFFCC2A6B88C6BD765F939D3D178A9
BDE9EF3AA131C61E31C1E42CDFAF4B4DCDE579A37E150EFBEF5555B4C1CB40439D835A724E2FAE7

j = 0
MD = 45104D68F25D0831553C1A55149C1B2ED9EC2753BD4FEB546BFE3F169411F4DA

j = 1
MD = D990361BB1F1E8FC92640FE104C446BBB7D6FC36CD867B84DA6D1E72BE84BD0E

j = 2
MD = 2A58D21F19B0CF4A3592D87EA0932EEFBA0704F5E2AF13EC78694BA959524F67

j = 3
MD = FB4CFC71DDB93ED9EFDD11234664B23A0395A4B34ABF97676294976B6A285944

j = 4
MD = 288A73BD54A0C6108712B87F7CA2E4CD1FE6AE9DC98F92CE77BFEC76B801A5BC

j = 5
MD = 257D61408678F6D8EF6383DA1710AC4A08A1EF79ACE244E5F2E984BD9FF82D7A

ShortMsgKAT_384.txt
Algorithm Name: MCSSHA-4
Principal Submitter: Mikhail Maslennikov

Len = 0
Msg = 00
MD =
421F20E50910C18314CA41F921C367D30D15186FD05D62CC1DD144B6AD8DD20803D34D15D703B19B05503F32
4FC906F4

Len = 1
Msg = 00
MD
44C09676FD7A932651BD9FC3195E71DAFE8C3241FEB47A7ED72D3C1CBD601208A7D72E5774DA846876A96853042111AB

Len = 2
Msg = C0
MD
98BFEF8A0BA71CA1301FE3972DF52CB8D78FC48C554A0913D84BB40422C5986B0B032A590371156B9B9ACBDB2CEB3AC7

Len = 3
Msg = C0
MD
A6DE594C278F2CC6B98711365B2387359AFE0BF19A1C87FE4DCD2944563D8B4DE6B77E49E7FF01A7285D4FCA186F632A

Len = 4
Msg = 80
MD
8949277E62AEA803FE66A0B56A23A45C7662145418F69110414F1373F82049742F8EB172EA47F8E8FF3C65F562AEACEF

Len = 5
Msg = 48
MD
D1C41BE4C71F5B79E22F46B6006B81505F0DD8CFAF77490F5750966D26831E3BF4427BA6B4D4482E1BB62B2DD EDDA70E

LongMsgKAT_384.txt
Algorithm Name: MCSSHA-4
Principal Submitter: Mikhail Maslennikov

Len = 2048
Msg
724627916C50338643E6996F07877EAFD96BDF01DA7E991D4155B9BE1295EA7D21C9391F4C4A41C75F77E5D27389253393725F1427F57914B273AB862B9E31DABCE506E558720520D33352D119F699E784F9E548FF91BC35CA147042128709820D69A8287EA3257857615EB0321270E94B84F446942765CE882B191FAEE7E1C87E0F0BD4E0CD8A927703524B559B769CA4ECE1F6DBF313FDC67C572EC4185C1A88E86EC11B6454B371980020F19633B6B95BD280E4FBCB0161E1A82470320CEC6ECFA25AC73D09F1536F286D3F9DACAFB2CD1D0CE72D64D197F5C7520B3CCB2FD74EB72664BA93853EF41EABF52F015DD591500D018DD162815CC993595B195
MD
18314AE887A1F44BBC0D12246E2325A532B9F10636200F2F52B021C05EBD6BB9498D431035C1642FA8942A7EE236F27F

Len = 2111
Msg
919FE5E7F35F64A7487649E564771DBBF10AE204ECC2181312D1A79FB579297C94F0DB9EAAE9E009A4F02057AF2C973C5DAFA7B60154371A5D2C8E992FB6429176F8424B1A866BC1D1BED00438E97FAB42040DCACDEF7CA9FC2033059B8898BB40CCFB2634B051797BDF3B915C503EC81839AD01E0F4F2F871EFF2008D40011730BE7A47888E7955A806876BE120CB0F3A139A3620154ECC6482A70F5629F6A9D3341BE6FBBF48E5AA0C53589A04F057DD44268AFFCABF75ADFC549F73F454264D46A98CCA80E3000C7446853DD5B430C9344E87E3230555B09FB3E7E64B5AD3989293AC0FEEC0E75F909696F028A5525D26DDEA5D2B2C813FB3613DFF38CE23209285CC77C60860
MD
4197EF296C6E85AA57F39DA4D72D61B55C8867717B6C0AD98DDC0C67D9AF579105A9C8F68DCC5692C9024C6F3826636E

Len = 2174
Msg
BD687B6D6684949FBD52A8196DF5D5927B403DEE88A47E4E4B52071BDDA6A6284A9EA1EB84950BA17A60277B0FEA83C930E5619D5A6D232901B9D3A696662C7FD5F1349B494BC166C67B717C06D03E9FB05DB9EE292D4792F459E0ACC08369E3D14684CFF388C940F30738FB71D97EFEB51C7DB553CB85B6FC18429815EC71420822151BB8F5135DD698EFE3D3118963EE194F94682DFA62EC9D3BCB5F826DA790779704DF2AC5C8A9FA2B50A42A87ED2FBADF1E1C8E55689531786A9858DE9E88009E56873FD2D431FCFC99B85574342DC7E78406678BDE94B9A06974DFF154EAC3BC7977AC7C123EBCDAC0641A69B792058BA373EDD1BA45E3339C2ABC032993B25F4E3BFA3D5FF620C621D94C40F8
MD
1C205F4028B73EE91B71FB8BD1C181CF65BA328789199EEEC75B96B04E3928F8CD458AF4925094D71C26BC1272CF1D52

Len = 2237
Msg
D13409007A6B3242CBAD4CE01D9AED77EFEF0A7725B96A30097EA092FA1E49A136DE03F3F348464C9BEA033216

F380440C7EC81E284738DCC640D485ED32F5D7DD1CF936C1677CBB3CDD8E0E001783FD5A3F388AE6EF7085FF9
A22FA722C7FCCF4CDC239B200D5D11884B565D01C84E4D563C6623C241C5AE0812CE8F9201BBADE48198378A3
E232EF3E10C03022620A266D0A346A6A22F202333A94D2CEF495DBA102B133B8237449C3350BF80EE51B6EE8A9
72CCFC3ED5FD7790444DA253922EEF6C611180F91DF1B6E58E843D318D94A958A017590B14D383C0F385F9CF25
14E8AE1EA749795E10F991E3FB744C6030EF6B02989E8EFFBF8E8BF31FC39B692C517C7C012ECBD0E0785BDEF48
01C4E036C98C6CD0C9328

MD =
6CF3E5EA75EF471CA2B21894F86E3EF9AE361D07150DD8F7DD031D990E5FE36EEC8247F1DF31E6FB7FB80B6455
FFD7F6

Len = 2300

Msg =
68F891C11459B2E9B71774E2B8A2A5C3C9CC36072E3498498496F1C7901684F3E9DACF13A3F1BAE22140DEE525
3732E4D4196B534F675264B53D38659727797F0A18910CCB5B48FE2346C2E998B6537357AF8D15826FCB57BA80
4FE143E765F4680A0B28A9E3716A59ABC60EF253E357A4784FF1BE4680C82D797813CE50355D8FDB3C75936CC3
3E1717B99D9A8ADE9D0EA9172662B708EBCBC31C05064FE67B287C56D01C12411E9B890AD16238B36E192B15C
D86D26F4EFDE5B523D71656F5CEA6CA73BDC04FEB973D303BBAF4C0264761092E23220CEB8359FC91C1D918FB
3F32DBBA92DEAC1C71DA8BC4BE806803F6E7970FA64721C645EED4C2BED7EEFA2B720931FDBD6C67B83756B1C
E51C51F839C250AD900B9D49FE5188FC4A2B5D0

MD =
721BBDCE29C80F1A32F54A3FCA5561E9136A8392316675497A431E0B6209B92CB6B69A6EB3243746535A9B911E
B437D7

Len = 2363

Msg =
7D9222C58DC49F14BFD7198A9A1C338D17201C007822A91DCD262860364CA1DA8C0056033EB58E406E36D5A4F
6F7E9D98BE57126C9FE7676B58FDF0F9899432FF78DE2AB65C9000071EBA6967123F97BA3DC1F3825D3C8C5148
EAD7AEF0334F40CB0F6B982CB7C99CA39E1B4B2E3A3541683D1EC5560466F52175518390D38C7461C116DB2D5
6EF913784D2E8B20959BBDD6F8F3282C597D94A1EDBFA8F25089E9D2E8DC465EAD90FA23E4388BD6BAFE226327
49B7AAEA53D5CBCF9678227ADC3F4109F1849AC2539B6F2B25B4D8EDAB41E8BFCFC337728DC48A8EA5119115F
C1B133300D68231C96A9D518F6DC3CA51581309C53F49510FE18F608A215069D41F2CFC84E53A9347FD723DFF9
D3F5006F7C0B18441A29BDEF7725920260B1613C6532A0A994B488E0

MD =
79637151025E23D57757C19861F43BB89A611C64AFA25B8A3BA9B3761C263EF84A43389D783F7A09B748570CB6
7B0DFD

ExtremelyLongMsgKAT_384.txt
Algorithm Name: MCSSHA-4
Principal Submitter: Mikhail Maslennikov

Repeat = 16777216

Text = abcdefghbcdefghicdefghijdefghijklfghijklmghijklmnhijklmno

MD =
59818D9C7918A4BB925255E4F3F0374A40CE3C91B6189092C531F15A4EA59BE51A2D603A11C8E12ECD8088ABBE
DAABBF

MonteCarlo_384.txt
Algorithm Name: MCSSHA-4
Principal Submitter: Mikhail Maslennikov

Seed =
6CD4C0C5CB2CA2A0F1D1AECEBAC03B52E64EA03D1A1654372936545B92BBC5484A59DB74BB60F9C40CEB1A5A
A35A6FAFE80349E14C253A4E8B1D77612DDD81ACE926AE8B0AF6E53176DBFFCC2A6B88C6BD765F939D3D178A9
BDE9EF3AA131C61E31C1E42CDFAF4B4DCDE579A37E150EFBEF5555B4C1CB40439D835A724E2FAE7

j = 0
MD =
B24569C5AE07B57D888D02742DF893249531B9B4CCC13BD3370745ACA7D83A97E9EE1EDDD91B6A03EC2021D7
A6EAEEC4

j = 1
MD =
39866894CCD63BAF397CD0788631376727BBCC7531B5A6DD5644813E78AB574E0BC74EF6A934C51541C0EFFB1
392BDB2

j = 2
MD =
2AA0661EC5FBC92E9FA943E05A06FA5B29446876564C2E03B8D4EDC7EC360C703E0A32D7D375394E4B9B1EBAB
647DD30

j = 3

MD =
224A80B0EB29E8A7ADC1D1EA6D6F9F6FB8A6C386C3192CC07CCF27EC43E52A727E5B65762CE7E0C36E422EC0E
281CC88

j = 4
MD =
65D125722C354F24ADB782F00C4A71D5FB7C9E4B92C16307E776B22F38F202A66B610E5F793F0935FCCC37C5CE
7355B7

j = 5
MD =
663E4429E41B2F20CB320646B50EAB6BA2EB20B2001C5BAB088351A1579B972ABB3BA48782428E5FD345E97899
A24F9C

ShortMsgKAT_512.txt
Algorithm Name: MCSSHA-4
Principal Submitter: Mikhail Maslennikov

Len = 0
Msg = 00
MD =
1D5F50E66DA4D2188546FB3001272900B9E40145FD8ADD88B88E7AA36AFEB2362E84458B0D3E96CEB5B9846CE
E0AFB289DCD67CB194D27273E51A3E51A285D1D

Len = 1
Msg = 00
MD =
8D44E3432874636B8E187A99D6C132B582B7058582B03FC4A97F4A97A16BCD7204694AE26855AB35BC50214D5
BA0988C8A5174C87299F7C15145FCCB2327088C

Len = 2
Msg = C0
MD =
CC286D000A10B6235323A309F8710C54B4FAA7BB175227562628B31C587074EA556042330A7207499E30BFA95C
DBA6C35956FB27D3DF6E1C4232A1D020139BD6

Len = 3
Msg = C0
MD =
E987810507D6ED79035060866CCFA00C58B0D673ECBBBA44BCECC46FAF8A9C3116FC4EC2B741500DB28119DD0
761F7CD2E1C4D2EAF6B822E1CD31ADA1FCD72E7

Len = 4
Msg = 80
MD =
80AAF2BA2D0021FB94A63FD6E1EDF87A2DD74CD194070BDE2B3B2609ABBB4D85A1FB1A2F9794B37DD4FFFA1EB
FA14DB3E9FD91DF3E9C8C9BE828694FD9E12577

LongMsgKAT_512.txt
Algorithm Name: MCSSHA-4
Principal Submitter: Mikhail Maslennikov

Len = 2048
Msg =
724627916C50338643E6996F07877EAFD96BDF01DA7E991D4155B9BE1295EA7D21C9391F4C4A41C75F77E5D273
89253393725F1427F57914B273AB862B9E31DABCE506E558720520D33352D119F699E784F9E548FF91BC35CA147
042128709820D69A8287EA3257857615EB0321270E94B84F446942765CE882B191FAEE7E1C87E0F0BD4E0CD8A9
27703524B559B769CA4ECE1F6DBF313FDCF67C572EC4185C1A88E86EC11B6454B371980020F19633B6B95BD280
E4FBCB0161E1A82470320CEC6E6CFA25AC73D09F1536F286D3F9DACAFA2CD1D0CE72D64D197F5C7520B3CCB2FD
74EB72664BA93853EF41EABF52F015DD591500D018DD162815CC993595B195
MD =
667C7A236734E59CCDBFDF564657E4561E4AE571351543704AE2574CC20548599B8F822BFD69A920126E62FD33
2730F14B8769F8329FA09DDD96016B83D95CD7

Len = 2111
Msg =
919FE5E7F35F64A7487649E564771DBBF10AE204ECC2181312D1A79FB579297C94F0DB9EAAE9E009A4F02057AF2
C973C5DAFA7B60154371A5D2C8E992FB6429176F8424B1A866BC1D1BED00438E97FAB42040DCACDEF7CA9FC20
33059B8898BB40CCFB2634B051797BDF3B915C503EC81839AD01E0F4F2F871EFF2008D40011730BE7A47888E79

55A806876BE120CB0F3A139A3620154ECC6482A70F5629F6A9D3341BE6FBBF48E5AA0C53589A04F057DD44268A
FFCABF75ADFC549F73F454264D46A98CCA80E3000C7446853DD5B430C9344E87E3230555B09FB3E7E64B5AD398
9293AC0FECE0E75F909696F028A5525D26DDEA5D2B2C813FB3613DFF38CE23209285CC77C60860

MD

0D4AB5B7A20CFD6F85EBEF91AF4CA137E2D06077DCC118DDCACE2FFBA21CA0A8F4F8921012C08B446B22461D4
CB72DD44B5701EF4DAD3107064803EFF157E742

Len = 2174

Msg

BD687B6D6684949FBD52A8196DF5D5927B403DEE88A47E4E4B52071BDDA6A6284A9EA1EB84950BA17A60277B0
FEA83C930E5619D5A6D232901B9D3A696662C7FD5F1349B494BC166C67B717C06D03E9FB05DB9EE292D4792F4
59E0ACC08369E3D14684CFF388C940F30738FB71D97EFEB51C7DB553CB85B6FC18429815EC71420822151BB8F5
135DD698EFE3D3118963EE194F94682DFA62EC9D3BCB5F826DA790779704DF2AC5C8A9FA2B50A42A87ED2FBAD
F1E1C8E55689531786A9858DE9E88009E56873FD2D431FCFC99B85574342DC7E78406678BDE94B9A06974DFF15
4EAC3BC7977AC7C123EBCDAC0641A69B792058BA373EDD1BA45E3339C2ABC032993B25F4E3BFA3D5FF620C621
D94C40F8

MD

983F4DDEBAB743F5EE02CCC19D0AE24A7BD22440D6DDCF81B91F99D2A061BD4A811827E13C4E9B2794FFD578C
A4BF5B956B0C567C8481D9170D6273505E9245C

Len = 2237

Msg

D13409007A6B3242CBAD4CE01D9AED77EFEF0A7725B96A30097EA092FA1E49A136DE03F3F348464C9BEA033216
F380440C7EC81E284738DCC640D485ED32F5D7DD1CF936C1677CBB3CDD8E0E001783FD5A3F388AE6F7085FF9
A22FA722C7FCCF4CDC239B200D5D11884B565D01C84E4D563C6623C241C5AE0812CE8F9201BBADE48198378A3
E232EF3E10C03022620A266D0A346A6A22F202333A94D2CEF495D8A102B133B8237449C3350BF80EE51B6EE8A9
72CCFC3ED5FD7790444DA253922EEF6C611180F91DF1B6E58E843D318D94A958A017590B14D383C0F385F9CF25
14E8AE1EA749795E10F991E3FB744C6030EF6B02989E8EFFBF8E8BF31FC39B692C517C7C012ECBD0E0785BDEF48
01C4E036C98C6CD0C9328

MD

CF7B2C39A2BB2F7CE22F9463A361E991AA16437B40AA70E98005F2F1F71E2D1DC75217F033A558D8F02A4D6A2D
40FDD66E74CE8696012A3A22BD8773219EE02B

Len = 2300

Msg

68F891C11459B2E9B71774E2B8A2A5C3C9CC36072E3498498496F1C7901684F3E9DACF13A3F1BAE22140DEE525
3732E4D4196B534F675264B53D38659727797F0A18910CCB5B48FE2346C2E998B6537357AF8D15826FCB57BA80
4FE143E765F4680A0B28A9E3716A59ABC60EF253E357A4784FF1BE4680C82D797813CE50355D8FDB3C75936CC3
3E1717B99D9A8ADE9D0EA9172662B708EBCBC31C05064FE67B287C56D01C12411E9B890AD16238B36E192B15C
D86D26F4EFDE5B523D71656F5CEA6CA73BDC04FEB973D303BBAF4C0264761092E23220CEB8359FC91C1D918FB
3F32DBBA92DEAC1C71DA8BC4BE806803F6E7970FA64721C645EED4C2BED7EEFA2B720931FDBD6C67B83756B1C
E51C51F839C250AD900B9D49FE5188FC4A2B5D0

MD

8FA267BC31B6CBF885E405298AF56F708E07F1F39C22854D70CC849A32D3C306DF06BADF75F967F45E9BE88058
0ED6322D7F01DD0A295DC382F2A260C910B25E

Len = 2363

Msg

7D9222C58DC49F14BFD7198A9A1C338D17201C007822A91DCD262860364CA1DA8C0056033EB58E406E36D5A4F
6F7E9D98BE57126C9FE7676B58FDF0F9899432FF78DE2AB65C9000071EBA6967123F97BA3DC1F3825D3C8C5148
EAD7AEF0334F40CB0F6B982CB7C99CA39E1B4B2E3A3541683D1EC5560466F52175518390D38C7461C116DB2D5
6EF913784D2E8B20959BBD6F8F3282C597D94A1EDBFA8F25089E9D2E8DC465EAD90FA23E4388BD6BAFE226327
49B7AAEA53D5CBCF9678227ADC3F4109F1849AC2539B6F2B25B4D8EDAB41E8BFCFC337728DC48A8EA5119115F
C1B133300D68231C96A9D518F6DC3CA51581309C53F49510FE18F608A215069D41F2CFC84E53A9347FD723DFF9
D3F5006F7C0B18441A29BDEF7725920260B1613C6532A0A994B488E0

MD

04BCF87A7616BC08C8FB2401316C9F82D8642E2FCD44A630168E7B33CD0BF9765055B3091F5FF509B22FD6D00F
4CAFDD276EF737FCE2AB16F7CB67990457DEDD4

ExtremelyLongMsgKAT_512.txt
Algorithm Name: MCSSHA-4
Principal Submitter: Mikhail Maslennikov

Repeat = 16777216

Text = abcdefghbcdefghicdefghijdefghijklfghijklmghijklmnhijklmno

MD

EC288CE604E9EF4914454EE5260C6CB6C9AB410E268D77DA803D87F0D82E21C3CBB467CD4DFE0BD2AC70145A5
7F55DE5D18ACEA3C067272154B1C9AF7093D818

MonteCarlo_512.txt
Algorithm Name: MCSSHA-4
Principal Submitter: Mikhail Maslennikov

Seed =
6CD4C0C5CB2CA2A0F1D1AECEBAC03B52E64EA03D1A1654372936545B92BBC5484A59DB74BB60F9C40CEB1A5A
A35A6FAFE80349E14C253A4E8B1D77612DDD81ACE926AE8B0AF6E53176DBFFCC2A6B88C6BD765F939D3D178A9
BDE9EF3AA131C61E31C1E42CDFAF4B4DCDE579A37E150EFBEF5555B4C1CB40439D835A724E2FAE7

j = 0 =
MD =
75A7C5E9E1D8C3D6716DE651E322C8573EE8A9313F4DB6EC32BFE299A6A93E4C16653F13EC773B5FDE391626D
BF761001467FC88F6F409DA7F032E4A614F119D

j = 1 =
MD =
0D41564AC8E0862FB47981D213ABCAF30392CAE7C49F8ED8657DB8477DB690FCDD723F6998F2016D98FED52A2
C8251EAEC95F1DCD69F9815A112B5AA85849138

j = 2 =
MD =
CBA5577E8F115FEE95EBD40B6EDD2E3A8C846326C04C285D6A342F4E285F5AEEA87BB0997E20254754743EB2DE
B30C05D60EA0D8181895B265C132231F78C82D

j = 3 =
MD =
DF8794A3AAB30FE7FA650560A79130DB87C9937FDBCFDC73B08C98E810AE54670487948AE1C7BC4DF4C3947F5
B475939D7756C79B236F216DFE3371CCC382809

j = 4 =
MD =
F24A413ED1A61FFFD5C7DF3C42FF36ED83A127ABA4F46D63B3E37391BE1F60C06572B59A59F86102CEAA0C2C68
2EAEF1715D9FD1F039529768F9A175F8334A77

j = 5 =
MD =
BCF3E015C82DE968AC59AAF9C9CD4A117E361D2B29550A621B49649FAFFE9C0D3C5E3F0A8DBC5B32EF37AB0CDE
AF9BE242F9B5B39407E526C6DFEF8A08E320FED