Algorithm name: **MCSSHA-3**
Principal submitter: **Mikhail Maslennikov**

Revision: September 23, 2008

SECURE HASH ALGORITHM MCSSHA-3

Table Of Contents

1. INTRODUCTION 3
2. DEFINITIONS 4
   2.1 Glossary of Terms and Acronyms 4
   2.2 Algorithm Parameters, Symbols, and Terms 4
      2.2.1 Parameters 4
      2.2.2 Symbols 5
3. NOTATION AND CONVENTIONS 6
   3.1 Substitution 6
   3.2 Shift Registry Steps 6
4. FUNCTIONS AND CONSTANTS 7
   4.1 Constants 7
   4.2 Functions 7
5. PREPROCESSING 9
6. PRE-HASH COMPUTATION 10
7. FINAL HASH COMPUTATION 12
   7.1 Creating input sequence 12
   7.2 Calculating final SR state 12
8. EXAMPLES 14
   8.1 Calculate message digest for 224 hash bit length 14
   8.2 Calculate message digest for 256 hash bit length 20
   8.3 Calculate message digest for 384 hash bit length 27
   8.4 Calculate message digest for 512 hash bit length 40
9. ESTIMATED COMPUTATIONAL EFFICIENCY AND MEMORY REQUIREMENTS 62
   9.1 Memory Requirement 62
   9.2 Computation Efficiency 62
   9.3 HMAC support. 68
10. CRYPTOGRAPHY ANALYSIS 70
   10.1 Mathematical bases of algorithm MCSSHA-3. 70
      10.1.1 Logarithmic substitution π. 70

10.2 Strategy of possible cryptographic attacks. 73
10.2.1 Birthday attack method. 73
10.2.2 Method of “capture” SR states during pre-hash computation. 73
10.2.3 Conformity of MCSSHA-3 algorithm to cryptography requirements 78
10.3 Provenance of constants and tables. 79
10.3.1 Initial SR states. 79
10.3.2 Substitution. 79
10.3.3 SR points and delay. 79
Appendix A. KAT and MCT tests. 81
Appendix B. Literature. 90

1. INTRODUCTION

This document specifies secure hash algorithm MCSSHA-3. 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-3 algorithm can be described in three stages: preprocessing, pre-hash computation and final hash computation. Each stage change *Shift Registry state* (SR-state) and final SR-state is message digest.

Preprocessing setting initial SR-state to be used in the hash computation. Initial SR-state not depended from message and padding not used in MCSSHA-3 algorithm. 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.

2. DEFINITIONS

2.1 Glossary of Terms and Acronyms

Bit A binary digit having a value of 0 or 1.

Byte A group of eight bits.

Hash bit length (n) Length (in bits) of the message digest. It may be 224, 256, 384 or 512.

Hash byte length (N) Length (in bytes) of the message digest. It may be 28, 32, 48 or 64.

Shift Registry state (SR state) A group of N bytes.

Initial SR state SR state before pre-hash computation.

Shift Registry point (SR point) Digit from 0 to N-1.

SR points A group of four SR points

Initial SR points SR points before pre-hash computation.

Shift Registry Substitution A group of 256 bytes where all values are various.

Shift Registry step (SR step) Transformation of a SR state during one step.

Input byte for SR step Byte that use SR step.

Message A group of bits.

Message length in bits Number of bits in message.

Message length in bytes Number of full bytes in message.

Message remain bits Message's last bits not included in the last byte.

2.2 Algorithm Parameters, Symbols, and Terms

2.2.1 Parameters

The following parameters are used in MCSSHA-3 algorithm specifications in this document.

n Hash bit length

N Hash byte length, N = n/8.

M Message to be hashed.

l Length of the message M, in bits.

L Length of the message M, in bytes, $L = l/8$.

r Number of message remain bits, i.e. $r = l - 8L$.

m_i byte number i in message M.

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

π Shift Registry Substitution.

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

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

2.2.2 Symbols

The following symbols are used in MCSSHA-3 algorithm specifications.

+ Addition on the module 256.

- Subtraction on the module 256.

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

$a(mod\ N)$ Reduction of value a on the module N.

3. NOTATION AND CONVENTIONS

3.1 Substitution

The following terminology related to substitution will be used.

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

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

3.2 Shift Registry Steps

The following terminology related to SR steps will be used.

$Y = (y_0,y_1, \ldots,y_{N-1})$	SR state before step.
$P=(p_1,p_2,p_3,p_4)$	SR points before step.
p	Changeable position: $p= (p_4+1)(\text{mod } N)$.
x	Input byte for step.

4. FUNCTIONS AND CONSTANTS

This section defines the functions and constants that are used by MCSSHA-3 algorithms. All stages of MCSSHA-3 algorithm 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-3 algorithm's parameters. This is group of 256 bytes where all values are various. In hex, these group are

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

4.2 Functions

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

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

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

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

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

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

For example, if n=224, SR state before step are

```
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
```

SR points before step are 00 01 18 1B, input byte x = 61, then

$y_{p1} - y_{p2} - y_{p3} + y_{p4} = 00 - 01 - 18 + 1B = 02$

$\pi(y_{p1} - y_{p2} - y_{p3} + y_{p4}) = \pi(02) = 67$

$z = \pi(y_{p1} - y_{p2} - y_{p3} + y_{p4}) + x = 67 + 61 = C8$

SR state after step are

```
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
```

and SR points after step are 01 02 19 00.

5. PREPROCESSING

Preprocessing shall take place before hash computation begins. In this stage MCSSHA-3 algorithm set initial SR state and points as follow.

In hex, initial SR state are

for n = 224

```
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
```

for n = 256

```
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
```

for n = 384

```
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
```

for n = 512

```
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
```

In hex, initial SR points are

for n = 224: 00 01 18 1B

for n = 256: 00 01 1C 1F

for n = 384: 00 01 2C 2F

for n = 512: 00 01 3C 3F

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 4 steps:

Step 1: SR step with input byte m_i.

Step 2 – 4: SR step with input byte 0.

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

For example, if n=224, message byte is 61, and before one message byte computation

SR state are

```
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
```

SR points are 00 01 18 1B, then

Step 1.

$y_{p1} - y_{p2} - y_{p3} + y_{p4} = 00 - 01 - 18 + 1B = 02$

$\pi(y_{p1} - y_{p2} - y_{p3} + y_{p4}) = \pi(02) = 67$

$z = \pi(y_{p1} - y_{p2} - y_{p3} + y_{p4}) + x = 67 + 61 = C8$

SR state after step 1 are

```
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
```

and SR points after step 1 are 01 02 19 00.

Step 2.

$y_{p1} - y_{p2} - y_{p3} + y_{p4} = 01 - 02 - 19 + C8 = AE$

$z = \pi(y_{p1} - y_{p2} - y_{p3} + y_{p4}) = \pi(AE) = 53$

SR state after step 2 are

```
C8  53  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
```

and SR points after step 2 are 02 03 1A 01.

Step 3.

$y_{p1} - y_{p2} - y_{p3} + y_{p4} = 02 - 03 - 1A + 53 = 38$

$z = \pi(y_{p1} - y_{p2} - y_{p3} + y_{p4}) = \pi(38) = C0$

SR state after step 3 are

```
C8  53  C0  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
```

and SR points after step 3 are 03 04 1B 02.

Step 4.

$y_{p1} - y_{p2} - y_{p3} + y_{p4} = 03 - 04 - 1B + C0 = A4$

$z = \pi(y_{p1} - y_{p2} - y_{p3} + y_{p4}) = \pi(A4) = 4F$

SR state after step 4 are

```
C8  53  C0  4F  04  05  06  07  08  09  0A  0B  0C  0D  0E  0F
10  11  12  13  14  15  16  17  18  19  1A  1B
```

and SR points after step 4 are 04 05 00 03.

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

$Z = b_1,b_2,...,b_r,a_1,a_2,...,a_n,a_1,a_2,...,a_n, a_1,a_2,...,a_n, a_1,a_2,...,a_{n-r}.$ (7.1)

The length in bits of the input sequence if exactly 4n bits, in bytes – exactly 4N bytes.

If remain bits absent, then

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

7.2 Calculating final SR state

Lets $Z = z_1,z_2,...,z_{4N}$ – input sequence in bytes. Calculating final SR state consist from 4N steps. For each step i MCSSHA-3 algorithm perform SR step with input byte z_i. Final SR state is message digest.

For example, if n=224, remain bits absent, and

SR state before final hash computation are

```
C8  53  C0  4F  31  19  E4  3A  AB  6E  1F  75  0C  0D  0E  0F  10
11  12  13  14  15  16  17  18  19  1A  1B
```

and SR points before final hash computation are 0C 0D 08 0B, then

```
Z =  C8  53  C0  4F  31  19  E4  3A  AB  6E  1F  75  0C  0D  0E  0F
     10  11  12  13  14  15  16  17  18  19  1A  1B  C8  53  C0  4F
     31  19  E4  3A  AB  6E  1F  75  0C  0D  0E  0F  10  11  12  13
     14  15  16  17  18  19  1A  1B  C8  53  C0  4F  31  19  E4  3A
     AB  6E  1F  75  0C  0D  0E  0F  10  11  12  13  14  15  16  17
     18  19  1A  1B  C8  53  C0  4F  31  19  E4  3A  AB  6E  1F  75
     0C  0D  0E  0F  10  11  12  13  14  15  16  17  18  19  1A  1B
```

Step 1.

$y_{p1} - y_{p2} - y_{p3} + y_{p4} = 0C - 0D - AB + 75 = C9$

$\pi(y_{p1} - y_{p2} - y_{p3} + y_{p4}) = \pi(C9) = FA$

$z = \pi(y_{p1} - y_{p2} - y_{p3} + y_{p4}) + x = FA + C8 = C2$

SR state after step 1 are

```
C8  53  C0  4F  31  19  E4  3A  AB  6E  1F  75  C2  0D  0E  0F  10
11  12  13  14  15  16  17  18  19  1A  1B
```

and SR points after step 1 are 0D 0E 09 0C.

8. EXAMPLES

8.1 Calculate message digest for 224 hash bit length

Let the message, *M*, be the 24-bit (l = 24) ASCII string "**abc**", which is equivalent to the following hex string: 61 62 63.
For this message digest calculation consist from:

12 steps for pre-hash computation;
112 steps for final hash computation.

Total: 124 steps.

This is SR states for all this steps. 0 – initial SR state.

Stage 1. Preprocessing

```
        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
```

Stage 2. Pre-hash computation – 12 steps

Input byte 61

```
1.      C8  01  02  03  04  05  06  07  08  09  0A  0B  0C  0D  0E  0F
        10  11  12  13  14  15  16  17  18  19  1A  1B

2.      C8  53  02  03  04  05  06  07  08  09  0A  0B  0C  0D  0E  0F
        10  11  12  13  14  15  16  17  18  19  1A  1B

3.      C8  53  C0  03  04  05  06  07  08  09  0A  0B  0C  0D  0E  0F
        10  11  12  13  14  15  16  17  18  19  1A  1B

4.      C8  53  C0  4F  04  05  06  07  08  09  0A  0B  0C  0D  0E  0F
        10  11  12  13  14  15  16  17  18  19  1A  1B
```

Input byte 62

```
5.      C8  53  C0  4F  31  05  06  07  08  09  0A  0B  0C  0D  0E  0F
        10  11  12  13  14  15  16  17  18  19  1A  1B

6.      C8  53  C0  4F  31  19  06  07  08  09  0A  0B  0C  0D  0E  0F
        10  11  12  13  14  15  16  17  18  19  1A  1B

7.      C8  53  C0  4F  31  19  E4  07  08  09  0A  0B  0C  0D  0E  0F
        10  11  12  13  14  15  16  17  18  19  1A  1B

8.      C8  53  C0  4F  31  19  E4  3A  08  09  0A  0B  0C  0D  0E  0F
        10  11  12  13  14  15  16  17  18  19  1A  1B
```

Input byte 63

```
9.      C8  53  C0  4F  31  19  E4  3A  AB  09  0A  0B  0C  0D  0E  0F
        10  11  12  13  14  15  16  17  18  19  1A  1B

10.     C8  53  C0  4F  31  19  E4  3A  AB  6E  0A  0B  0C  0D  0E  0F
```

```
        10  11  12  13  14  15  16  17  18  19  1A  1B

11.     C8  53  C0  4F  31  19  E4  3A  AB  6E  1F  0B  0C  0D  0E  0F
        10  11  12  13  14  15  16  17  18  19  1A  1B

12.     C8  53  C0  4F  31  19  E4  3A  AB  6E  1F  75  0C  0D  0E  0F
        10  11  12  13  14  15  16  17  18  19  1A  1B
```

Stage 3. Final hash computation – 112 steps

```
13.     C8  53  C0  4F  31  19  E4  3A  AB  6E  1F  75  C2  0D  0E  0F
        10  11  12  13  14  15  16  17  18  19  1A  1B

14.     C8  53  C0  4F  31  19  E4  3A  AB  6E  1F  75  C2  11  0E  0F
        10  11  12  13  14  15  16  17  18  19  1A  1B

15.     C8  53  C0  4F  31  19  E4  3A  AB  6E  1F  75  C2  11  67  0F
        10  11  12  13  14  15  16  17  18  19  1A  1B

16.     C8  53  C0  4F  31  19  E4  3A  AB  6E  1F  75  C2  11  67  F6
        10  11  12  13  14  15  16  17  18  19  1A  1B

17.     C8  53  C0  4F  31  19  E4  3A  AB  6E  1F  75  C2  11  67  F6
        2C  11  12  13  14  15  16  17  18  19  1A  1B

18.     C8  53  C0  4F  31  19  E4  3A  AB  6E  1F  75  C2  11  67  F6
        2C  07  12  13  14  15  16  17  18  19  1A  1B

19.     C8  53  C0  4F  31  19  E4  3A  AB  6E  1F  75  C2  11  67  F6
        2C  07  ED  13  14  15  16  17  18  19  1A  1B

20.     C8  53  C0  4F  31  19  E4  3A  AB  6E  1F  75  C2  11  67  F6
        2C  07  ED  48  14  15  16  17  18  19  1A  1B

21.     C8  53  C0  4F  31  19  E4  3A  AB  6E  1F  75  C2  11  67  F6
        2C  07  ED  48  44  15  16  17  18  19  1A  1B

22.     C8  53  C0  4F  31  19  E4  3A  AB  6E  1F  75  C2  11  67  F6
        2C  07  ED  48  44  0B  16  17  18  19  1A  1B

23.     C8  53  C0  4F  31  19  E4  3A  AB  6E  1F  75  C2  11  67  F6
        2C  07  ED  48  44  0B  DB  17  18  19  1A  1B

24.     C8  53  C0  4F  31  19  E4  3A  AB  6E  1F  75  C2  11  67  F6
        2C  07  ED  48  44  0B  DB  A1  18  19  1A  1B

25.     C8  53  C0  4F  31  19  E4  3A  AB  6E  1F  75  C2  11  67  F6
        2C  07  ED  48  44  0B  DB  A1  B7  19  1A  1B

26.     C8  53  C0  4F  31  19  E4  3A  AB  6E  1F  75  C2  11  67  F6
        2C  07  ED  48  44  0B  DB  A1  B7  48  1A  1B

27.     C8  53  C0  4F  31  19  E4  3A  AB  6E  1F  75  C2  11  67  F6
        2C  07  ED  48  44  0B  DB  A1  B7  48  B4  1B

28.     C8  53  C0  4F  31  19  E4  3A  AB  6E  1F  75  C2  11  67  F6
        2C  07  ED  48  44  0B  DB  A1  B7  48  B4  78

29.     9F  53  C0  4F  31  19  E4  3A  AB  6E  1F  75  C2  11  67  F6
        2C  07  ED  48  44  0B  DB  A1  B7  48  B4  78

30.     9F  F2  C0  4F  31  19  E4  3A  AB  6E  1F  75  C2  11  67  F6
        2C  07  ED  48  44  0B  DB  A1  B7  48  B4  78

31.     9F  F2  11  4F  31  19  E4  3A  AB  6E  1F  75  C2  11  67  F6
```

2C 07 ED 48 44 0B DB A1 B7 48 B4 78

32. 9F F2 11 F3 31 19 E4 3A AB 6E 1F 75 C2 11 67 F6
2C 07 ED 48 44 0B DB A1 B7 48 B4 78

33. 9F F2 11 F3 BA 19 E4 3A AB 6E 1F 75 C2 11 67 F6
2C 07 ED 48 44 0B DB A1 B7 48 B4 78

34. 9F F2 11 F3 BA C7 E4 3A AB 6E 1F 75 C2 11 67 F6
2C 07 ED 48 44 0B DB A1 B7 48 B4 78

35. 9F F2 11 F3 BA C7 4D 3A AB 6E 1F 75 C2 11 67 F6
2C 07 ED 48 44 0B DB A1 B7 48 B4 78

36. 9F F2 11 F3 BA C7 4D FD AB 6E 1F 75 C2 11 67 F6
2C 07 ED 48 44 0B DB A1 B7 48 B4 78

37. 9F F2 11 F3 BA C7 4D FD 18 6E 1F 75 C2 11 67 F6
2C 07 ED 48 44 0B DB A1 B7 48 B4 78

38. 9F F2 11 F3 BA C7 4D FD 18 F0 1F 75 C2 11 67 F6
2C 07 ED 48 44 0B DB A1 B7 48 B4 78

39. 9F F2 11 F3 BA C7 4D FD 18 F0 40 75 C2 11 67 F6
2C 07 ED 48 44 0B DB A1 B7 48 B4 78

40. 9F F2 11 F3 BA C7 4D FD 18 F0 40 29 C2 11 67 F6
2C 07 ED 48 44 0B DB A1 B7 48 B4 78

41. 9F F2 11 F3 BA C7 4D FD 18 F0 40 29 5D 11 67 F6
2C 07 ED 48 44 0B DB A1 B7 48 B4 78

42. 9F F2 11 F3 BA C7 4D FD 18 F0 40 29 5D 50 67 F6
2C 07 ED 48 44 0B DB A1 B7 48 B4 78

43. 9F F2 11 F3 BA C7 4D FD 18 F0 40 29 5D 50 70 F6
2C 07 ED 48 44 0B DB A1 B7 48 B4 78

44. 9F F2 11 F3 BA C7 4D FD 18 F0 40 29 5D 50 70 EB
2C 07 ED 48 44 0B DB A1 B7 48 B4 78

45. 9F F2 11 F3 BA C7 4D FD 18 F0 40 29 5D 50 70 EB
0A 07 ED 48 44 0B DB A1 B7 48 B4 78

46. 9F F2 11 F3 BA C7 4D FD 18 F0 40 29 5D 50 70 EB
0A F8 ED 48 44 0B DB A1 B7 48 B4 78

47. 9F F2 11 F3 BA C7 4D FD 18 F0 40 29 5D 50 70 EB
0A F8 3F 48 44 0B DB A1 B7 48 B4 78

48. 9F F2 11 F3 BA C7 4D FD 18 F0 40 29 5D 50 70 EB
0A F8 3F 1E 44 0B DB A1 B7 48 B4 78

49. 9F F2 11 F3 BA C7 4D FD 18 F0 40 29 5D 50 70 EB
0A F8 3F 1E D1 0B DB A1 B7 48 B4 78

50. 9F F2 11 F3 BA C7 4D FD 18 F0 40 29 5D 50 70 EB
0A F8 3F 1E D1 7B DB A1 B7 48 B4 78

51. 9F F2 11 F3 BA C7 4D FD 18 F0 40 29 5D 50 70 EB
0A F8 3F 1E D1 7B B7 A1 B7 48 B4 78

52. 9F F2 11 F3 BA C7 4D FD 18 F0 40 29 5D 50 70 EB
0A F8 3F 1E D1 7B B7 8F B7 48 B4 78

53. 9F F2 11 F3 BA C7 4D FD 18 F0 40 29 5D 50 70 EB

0A F8 3F 1E D1 7B B7 8F 67 48 B4 78

54. 9F F2 11 F3 BA C7 4D FD 18 F0 40 29 5D 50 70 EB
0A F8 3F 1E D1 7B B7 8F 67 0D B4 78

55. 9F F2 11 F3 BA C7 4D FD 18 F0 40 29 5D 50 70 EB
0A F8 3F 1E D1 7B B7 8F 67 0D 3A 78

56. 9F F2 11 F3 BA C7 4D FD 18 F0 40 29 5D 50 70 EB
0A F8 3F 1E D1 7B B7 8F 67 0D 3A 86

57. C9 F2 11 F3 BA C7 4D FD 18 F0 40 29 5D 50 70 EB
0A F8 3F 1E D1 7B B7 8F 67 0D 3A 86

58. C9 69 11 F3 BA C7 4D FD 18 F0 40 29 5D 50 70 EB
0A F8 3F 1E D1 7B B7 8F 67 0D 3A 86

59. C9 69 38 F3 BA C7 4D FD 18 F0 40 29 5D 50 70 EB
0A F8 3F 1E D1 7B B7 8F 67 0D 3A 86

60. C9 69 38 40 BA C7 4D FD 18 F0 40 29 5D 50 70 EB
0A F8 3F 1E D1 7B B7 8F 67 0D 3A 86

61. C9 69 38 40 99 C7 4D FD 18 F0 40 29 5D 50 70 EB
0A F8 3F 1E D1 7B B7 8F 67 0D 3A 86

62. C9 69 38 40 99 B3 4D FD 18 F0 40 29 5D 50 70 EB
0A F8 3F 1E D1 7B B7 8F 67 0D 3A 86

63. C9 69 38 40 99 B3 64 FD 18 F0 40 29 5D 50 70 EB
0A F8 3F 1E D1 7B B7 8F 67 0D 3A 86

64. C9 69 38 40 99 B3 64 24 18 F0 40 29 5D 50 70 EB
0A F8 3F 1E D1 7B B7 8F 67 0D 3A 86

65. C9 69 38 40 99 B3 64 24 F1 F0 40 29 5D 50 70 EB
0A F8 3F 1E D1 7B B7 8F 67 0D 3A 86

66. C9 69 38 40 99 B3 64 24 F1 2A 40 29 5D 50 70 EB
0A F8 3F 1E D1 7B B7 8F 67 0D 3A 86

67. C9 69 38 40 99 B3 64 24 F1 2A 33 29 5D 50 70 EB
0A F8 3F 1E D1 7B B7 8F 67 0D 3A 86

68. C9 69 38 40 99 B3 64 24 F1 2A 33 C8 5D 50 70 EB
0A F8 3F 1E D1 7B B7 8F 67 0D 3A 86

69. C9 69 38 40 99 B3 64 24 F1 2A 33 C8 3D 50 70 EB
0A F8 3F 1E D1 7B B7 8F 67 0D 3A 86

70. C9 69 38 40 99 B3 64 24 F1 2A 33 C8 3D C0 70 EB
0A F8 3F 1E D1 7B B7 8F 67 0D 3A 86

71. C9 69 38 40 99 B3 64 24 F1 2A 33 C8 3D C0 E3 EB
0A F8 3F 1E D1 7B B7 8F 67 0D 3A 86

72. C9 69 38 40 99 B3 64 24 F1 2A 33 C8 3D C0 E3 8E
0A F8 3F 1E D1 7B B7 8F 67 0D 3A 86

73. C9 69 38 40 99 B3 64 24 F1 2A 33 C8 3D C0 E3 8E
EC F8 3F 1E D1 7B B7 8F 67 0D 3A 86

74. C9 69 38 40 99 B3 64 24 F1 2A 33 C8 3D C0 E3 8E
EC 97 3F 1E D1 7B B7 8F 67 0D 3A 86

75. C9 69 38 40 99 B3 64 24 F1 2A 33 C8 3D C0 E3 8E

EC 97 95 1E D1 7B B7 8F 67 0D 3A 86

76. C9 69 38 40 99 B3 64 24 F1 2A 33 C8 3D C0 E3 8E
EC 97 95 A0 D1 7B B7 8F 67 0D 3A 86

77. C9 69 38 40 99 B3 64 24 F1 2A 33 C8 3D C0 E3 8E
EC 97 95 A0 C3 7B B7 8F 67 0D 3A 86

78. C9 69 38 40 99 B3 64 24 F1 2A 33 C8 3D C0 E3 8E
EC 97 95 A0 C3 33 B7 8F 67 0D 3A 86

79. C9 69 38 40 99 B3 64 24 F1 2A 33 C8 3D C0 E3 8E
EC 97 95 A0 C3 33 ED 8F 67 0D 3A 86

80. C9 69 38 40 99 B3 64 24 F1 2A 33 C8 3D C0 E3 8E
EC 97 95 A0 C3 33 ED 96 67 0D 3A 86

81. C9 69 38 40 99 B3 64 24 F1 2A 33 C8 3D C0 E3 8E
EC 97 95 A0 C3 33 ED 96 67 0D 3A 86

82. C9 69 38 40 99 B3 64 24 F1 2A 33 C8 3D C0 E3 8E
EC 97 95 A0 C3 33 ED 96 67 32 3A 86

83. C9 69 38 40 99 B3 64 24 F1 2A 33 C8 3D C0 E3 8E
EC 97 95 A0 C3 33 ED 96 67 32 2C 86

84. C9 69 38 40 99 B3 64 24 F1 2A 33 C8 3D C0 E3 8E
EC 97 95 A0 C3 33 ED 96 67 32 2C CD

85. DE 69 38 40 99 B3 64 24 F1 2A 33 C8 3D C0 E3 8E
EC 97 95 A0 C3 33 ED 96 67 32 2C CD

86. DE 2A 38 40 99 B3 64 24 F1 2A 33 C8 3D C0 E3 8E
EC 97 95 A0 C3 33 ED 96 67 32 2C CD

87. DE 2A 20 40 99 B3 64 24 F1 2A 33 C8 3D C0 E3 8E
EC 97 95 A0 C3 33 ED 96 67 32 2C CD

88. DE 2A 20 A0 99 B3 64 24 F1 2A 33 C8 3D C0 E3 8E
EC 97 95 A0 C3 33 ED 96 67 32 2C CD

89. DE 2A 20 A0 A0 B3 64 24 F1 2A 33 C8 3D C0 E3 8E
EC 97 95 A0 C3 33 ED 96 67 32 2C CD

90. DE 2A 20 A0 A0 BD 64 24 F1 2A 33 C8 3D C0 E3 8E
EC 97 95 A0 C3 33 ED 96 67 32 2C CD

91. DE 2A 20 A0 A0 BD 2F 24 F1 2A 33 C8 3D C0 E3 8E
EC 97 95 A0 C3 33 ED 96 67 32 2C CD

92. DE 2A 20 A0 A0 BD 2F AC F1 2A 33 C8 3D C0 E3 8E
EC 97 95 A0 C3 33 ED 96 67 32 2C CD

93. DE 2A 20 A0 A0 BD 2F AC 46 2A 33 C8 3D C0 E3 8E
EC 97 95 A0 C3 33 ED 96 67 32 2C CD

94. DE 2A 20 A0 A0 BD 2F AC 46 19 33 C8 3D C0 E3 8E
EC 97 95 A0 C3 33 ED 96 67 32 2C CD

95. DE 2A 20 A0 A0 BD 2F AC 46 19 AA C8 3D C0 E3 8E
EC 97 95 A0 C3 33 ED 96 67 32 2C CD

96. DE 2A 20 A0 A0 BD 2F AC 46 19 AA 3A 3D C0 E3 8E
EC 97 95 A0 C3 33 ED 96 67 32 2C CD

97. DE 2A 20 A0 A0 BD 2F AC 46 19 AA 3A FC C0 E3 8E

EC 97 95 A0 C3 33 ED 96 67 32 2C CD

98. DE 2A 20 A0 A0 BD 2F AC 46 19 AA 3A FC CB E3 8E
EC 97 95 A0 C3 33 ED 96 67 32 2C CD

99. DE 2A 20 A0 A0 BD 2F AC 46 19 AA 3A FC CB 58 8E
EC 97 95 A0 C3 33 ED 96 67 32 2C CD

100. DE 2A 20 A0 A0 BD 2F AC 46 19 AA 3A FC CB 58 C7
EC 97 95 A0 C3 33 ED 96 67 32 2C CD

101. DE 2A 20 A0 A0 BD 2F AC 46 19 AA 3A FC CB 58 C7
D2 97 95 A0 C3 33 ED 96 67 32 2C CD

102. DE 2A 20 A0 A0 BD 2F AC 46 19 AA 3A FC CB 58 C7
D2 26 95 A0 C3 33 ED 96 67 32 2C CD

103. DE 2A 20 A0 A0 BD 2F AC 46 19 AA 3A FC CB 58 C7
D2 26 68 A0 C3 33 ED 96 67 32 2C CD

104. DE 2A 20 A0 A0 BD 2F AC 46 19 AA 3A FC CB 58 C7
D2 26 68 C8 C3 33 ED 96 67 32 2C CD

105. DE 2A 20 A0 A0 BD 2F AC 46 19 AA 3A FC CB 58 C7
D2 26 68 C8 7A 33 ED 96 67 32 2C CD

106. DE 2A 20 A0 A0 BD 2F AC 46 19 AA 3A FC CB 58 C7
D2 26 68 C8 7A 71 ED 96 67 32 2C CD

107. DE 2A 20 A0 A0 BD 2F AC 46 19 AA 3A FC CB 58 C7
D2 26 68 C8 7A 71 56 96 67 32 2C CD

108. DE 2A 20 A0 A0 BD 2F AC 46 19 AA 3A FC CB 58 C7
D2 26 68 C8 7A 71 56 41 67 32 2C CD

109. DE 2A 20 A0 A0 BD 2F AC 46 19 AA 3A FC CB 58 C7
D2 26 68 C8 7A 71 56 41 4B 32 2C CD

110. DE 2A 20 A0 A0 BD 2F AC 46 19 AA 3A FC CB 58 C7
D2 26 68 C8 7A 71 56 41 4B 8E 2C CD

111. DE 2A 20 A0 A0 BD 2F AC 46 19 AA 3A FC CB 58 C7
D2 26 68 C8 7A 71 56 41 4B 8E 64 CD

112. DE 2A 20 A0 A0 BD 2F AC 46 19 AA 3A FC CB 58 C7
D2 26 68 C8 7A 71 56 41 4B 8E 64 32

113. 26 2A 20 A0 A0 BD 2F AC 46 19 AA 3A FC CB 58 C7
D2 26 68 C8 7A 71 56 41 4B 8E 64 32

114. 26 1B 20 A0 A0 BD 2F AC 46 19 AA 3A FC CB 58 C7
D2 26 68 C8 7A 71 56 41 4B 8E 64 32

115. 26 1B 43 A0 A0 BD 2F AC 46 19 AA 3A FC CB 58 C7
D2 26 68 C8 7A 71 56 41 4B 8E 64 32

116. 26 1B 43 AF A0 BD 2F AC 46 19 AA 3A FC CB 58 C7
D2 26 68 C8 7A 71 56 41 4B 8E 64 32

117. 26 1B 43 AF BA BD 2F AC 46 19 AA 3A FC CB 58 C7
D2 26 68 C8 7A 71 56 41 4B 8E 64 32

118. 26 1B 43 AF BA 70 2F AC 46 19 AA 3A FC CB 58 C7
D2 26 68 C8 7A 71 56 41 4B 8E 64 32

119. 26 1B 43 AF BA 70 96 AC 46 19 AA 3A FC CB 58 C7

```
        D2  26  68  C8  7A  71  56  41  4B  8E  64  32

120.    26  1B  43  AF  BA  70  96  3D  46  19  AA  3A  FC  CB  58  C7
        D2  26  68  C8  7A  71  56  41  4B  8E  64  32

121.    26  1B  43  AF  BA  70  96  3D  98  19  AA  3A  FC  CB  58  C7
        D2  26  68  C8  7A  71  56  41  4B  8E  64  32

122.    26  1B  43  AF  BA  70  96  3D  98  6F  AA  3A  FC  CB  58  C7
        D2  26  68  C8  7A  71  56  41  4B  8E  64  32

123.    26  1B  43  AF  BA  70  96  3D  98  6F  43  3A  FC  CB  58  C7
        D2  26  68  C8  7A  71  56  41  4B  8E  64  32

124.    26  1B  43  AF  BA  70  96  3D  98  6F  43  02  FC  CB  58  C7
        D2  26  68  C8  7A  71  56  41  4B  8E  64  32
```

Message digest:

```
        26  1B  43  AF  BA  70  96  3D  98  6F  43  02  FC  CB  58  C7
        D2  26  68  C8  7A  71  56  41  4B  8E  64  32
```

8.2 Calculate message digest for 256 hash bit length

Let the message, *M*, be the 24-bit (l = 24) ASCII string "**abc**", which is equivalent to the following hex string: 61 62 63.
For this message digest calculation consist from:

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

Total: 140 steps.

This is SR states for all this steps. 0 – initial SR state.

Stage 1. Preprocessing

```
        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
```

Stage 2. Pre-hash computation – 12 steps

Input byte 61

```
1.      C8  01  02  03  04  05  06  07  08  09  0A  0B  0C  0D  0E  0F
        10  11  12  13  14  15  16  17  18  19  1A  1B  1C  1D  1E  1F

2.      C8  9E  02  03  04  05  06  07  08  09  0A  0B  0C  0D  0E  0F
        10  11  12  13  14  15  16  17  18  19  1A  1B  1C  1D  1E  1F

3.      C8  9E  2F  03  04  05  06  07  08  09  0A  0B  0C  0D  0E  0F
        10  11  12  13  14  15  16  17  18  19  1A  1B  1C  1D  1E  1F

4.      C8  9E  2F  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
```

Input byte 62

5. C8 9E 2F B6 D5 05 06 07 08 09 0A 0B 0C 0D 0E 0F
10 11 12 13 14 15 16 17 18 19 1A 1B 1C 1D 1E 1F

6. C8 9E 2F B6 D5 8F 06 07 08 09 0A 0B 0C 0D 0E 0F
10 11 12 13 14 15 16 17 18 19 1A 1B 1C 1D 1E 1F

7. C8 9E 2F B6 D5 8F 54 07 08 09 0A 0B 0C 0D 0E 0F
10 11 12 13 14 15 16 17 18 19 1A 1B 1C 1D 1E 1F

8. C8 9E 2F B6 D5 8F 54 58 08 09 0A 0B 0C 0D 0E 0F
10 11 12 13 14 15 16 17 18 19 1A 1B 1C 1D 1E 1F

Input byte 63

9. C8 9E 2F B6 D5 8F 54 58 73 09 0A 0B 0C 0D 0E 0F
10 11 12 13 14 15 16 17 18 19 1A 1B 1C 1D 1E 1F

10. C8 9E 2F B6 D5 8F 54 58 73 9F 0A 0B 0C 0D 0E 0F
10 11 12 13 14 15 16 17 18 19 1A 1B 1C 1D 1E 1F

11. C8 9E 2F B6 D5 8F 54 58 73 9F F9 0B 0C 0D 0E 0F
10 11 12 13 14 15 16 17 18 19 1A 1B 1C 1D 1E 1F

12. C8 9E 2F B6 D5 8F 54 58 73 9F F9 D7 0C 0D 0E 0F
10 11 12 13 14 15 16 17 18 19 1A 1B 1C 1D 1E 1F

Stage 3. Final hash computation – 128 steps

13. C8 9E 2F B6 D5 8F 54 58 73 9F F9 D7 83 0D 0E 0F
10 11 12 13 14 15 16 17 18 19 1A 1B 1C 1D 1E 1F

14. C8 9E 2F B6 D5 8F 54 58 73 9F F9 D7 83 3D 0E 0F
10 11 12 13 14 15 16 17 18 19 1A 1B 1C 1D 1E 1F

15. C8 9E 2F B6 D5 8F 54 58 73 9F F9 D7 83 3D 3E 0F
10 11 12 13 14 15 16 17 18 19 1A 1B 1C 1D 1E 1F

16. C8 9E 2F B6 D5 8F 54 58 73 9F F9 D7 83 3D 3E 1F
10 11 12 13 14 15 16 17 18 19 1A 1B 1C 1D 1E 1F

17. C8 9E 2F B6 D5 8F 54 58 73 9F F9 D7 83 3D 3E 1F
EB 11 12 13 14 15 16 17 18 19 1A 1B 1C 1D 1E 1F

18. C8 9E 2F B6 D5 8F 54 58 73 9F F9 D7 83 3D 3E 1F
EB FA 12 13 14 15 16 17 18 19 1A 1B 1C 1D 1E 1F

19. C8 9E 2F B6 D5 8F 54 58 73 9F F9 D7 83 3D 3E 1F
EB FA 7F 13 14 15 16 17 18 19 1A 1B 1C 1D 1E 1F

20. C8 9E 2F B6 D5 8F 54 58 73 9F F9 D7 83 3D 3E 1F
EB FA 7F AC 14 15 16 17 18 19 1A 1B 1C 1D 1E 1F

21. C8 9E 2F B6 D5 8F 54 58 73 9F F9 D7 83 3D 3E 1F
EB FA 7F AC EB 15 16 17 18 19 1A 1B 1C 1D 1E 1F

22. C8 9E 2F B6 D5 8F 54 58 73 9F F9 D7 83 3D 3E 1F
EB FA 7F AC EB 64 16 17 18 19 1A 1B 1C 1D 1E 1F

23. C8 9E 2F B6 D5 8F 54 58 73 9F F9 D7 83 3D 3E 1F
EB FA 7F AC EB 64 6E 17 18 19 1A 1B 1C 1D 1E 1F

24. C8 9E 2F B6 D5 8F 54 58 73 9F F9 D7 83 3D 3E 1F
EB FA 7F AC EB 64 6E 81 18 19 1A 1B 1C 1D 1E 1F

25. C8 9E 2F B6 D5 8F 54 58 73 9F F9 D7 83 3D 3E 1F
EB FA 7F AC EB 64 6E 81 68 19 1A 1B 1C 1D 1E 1F

26. C8 9E 2F B6 D5 8F 54 58 73 9F F9 D7 83 3D 3E 1F
EB FA 7F AC EB 64 6E 81 68 C2 1A 1B 1C 1D 1E 1F

27. C8 9E 2F B6 D5 8F 54 58 73 9F F9 D7 83 3D 3E 1F
EB FA 7F AC EB 64 6E 81 68 C2 CC 1B 1C 1D 1E 1F

28. C8 9E 2F B6 D5 8F 54 58 73 9F F9 D7 83 3D 3E 1F
EB FA 7F AC EB 64 6E 81 68 C2 CC 08 1C 1D 1E 1F

29. C8 9E 2F B6 D5 8F 54 58 73 9F F9 D7 83 3D 3E 1F
EB FA 7F AC EB 64 6E 81 68 C2 CC 08 19 1D 1E 1F

30. C8 9E 2F B6 D5 8F 54 58 73 9F F9 D7 83 3D 3E 1F
EB FA 7F AC EB 64 6E 81 68 C2 CC 08 19 05 1E 1F

31. C8 9E 2F B6 D5 8F 54 58 73 9F F9 D7 83 3D 3E 1F
EB FA 7F AC EB 64 6E 81 68 C2 CC 08 19 05 D2 1F

32. C8 9E 2F B6 D5 8F 54 58 73 9F F9 D7 83 3D 3E 1F
EB FA 7F AC EB 64 6E 81 68 C2 CC 08 19 05 D2 B3

33. 75 9E 2F B6 D5 8F 54 58 73 9F F9 D7 83 3D 3E 1F
EB FA 7F AC EB 64 6E 81 68 C2 CC 08 19 05 D2 B3

34. 75 94 2F B6 D5 8F 54 58 73 9F F9 D7 83 3D 3E 1F
EB FA 7F AC EB 64 6E 81 68 C2 CC 08 19 05 D2 B3

35. 75 94 F9 B6 D5 8F 54 58 73 9F F9 D7 83 3D 3E 1F
EB FA 7F AC EB 64 6E 81 68 C2 CC 08 19 05 D2 B3

36. 75 94 F9 88 D5 8F 54 58 73 9F F9 D7 83 3D 3E 1F
EB FA 7F AC EB 64 6E 81 68 C2 CC 08 19 05 D2 B3

37. 75 94 F9 88 4B 8F 54 58 73 9F F9 D7 83 3D 3E 1F
EB FA 7F AC EB 64 6E 81 68 C2 CC 08 19 05 D2 B3

38. 75 94 F9 88 4B 09 54 58 73 9F F9 D7 83 3D 3E 1F
EB FA 7F AC EB 64 6E 81 68 C2 CC 08 19 05 D2 B3

39. 75 94 F9 88 4B 09 42 58 73 9F F9 D7 83 3D 3E 1F
EB FA 7F AC EB 64 6E 81 68 C2 CC 08 19 05 D2 B3

40. 75 94 F9 88 4B 09 42 24 73 9F F9 D7 83 3D 3E 1F
EB FA 7F AC EB 64 6E 81 68 C2 CC 08 19 05 D2 B3

41. 75 94 F9 88 4B 09 42 24 87 9F F9 D7 83 3D 3E 1F
EB FA 7F AC EB 64 6E 81 68 C2 CC 08 19 05 D2 B3

42. 75 94 F9 88 4B 09 42 24 87 56 F9 D7 83 3D 3E 1F
EB FA 7F AC EB 64 6E 81 68 C2 CC 08 19 05 D2 B3

43. 75 94 F9 88 4B 09 42 24 87 56 AD D7 83 3D 3E 1F
EB FA 7F AC EB 64 6E 81 68 C2 CC 08 19 05 D2 B3

44. 75 94 F9 88 4B 09 42 24 87 56 AD 38 83 3D 3E 1F
EB FA 7F AC EB 64 6E 81 68 C2 CC 08 19 05 D2 B3

45. 75 94 F9 88 4B 09 42 24 87 56 AD 38 CC 3D 3E 1F
EB FA 7F AC EB 64 6E 81 68 C2 CC 08 19 05 D2 B3

46. 75 94 F9 88 4B 09 42 24 87 56 AD 38 CC BF 3E 1F
EB FA 7F AC EB 64 6E 81 68 C2 CC 08 19 05 D2 B3

47. 75 94 F9 88 4B 09 42 24 87 56 AD 38 CC BF 84 1F
EB FA 7F AC EB 64 6E 81 68 C2 CC 08 19 05 D2 B3

48. 75 94 F9 88 4B 09 42 24 87 56 AD 38 CC BF 84 B6
EB FA 7F AC EB 64 6E 81 68 C2 CC 08 19 05 D2 B3

49. 75 94 F9 88 4B 09 42 24 87 56 AD 38 CC BF 84 B6
82 FA 7F AC EB 64 6E 81 68 C2 CC 08 19 05 D2 B3

50. 75 94 F9 88 4B 09 42 24 87 56 AD 38 CC BF 84 B6
82 62 7F AC EB 64 6E 81 68 C2 CC 08 19 05 D2 B3

51. 75 94 F9 88 4B 09 42 24 87 56 AD 38 CC BF 84 B6
82 62 0B AC EB 64 6E 81 68 C2 CC 08 19 05 D2 B3

52. 75 94 F9 88 4B 09 42 24 87 56 AD 38 CC BF 84 B6
82 62 0B 4F EB 64 6E 81 68 C2 CC 08 19 05 D2 B3

53. 75 94 F9 88 4B 09 42 24 87 56 AD 38 CC BF 84 B6
82 62 0B 4F D9 64 6E 81 68 C2 CC 08 19 05 D2 B3

54. 75 94 F9 88 4B 09 42 24 87 56 AD 38 CC BF 84 B6
82 62 0B 4F D9 53 6E 81 68 C2 CC 08 19 05 D2 B3

55. 75 94 F9 88 4B 09 42 24 87 56 AD 38 CC BF 84 B6
82 62 0B 4F D9 53 7C 81 68 C2 CC 08 19 05 D2 B3

56. 75 94 F9 88 4B 09 42 24 87 56 AD 38 CC BF 84 B6
82 62 0B 4F D9 53 7C 31 68 C2 CC 08 19 05 D2 B3

57. 75 94 F9 88 4B 09 42 24 87 56 AD 38 CC BF 84 B6
82 62 0B 4F D9 53 7C 31 71 C2 CC 08 19 05 D2 B3

58. 75 94 F9 88 4B 09 42 24 87 56 AD 38 CC BF 84 B6
82 62 0B 4F D9 53 7C 31 71 5F CC 08 19 05 D2 B3

59. 75 94 F9 88 4B 09 42 24 87 56 AD 38 CC BF 84 B6
82 62 0B 4F D9 53 7C 31 71 5F E8 08 19 05 D2 B3

60. 75 94 F9 88 4B 09 42 24 87 56 AD 38 CC BF 84 B6
82 62 0B 4F D9 53 7C 31 71 5F E8 DC 19 05 D2 B3

61. 75 94 F9 88 4B 09 42 24 87 56 AD 38 CC BF 84 B6
82 62 0B 4F D9 53 7C 31 71 5F E8 DC 3F 05 D2 B3

62. 75 94 F9 88 4B 09 42 24 87 56 AD 38 CC BF 84 B6
82 62 0B 4F D9 53 7C 31 71 5F E8 DC 3F 97 D2 B3

63. 75 94 F9 88 4B 09 42 24 87 56 AD 38 CC BF 84 B6
82 62 0B 4F D9 53 7C 31 71 5F E8 DC 3F 97 5D B3

64. 75 94 F9 88 4B 09 42 24 87 56 AD 38 CC BF 84 B6
82 62 0B 4F D9 53 7C 31 71 5F E8 DC 3F 97 5D 8F

65. 69 94 F9 88 4B 09 42 24 87 56 AD 38 CC BF 84 B6
82 62 0B 4F D9 53 7C 31 71 5F E8 DC 3F 97 5D 8F

66. 69 C9 F9 88 4B 09 42 24 87 56 AD 38 CC BF 84 B6
82 62 0B 4F D9 53 7C 31 71 5F E8 DC 3F 97 5D 8F

67. 69 C9 2F 88 4B 09 42 24 87 56 AD 38 CC BF 84 B6
82 62 0B 4F D9 53 7C 31 71 5F E8 DC 3F 97 5D 8F

68. 69 C9 2F 30 4B 09 42 24 87 56 AD 38 CC BF 84 B6
82 62 0B 4F D9 53 7C 31 71 5F E8 DC 3F 97 5D 8F

69. 69 C9 2F 30 25 09 42 24 87 56 AD 38 CC BF 84 B6
82 62 0B 4F D9 53 7C 31 71 5F E8 DC 3F 97 5D 8F

70. 69 C9 2F 30 25 55 42 24 87 56 AD 38 CC BF 84 B6
82 62 0B 4F D9 53 7C 31 71 5F E8 DC 3F 97 5D 8F

71. 69 C9 2F 30 25 55 01 24 87 56 AD 38 CC BF 84 B6
82 62 0B 4F D9 53 7C 31 71 5F E8 DC 3F 97 5D 8F

72. 69 C9 2F 30 25 55 01 B5 87 56 AD 38 CC BF 84 B6
82 62 0B 4F D9 53 7C 31 71 5F E8 DC 3F 97 5D 8F

73. 69 C9 2F 30 25 55 01 B5 C6 56 AD 38 CC BF 84 B6
82 62 0B 4F D9 53 7C 31 71 5F E8 DC 3F 97 5D 8F

74. 69 C9 2F 30 25 55 01 B5 C6 0B AD 38 CC BF 84 B6
82 62 0B 4F D9 53 7C 31 71 5F E8 DC 3F 97 5D 8F

75. 69 C9 2F 30 25 55 01 B5 C6 0B 4D 38 CC BF 84 B6
82 62 0B 4F D9 53 7C 31 71 5F E8 DC 3F 97 5D 8F

76. 69 C9 2F 30 25 55 01 B5 C6 0B 4D 62 CC BF 84 B6
82 62 0B 4F D9 53 7C 31 71 5F E8 DC 3F 97 5D 8F

77. 69 C9 2F 30 25 55 01 B5 C6 0B 4D 62 91 BF 84 B6
82 62 0B 4F D9 53 7C 31 71 5F E8 DC 3F 97 5D 8F

78. 69 C9 2F 30 25 55 01 B5 C6 0B 4D 62 91 48 84 B6
82 62 0B 4F D9 53 7C 31 71 5F E8 DC 3F 97 5D 8F

79. 69 C9 2F 30 25 55 01 B5 C6 0B 4D 62 91 48 29 B6
82 62 0B 4F D9 53 7C 31 71 5F E8 DC 3F 97 5D 8F

80. 69 C9 2F 30 25 55 01 B5 C6 0B 4D 62 91 48 29 9B
82 62 0B 4F D9 53 7C 31 71 5F E8 DC 3F 97 5D 8F

81. 69 C9 2F 30 25 55 01 B5 C6 0B 4D 62 91 48 29 9B
16 62 0B 4F D9 53 7C 31 71 5F E8 DC 3F 97 5D 8F

82. 69 C9 2F 30 25 55 01 B5 C6 0B 4D 62 91 48 29 9B
16 61 0B 4F D9 53 7C 31 71 5F E8 DC 3F 97 5D 8F

83. 69 C9 2F 30 25 55 01 B5 C6 0B 4D 62 91 48 29 9B
16 61 70 4F D9 53 7C 31 71 5F E8 DC 3F 97 5D 8F

84. 69 C9 2F 30 25 55 01 B5 C6 0B 4D 62 91 48 29 9B
16 61 70 01 D9 53 7C 31 71 5F E8 DC 3F 97 5D 8F

85. 69 C9 2F 30 25 55 01 B5 C6 0B 4D 62 91 48 29 9B
16 61 70 01 A7 53 7C 31 71 5F E8 DC 3F 97 5D 8F

86. 69 C9 2F 30 25 55 01 B5 C6 0B 4D 62 91 48 29 9B
16 61 70 01 A7 5B 7C 31 71 5F E8 DC 3F 97 5D 8F

87. 69 C9 2F 30 25 55 01 B5 C6 0B 4D 62 91 48 29 9B
16 61 70 01 A7 5B 88 31 71 5F E8 DC 3F 97 5D 8F

88. 69 C9 2F 30 25 55 01 B5 C6 0B 4D 62 91 48 29 9B
16 61 70 01 A7 5B 88 C2 71 5F E8 DC 3F 97 5D 8F

89. 69 C9 2F 30 25 55 01 B5 C6 0B 4D 62 91 48 29 9B
16 61 70 01 A7 5B 88 C2 67 5F E8 DC 3F 97 5D 8F

90. 69 C9 2F 30 25 55 01 B5 C6 0B 4D 62 91 48 29 9B
16 61 70 01 A7 5B 88 C2 67 27 E8 DC 3F 97 5D 8F

91. 69 C9 2F 30 25 55 01 B5 C6 0B 4D 62 91 48 29 9B
16 61 70 01 A7 5B 88 C2 67 27 49 DC 3F 97 5D 8F

92. 69 C9 2F 30 25 55 01 B5 C6 0B 4D 62 91 48 29 9B
16 61 70 01 A7 5B 88 C2 67 27 49 48 3F 97 5D 8F

93. 69 C9 2F 30 25 55 01 B5 C6 0B 4D 62 91 48 29 9B
16 61 70 01 A7 5B 88 C2 67 27 49 48 2F 97 5D 8F

94. 69 C9 2F 30 25 55 01 B5 C6 0B 4D 62 91 48 29 9B
16 61 70 01 A7 5B 88 C2 67 27 49 48 2F BF 5D 8F

95. 69 C9 2F 30 25 55 01 B5 C6 0B 4D 62 91 48 29 9B
16 61 70 01 A7 5B 88 C2 67 27 49 48 2F BF F9 8F

96. 69 C9 2F 30 25 55 01 B5 C6 0B 4D 62 91 48 29 9B
16 61 70 01 A7 5B 88 C2 67 27 49 48 2F BF F9 B5

97. 00 C9 2F 30 25 55 01 B5 C6 0B 4D 62 91 48 29 9B
16 61 70 01 A7 5B 88 C2 67 27 49 48 2F BF F9 B5

98. 00 C2 2F 30 25 55 01 B5 C6 0B 4D 62 91 48 29 9B
16 61 70 01 A7 5B 88 C2 67 27 49 48 2F BF F9 B5

99. 00 C2 9E 30 25 55 01 B5 C6 0B 4D 62 91 48 29 9B
16 61 70 01 A7 5B 88 C2 67 27 49 48 2F BF F9 B5

100. 00 C2 9E 33 25 55 01 B5 C6 0B 4D 62 91 48 29 9B
16 61 70 01 A7 5B 88 C2 67 27 49 48 2F BF F9 B5

101. 00 C2 9E 33 CD 55 01 B5 C6 0B 4D 62 91 48 29 9B
16 61 70 01 A7 5B 88 C2 67 27 49 48 2F BF F9 B5

102. 00 C2 9E 33 CD 6D 01 B5 C6 0B 4D 62 91 48 29 9B
16 61 70 01 A7 5B 88 C2 67 27 49 48 2F BF F9 B5

103. 00 C2 9E 33 CD 6D B3 B5 C6 0B 4D 62 91 48 29 9B
16 61 70 01 A7 5B 88 C2 67 27 49 48 2F BF F9 B5

104. 00 C2 9E 33 CD 6D B3 F8 C6 0B 4D 62 91 48 29 9B
16 61 70 01 A7 5B 88 C2 67 27 49 48 2F BF F9 B5

105. 00 C2 9E 33 CD 6D B3 F8 F0 0B 4D 62 91 48 29 9B
16 61 70 01 A7 5B 88 C2 67 27 49 48 2F BF F9 B5

106. 00 C2 9E 33 CD 6D B3 F8 F0 DA 4D 62 91 48 29 9B
16 61 70 01 A7 5B 88 C2 67 27 49 48 2F BF F9 B5

107. 00 C2 9E 33 CD 6D B3 F8 F0 DA 41 62 91 48 29 9B
16 61 70 01 A7 5B 88 C2 67 27 49 48 2F BF F9 B5

108. 00 C2 9E 33 CD 6D B3 F8 F0 DA 41 0D 91 48 29 9B
16 61 70 01 A7 5B 88 C2 67 27 49 48 2F BF F9 B5

109. 00 C2 9E 33 CD 6D B3 F8 F0 DA 41 0D 31 48 29 9B
16 61 70 01 A7 5B 88 C2 67 27 49 48 2F BF F9 B5

110. 00 C2 9E 33 CD 6D B3 F8 F0 DA 41 0D 31 36 29 9B
16 61 70 01 A7 5B 88 C2 67 27 49 48 2F BF F9 B5

111. 00 C2 9E 33 CD 6D B3 F8 F0 DA 41 0D 31 36 49 9B
16 61 70 01 A7 5B 88 C2 67 27 49 48 2F BF F9 B5

112. 00 C2 9E 33 CD 6D B3 F8 F0 DA 41 0D 31 36 49 60
16 61 70 01 A7 5B 88 C2 67 27 49 48 2F BF F9 B5

113. 00 C2 9E 33 CD 6D B3 F8 F0 DA 41 0D 31 36 49 60
4A 61 70 01 A7 5B 88 C2 67 27 49 48 2F BF F9 B5

114. 00 C2 9E 33 CD 6D B3 F8 F0 DA 41 0D 31 36 49 60
4A 79 70 01 A7 5B 88 C2 67 27 49 48 2F BF F9 B5

115. 00 C2 9E 33 CD 6D B3 F8 F0 DA 41 0D 31 36 49 60
4A 79 5D 01 A7 5B 88 C2 67 27 49 48 2F BF F9 B5

116. 00 C2 9E 33 CD 6D B3 F8 F0 DA 41 0D 31 36 49 60
4A 79 5D 78 A7 5B 88 C2 67 27 49 48 2F BF F9 B5

117. 00 C2 9E 33 CD 6D B3 F8 F0 DA 41 0D 31 36 49 60
4A 79 5D 78 BC 5B 88 C2 67 27 49 48 2F BF F9 B5

118. 00 C2 9E 33 CD 6D B3 F8 F0 DA 41 0D 31 36 49 60
4A 79 5D 78 BC 96 88 C2 67 27 49 48 2F BF F9 B5

119. 00 C2 9E 33 CD 6D B3 F8 F0 DA 41 0D 31 36 49 60
4A 79 5D 78 BC 96 58 C2 67 27 49 48 2F BF F9 B5

120. 00 C2 9E 33 CD 6D B3 F8 F0 DA 41 0D 31 36 49 60
4A 79 5D 78 BC 96 58 BA 67 27 49 48 2F BF F9 B5

121. 00 C2 9E 33 CD 6D B3 F8 F0 DA 41 0D 31 36 49 60
4A 79 5D 78 BC 96 58 BA DF 27 49 48 2F BF F9 B5

122. 00 C2 9E 33 CD 6D B3 F8 F0 DA 41 0D 31 36 49 60
4A 79 5D 78 BC 96 58 BA DF 7E 49 48 2F BF F9 B5

123. 00 C2 9E 33 CD 6D B3 F8 F0 DA 41 0D 31 36 49 60
4A 79 5D 78 BC 96 58 BA DF 7E 7F 48 2F BF F9 B5

124. 00 C2 9E 33 CD 6D B3 F8 F0 DA 41 0D 31 36 49 60
4A 79 5D 78 BC 96 58 BA DF 7E 7F 44 2F BF F9 B5

125. 00 C2 9E 33 CD 6D B3 F8 F0 DA 41 0D 31 36 49 60
4A 79 5D 78 BC 96 58 BA DF 7E 7F 44 C1 BF F9 B5

126. 00 C2 9E 33 CD 6D B3 F8 F0 DA 41 0D 31 36 49 60
4A 79 5D 78 BC 96 58 BA DF 7E 7F 44 C1 1E F9 B5

127. 00 C2 9E 33 CD 6D B3 F8 F0 DA 41 0D 31 36 49 60
4A 79 5D 78 BC 96 58 BA DF 7E 7F 44 C1 1E B1 B5

128. 00 C2 9E 33 CD 6D B3 F8 F0 DA 41 0D 31 36 49 60
4A 79 5D 78 BC 96 58 BA DF 7E 7F 44 C1 1E B1 6A

129. 96 C2 9E 33 CD 6D B3 F8 F0 DA 41 0D 31 36 49 60
4A 79 5D 78 BC 96 58 BA DF 7E 7F 44 C1 1E B1 6A

130. 96 89 9E 33 CD 6D B3 F8 F0 DA 41 0D 31 36 49 60
4A 79 5D 78 BC 96 58 BA DF 7E 7F 44 C1 1E B1 6A

131. 96 89 25 33 CD 6D B3 F8 F0 DA 41 0D 31 36 49 60
4A 79 5D 78 BC 96 58 BA DF 7E 7F 44 C1 1E B1 6A

132. 96 89 25 B7 CD 6D B3 F8 F0 DA 41 0D 31 36 49 60
4A 79 5D 78 BC 96 58 BA DF 7E 7F 44 C1 1E B1 6A

133. 96 89 25 B7 C8 6D B3 F8 F0 DA 41 0D 31 36 49 60
4A 79 5D 78 BC 96 58 BA DF 7E 7F 44 C1 1E B1 6A

134. 96 89 25 B7 C8 37 B3 F8 F0 DA 41 0D 31 36 49 60
4A 79 5D 78 BC 96 58 BA DF 7E 7F 44 C1 1E B1 6A

```
135.    96  89  25  B7  C8  37  E2  F8  F0  DA  41  0D  31  36  49  60
        4A  79  5D  78  BC  96  58  BA  DF  7E  7F  44  C1  1E  B1  6A

136.    96  89  25  B7  C8  37  E2  16  F0  DA  41  0D  31  36  49  60
        4A  79  5D  78  BC  96  58  BA  DF  7E  7F  44  C1  1E  B1  6A

137.    96  89  25  B7  C8  37  E2  16  F4  DA  41  0D  31  36  49  60
        4A  79  5D  78  BC  96  58  BA  DF  7E  7F  44  C1  1E  B1  6A

138.    96  89  25  B7  C8  37  E2  16  F4  11  41  0D  31  36  49  60
        4A  79  5D  78  BC  96  58  BA  DF  7E  7F  44  C1  1E  B1  6A

139.    96  89  25  B7  C8  37  E2  16  F4  11  D9  0D  31  36  49  60
        4A  79  5D  78  BC  96  58  BA  DF  7E  7F  44  C1  1E  B1  6A

140.    96  89  25  B7  C8  37  E2  16  F4  11  D9  28  31  36  49  60
        4A  79  5D  78  BC  96  58  BA  DF  7E  7F  44  C1  1E  B1  6A
```

Message digest:

```
        96  89  25  B7  C8  37  E2  16  F4  11  D9  28  31  36  49  60
        4A  79  5D  78  BC  96  58  BA  DF  7E  7F  44  C1  1E  B1  6A
```

8.3 Calculate message digest for 384 hash bit length

Let the message, *M*, be the 24-bit (l = 24) ASCII string "**abc**", which is equivalent to the following hex string: 61 62 63.
For this message digest calculation consist from:

12 steps for pre-hash computation;
192 steps for final hash computation.

Total: 204 steps.

This is SR states for all this steps. 0 – initial SR state.

Stage 1. Preprocessing

```
        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
```

Stage 2. Pre-hash computation – 12 steps

Input byte 61

```
1.      C8  01  02  03  04  05  06  07  08  09  0A  0B  0C  0D  0E  0F
        10  11  12  13  14  15  16  17  18  19  1A  1B  1C  1D  1E  1F
        20  21  22  23  24  25  26  27  28  29  2A  2B  2C  2D  2E  2F

2.      C8  03  02  03  04  05  06  07  08  09  0A  0B  0C  0D  0E  0F
        10  11  12  13  14  15  16  17  18  19  1A  1B  1C  1D  1E  1F
        20  21  22  23  24  25  26  27  28  29  2A  2B  2C  2D  2E  2F

3.      C8  03  DF  03  04  05  06  07  08  09  0A  0B  0C  0D  0E  0F
        10  11  12  13  14  15  16  17  18  19  1A  1B  1C  1D  1E  1F
        20  21  22  23  24  25  26  27  28  29  2A  2B  2C  2D  2E  2F
```

4. C8 03 DF FF 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

Input byte 62

5. C8 03 DF FF F1 05 06 07 08 09 0A 0B 0C 0D 0E 0F
10 11 12 13 14 15 16 17 18 19 1A 1B 1C 1D 1E 1F
20 21 22 23 24 25 26 27 28 29 2A 2B 2C 2D 2E 2F

6. C8 03 DF FF F1 73 06 07 08 09 0A 0B 0C 0D 0E 0F
10 11 12 13 14 15 16 17 18 19 1A 1B 1C 1D 1E 1F
20 21 22 23 24 25 26 27 28 29 2A 2B 2C 2D 2E 2F

7. C8 03 DF FF F1 73 47 07 08 09 0A 0B 0C 0D 0E 0F
10 11 12 13 14 15 16 17 18 19 1A 1B 1C 1D 1E 1F
20 21 22 23 24 25 26 27 28 29 2A 2B 2C 2D 2E 2F

8. C8 03 DF FF F1 73 47 EB 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

Input byte 63

9. C8 03 DF FF F1 73 47 EB 81 09 0A 0B 0C 0D 0E 0F
10 11 12 13 14 15 16 17 18 19 1A 1B 1C 1D 1E 1F
20 21 22 23 24 25 26 27 28 29 2A 2B 2C 2D 2E 2F

10. C8 03 DF FF F1 73 47 EB 81 7A 0A 0B 0C 0D 0E 0F
10 11 12 13 14 15 16 17 18 19 1A 1B 1C 1D 1E 1F
20 21 22 23 24 25 26 27 28 29 2A 2B 2C 2D 2E 2F

11. C8 03 DF FF F1 73 47 EB 81 7A 7D 0B 0C 0D 0E 0F
10 11 12 13 14 15 16 17 18 19 1A 1B 1C 1D 1E 1F
20 21 22 23 24 25 26 27 28 29 2A 2B 2C 2D 2E 2F

12. C8 03 DF FF F1 73 47 EB 81 7A 7D 6E 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

Stage 3. Final hash computation – 192 steps

13. C8 03 DF FF F1 73 47 EB 81 7A 7D 6E 06 0D 0E 0F
10 11 12 13 14 15 16 17 18 19 1A 1B 1C 1D 1E 1F
20 21 22 23 24 25 26 27 28 29 2A 2B 2C 2D 2E 2F

14. C8 03 DF FF F1 73 47 EB 81 7A 7D 6E 06 AF 0E 0F
10 11 12 13 14 15 16 17 18 19 1A 1B 1C 1D 1E 1F
20 21 22 23 24 25 26 27 28 29 2A 2B 2C 2D 2E 2F

15. C8 03 DF FF F1 73 47 EB 81 7A 7D 6E 06 AF 34 0F
10 11 12 13 14 15 16 17 18 19 1A 1B 1C 1D 1E 1F
20 21 22 23 24 25 26 27 28 29 2A 2B 2C 2D 2E 2F

16. C8 03 DF FF F1 73 47 EB 81 7A 7D 6E 06 AF 34 A7
10 11 12 13 14 15 16 17 18 19 1A 1B 1C 1D 1E 1F
20 21 22 23 24 25 26 27 28 29 2A 2B 2C 2D 2E 2F

17. C8 03 DF FF F1 73 47 EB 81 7A 7D 6E 06 AF 34 A7
C8 11 12 13 14 15 16 17 18 19 1A 1B 1C 1D 1E 1F
20 21 22 23 24 25 26 27 28 29 2A 2B 2C 2D 2E 2F

18. C8 03 DF FF F1 73 47 EB 81 7A 7D 6E 06 AF 34 A7
C8 69 12 13 14 15 16 17 18 19 1A 1B 1C 1D 1E 1F
20 21 22 23 24 25 26 27 28 29 2A 2B 2C 2D 2E 2F

19. C8 03 DF FF F1 73 47 EB 81 7A 7D 6E 06 AF 34 A7
C8 69 34 13 14 15 16 17 18 19 1A 1B 1C 1D 1E 1F
20 21 22 23 24 25 26 27 28 29 2A 2B 2C 2D 2E 2F

20. C8 03 DF FF F1 73 47 EB 81 7A 7D 6E 06 AF 34 A7
C8 69 34 4D 14 15 16 17 18 19 1A 1B 1C 1D 1E 1F
20 21 22 23 24 25 26 27 28 29 2A 2B 2C 2D 2E 2F

21. C8 03 DF FF F1 73 47 EB 81 7A 7D 6E 06 AF 34 A7
C8 69 34 4D F8 15 16 17 18 19 1A 1B 1C 1D 1E 1F
20 21 22 23 24 25 26 27 28 29 2A 2B 2C 2D 2E 2F

22. C8 03 DF FF F1 73 47 EB 81 7A 7D 6E 06 AF 34 A7
C8 69 34 4D F8 F0 16 17 18 19 1A 1B 1C 1D 1E 1F
20 21 22 23 24 25 26 27 28 29 2A 2B 2C 2D 2E 2F

23. C8 03 DF FF F1 73 47 EB 81 7A 7D 6E 06 AF 34 A7
C8 69 34 4D F8 F0 A8 17 18 19 1A 1B 1C 1D 1E 1F
20 21 22 23 24 25 26 27 28 29 2A 2B 2C 2D 2E 2F

24. C8 03 DF FF F1 73 47 EB 81 7A 7D 6E 06 AF 34 A7
C8 69 34 4D F8 F0 A8 95 18 19 1A 1B 1C 1D 1E 1F
20 21 22 23 24 25 26 27 28 29 2A 2B 2C 2D 2E 2F

25. C8 03 DF FF F1 73 47 EB 81 7A 7D 6E 06 AF 34 A7
C8 69 34 4D F8 F0 A8 95 80 19 1A 1B 1C 1D 1E 1F
20 21 22 23 24 25 26 27 28 29 2A 2B 2C 2D 2E 2F

26. C8 03 DF FF F1 73 47 EB 81 7A 7D 6E 06 AF 34 A7
C8 69 34 4D F8 F0 A8 95 80 D0 1A 1B 1C 1D 1E 1F
20 21 22 23 24 25 26 27 28 29 2A 2B 2C 2D 2E 2F

27. C8 03 DF FF F1 73 47 EB 81 7A 7D 6E 06 AF 34 A7
C8 69 34 4D F8 F0 A8 95 80 D0 7F 1B 1C 1D 1E 1F
20 21 22 23 24 25 26 27 28 29 2A 2B 2C 2D 2E 2F

28. C8 03 DF FF F1 73 47 EB 81 7A 7D 6E 06 AF 34 A7
C8 69 34 4D F8 F0 A8 95 80 D0 7F F5 1C 1D 1E 1F
20 21 22 23 24 25 26 27 28 29 2A 2B 2C 2D 2E 2F

29. C8 03 DF FF F1 73 47 EB 81 7A 7D 6E 06 AF 34 A7
C8 69 34 4D F8 F0 A8 95 80 D0 7F F5 E6 1D 1E 1F
20 21 22 23 24 25 26 27 28 29 2A 2B 2C 2D 2E 2F

30. C8 03 DF FF F1 73 47 EB 81 7A 7D 6E 06 AF 34 A7
C8 69 34 4D F8 F0 A8 95 80 D0 7F F5 E6 53 1E 1F
20 21 22 23 24 25 26 27 28 29 2A 2B 2C 2D 2E 2F

31. C8 03 DF FF F1 73 47 EB 81 7A 7D 6E 06 AF 34 A7
C8 69 34 4D F8 F0 A8 95 80 D0 7F F5 E6 53 40 1F
20 21 22 23 24 25 26 27 28 29 2A 2B 2C 2D 2E 2F

32. C8 03 DF FF F1 73 47 EB 81 7A 7D 6E 06 AF 34 A7
C8 69 34 4D F8 F0 A8 95 80 D0 7F F5 E6 53 40 0C
20 21 22 23 24 25 26 27 28 29 2A 2B 2C 2D 2E 2F

33. C8 03 DF FF F1 73 47 EB 81 7A 7D 6E 06 AF 34 A7
C8 69 34 4D F8 F0 A8 95 80 D0 7F F5 E6 53 40 0C
E6 21 22 23 24 25 26 27 28 29 2A 2B 2C 2D 2E 2F

34. C8 03 DF FF F1 73 47 EB 81 7A 7D 6E 06 AF 34 A7
C8 69 34 4D F8 F0 A8 95 80 D0 7F F5 E6 53 40 0C
E6 41 22 23 24 25 26 27 28 29 2A 2B 2C 2D 2E 2F

35. C8 03 DF FF F1 73 47 EB 81 7A 7D 6E 06 AF 34 A7

C8 69 34 4D F8 F0 A8 95 80 D0 7F F5 E6 53 40 0C
E6 41 46 23 24 25 26 27 28 29 2A 2B 2C 2D 2E 2F

36. C8 03 DF FF F1 73 47 EB 81 7A 7D 6E 06 AF 34 A7
C8 69 34 4D F8 F0 A8 95 80 D0 7F F5 E6 53 40 0C
E6 41 46 63 24 25 26 27 28 29 2A 2B 2C 2D 2E 2F

37. C8 03 DF FF F1 73 47 EB 81 7A 7D 6E 06 AF 34 A7
C8 69 34 4D F8 F0 A8 95 80 D0 7F F5 E6 53 40 0C
E6 41 46 63 0B 25 26 27 28 29 2A 2B 2C 2D 2E 2F

38. C8 03 DF FF F1 73 47 EB 81 7A 7D 6E 06 AF 34 A7
C8 69 34 4D F8 F0 A8 95 80 D0 7F F5 E6 53 40 0C
E6 41 46 63 0B 13 26 27 28 29 2A 2B 2C 2D 2E 2F

39. C8 03 DF FF F1 73 47 EB 81 7A 7D 6E 06 AF 34 A7
C8 69 34 4D F8 F0 A8 95 80 D0 7F F5 E6 53 40 0C
E6 41 46 63 0B 13 D3 27 28 29 2A 2B 2C 2D 2E 2F

40. C8 03 DF FF F1 73 47 EB 81 7A 7D 6E 06 AF 34 A7
C8 69 34 4D F8 F0 A8 95 80 D0 7F F5 E6 53 40 0C
E6 41 46 63 0B 13 D3 F8 28 29 2A 2B 2C 2D 2E 2F

41. C8 03 DF FF F1 73 47 EB 81 7A 7D 6E 06 AF 34 A7
C8 69 34 4D F8 F0 A8 95 80 D0 7F F5 E6 53 40 0C
E6 41 46 63 0B 13 D3 F8 5A 29 2A 2B 2C 2D 2E 2F

42. C8 03 DF FF F1 73 47 EB 81 7A 7D 6E 06 AF 34 A7
C8 69 34 4D F8 F0 A8 95 80 D0 7F F5 E6 53 40 0C
E6 41 46 63 0B 13 D3 F8 5A 77 2A 2B 2C 2D 2E 2F

43. C8 03 DF FF F1 73 47 EB 81 7A 7D 6E 06 AF 34 A7
C8 69 34 4D F8 F0 A8 95 80 D0 7F F5 E6 53 40 0C
E6 41 46 63 0B 13 D3 F8 5A 77 B0 2B 2C 2D 2E 2F

44. C8 03 DF FF F1 73 47 EB 81 7A 7D 6E 06 AF 34 A7
C8 69 34 4D F8 F0 A8 95 80 D0 7F F5 E6 53 40 0C
E6 41 46 63 0B 13 D3 F8 5A 77 B0 FF 2C 2D 2E 2F

45. C8 03 DF FF F1 73 47 EB 81 7A 7D 6E 06 AF 34 A7
C8 69 34 4D F8 F0 A8 95 80 D0 7F F5 E6 53 40 0C
E6 41 46 63 0B 13 D3 F8 5A 77 B0 FF 6F 2D 2E 2F

46. C8 03 DF FF F1 73 47 EB 81 7A 7D 6E 06 AF 34 A7
C8 69 34 4D F8 F0 A8 95 80 D0 7F F5 E6 53 40 0C
E6 41 46 63 0B 13 D3 F8 5A 77 B0 FF 6F 25 2E 2F

47. C8 03 DF FF F1 73 47 EB 81 7A 7D 6E 06 AF 34 A7
C8 69 34 4D F8 F0 A8 95 80 D0 7F F5 E6 53 40 0C
E6 41 46 63 0B 13 D3 F8 5A 77 B0 FF 6F 25 F8 2F

48. C8 03 DF FF F1 73 47 EB 81 7A 7D 6E 06 AF 34 A7
C8 69 34 4D F8 F0 A8 95 80 D0 7F F5 E6 53 40 0C
E6 41 46 63 0B 13 D3 F8 5A 77 B0 FF 6F 25 F8 5A

49. A4 03 DF FF F1 73 47 EB 81 7A 7D 6E 06 AF 34 A7
C8 69 34 4D F8 F0 A8 95 80 D0 7F F5 E6 53 40 0C
E6 41 46 63 0B 13 D3 F8 5A 77 B0 FF 6F 25 F8 5A

50. A4 B7 DF FF F1 73 47 EB 81 7A 7D 6E 06 AF 34 A7
C8 69 34 4D F8 F0 A8 95 80 D0 7F F5 E6 53 40 0C
E6 41 46 63 0B 13 D3 F8 5A 77 B0 FF 6F 25 F8 5A

51. A4 B7 2F FF F1 73 47 EB 81 7A 7D 6E 06 AF 34 A7
C8 69 34 4D F8 F0 A8 95 80 D0 7F F5 E6 53 40 0C
E6 41 46 63 0B 13 D3 F8 5A 77 B0 FF 6F 25 F8 5A

52. A4 B7 2F C6 F1 73 47 EB 81 7A 7D 6E 06 AF 34 A7
C8 69 34 4D F8 F0 A8 95 80 D0 7F F5 E6 53 40 0C
E6 41 46 63 0B 13 D3 F8 5A 77 B0 FF 6F 25 F8 5A

53. A4 B7 2F C6 FF 73 47 EB 81 7A 7D 6E 06 AF 34 A7
C8 69 34 4D F8 F0 A8 95 80 D0 7F F5 E6 53 40 0C
E6 41 46 63 0B 13 D3 F8 5A 77 B0 FF 6F 25 F8 5A

54. A4 B7 2F C6 FF FF 47 EB 81 7A 7D 6E 06 AF 34 A7
C8 69 34 4D F8 F0 A8 95 80 D0 7F F5 E6 53 40 0C
E6 41 46 63 0B 13 D3 F8 5A 77 B0 FF 6F 25 F8 5A

55. A4 B7 2F C6 FF FF 35 EB 81 7A 7D 6E 06 AF 34 A7
C8 69 34 4D F8 F0 A8 95 80 D0 7F F5 E6 53 40 0C
E6 41 46 63 0B 13 D3 F8 5A 77 B0 FF 6F 25 F8 5A

56. A4 B7 2F C6 FF FF 35 75 81 7A 7D 6E 06 AF 34 A7
C8 69 34 4D F8 F0 A8 95 80 D0 7F F5 E6 53 40 0C
E6 41 46 63 0B 13 D3 F8 5A 77 B0 FF 6F 25 F8 5A

57. A4 B7 2F C6 FF FF 35 75 C3 7A 7D 6E 06 AF 34 A7
C8 69 34 4D F8 F0 A8 95 80 D0 7F F5 E6 53 40 0C
E6 41 46 63 0B 13 D3 F8 5A 77 B0 FF 6F 25 F8 5A

58. A4 B7 2F C6 FF FF 35 75 C3 D7 7D 6E 06 AF 34 A7
C8 69 34 4D F8 F0 A8 95 80 D0 7F F5 E6 53 40 0C
E6 41 46 63 0B 13 D3 F8 5A 77 B0 FF 6F 25 F8 5A

59. A4 B7 2F C6 FF FF 35 75 C3 D7 E5 6E 06 AF 34 A7
C8 69 34 4D F8 F0 A8 95 80 D0 7F F5 E6 53 40 0C
E6 41 46 63 0B 13 D3 F8 5A 77 B0 FF 6F 25 F8 5A

60. A4 B7 2F C6 FF FF 35 75 C3 D7 E5 4C 06 AF 34 A7
C8 69 34 4D F8 F0 A8 95 80 D0 7F F5 E6 53 40 0C
E6 41 46 63 0B 13 D3 F8 5A 77 B0 FF 6F 25 F8 5A

61. A4 B7 2F C6 FF FF 35 75 C3 D7 E5 4C 49 AF 34 A7
C8 69 34 4D F8 F0 A8 95 80 D0 7F F5 E6 53 40 0C
E6 41 46 63 0B 13 D3 F8 5A 77 B0 FF 6F 25 F8 5A

62. A4 B7 2F C6 FF FF 35 75 C3 D7 E5 4C 49 76 34 A7
C8 69 34 4D F8 F0 A8 95 80 D0 7F F5 E6 53 40 0C
E6 41 46 63 0B 13 D3 F8 5A 77 B0 FF 6F 25 F8 5A

63. A4 B7 2F C6 FF FF 35 75 C3 D7 E5 4C 49 76 09 A7
C8 69 34 4D F8 F0 A8 95 80 D0 7F F5 E6 53 40 0C
E6 41 46 63 0B 13 D3 F8 5A 77 B0 FF 6F 25 F8 5A

64. A4 B7 2F C6 FF FF 35 75 C3 D7 E5 4C 49 76 09 73
C8 69 34 4D F8 F0 A8 95 80 D0 7F F5 E6 53 40 0C
E6 41 46 63 0B 13 D3 F8 5A 77 B0 FF 6F 25 F8 5A

65. A4 B7 2F C6 FF FF 35 75 C3 D7 E5 4C 49 76 09 73
10 69 34 4D F8 F0 A8 95 80 D0 7F F5 E6 53 40 0C
E6 41 46 63 0B 13 D3 F8 5A 77 B0 FF 6F 25 F8 5A

66. A4 B7 2F C6 FF FF 35 75 C3 D7 E5 4C 49 76 09 73
10 97 34 4D F8 F0 A8 95 80 D0 7F F5 E6 53 40 0C
E6 41 46 63 0B 13 D3 F8 5A 77 B0 FF 6F 25 F8 5A

67. A4 B7 2F C6 FF FF 35 75 C3 D7 E5 4C 49 76 09 73
10 97 68 4D F8 F0 A8 95 80 D0 7F F5 E6 53 40 0C
E6 41 46 63 0B 13 D3 F8 5A 77 B0 FF 6F 25 F8 5A

68. A4 B7 2F C6 FF FF 35 75 C3 D7 E5 4C 49 76 09 73

10 97 68 E4 F8 F0 A8 95 80 D0 7F F5 E6 53 40 0C
E6 41 46 63 0B 13 D3 F8 5A 77 B0 FF 6F 25 F8 5A

69. A4 B7 2F C6 FF FF 35 75 C3 D7 E5 4C 49 76 09 73
10 97 68 E4 96 F0 A8 95 80 D0 7F F5 E6 53 40 0C
E6 41 46 63 0B 13 D3 F8 5A 77 B0 FF 6F 25 F8 5A

70. A4 B7 2F C6 FF FF 35 75 C3 D7 E5 4C 49 76 09 73
10 97 68 E4 96 65 A8 95 80 D0 7F F5 E6 53 40 0C
E6 41 46 63 0B 13 D3 F8 5A 77 B0 FF 6F 25 F8 5A

71. A4 B7 2F C6 FF FF 35 75 C3 D7 E5 4C 49 76 09 73
10 97 68 E4 96 65 52 95 80 D0 7F F5 E6 53 40 0C
E6 41 46 63 0B 13 D3 F8 5A 77 B0 FF 6F 25 F8 5A

72. A4 B7 2F C6 FF FF 35 75 C3 D7 E5 4C 49 76 09 73
10 97 68 E4 96 65 52 88 80 D0 7F F5 E6 53 40 0C
E6 41 46 63 0B 13 D3 F8 5A 77 B0 FF 6F 25 F8 5A

73. A4 B7 2F C6 FF FF 35 75 C3 D7 E5 4C 49 76 09 73
10 97 68 E4 96 65 52 88 16 D0 7F F5 E6 53 40 0C
E6 41 46 63 0B 13 D3 F8 5A 77 B0 FF 6F 25 F8 5A

74. A4 B7 2F C6 FF FF 35 75 C3 D7 E5 4C 49 76 09 73
10 97 68 E4 96 65 52 88 16 74 7F F5 E6 53 40 0C
E6 41 46 63 0B 13 D3 F8 5A 77 B0 FF 6F 25 F8 5A

75. A4 B7 2F C6 FF FF 35 75 C3 D7 E5 4C 49 76 09 73
10 97 68 E4 96 65 52 88 16 74 20 F5 E6 53 40 0C
E6 41 46 63 0B 13 D3 F8 5A 77 B0 FF 6F 25 F8 5A

76. A4 B7 2F C6 FF FF 35 75 C3 D7 E5 4C 49 76 09 73
10 97 68 E4 96 65 52 88 16 74 20 E9 E6 53 40 0C
E6 41 46 63 0B 13 D3 F8 5A 77 B0 FF 6F 25 F8 5A

77. A4 B7 2F C6 FF FF 35 75 C3 D7 E5 4C 49 76 09 73
10 97 68 E4 96 65 52 88 16 74 20 E9 79 53 40 0C
E6 41 46 63 0B 13 D3 F8 5A 77 B0 FF 6F 25 F8 5A

78. A4 B7 2F C6 FF FF 35 75 C3 D7 E5 4C 49 76 09 73
10 97 68 E4 96 65 52 88 16 74 20 E9 79 07 40 0C
E6 41 46 63 0B 13 D3 F8 5A 77 B0 FF 6F 25 F8 5A

79. A4 B7 2F C6 FF FF 35 75 C3 D7 E5 4C 49 76 09 73
10 97 68 E4 96 65 52 88 16 74 20 E9 79 07 AB 0C
E6 41 46 63 0B 13 D3 F8 5A 77 B0 FF 6F 25 F8 5A

80. A4 B7 2F C6 FF FF 35 75 C3 D7 E5 4C 49 76 09 73
10 97 68 E4 96 65 52 88 16 74 20 E9 79 07 AB F1
E6 41 46 63 0B 13 D3 F8 5A 77 B0 FF 6F 25 F8 5A

81. A4 B7 2F C6 FF FF 35 75 C3 D7 E5 4C 49 76 09 73
10 97 68 E4 96 65 52 88 16 74 20 E9 79 07 AB F1
D0 41 46 63 0B 13 D3 F8 5A 77 B0 FF 6F 25 F8 5A

82. A4 B7 2F C6 FF FF 35 75 C3 D7 E5 4C 49 76 09 73
10 97 68 E4 96 65 52 88 16 74 20 E9 79 07 AB F1
D0 76 46 63 0B 13 D3 F8 5A 77 B0 FF 6F 25 F8 5A

83. A4 B7 2F C6 FF FF 35 75 C3 D7 E5 4C 49 76 09 73
10 97 68 E4 96 65 52 88 16 74 20 E9 79 07 AB F1
D0 76 69 63 0B 13 D3 F8 5A 77 B0 FF 6F 25 F8 5A

84. A4 B7 2F C6 FF FF 35 75 C3 D7 E5 4C 49 76 09 73
10 97 68 E4 96 65 52 88 16 74 20 E9 79 07 AB F1
D0 76 69 E8 0B 13 D3 F8 5A 77 B0 FF 6F 25 F8 5A

85. A4 B7 2F C6 FF FF 35 75 C3 D7 E5 4C 49 76 09 73
10 97 68 E4 96 65 52 88 16 74 20 E9 79 07 AB F1
D0 76 69 E8 ED 13 D3 F8 5A 77 B0 FF 6F 25 F8 5A

86. A4 B7 2F C6 FF FF 35 75 C3 D7 E5 4C 49 76 09 73
10 97 68 E4 96 65 52 88 16 74 20 E9 79 07 AB F1
D0 76 69 E8 ED F9 D3 F8 5A 77 B0 FF 6F 25 F8 5A

87. A4 B7 2F C6 FF FF 35 75 C3 D7 E5 4C 49 76 09 73
10 97 68 E4 96 65 52 88 16 74 20 E9 79 07 AB F1
D0 76 69 E8 ED F9 E1 F8 5A 77 B0 FF 6F 25 F8 5A

88. A4 B7 2F C6 FF FF 35 75 C3 D7 E5 4C 49 76 09 73
10 97 68 E4 96 65 52 88 16 74 20 E9 79 07 AB F1
D0 76 69 E8 ED F9 E1 71 5A 77 B0 FF 6F 25 F8 5A

89. A4 B7 2F C6 FF FF 35 75 C3 D7 E5 4C 49 76 09 73
10 97 68 E4 96 65 52 88 16 74 20 E9 79 07 AB F1
D0 76 69 E8 ED F9 E1 71 E0 77 B0 FF 6F 25 F8 5A

90. A4 B7 2F C6 FF FF 35 75 C3 D7 E5 4C 49 76 09 73
10 97 68 E4 96 65 52 88 16 74 20 E9 79 07 AB F1
D0 76 69 E8 ED F9 E1 71 E0 70 B0 FF 6F 25 F8 5A

91. A4 B7 2F C6 FF FF 35 75 C3 D7 E5 4C 49 76 09 73
10 97 68 E4 96 65 52 88 16 74 20 E9 79 07 AB F1
D0 76 69 E8 ED F9 E1 71 E0 70 D6 FF 6F 25 F8 5A

92. A4 B7 2F C6 FF FF 35 75 C3 D7 E5 4C 49 76 09 73
10 97 68 E4 96 65 52 88 16 74 20 E9 79 07 AB F1
D0 76 69 E8 ED F9 E1 71 E0 70 D6 83 6F 25 F8 5A

93. A4 B7 2F C6 FF FF 35 75 C3 D7 E5 4C 49 76 09 73
10 97 68 E4 96 65 52 88 16 74 20 E9 79 07 AB F1
D0 76 69 E8 ED F9 E1 71 E0 70 D6 83 93 25 F8 5A

94. A4 B7 2F C6 FF FF 35 75 C3 D7 E5 4C 49 76 09 73
10 97 68 E4 96 65 52 88 16 74 20 E9 79 07 AB F1
D0 76 69 E8 ED F9 E1 71 E0 70 D6 83 93 F1 F8 5A

95. A4 B7 2F C6 FF FF 35 75 C3 D7 E5 4C 49 76 09 73
10 97 68 E4 96 65 52 88 16 74 20 E9 79 07 AB F1
D0 76 69 E8 ED F9 E1 71 E0 70 D6 83 93 F1 C6 5A

96. A4 B7 2F C6 FF FF 35 75 C3 D7 E5 4C 49 76 09 73
10 97 68 E4 96 65 52 88 16 74 20 E9 79 07 AB F1
D0 76 69 E8 ED F9 E1 71 E0 70 D6 83 93 F1 C6 41

97. 3A B7 2F C6 FF FF 35 75 C3 D7 E5 4C 49 76 09 73
10 97 68 E4 96 65 52 88 16 74 20 E9 79 07 AB F1
D0 76 69 E8 ED F9 E1 71 E0 70 D6 83 93 F1 C6 41

98. 3A 2C 2F C6 FF FF 35 75 C3 D7 E5 4C 49 76 09 73
10 97 68 E4 96 65 52 88 16 74 20 E9 79 07 AB F1
D0 76 69 E8 ED F9 E1 71 E0 70 D6 83 93 F1 C6 41

99. 3A 2C 4A C6 FF FF 35 75 C3 D7 E5 4C 49 76 09 73
10 97 68 E4 96 65 52 88 16 74 20 E9 79 07 AB F1
D0 76 69 E8 ED F9 E1 71 E0 70 D6 83 93 F1 C6 41

100. 3A 2C 4A F8 FF FF 35 75 C3 D7 E5 4C 49 76 09 73
10 97 68 E4 96 65 52 88 16 74 20 E9 79 07 AB F1
D0 76 69 E8 ED F9 E1 71 E0 70 D6 83 93 F1 C6 41

101. 3A 2C 4A F8 94 FF 35 75 C3 D7 E5 4C 49 76 09 73

10 97 68 E4 96 65 52 88 16 74 20 E9 79 07 AB F1
D0 76 69 E8 ED F9 E1 71 E0 70 D6 83 93 F1 C6 41

102. 3A 2C 4A F8 94 A6 35 75 C3 D7 E5 4C 49 76 09 73
10 97 68 E4 96 65 52 88 16 74 20 E9 79 07 AB F1
D0 76 69 E8 ED F9 E1 71 E0 70 D6 83 93 F1 C6 41

103. 3A 2C 4A F8 94 A6 BB 75 C3 D7 E5 4C 49 76 09 73
10 97 68 E4 96 65 52 88 16 74 20 E9 79 07 AB F1
D0 76 69 E8 ED F9 E1 71 E0 70 D6 83 93 F1 C6 41

104. 3A 2C 4A F8 94 A6 BB 4C C3 D7 E5 4C 49 76 09 73
10 97 68 E4 96 65 52 88 16 74 20 E9 79 07 AB F1
D0 76 69 E8 ED F9 E1 71 E0 70 D6 83 93 F1 C6 41

105. 3A 2C 4A F8 94 A6 BB 4C 7B D7 E5 4C 49 76 09 73
10 97 68 E4 96 65 52 88 16 74 20 E9 79 07 AB F1
D0 76 69 E8 ED F9 E1 71 E0 70 D6 83 93 F1 C6 41

106. 3A 2C 4A F8 94 A6 BB 4C 7B 40 E5 4C 49 76 09 73
10 97 68 E4 96 65 52 88 16 74 20 E9 79 07 AB F1
D0 76 69 E8 ED F9 E1 71 E0 70 D6 83 93 F1 C6 41

107. 3A 2C 4A F8 94 A6 BB 4C 7B 40 58 4C 49 76 09 73
10 97 68 E4 96 65 52 88 16 74 20 E9 79 07 AB F1
D0 76 69 E8 ED F9 E1 71 E0 70 D6 83 93 F1 C6 41

108. 3A 2C 4A F8 94 A6 BB 4C 7B 40 58 E5 49 76 09 73
10 97 68 E4 96 65 52 88 16 74 20 E9 79 07 AB F1
D0 76 69 E8 ED F9 E1 71 E0 70 D6 83 93 F1 C6 41

109. 3A 2C 4A F8 94 A6 BB 4C 7B 40 58 E5 89 76 09 73
10 97 68 E4 96 65 52 88 16 74 20 E9 79 07 AB F1
D0 76 69 E8 ED F9 E1 71 E0 70 D6 83 93 F1 C6 41

110. 3A 2C 4A F8 94 A6 BB 4C 7B 40 58 E5 89 B2 09 73
10 97 68 E4 96 65 52 88 16 74 20 E9 79 07 AB F1
D0 76 69 E8 ED F9 E1 71 E0 70 D6 83 93 F1 C6 41

111. 3A 2C 4A F8 94 A6 BB 4C 7B 40 58 E5 89 B2 A4 73
10 97 68 E4 96 65 52 88 16 74 20 E9 79 07 AB F1
D0 76 69 E8 ED F9 E1 71 E0 70 D6 83 93 F1 C6 41

112. 3A 2C 4A F8 94 A6 BB 4C 7B 40 58 E5 89 B2 A4 56
10 97 68 E4 96 65 52 88 16 74 20 E9 79 07 AB F1
D0 76 69 E8 ED F9 E1 71 E0 70 D6 83 93 F1 C6 41

113. 3A 2C 4A F8 94 A6 BB 4C 7B 40 58 E5 89 B2 A4 56
4B 97 68 E4 96 65 52 88 16 74 20 E9 79 07 AB F1
D0 76 69 E8 ED F9 E1 71 E0 70 D6 83 93 F1 C6 41

114. 3A 2C 4A F8 94 A6 BB 4C 7B 40 58 E5 89 B2 A4 56
4B FB 68 E4 96 65 52 88 16 74 20 E9 79 07 AB F1
D0 76 69 E8 ED F9 E1 71 E0 70 D6 83 93 F1 C6 41

115. 3A 2C 4A F8 94 A6 BB 4C 7B 40 58 E5 89 B2 A4 56
4B FB F4 E4 96 65 52 88 16 74 20 E9 79 07 AB F1
D0 76 69 E8 ED F9 E1 71 E0 70 D6 83 93 F1 C6 41

116. 3A 2C 4A F8 94 A6 BB 4C 7B 40 58 E5 89 B2 A4 56
4B FB F4 29 96 65 52 88 16 74 20 E9 79 07 AB F1
D0 76 69 E8 ED F9 E1 71 E0 70 D6 83 93 F1 C6 41

117. 3A 2C 4A F8 94 A6 BB 4C 7B 40 58 E5 89 B2 A4 56
4B FB F4 29 37 65 52 88 16 74 20 E9 79 07 AB F1
D0 76 69 E8 ED F9 E1 71 E0 70 D6 83 93 F1 C6 41

118. 3A 2C 4A F8 94 A6 BB 4C 7B 40 58 E5 89 B2 A4 56
4B FB F4 29 37 80 52 88 16 74 20 E9 79 07 AB F1
D0 76 69 E8 ED F9 E1 71 E0 70 D6 83 93 F1 C6 41

119. 3A 2C 4A F8 94 A6 BB 4C 7B 40 58 E5 89 B2 A4 56
4B FB F4 29 37 80 71 88 16 74 20 E9 79 07 AB F1
D0 76 69 E8 ED F9 E1 71 E0 70 D6 83 93 F1 C6 41

120. 3A 2C 4A F8 94 A6 BB 4C 7B 40 58 E5 89 B2 A4 56
4B FB F4 29 37 80 71 82 16 74 20 E9 79 07 AB F1
D0 76 69 E8 ED F9 E1 71 E0 70 D6 83 93 F1 C6 41

121. 3A 2C 4A F8 94 A6 BB 4C 7B 40 58 E5 89 B2 A4 56
4B FB F4 29 37 80 71 82 7F 74 20 E9 79 07 AB F1
D0 76 69 E8 ED F9 E1 71 E0 70 D6 83 93 F1 C6 41

122. 3A 2C 4A F8 94 A6 BB 4C 7B 40 58 E5 89 B2 A4 56
4B FB F4 29 37 80 71 82 7F CB 20 E9 79 07 AB F1
D0 76 69 E8 ED F9 E1 71 E0 70 D6 83 93 F1 C6 41

123. 3A 2C 4A F8 94 A6 BB 4C 7B 40 58 E5 89 B2 A4 56
4B FB F4 29 37 80 71 82 7F CB 7C E9 79 07 AB F1
D0 76 69 E8 ED F9 E1 71 E0 70 D6 83 93 F1 C6 41

124. 3A 2C 4A F8 94 A6 BB 4C 7B 40 58 E5 89 B2 A4 56
4B FB F4 29 37 80 71 82 7F CB 7C 94 79 07 AB F1
D0 76 69 E8 ED F9 E1 71 E0 70 D6 83 93 F1 C6 41

125. 3A 2C 4A F8 94 A6 BB 4C 7B 40 58 E5 89 B2 A4 56
4B FB F4 29 37 80 71 82 7F CB 7C 94 61 07 AB F1
D0 76 69 E8 ED F9 E1 71 E0 70 D6 83 93 F1 C6 41

126. 3A 2C 4A F8 94 A6 BB 4C 7B 40 58 E5 89 B2 A4 56
4B FB F4 29 37 80 71 82 7F CB 7C 94 61 01 AB F1
D0 76 69 E8 ED F9 E1 71 E0 70 D6 83 93 F1 C6 41

127. 3A 2C 4A F8 94 A6 BB 4C 7B 40 58 E5 89 B2 A4 56
4B FB F4 29 37 80 71 82 7F CB 7C 94 61 01 FB F1
D0 76 69 E8 ED F9 E1 71 E0 70 D6 83 93 F1 C6 41

128. 3A 2C 4A F8 94 A6 BB 4C 7B 40 58 E5 89 B2 A4 56
4B FB F4 29 37 80 71 82 7F CB 7C 94 61 01 FB CD
D0 76 69 E8 ED F9 E1 71 E0 70 D6 83 93 F1 C6 41

129. 3A 2C 4A F8 94 A6 BB 4C 7B 40 58 E5 89 B2 A4 56
4B FB F4 29 37 80 71 82 7F CB 7C 94 61 01 FB CD
E2 76 69 E8 ED F9 E1 71 E0 70 D6 83 93 F1 C6 41

130. 3A 2C 4A F8 94 A6 BB 4C 7B 40 58 E5 89 B2 A4 56
4B FB F4 29 37 80 71 82 7F CB 7C 94 61 01 FB CD
E2 26 69 E8 ED F9 E1 71 E0 70 D6 83 93 F1 C6 41

131. 3A 2C 4A F8 94 A6 BB 4C 7B 40 58 E5 89 B2 A4 56
4B FB F4 29 37 80 71 82 7F CB 7C 94 61 01 FB CD
E2 26 28 E8 ED F9 E1 71 E0 70 D6 83 93 F1 C6 41

132. 3A 2C 4A F8 94 A6 BB 4C 7B 40 58 E5 89 B2 A4 56
4B FB F4 29 37 80 71 82 7F CB 7C 94 61 01 FB CD
E2 26 28 0B ED F9 E1 71 E0 70 D6 83 93 F1 C6 41

133. 3A 2C 4A F8 94 A6 BB 4C 7B 40 58 E5 89 B2 A4 56
4B FB F4 29 37 80 71 82 7F CB 7C 94 61 01 FB CD
E2 26 28 0B D4 F9 E1 71 E0 70 D6 83 93 F1 C6 41

134. 3A 2C 4A F8 94 A6 BB 4C 7B 40 58 E5 89 B2 A4 56

4B FB F4 29 37 80 71 82 7F CB 7C 94 61 01 FB CD
E2 26 28 0B D4 E7 E1 71 E0 70 D6 83 93 F1 C6 41

135. 3A 2C 4A F8 94 A6 BB 4C 7B 40 58 E5 89 B2 A4 56
4B FB F4 29 37 80 71 82 7F CB 7C 94 61 01 FB CD
E2 26 28 0B D4 E7 50 71 E0 70 D6 83 93 F1 C6 41

136. 3A 2C 4A F8 94 A6 BB 4C 7B 40 58 E5 89 B2 A4 56
4B FB F4 29 37 80 71 82 7F CB 7C 94 61 01 FB CD
E2 26 28 0B D4 E7 50 32 E0 70 D6 83 93 F1 C6 41

137. 3A 2C 4A F8 94 A6 BB 4C 7B 40 58 E5 89 B2 A4 56
4B FB F4 29 37 80 71 82 7F CB 7C 94 61 01 FB CD
E2 26 28 0B D4 E7 50 32 67 70 D6 83 93 F1 C6 41

138. 3A 2C 4A F8 94 A6 BB 4C 7B 40 58 E5 89 B2 A4 56
4B FB F4 29 37 80 71 82 7F CB 7C 94 61 01 FB CD
E2 26 28 0B D4 E7 50 32 67 0B D6 83 93 F1 C6 41

139. 3A 2C 4A F8 94 A6 BB 4C 7B 40 58 E5 89 B2 A4 56
4B FB F4 29 37 80 71 82 7F CB 7C 94 61 01 FB CD
E2 26 28 0B D4 E7 50 32 67 0B 1C 83 93 F1 C6 41

140. 3A 2C 4A F8 94 A6 BB 4C 7B 40 58 E5 89 B2 A4 56
4B FB F4 29 37 80 71 82 7F CB 7C 94 61 01 FB CD
E2 26 28 0B D4 E7 50 32 67 0B 1C E5 93 F1 C6 41

141. 3A 2C 4A F8 94 A6 BB 4C 7B 40 58 E5 89 B2 A4 56
4B FB F4 29 37 80 71 82 7F CB 7C 94 61 01 FB CD
E2 26 28 0B D4 E7 50 32 67 0B 1C E5 C1 F1 C6 41

142. 3A 2C 4A F8 94 A6 BB 4C 7B 40 58 E5 89 B2 A4 56
4B FB F4 29 37 80 71 82 7F CB 7C 94 61 01 FB CD
E2 26 28 0B D4 E7 50 32 67 0B 1C E5 C1 65 C6 41

143. 3A 2C 4A F8 94 A6 BB 4C 7B 40 58 E5 89 B2 A4 56
4B FB F4 29 37 80 71 82 7F CB 7C 94 61 01 FB CD
E2 26 28 0B D4 E7 50 32 67 0B 1C E5 C1 65 6D 41

144. 3A 2C 4A F8 94 A6 BB 4C 7B 40 58 E5 89 B2 A4 56
4B FB F4 29 37 80 71 82 7F CB 7C 94 61 01 FB CD
E2 26 28 0B D4 E7 50 32 67 0B 1C E5 C1 65 6D E6

145. 1F 2C 4A F8 94 A6 BB 4C 7B 40 58 E5 89 B2 A4 56
4B FB F4 29 37 80 71 82 7F CB 7C 94 61 01 FB CD
E2 26 28 0B D4 E7 50 32 67 0B 1C E5 C1 65 6D E6

146. 1F 99 4A F8 94 A6 BB 4C 7B 40 58 E5 89 B2 A4 56
4B FB F4 29 37 80 71 82 7F CB 7C 94 61 01 FB CD
E2 26 28 0B D4 E7 50 32 67 0B 1C E5 C1 65 6D E6

147. 1F 99 B4 F8 94 A6 BB 4C 7B 40 58 E5 89 B2 A4 56
4B FB F4 29 37 80 71 82 7F CB 7C 94 61 01 FB CD
E2 26 28 0B D4 E7 50 32 67 0B 1C E5 C1 65 6D E6

148. 1F 99 B4 A4 94 A6 BB 4C 7B 40 58 E5 89 B2 A4 56
4B FB F4 29 37 80 71 82 7F CB 7C 94 61 01 FB CD
E2 26 28 0B D4 E7 50 32 67 0B 1C E5 C1 65 6D E6

149. 1F 99 B4 A4 24 A6 BB 4C 7B 40 58 E5 89 B2 A4 56
4B FB F4 29 37 80 71 82 7F CB 7C 94 61 01 FB CD
E2 26 28 0B D4 E7 50 32 67 0B 1C E5 C1 65 6D E6

150. 1F 99 B4 A4 24 C1 BB 4C 7B 40 58 E5 89 B2 A4 56
4B FB F4 29 37 80 71 82 7F CB 7C 94 61 01 FB CD
E2 26 28 0B D4 E7 50 32 67 0B 1C E5 C1 65 6D E6

151. 1F 99 B4 A4 24 C1 1D 4C 7B 40 58 E5 89 B2 A4 56
4B FB F4 29 37 80 71 82 7F CB 7C 94 61 01 FB CD
E2 26 28 0B D4 E7 50 32 67 0B 1C E5 C1 65 6D E6

152. 1F 99 B4 A4 24 C1 1D 24 7B 40 58 E5 89 B2 A4 56
4B FB F4 29 37 80 71 82 7F CB 7C 94 61 01 FB CD
E2 26 28 0B D4 E7 50 32 67 0B 1C E5 C1 65 6D E6

153. 1F 99 B4 A4 24 C1 1D 24 0F 40 58 E5 89 B2 A4 56
4B FB F4 29 37 80 71 82 7F CB 7C 94 61 01 FB CD
E2 26 28 0B D4 E7 50 32 67 0B 1C E5 C1 65 6D E6

154. 1F 99 B4 A4 24 C1 1D 24 0F BC 58 E5 89 B2 A4 56
4B FB F4 29 37 80 71 82 7F CB 7C 94 61 01 FB CD
E2 26 28 0B D4 E7 50 32 67 0B 1C E5 C1 65 6D E6

155. 1F 99 B4 A4 24 C1 1D 24 0F BC 51 E5 89 B2 A4 56
4B FB F4 29 37 80 71 82 7F CB 7C 94 61 01 FB CD
E2 26 28 0B D4 E7 50 32 67 0B 1C E5 C1 65 6D E6

156. 1F 99 B4 A4 24 C1 1D 24 0F BC 51 4E 89 B2 A4 56
4B FB F4 29 37 80 71 82 7F CB 7C 94 61 01 FB CD
E2 26 28 0B D4 E7 50 32 67 0B 1C E5 C1 65 6D E6

157. 1F 99 B4 A4 24 C1 1D 24 0F BC 51 4E BF B2 A4 56
4B FB F4 29 37 80 71 82 7F CB 7C 94 61 01 FB CD
E2 26 28 0B D4 E7 50 32 67 0B 1C E5 C1 65 6D E6

158. 1F 99 B4 A4 24 C1 1D 24 0F BC 51 4E BF 9F A4 56
4B FB F4 29 37 80 71 82 7F CB 7C 94 61 01 FB CD
E2 26 28 0B D4 E7 50 32 67 0B 1C E5 C1 65 6D E6

159. 1F 99 B4 A4 24 C1 1D 24 0F BC 51 4E BF 9F 53 56
4B FB F4 29 37 80 71 82 7F CB 7C 94 61 01 FB CD
E2 26 28 0B D4 E7 50 32 67 0B 1C E5 C1 65 6D E6

160. 1F 99 B4 A4 24 C1 1D 24 0F BC 51 4E BF 9F 53 D4
4B FB F4 29 37 80 71 82 7F CB 7C 94 61 01 FB CD
E2 26 28 0B D4 E7 50 32 67 0B 1C E5 C1 65 6D E6

161. 1F 99 B4 A4 24 C1 1D 24 0F BC 51 4E BF 9F 53 D4
6C FB F4 29 37 80 71 82 7F CB 7C 94 61 01 FB CD
E2 26 28 0B D4 E7 50 32 67 0B 1C E5 C1 65 6D E6

162. 1F 99 B4 A4 24 C1 1D 24 0F BC 51 4E BF 9F 53 D4
6C 52 F4 29 37 80 71 82 7F CB 7C 94 61 01 FB CD
E2 26 28 0B D4 E7 50 32 67 0B 1C E5 C1 65 6D E6

163. 1F 99 B4 A4 24 C1 1D 24 0F BC 51 4E BF 9F 53 D4
6C 52 A0 29 37 80 71 82 7F CB 7C 94 61 01 FB CD
E2 26 28 0B D4 E7 50 32 67 0B 1C E5 C1 65 6D E6

164. 1F 99 B4 A4 24 C1 1D 24 0F BC 51 4E BF 9F 53 D4
6C 52 A0 57 37 80 71 82 7F CB 7C 94 61 01 FB CD
E2 26 28 0B D4 E7 50 32 67 0B 1C E5 C1 65 6D E6

165. 1F 99 B4 A4 24 C1 1D 24 0F BC 51 4E BF 9F 53 D4
6C 52 A0 57 8B 80 71 82 7F CB 7C 94 61 01 FB CD
E2 26 28 0B D4 E7 50 32 67 0B 1C E5 C1 65 6D E6

166. 1F 99 B4 A4 24 C1 1D 24 0F BC 51 4E BF 9F 53 D4
6C 52 A0 57 8B C7 71 82 7F CB 7C 94 61 01 FB CD
E2 26 28 0B D4 E7 50 32 67 0B 1C E5 C1 65 6D E6

167. 1F 99 B4 A4 24 C1 1D 24 0F BC 51 4E BF 9F 53 D4

```
      6C 52 A0 57 8B C7 74 82 7F CB 7C 94 61 01 FB CD
      E2 26 28 0B D4 E7 50 32 67 0B 1C E5 C1 65 6D E6

168.  1F 99 B4 A4 24 C1 1D 24 0F BC 51 4E BF 9F 53 D4
      6C 52 A0 57 8B C7 74 0F 7F CB 7C 94 61 01 FB CD
      E2 26 28 0B D4 E7 50 32 67 0B 1C E5 C1 65 6D E6

169.  1F 99 B4 A4 24 C1 1D 24 0F BC 51 4E BF 9F 53 D4
      6C 52 A0 57 8B C7 74 0F CC CB 7C 94 61 01 FB CD
      E2 26 28 0B D4 E7 50 32 67 0B 1C E5 C1 65 6D E6

170.  1F 99 B4 A4 24 C1 1D 24 0F BC 51 4E BF 9F 53 D4
      6C 52 A0 57 8B C7 74 0F CC 73 7C 94 61 01 FB CD
      E2 26 28 0B D4 E7 50 32 67 0B 1C E5 C1 65 6D E6

171.  1F 99 B4 A4 24 C1 1D 24 0F BC 51 4E BF 9F 53 D4
      6C 52 A0 57 8B C7 74 0F CC 73 90 94 61 01 FB CD
      E2 26 28 0B D4 E7 50 32 67 0B 1C E5 C1 65 6D E6

172.  1F 99 B4 A4 24 C1 1D 24 0F BC 51 4E BF 9F 53 D4
      6C 52 A0 57 8B C7 74 0F CC 73 90 00 61 01 FB CD
      E2 26 28 0B D4 E7 50 32 67 0B 1C E5 C1 65 6D E6

173.  1F 99 B4 A4 24 C1 1D 24 0F BC 51 4E BF 9F 53 D4
      6C 52 A0 57 8B C7 74 0F CC 73 90 00 4A 01 FB CD
      E2 26 28 0B D4 E7 50 32 67 0B 1C E5 C1 65 6D E6

174.  1F 99 B4 A4 24 C1 1D 24 0F BC 51 4E BF 9F 53 D4
      6C 52 A0 57 8B C7 74 0F CC 73 90 00 4A 2A FB CD
      E2 26 28 0B D4 E7 50 32 67 0B 1C E5 C1 65 6D E6

175.  1F 99 B4 A4 24 C1 1D 24 0F BC 51 4E BF 9F 53 D4
      6C 52 A0 57 8B C7 74 0F CC 73 90 00 4A 2A 9A CD
      E2 26 28 0B D4 E7 50 32 67 0B 1C E5 C1 65 6D E6

176.  1F 99 B4 A4 24 C1 1D 24 0F BC 51 4E BF 9F 53 D4
      6C 52 A0 57 8B C7 74 0F CC 73 90 00 4A 2A 9A 4B
      E2 26 28 0B D4 E7 50 32 67 0B 1C E5 C1 65 6D E6

177.  1F 99 B4 A4 24 C1 1D 24 0F BC 51 4E BF 9F 53 D4
      6C 52 A0 57 8B C7 74 0F CC 73 90 00 4A 2A 9A 4B
      E0 26 28 0B D4 E7 50 32 67 0B 1C E5 C1 65 6D E6

178.  1F 99 B4 A4 24 C1 1D 24 0F BC 51 4E BF 9F 53 D4
      6C 52 A0 57 8B C7 74 0F CC 73 90 00 4A 2A 9A 4B
      E0 06 28 0B D4 E7 50 32 67 0B 1C E5 C1 65 6D E6

179.  1F 99 B4 A4 24 C1 1D 24 0F BC 51 4E BF 9F 53 D4
      6C 52 A0 57 8B C7 74 0F CC 73 90 00 4A 2A 9A 4B
      E0 06 35 0B D4 E7 50 32 67 0B 1C E5 C1 65 6D E6

180.  1F 99 B4 A4 24 C1 1D 24 0F BC 51 4E BF 9F 53 D4
      6C 52 A0 57 8B C7 74 0F CC 73 90 00 4A 2A 9A 4B
      E0 06 35 B7 D4 E7 50 32 67 0B 1C E5 C1 65 6D E6

181.  1F 99 B4 A4 24 C1 1D 24 0F BC 51 4E BF 9F 53 D4
      6C 52 A0 57 8B C7 74 0F CC 73 90 00 4A 2A 9A 4B
      E0 06 35 B7 79 E7 50 32 67 0B 1C E5 C1 65 6D E6

182.  1F 99 B4 A4 24 C1 1D 24 0F BC 51 4E BF 9F 53 D4
      6C 52 A0 57 8B C7 74 0F CC 73 90 00 4A 2A 9A 4B
      E0 06 35 B7 79 31 50 32 67 0B 1C E5 C1 65 6D E6

183.  1F 99 B4 A4 24 C1 1D 24 0F BC 51 4E BF 9F 53 D4
      6C 52 A0 57 8B C7 74 0F CC 73 90 00 4A 2A 9A 4B
      E0 06 35 B7 79 31 08 32 67 0B 1C E5 C1 65 6D E6
```

184. 1F 99 B4 A4 24 C1 1D 24 0F BC 51 4E BF 9F 53 D4
6C 52 A0 57 8B C7 74 0F CC 73 90 00 4A 2A 9A 4B
E0 06 35 B7 79 31 08 AC 67 0B 1C E5 C1 65 6D E6

185. 1F 99 B4 A4 24 C1 1D 24 0F BC 51 4E BF 9F 53 D4
6C 52 A0 57 8B C7 74 0F CC 73 90 00 4A 2A 9A 4B
E0 06 35 B7 79 31 08 AC DF 0B 1C E5 C1 65 6D E6

186. 1F 99 B4 A4 24 C1 1D 24 0F BC 51 4E BF 9F 53 D4
6C 52 A0 57 8B C7 74 0F CC 73 90 00 4A 2A 9A 4B
E0 06 35 B7 79 31 08 AC DF 75 1C E5 C1 65 6D E6

187. 1F 99 B4 A4 24 C1 1D 24 0F BC 51 4E BF 9F 53 D4
6C 52 A0 57 8B C7 74 0F CC 73 90 00 4A 2A 9A 4B
E0 06 35 B7 79 31 08 AC DF 75 6D E5 C1 65 6D E6

188. 1F 99 B4 A4 24 C1 1D 24 0F BC 51 4E BF 9F 53 D4
6C 52 A0 57 8B C7 74 0F CC 73 90 00 4A 2A 9A 4B
E0 06 35 B7 79 31 08 AC DF 75 6D 9D C1 65 6D E6

189. 1F 99 B4 A4 24 C1 1D 24 0F BC 51 4E BF 9F 53 D4
6C 52 A0 57 8B C7 74 0F CC 73 90 00 4A 2A 9A 4B
E0 06 35 B7 79 31 08 AC DF 75 6D 9D 0E 65 6D E6

190. 1F 99 B4 A4 24 C1 1D 24 0F BC 51 4E BF 9F 53 D4
6C 52 A0 57 8B C7 74 0F CC 73 90 00 4A 2A 9A 4B
E0 06 35 B7 79 31 08 AC DF 75 6D 9D 0E 8F 6D E6

191. 1F 99 B4 A4 24 C1 1D 24 0F BC 51 4E BF 9F 53 D4
6C 52 A0 57 8B C7 74 0F CC 73 90 00 4A 2A 9A 4B
E0 06 35 B7 79 31 08 AC DF 75 6D 9D 0E 8F EB E6

192. 1F 99 B4 A4 24 C1 1D 24 0F BC 51 4E BF 9F 53 D4
6C 52 A0 57 8B C7 74 0F CC 73 90 00 4A 2A 9A 4B
E0 06 35 B7 79 31 08 AC DF 75 6D 9D 0E 8F EB 65

193. 3D 99 B4 A4 24 C1 1D 24 0F BC 51 4E BF 9F 53 D4
6C 52 A0 57 8B C7 74 0F CC 73 90 00 4A 2A 9A 4B
E0 06 35 B7 79 31 08 AC DF 75 6D 9D 0E 8F EB 65

194. 3D 6C B4 A4 24 C1 1D 24 0F BC 51 4E BF 9F 53 D4
6C 52 A0 57 8B C7 74 0F CC 73 90 00 4A 2A 9A 4B
E0 06 35 B7 79 31 08 AC DF 75 6D 9D 0E 8F EB 65

195. 3D 6C 94 A4 24 C1 1D 24 0F BC 51 4E BF 9F 53 D4
6C 52 A0 57 8B C7 74 0F CC 73 90 00 4A 2A 9A 4B
E0 06 35 B7 79 31 08 AC DF 75 6D 9D 0E 8F EB 65

196. 3D 6C 94 26 24 C1 1D 24 0F BC 51 4E BF 9F 53 D4
6C 52 A0 57 8B C7 74 0F CC 73 90 00 4A 2A 9A 4B
E0 06 35 B7 79 31 08 AC DF 75 6D 9D 0E 8F EB 65

197. 3D 6C 94 26 65 C1 1D 24 0F BC 51 4E BF 9F 53 D4
6C 52 A0 57 8B C7 74 0F CC 73 90 00 4A 2A 9A 4B
E0 06 35 B7 79 31 08 AC DF 75 6D 9D 0E 8F EB 65

198. 3D 6C 94 26 65 81 1D 24 0F BC 51 4E BF 9F 53 D4
6C 52 A0 57 8B C7 74 0F CC 73 90 00 4A 2A 9A 4B
E0 06 35 B7 79 31 08 AC DF 75 6D 9D 0E 8F EB 65

199. 3D 6C 94 26 65 81 FE 24 0F BC 51 4E BF 9F 53 D4
6C 52 A0 57 8B C7 74 0F CC 73 90 00 4A 2A 9A 4B
E0 06 35 B7 79 31 08 AC DF 75 6D 9D 0E 8F EB 65

200. 3D 6C 94 26 65 81 FE 9E 0F BC 51 4E BF 9F 53 D4

```
        6C  52  A0  57  8B  C7  74  0F  CC  73  90  00  4A  2A  9A  4B
        E0  06  35  B7  79  31  08  AC  DF  75  6D  9D  0E  8F  EB  65

201.    3D  6C  94  26  65  81  FE  9E  8E  BC  51  4E  BF  9F  53  D4
        6C  52  A0  57  8B  C7  74  0F  CC  73  90  00  4A  2A  9A  4B
        E0  06  35  B7  79  31  08  AC  DF  75  6D  9D  0E  8F  EB  65

202.    3D  6C  94  26  65  81  FE  9E  8E  5F  51  4E  BF  9F  53  D4
        6C  52  A0  57  8B  C7  74  0F  CC  73  90  00  4A  2A  9A  4B
        E0  06  35  B7  79  31  08  AC  DF  75  6D  9D  0E  8F  EB  65

203.    3D  6C  94  26  65  81  FE  9E  8E  5F  06  4E  BF  9F  53  D4
        6C  52  A0  57  8B  C7  74  0F  CC  73  90  00  4A  2A  9A  4B
        E0  06  35  B7  79  31  08  AC  DF  75  6D  9D  0E  8F  EB  65

204.    3D  6C  94  26  65  81  FE  9E  8E  5F  06  33  BF  9F  53  D4
        6C  52  A0  57  8B  C7  74  0F  CC  73  90  00  4A  2A  9A  4B
        E0  06  35  B7  79  31  08  AC  DF  75  6D  9D  0E  8F  EB  65
```

Message digest:

```
        3D  6C  94  26  65  81  FE  9E  8E  5F  06  33  BF  9F  53  D4
        6C  52  A0  57  8B  C7  74  0F  CC  73  90  00  4A  2A  9A  4B
        E0  06  35  B7  79  31  08  AC  DF  75  6D  9D  0E  8F  EB  65
```

8.4 Calculate message digest for 512 hash bit length

Let the message, *M*, be the 24-bit (l = 24) ASCII string "**abc**", which is equivalent to the following hex string: 61 62 63.
For this message digest calculation consist from:

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

Total: 268 steps.

This is SR states for all this steps. 0 – initial SR state.

Stage 1. Preprocessing

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

Stage 2. Pre-hash computation – 12 steps

Input byte 61

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

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

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

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

Input byte 62

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

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

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

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

Input byte 63

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

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

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

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

Stage 3. Final hash computation – 256 steps

13. C8 22 9F 54 0E 2D 89 ED 98 85 E5 04 8F 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. C8 22 9F 54 0E 2D 89 ED 98 85 E5 04 8F 2F 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.
C8 22 9F 54 0E 2D 89 ED 98 85 E5 04 8F 2F C8 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.
C8 22 9F 54 0E 2D 89 ED 98 85 E5 04 8F 2F C8 D8
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.
C8 22 9F 54 0E 2D 89 ED 98 85 E5 04 8F 2F C8 D8
5B 11 12 13 14 15 16 17 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.
C8 22 9F 54 0E 2D 89 ED 98 85 E5 04 8F 2F C8 D8
5B 09 12 13 14 15 16 17 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.
C8 22 9F 54 0E 2D 89 ED 98 85 E5 04 8F 2F C8 D8
5B 09 41 13 14 15 16 17 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.
C8 22 9F 54 0E 2D 89 ED 98 85 E5 04 8F 2F C8 D8
5B 09 41 DF 14 15 16 17 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.
C8 22 9F 54 0E 2D 89 ED 98 85 E5 04 8F 2F C8 D8
5B 09 41 DF B2 15 16 17 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.
C8 22 9F 54 0E 2D 89 ED 98 85 E5 04 8F 2F C8 D8
5B 09 41 DF B2 11 16 17 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.
C8 22 9F 54 0E 2D 89 ED 98 85 E5 04 8F 2F C8 D8
5B 09 41 DF B2 11 09 17 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.
C8 22 9F 54 0E 2D 89 ED 98 85 E5 04 8F 2F C8 D8
5B 09 41 DF B2 11 09 CF 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.
C8 22 9F 54 0E 2D 89 ED 98 85 E5 04 8F 2F C8 D8
5B 09 41 DF B2 11 09 CF 9D 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.
C8 22 9F 54 0E 2D 89 ED 98 85 E5 04 8F 2F C8 D8
5B 09 41 DF B2 11 09 CF 9D B9 1A 1B 1C 1D 1E 1F
20 21 22 23 24 25 26 27 28 29 2A 2B 2C 2D 2E 2F
30 31 32 33 34 35 36 37 38 39 3A 3B 3C 3D 3E 3F

27.
C8 22 9F 54 0E 2D 89 ED 98 85 E5 04 8F 2F C8 D8
5B 09 41 DF B2 11 09 CF 9D B9 0D 1B 1C 1D 1E 1F
20 21 22 23 24 25 26 27 28 29 2A 2B 2C 2D 2E 2F
30 31 32 33 34 35 36 37 38 39 3A 3B 3C 3D 3E 3F

28.
C8 22 9F 54 0E 2D 89 ED 98 85 E5 04 8F 2F C8 D8

```
    5B 09 41 DF B2 11 09 CF 9D B9 0D D0 1C 1D 1E 1F
    20 21 22 23 24 25 26 27 28 29 2A 2B 2C 2D 2E 2F
    30 31 32 33 34 35 36 37 38 39 3A 3B 3C 3D 3E 3F

29. C8 22 9F 54 0E 2D 89 ED 98 85 E5 04 8F 2F C8 D8
    5B 09 41 DF B2 11 09 CF 9D B9 0D D0 8D 1D 1E 1F
    20 21 22 23 24 25 26 27 28 29 2A 2B 2C 2D 2E 2F
    30 31 32 33 34 35 36 37 38 39 3A 3B 3C 3D 3E 3F

30. C8 22 9F 54 0E 2D 89 ED 98 85 E5 04 8F 2F C8 D8
    5B 09 41 DF B2 11 09 CF 9D B9 0D D0 8D 3F 1E 1F
    20 21 22 23 24 25 26 27 28 29 2A 2B 2C 2D 2E 2F
    30 31 32 33 34 35 36 37 38 39 3A 3B 3C 3D 3E 3F

31. C8 22 9F 54 0E 2D 89 ED 98 85 E5 04 8F 2F C8 D8
    5B 09 41 DF B2 11 09 CF 9D B9 0D D0 8D 3F 67 1F
    20 21 22 23 24 25 26 27 28 29 2A 2B 2C 2D 2E 2F
    30 31 32 33 34 35 36 37 38 39 3A 3B 3C 3D 3E 3F

32. C8 22 9F 54 0E 2D 89 ED 98 85 E5 04 8F 2F C8 D8
    5B 09 41 DF B2 11 09 CF 9D B9 0D D0 8D 3F 67 2E
    20 21 22 23 24 25 26 27 28 29 2A 2B 2C 2D 2E 2F
    30 31 32 33 34 35 36 37 38 39 3A 3B 3C 3D 3E 3F

33. C8 22 9F 54 0E 2D 89 ED 98 85 E5 04 8F 2F C8 D8
    5B 09 41 DF B2 11 09 CF 9D B9 0D D0 8D 3F 67 2E
    EB 21 22 23 24 25 26 27 28 29 2A 2B 2C 2D 2E 2F
    30 31 32 33 34 35 36 37 38 39 3A 3B 3C 3D 3E 3F

34. C8 22 9F 54 0E 2D 89 ED 98 85 E5 04 8F 2F C8 D8
    5B 09 41 DF B2 11 09 CF 9D B9 0D D0 8D 3F 67 2E
    EB 50 22 23 24 25 26 27 28 29 2A 2B 2C 2D 2E 2F
    30 31 32 33 34 35 36 37 38 39 3A 3B 3C 3D 3E 3F

35. C8 22 9F 54 0E 2D 89 ED 98 85 E5 04 8F 2F C8 D8
    5B 09 41 DF B2 11 09 CF 9D B9 0D D0 8D 3F 67 2E
    EB 50 F4 23 24 25 26 27 28 29 2A 2B 2C 2D 2E 2F
    30 31 32 33 34 35 36 37 38 39 3A 3B 3C 3D 3E 3F

36. C8 22 9F 54 0E 2D 89 ED 98 85 E5 04 8F 2F C8 D8
    5B 09 41 DF B2 11 09 CF 9D B9 0D D0 8D 3F 67 2E
    EB 50 F4 BF 24 25 26 27 28 29 2A 2B 2C 2D 2E 2F
    30 31 32 33 34 35 36 37 38 39 3A 3B 3C 3D 3E 3F

37. C8 22 9F 54 0E 2D 89 ED 98 85 E5 04 8F 2F C8 D8
    5B 09 41 DF B2 11 09 CF 9D B9 0D D0 8D 3F 67 2E
    EB 50 F4 BF 46 25 26 27 28 29 2A 2B 2C 2D 2E 2F
    30 31 32 33 34 35 36 37 38 39 3A 3B 3C 3D 3E 3F

38. C8 22 9F 54 0E 2D 89 ED 98 85 E5 04 8F 2F C8 D8
    5B 09 41 DF B2 11 09 CF 9D B9 0D D0 8D 3F 67 2E
    EB 50 F4 BF 46 7D 26 27 28 29 2A 2B 2C 2D 2E 2F
    30 31 32 33 34 35 36 37 38 39 3A 3B 3C 3D 3E 3F

39. C8 22 9F 54 0E 2D 89 ED 98 85 E5 04 8F 2F C8 D8
    5B 09 41 DF B2 11 09 CF 9D B9 0D D0 8D 3F 67 2E
    EB 50 F4 BF 46 7D D4 27 28 29 2A 2B 2C 2D 2E 2F
    30 31 32 33 34 35 36 37 38 39 3A 3B 3C 3D 3E 3F

40. C8 22 9F 54 0E 2D 89 ED 98 85 E5 04 8F 2F C8 D8
    5B 09 41 DF B2 11 09 CF 9D B9 0D D0 8D 3F 67 2E
    EB 50 F4 BF 46 7D D4 6D 28 29 2A 2B 2C 2D 2E 2F
    30 31 32 33 34 35 36 37 38 39 3A 3B 3C 3D 3E 3F

41. C8 22 9F 54 0E 2D 89 ED 98 85 E5 04 8F 2F C8 D8
    5B 09 41 DF B2 11 09 CF 9D B9 0D D0 8D 3F 67 2E
```

EB 50 F4 BF 46 7D D4 6D 08 29 2A 2B 2C 2D 2E 2F
30 31 32 33 34 35 36 37 38 39 3A 3B 3C 3D 3E 3F

42. C8 22 9F 54 0E 2D 89 ED 98 85 E5 04 8F 2F C8 D8
5B 09 41 DF B2 11 09 CF 9D B9 0D D0 8D 3F 67 2E
EB 50 F4 BF 46 7D D4 6D 08 3F 2A 2B 2C 2D 2E 2F
30 31 32 33 34 35 36 37 38 39 3A 3B 3C 3D 3E 3F

43. C8 22 9F 54 0E 2D 89 ED 98 85 E5 04 8F 2F C8 D8
5B 09 41 DF B2 11 09 CF 9D B9 0D D0 8D 3F 67 2E
EB 50 F4 BF 46 7D D4 6D 08 3F A3 2B 2C 2D 2E 2F
30 31 32 33 34 35 36 37 38 39 3A 3B 3C 3D 3E 3F

44. C8 22 9F 54 0E 2D 89 ED 98 85 E5 04 8F 2F C8 D8
5B 09 41 DF B2 11 09 CF 9D B9 0D D0 8D 3F 67 2E
EB 50 F4 BF 46 7D D4 6D 08 3F A3 A2 2C 2D 2E 2F
30 31 32 33 34 35 36 37 38 39 3A 3B 3C 3D 3E 3F

45. C8 22 9F 54 0E 2D 89 ED 98 85 E5 04 8F 2F C8 D8
5B 09 41 DF B2 11 09 CF 9D B9 0D D0 8D 3F 67 2E
EB 50 F4 BF 46 7D D4 6D 08 3F A3 A2 7D 2D 2E 2F
30 31 32 33 34 35 36 37 38 39 3A 3B 3C 3D 3E 3F

46. C8 22 9F 54 0E 2D 89 ED 98 85 E5 04 8F 2F C8 D8
5B 09 41 DF B2 11 09 CF 9D B9 0D D0 8D 3F 67 2E
EB 50 F4 BF 46 7D D4 6D 08 3F A3 A2 7D E2 2E 2F
30 31 32 33 34 35 36 37 38 39 3A 3B 3C 3D 3E 3F

47. C8 22 9F 54 0E 2D 89 ED 98 85 E5 04 8F 2F C8 D8
5B 09 41 DF B2 11 09 CF 9D B9 0D D0 8D 3F 67 2E
EB 50 F4 BF 46 7D D4 6D 08 3F A3 A2 7D E2 F5 2F
30 31 32 33 34 35 36 37 38 39 3A 3B 3C 3D 3E 3F

48. C8 22 9F 54 0E 2D 89 ED 98 85 E5 04 8F 2F C8 D8
5B 09 41 DF B2 11 09 CF 9D B9 0D D0 8D 3F 67 2E
EB 50 F4 BF 46 7D D4 6D 08 3F A3 A2 7D E2 F5 C8
30 31 32 33 34 35 36 37 38 39 3A 3B 3C 3D 3E 3F

49. C8 22 9F 54 0E 2D 89 ED 98 85 E5 04 8F 2F C8 D8
5B 09 41 DF B2 11 09 CF 9D B9 0D D0 8D 3F 67 2E
EB 50 F4 BF 46 7D D4 6D 08 3F A3 A2 7D E2 F5 C8
1D 31 32 33 34 35 36 37 38 39 3A 3B 3C 3D 3E 3F

50. C8 22 9F 54 0E 2D 89 ED 98 85 E5 04 8F 2F C8 D8
5B 09 41 DF B2 11 09 CF 9D B9 0D D0 8D 3F 67 2E
EB 50 F4 BF 46 7D D4 6D 08 3F A3 A2 7D E2 F5 C8
1D 2D 32 33 34 35 36 37 38 39 3A 3B 3C 3D 3E 3F

51. C8 22 9F 54 0E 2D 89 ED 98 85 E5 04 8F 2F C8 D8
5B 09 41 DF B2 11 09 CF 9D B9 0D D0 8D 3F 67 2E
EB 50 F4 BF 46 7D D4 6D 08 3F A3 A2 7D E2 F5 C8
1D 2D 57 33 34 35 36 37 38 39 3A 3B 3C 3D 3E 3F

52. C8 22 9F 54 0E 2D 89 ED 98 85 E5 04 8F 2F C8 D8
5B 09 41 DF B2 11 09 CF 9D B9 0D D0 8D 3F 67 2E
EB 50 F4 BF 46 7D D4 6D 08 3F A3 A2 7D E2 F5 C8
1D 2D 57 9D 34 35 36 37 38 39 3A 3B 3C 3D 3E 3F

53. C8 22 9F 54 0E 2D 89 ED 98 85 E5 04 8F 2F C8 D8
5B 09 41 DF B2 11 09 CF 9D B9 0D D0 8D 3F 67 2E
EB 50 F4 BF 46 7D D4 6D 08 3F A3 A2 7D E2 F5 C8
1D 2D 57 9D 57 35 36 37 38 39 3A 3B 3C 3D 3E 3F

54. C8 22 9F 54 0E 2D 89 ED 98 85 E5 04 8F 2F C8 D8
5B 09 41 DF B2 11 09 CF 9D B9 0D D0 8D 3F 67 2E
EB 50 F4 BF 46 7D D4 6D 08 3F A3 A2 7D E2 F5 C8

	1D	2D	57	9D	57	F4	36	37	38	39	3A	3B	3C	3D	3E	3F
55.	C8	22	9F	54	0E	2D	89	ED	98	85	E5	04	8F	2F	C8	D8
	5B	09	41	DF	B2	11	09	CF	9D	B9	0D	D0	8D	3F	67	2E
	EB	50	F4	BF	46	7D	D4	6D	08	3F	A3	A2	7D	E2	F5	C8
	1D	2D	57	9D	57	F4	9E	37	38	39	3A	3B	3C	3D	3E	3F
56.	C8	22	9F	54	0E	2D	89	ED	98	85	E5	04	8F	2F	C8	D8
	5B	09	41	DF	B2	11	09	CF	9D	B9	0D	D0	8D	3F	67	2E
	EB	50	F4	BF	46	7D	D4	6D	08	3F	A3	A2	7D	E2	F5	C8
	1D	2D	57	9D	57	F4	9E	5B	38	39	3A	3B	3C	3D	3E	3F
57.	C8	22	9F	54	0E	2D	89	ED	98	85	E5	04	8F	2F	C8	D8
	5B	09	41	DF	B2	11	09	CF	9D	B9	0D	D0	8D	3F	67	2E
	EB	50	F4	BF	46	7D	D4	6D	08	3F	A3	A2	7D	E2	F5	C8
	1D	2D	57	9D	57	F4	9E	5B	E1	39	3A	3B	3C	3D	3E	3F
58.	C8	22	9F	54	0E	2D	89	ED	98	85	E5	04	8F	2F	C8	D8
	5B	09	41	DF	B2	11	09	CF	9D	B9	0D	D0	8D	3F	67	2E
	EB	50	F4	BF	46	7D	D4	6D	08	3F	A3	A2	7D	E2	F5	C8
	1D	2D	57	9D	57	F4	9E	5B	E1	6B	3A	3B	3C	3D	3E	3F
59.	C8	22	9F	54	0E	2D	89	ED	98	85	E5	04	8F	2F	C8	D8
	5B	09	41	DF	B2	11	09	CF	9D	B9	0D	D0	8D	3F	67	2E
	EB	50	F4	BF	46	7D	D4	6D	08	3F	A3	A2	7D	E2	F5	C8
	1D	2D	57	9D	57	F4	9E	5B	E1	6B	E7	3B	3C	3D	3E	3F
60.	C8	22	9F	54	0E	2D	89	ED	98	85	E5	04	8F	2F	C8	D8
	5B	09	41	DF	B2	11	09	CF	9D	B9	0D	D0	8D	3F	67	2E
	EB	50	F4	BF	46	7D	D4	6D	08	3F	A3	A2	7D	E2	F5	C8
	1D	2D	57	9D	57	F4	9E	5B	E1	6B	E7	DB	3C	3D	3E	3F
61.	C8	22	9F	54	0E	2D	89	ED	98	85	E5	04	8F	2F	C8	D8
	5B	09	41	DF	B2	11	09	CF	9D	B9	0D	D0	8D	3F	67	2E
	EB	50	F4	BF	46	7D	D4	6D	08	3F	A3	A2	7D	E2	F5	C8
	1D	2D	57	9D	57	F4	9E	5B	E1	6B	E7	DB	4E	3D	3E	3F
62.	C8	22	9F	54	0E	2D	89	ED	98	85	E5	04	8F	2F	C8	D8
	5B	09	41	DF	B2	11	09	CF	9D	B9	0D	D0	8D	3F	67	2E
	EB	50	F4	BF	46	7D	D4	6D	08	3F	A3	A2	7D	E2	F5	C8
	1D	2D	57	9D	57	F4	9E	5B	E1	6B	E7	DB	4E	3D	3E	3F
63.	C8	22	9F	54	0E	2D	89	ED	98	85	E5	04	8F	2F	C8	D8
	5B	09	41	DF	B2	11	09	CF	9D	B9	0D	D0	8D	3F	67	2E
	EB	50	F4	BF	46	7D	D4	6D	08	3F	A3	A2	7D	E2	F5	C8
	1D	2D	57	9D	57	F4	9E	5B	E1	6B	E7	DB	4E	3D	C2	3F
64.	C8	22	9F	54	0E	2D	89	ED	98	85	E5	04	8F	2F	C8	D8
	5B	09	41	DF	B2	11	09	CF	9D	B9	0D	D0	8D	3F	67	2E
	EB	50	F4	BF	46	7D	D4	6D	08	3F	A3	A2	7D	E2	F5	C8
	1D	2D	57	9D	57	F4	9E	5B	E1	6B	E7	DB	4E	3D	C2	9B
65.	A1	22	9F	54	0E	2D	89	ED	98	85	E5	04	8F	2F	C8	D8
	5B	09	41	DF	B2	11	09	CF	9D	B9	0D	D0	8D	3F	67	2E
	EB	50	F4	BF	46	7D	D4	6D	08	3F	A3	A2	7D	E2	F5	C8
	1D	2D	57	9D	57	F4	9E	5B	E1	6B	E7	DB	4E	3D	C2	9B
66.	A1	B7	9F	54	0E	2D	89	ED	98	85	E5	04	8F	2F	C8	D8
	5B	09	41	DF	B2	11	09	CF	9D	B9	0D	D0	8D	3F	67	2E
	EB	50	F4	BF	46	7D	D4	6D	08	3F	A3	A2	7D	E2	F5	C8
	1D	2D	57	9D	57	F4	9E	5B	E1	6B	E7	DB	4E	3D	C2	9B
67.	A1	B7	EE	54	0E	2D	89	ED	98	85	E5	04	8F	2F	C8	D8
	5B	09	41	DF	B2	11	09	CF	9D	B9	0D	D0	8D	3F	67	2E
	EB	50	F4	BF	46	7D	D4	6D	08	3F	A3	A2	7D	E2	F5	C8
	1D	2D	57	9D	57	F4	9E	5B	E1	6B	E7	DB	4E	3D	C2	9B

68.
A1 B7 EE 94 0E 2D 89 ED 98 85 E5 04 8F 2F C8 D8
5B 09 41 DF B2 11 09 CF 9D B9 0D D0 8D 3F 67 2E
EB 50 F4 BF 46 7D D4 6D 08 3F A3 A2 7D E2 F5 C8
1D 2D 57 9D 57 F4 9E 5B E1 6B E7 DB 4E 3D C2 9B

69.
A1 B7 EE 94 17 2D 89 ED 98 85 E5 04 8F 2F C8 D8
5B 09 41 DF B2 11 09 CF 9D B9 0D D0 8D 3F 67 2E
EB 50 F4 BF 46 7D D4 6D 08 3F A3 A2 7D E2 F5 C8
1D 2D 57 9D 57 F4 9E 5B E1 6B E7 DB 4E 3D C2 9B

70.
A1 B7 EE 94 17 7C 89 ED 98 85 E5 04 8F 2F C8 D8
5B 09 41 DF B2 11 09 CF 9D B9 0D D0 8D 3F 67 2E
EB 50 F4 BF 46 7D D4 6D 08 3F A3 A2 7D E2 F5 C8
1D 2D 57 9D 57 F4 9E 5B E1 6B E7 DB 4E 3D C2 9B

71.
A1 B7 EE 94 17 7C 7B ED 98 85 E5 04 8F 2F C8 D8
5B 09 41 DF B2 11 09 CF 9D B9 0D D0 8D 3F 67 2E
EB 50 F4 BF 46 7D D4 6D 08 3F A3 A2 7D E2 F5 C8
1D 2D 57 9D 57 F4 9E 5B E1 6B E7 DB 4E 3D C2 9B

72.
A1 B7 EE 94 17 7C 7B D8 98 85 E5 04 8F 2F C8 D8
5B 09 41 DF B2 11 09 CF 9D B9 0D D0 8D 3F 67 2E
EB 50 F4 BF 46 7D D4 6D 08 3F A3 A2 7D E2 F5 C8
1D 2D 57 9D 57 F4 9E 5B E1 6B E7 DB 4E 3D C2 9B

73.
A1 B7 EE 94 17 7C 7B D8 1B 85 E5 04 8F 2F C8 D8
5B 09 41 DF B2 11 09 CF 9D B9 0D D0 8D 3F 67 2E
EB 50 F4 BF 46 7D D4 6D 08 3F A3 A2 7D E2 F5 C8
1D 2D 57 9D 57 F4 9E 5B E1 6B E7 DB 4E 3D C2 9B

74.
A1 B7 EE 94 17 7C 7B D8 1B 26 E5 04 8F 2F C8 D8
5B 09 41 DF B2 11 09 CF 9D B9 0D D0 8D 3F 67 2E
EB 50 F4 BF 46 7D D4 6D 08 3F A3 A2 7D E2 F5 C8
1D 2D 57 9D 57 F4 9E 5B E1 6B E7 DB 4E 3D C2 9B

75.
A1 B7 EE 94 17 7C 7B D8 1B 26 A0 04 8F 2F C8 D8
5B 09 41 DF B2 11 09 CF 9D B9 0D D0 8D 3F 67 2E
EB 50 F4 BF 46 7D D4 6D 08 3F A3 A2 7D E2 F5 C8
1D 2D 57 9D 57 F4 9E 5B E1 6B E7 DB 4E 3D C2 9B

76.
A1 B7 EE 94 17 7C 7B D8 1B 26 A0 00 8F 2F C8 D8
5B 09 41 DF B2 11 09 CF 9D B9 0D D0 8D 3F 67 2E
EB 50 F4 BF 46 7D D4 6D 08 3F A3 A2 7D E2 F5 C8
1D 2D 57 9D 57 F4 9E 5B E1 6B E7 DB 4E 3D C2 9B

77.
A1 B7 EE 94 17 7C 7B D8 1B 26 A0 00 38 2F C8 D8
5B 09 41 DF B2 11 09 CF 9D B9 0D D0 8D 3F 67 2E
EB 50 F4 BF 46 7D D4 6D 08 3F A3 A2 7D E2 F5 C8
1D 2D 57 9D 57 F4 9E 5B E1 6B E7 DB 4E 3D C2 9B

78.
A1 B7 EE 94 17 7C 7B D8 1B 26 A0 00 38 EC C8 D8
5B 09 41 DF B2 11 09 CF 9D B9 0D D0 8D 3F 67 2E
EB 50 F4 BF 46 7D D4 6D 08 3F A3 A2 7D E2 F5 C8
1D 2D 57 9D 57 F4 9E 5B E1 6B E7 DB 4E 3D C2 9B

79.
A1 B7 EE 94 17 7C 7B D8 1B 26 A0 00 38 EC 3C D8
5B 09 41 DF B2 11 09 CF 9D B9 0D D0 8D 3F 67 2E
EB 50 F4 BF 46 7D D4 6D 08 3F A3 A2 7D E2 F5 C8
1D 2D 57 9D 57 F4 9E 5B E1 6B E7 DB 4E 3D C2 9B

80.
A1 B7 EE 94 17 7C 7B D8 1B 26 A0 00 38 EC 3C F8
5B 09 41 DF B2 11 09 CF 9D B9 0D D0 8D 3F 67 2E
EB 50 F4 BF 46 7D D4 6D 08 3F A3 A2 7D E2 F5 C8
1D 2D 57 9D 57 F4 9E 5B E1 6B E7 DB 4E 3D C2 9B

81. A1 B7 EE 94 17 7C 7B D8 1B 26 A0 00 38 EC 3C F8
31 09 41 DF B2 11 09 CF 9D B9 0D D0 8D 3F 67 2E
EB 50 F4 BF 46 7D D4 6D 08 3F A3 A2 7D E2 F5 C8
1D 2D 57 9D 57 F4 9E 5B E1 6B E7 DB 4E 3D C2 9B

82. A1 B7 EE 94 17 7C 7B D8 1B 26 A0 00 38 EC 3C F8
31 A7 41 DF B2 11 09 CF 9D B9 0D D0 8D 3F 67 2E
EB 50 F4 BF 46 7D D4 6D 08 3F A3 A2 7D E2 F5 C8
1D 2D 57 9D 57 F4 9E 5B E1 6B E7 DB 4E 3D C2 9B

83. A1 B7 EE 94 17 7C 7B D8 1B 26 A0 00 38 EC 3C F8
31 A7 51 DF B2 11 09 CF 9D B9 0D D0 8D 3F 67 2E
EB 50 F4 BF 46 7D D4 6D 08 3F A3 A2 7D E2 F5 C8
1D 2D 57 9D 57 F4 9E 5B E1 6B E7 DB 4E 3D C2 9B

84. A1 B7 EE 94 17 7C 7B D8 1B 26 A0 00 38 EC 3C F8
31 A7 51 BC B2 11 09 CF 9D B9 0D D0 8D 3F 67 2E
EB 50 F4 BF 46 7D D4 6D 08 3F A3 A2 7D E2 F5 C8
1D 2D 57 9D 57 F4 9E 5B E1 6B E7 DB 4E 3D C2 9B

85. A1 B7 EE 94 17 7C 7B D8 1B 26 A0 00 38 EC 3C F8
31 A7 51 BC A3 11 09 CF 9D B9 0D D0 8D 3F 67 2E
EB 50 F4 BF 46 7D D4 6D 08 3F A3 A2 7D E2 F5 C8
1D 2D 57 9D 57 F4 9E 5B E1 6B E7 DB 4E 3D C2 9B

86. A1 B7 EE 94 17 7C 7B D8 1B 26 A0 00 38 EC 3C F8
31 A7 51 BC A3 C8 09 CF 9D B9 0D D0 8D 3F 67 2E
EB 50 F4 BF 46 7D D4 6D 08 3F A3 A2 7D E2 F5 C8
1D 2D 57 9D 57 F4 9E 5B E1 6B E7 DB 4E 3D C2 9B

87. A1 B7 EE 94 17 7C 7B D8 1B 26 A0 00 38 EC 3C F8
31 A7 51 BC A3 C8 9C CF 9D B9 0D D0 8D 3F 67 2E
EB 50 F4 BF 46 7D D4 6D 08 3F A3 A2 7D E2 F5 C8
1D 2D 57 9D 57 F4 9E 5B E1 6B E7 DB 4E 3D C2 9B

88. A1 B7 EE 94 17 7C 7B D8 1B 26 A0 00 38 EC 3C F8
31 A7 51 BC A3 C8 9C 27 9D B9 0D D0 8D 3F 67 2E
EB 50 F4 BF 46 7D D4 6D 08 3F A3 A2 7D E2 F5 C8
1D 2D 57 9D 57 F4 9E 5B E1 6B E7 DB 4E 3D C2 9B

89. A1 B7 EE 94 17 7C 7B D8 1B 26 A0 00 38 EC 3C F8
31 A7 51 BC A3 C8 9C 27 FE B9 0D D0 8D 3F 67 2E
EB 50 F4 BF 46 7D D4 6D 08 3F A3 A2 7D E2 F5 C8
1D 2D 57 9D 57 F4 9E 5B E1 6B E7 DB 4E 3D C2 9B

90. A1 B7 EE 94 17 7C 7B D8 1B 26 A0 00 38 EC 3C F8
31 A7 51 BC A3 C8 9C 27 FE 19 0D D0 8D 3F 67 2E
EB 50 F4 BF 46 7D D4 6D 08 3F A3 A2 7D E2 F5 C8
1D 2D 57 9D 57 F4 9E 5B E1 6B E7 DB 4E 3D C2 9B

91. A1 B7 EE 94 17 7C 7B D8 1B 26 A0 00 38 EC 3C F8
31 A7 51 BC A3 C8 9C 27 FE 19 22 D0 8D 3F 67 2E
EB 50 F4 BF 46 7D D4 6D 08 3F A3 A2 7D E2 F5 C8
1D 2D 57 9D 57 F4 9E 5B E1 6B E7 DB 4E 3D C2 9B

92. A1 B7 EE 94 17 7C 7B D8 1B 26 A0 00 38 EC 3C F8
31 A7 51 BC A3 C8 9C 27 FE 19 22 E2 8D 3F 67 2E
EB 50 F4 BF 46 7D D4 6D 08 3F A3 A2 7D E2 F5 C8
1D 2D 57 9D 57 F4 9E 5B E1 6B E7 DB 4E 3D C2 9B

93. A1 B7 EE 94 17 7C 7B D8 1B 26 A0 00 38 EC 3C F8
31 A7 51 BC A3 C8 9C 27 FE 19 22 E2 8D 3F 67 2E
EB 50 F4 BF 46 7D D4 6D 08 3F A3 A2 7D E2 F5 C8
1D 2D 57 9D 57 F4 9E 5B E1 6B E7 DB 4E 3D C2 9B

94. A1 B7 EE 94 17 7C 7B D8 1B 26 A0 00 38 EC 3C F8

31 A7 51 BC A3 C8 9C 27 FE 19 22 E2 8D 4E 67 2E
EB 50 F4 BF 46 7D D4 6D 08 3F A3 A2 7D E2 F5 C8
1D 2D 57 9D 57 F4 9E 5B E1 6B E7 DB 4E 3D C2 9B

95. A1 B7 EE 94 17 7C 7B D8 1B 26 A0 00 38 EC 3C F8
31 A7 51 BC A3 C8 9C 27 FE 19 22 E2 8D 4E 8D 2E
EB 50 F4 BF 46 7D D4 6D 08 3F A3 A2 7D E2 F5 C8
1D 2D 57 9D 57 F4 9E 5B E1 6B E7 DB 4E 3D C2 9B

96. A1 B7 EE 94 17 7C 7B D8 1B 26 A0 00 38 EC 3C F8
31 A7 51 BC A3 C8 9C 27 FE 19 22 E2 8D 4E 8D 24
EB 50 F4 BF 46 7D D4 6D 08 3F A3 A2 7D E2 F5 C8
1D 2D 57 9D 57 F4 9E 5B E1 6B E7 DB 4E 3D C2 9B

97. A1 B7 EE 94 17 7C 7B D8 1B 26 A0 00 38 EC 3C F8
31 A7 51 BC A3 C8 9C 27 FE 19 22 E2 8D 4E 8D 24
91 50 F4 BF 46 7D D4 6D 08 3F A3 A2 7D E2 F5 C8
1D 2D 57 9D 57 F4 9E 5B E1 6B E7 DB 4E 3D C2 9B

98. A1 B7 EE 94 17 7C 7B D8 1B 26 A0 00 38 EC 3C F8
31 A7 51 BC A3 C8 9C 27 FE 19 22 E2 8D 4E 8D 24
91 1E F4 BF 46 7D D4 6D 08 3F A3 A2 7D E2 F5 C8
1D 2D 57 9D 57 F4 9E 5B E1 6B E7 DB 4E 3D C2 9B

99. A1 B7 EE 94 17 7C 7B D8 1B 26 A0 00 38 EC 3C F8
31 A7 51 BC A3 C8 9C 27 FE 19 22 E2 8D 4E 8D 24
91 1E E4 BF 46 7D D4 6D 08 3F A3 A2 7D E2 F5 C8
1D 2D 57 9D 57 F4 9E 5B E1 6B E7 DB 4E 3D C2 9B

100. A1 B7 EE 94 17 7C 7B D8 1B 26 A0 00 38 EC 3C F8
31 A7 51 BC A3 C8 9C 27 FE 19 22 E2 8D 4E 8D 24
91 1E E4 63 46 7D D4 6D 08 3F A3 A2 7D E2 F5 C8
1D 2D 57 9D 57 F4 9E 5B E1 6B E7 DB 4E 3D C2 9B

101. A1 B7 EE 94 17 7C 7B D8 1B 26 A0 00 38 EC 3C F8
31 A7 51 BC A3 C8 9C 27 FE 19 22 E2 8D 4E 8D 24
91 1E E4 63 2E 7D D4 6D 08 3F A3 A2 7D E2 F5 C8
1D 2D 57 9D 57 F4 9E 5B E1 6B E7 DB 4E 3D C2 9B

102. A1 B7 EE 94 17 7C 7B D8 1B 26 A0 00 38 EC 3C F8
31 A7 51 BC A3 C8 9C 27 FE 19 22 E2 8D 4E 8D 24
91 1E E4 63 2E BD D4 6D 08 3F A3 A2 7D E2 F5 C8
1D 2D 57 9D 57 F4 9E 5B E1 6B E7 DB 4E 3D C2 9B

103. A1 B7 EE 94 17 7C 7B D8 1B 26 A0 00 38 EC 3C F8
31 A7 51 BC A3 C8 9C 27 FE 19 22 E2 8D 4E 8D 24
91 1E E4 63 2E BD D2 6D 08 3F A3 A2 7D E2 F5 C8
1D 2D 57 9D 57 F4 9E 5B E1 6B E7 DB 4E 3D C2 9B

104. A1 B7 EE 94 17 7C 7B D8 1B 26 A0 00 38 EC 3C F8
31 A7 51 BC A3 C8 9C 27 FE 19 22 E2 8D 4E 8D 24
91 1E E4 63 2E BD D2 FA 08 3F A3 A2 7D E2 F5 C8
1D 2D 57 9D 57 F4 9E 5B E1 6B E7 DB 4E 3D C2 9B

105. A1 B7 EE 94 17 7C 7B D8 1B 26 A0 00 38 EC 3C F8
31 A7 51 BC A3 C8 9C 27 FE 19 22 E2 8D 4E 8D 24
91 1E E4 63 2E BD D2 FA 78 3F A3 A2 7D E2 F5 C8
1D 2D 57 9D 57 F4 9E 5B E1 6B E7 DB 4E 3D C2 9B

106. A1 B7 EE 94 17 7C 7B D8 1B 26 A0 00 38 EC 3C F8
31 A7 51 BC A3 C8 9C 27 FE 19 22 E2 8D 4E 8D 24
91 1E E4 63 2E BD D2 FA 78 3D A3 A2 7D E2 F5 C8
1D 2D 57 9D 57 F4 9E 5B E1 6B E7 DB 4E 3D C2 9B

107. A1 B7 EE 94 17 7C 7B D8 1B 26 A0 00 38 EC 3C F8
31 A7 51 BC A3 C8 9C 27 FE 19 22 E2 8D 4E 8D 24

91 1E E4 63 2E BD D2 FA 78 3D C4 A2 7D E2 F5 C8
1D 2D 57 9D 57 F4 9E 5B E1 6B E7 DB 4E 3D C2 9B

108. A1 B7 EE 94 17 7C 7B D8 1B 26 A0 00 38 EC 3C F8
31 A7 51 BC A3 C8 9C 27 FE 19 22 E2 8D 4E 8D 24
91 1E E4 63 2E BD D2 FA 78 3D C4 AA 7D E2 F5 C8
1D 2D 57 9D 57 F4 9E 5B E1 6B E7 DB 4E 3D C2 9B

109. A1 B7 EE 94 17 7C 7B D8 1B 26 A0 00 38 EC 3C F8
31 A7 51 BC A3 C8 9C 27 FE 19 22 E2 8D 4E 8D 24
91 1E E4 63 2E BD D2 FA 78 3D C4 AA E8 E2 F5 C8
1D 2D 57 9D 57 F4 9E 5B E1 6B E7 DB 4E 3D C2 9B

110. A1 B7 EE 94 17 7C 7B D8 1B 26 A0 00 38 EC 3C F8
31 A7 51 BC A3 C8 9C 27 FE 19 22 E2 8D 4E 8D 24
91 1E E4 63 2E BD D2 FA 78 3D C4 AA E8 AB F5 C8
1D 2D 57 9D 57 F4 9E 5B E1 6B E7 DB 4E 3D C2 9B

111. A1 B7 EE 94 17 7C 7B D8 1B 26 A0 00 38 EC 3C F8
31 A7 51 BC A3 C8 9C 27 FE 19 22 E2 8D 4E 8D 24
91 1E E4 63 2E BD D2 FA 78 3D C4 AA E8 AB 74 C8
1D 2D 57 9D 57 F4 9E 5B E1 6B E7 DB 4E 3D C2 9B

112. A1 B7 EE 94 17 7C 7B D8 1B 26 A0 00 38 EC 3C F8
31 A7 51 BC A3 C8 9C 27 FE 19 22 E2 8D 4E 8D 24
91 1E E4 63 2E BD D2 FA 78 3D C4 AA E8 AB 74 44
1D 2D 57 9D 57 F4 9E 5B E1 6B E7 DB 4E 3D C2 9B

113. A1 B7 EE 94 17 7C 7B D8 1B 26 A0 00 38 EC 3C F8
31 A7 51 BC A3 C8 9C 27 FE 19 22 E2 8D 4E 8D 24
91 1E E4 63 2E BD D2 FA 78 3D C4 AA E8 AB 74 44
61 2D 57 9D 57 F4 9E 5B E1 6B E7 DB 4E 3D C2 9B

114. A1 B7 EE 94 17 7C 7B D8 1B 26 A0 00 38 EC 3C F8
31 A7 51 BC A3 C8 9C 27 FE 19 22 E2 8D 4E 8D 24
91 1E E4 63 2E BD D2 FA 78 3D C4 AA E8 AB 74 44
61 87 57 9D 57 F4 9E 5B E1 6B E7 DB 4E 3D C2 9B

115. A1 B7 EE 94 17 7C 7B D8 1B 26 A0 00 38 EC 3C F8
31 A7 51 BC A3 C8 9C 27 FE 19 22 E2 8D 4E 8D 24
91 1E E4 63 2E BD D2 FA 78 3D C4 AA E8 AB 74 44
61 87 EE 9D 57 F4 9E 5B E1 6B E7 DB 4E 3D C2 9B

116. A1 B7 EE 94 17 7C 7B D8 1B 26 A0 00 38 EC 3C F8
31 A7 51 BC A3 C8 9C 27 FE 19 22 E2 8D 4E 8D 24
91 1E E4 63 2E BD D2 FA 78 3D C4 AA E8 AB 74 44
61 87 EE EC 57 F4 9E 5B E1 6B E7 DB 4E 3D C2 9B

117. A1 B7 EE 94 17 7C 7B D8 1B 26 A0 00 38 EC 3C F8
31 A7 51 BC A3 C8 9C 27 FE 19 22 E2 8D 4E 8D 24
91 1E E4 63 2E BD D2 FA 78 3D C4 AA E8 AB 74 44
61 87 EE EC 39 F4 9E 5B E1 6B E7 DB 4E 3D C2 9B

118. A1 B7 EE 94 17 7C 7B D8 1B 26 A0 00 38 EC 3C F8
31 A7 51 BC A3 C8 9C 27 FE 19 22 E2 8D 4E 8D 24
91 1E E4 63 2E BD D2 FA 78 3D C4 AA E8 AB 74 44
61 87 EE EC 39 71 9E 5B E1 6B E7 DB 4E 3D C2 9B

119. A1 B7 EE 94 17 7C 7B D8 1B 26 A0 00 38 EC 3C F8
31 A7 51 BC A3 C8 9C 27 FE 19 22 E2 8D 4E 8D 24
91 1E E4 63 2E BD D2 FA 78 3D C4 AA E8 AB 74 44
61 87 EE EC 39 71 F8 5B E1 6B E7 DB 4E 3D C2 9B

120. A1 B7 EE 94 17 7C 7B D8 1B 26 A0 00 38 EC 3C F8
31 A7 51 BC A3 C8 9C 27 FE 19 22 E2 8D 4E 8D 24
91 1E E4 63 2E BD D2 FA 78 3D C4 AA E8 AB 74 44

61 87 EE EC 39 71 F8 FA E1 6B E7 DB 4E 3D C2 9B

121. A1 B7 EE 94 17 7C 7B D8 1B 26 A0 00 38 EC 3C F8
31 A7 51 BC A3 C8 9C 27 FE 19 22 E2 8D 4E 8D 24
91 1E E4 63 2E BD D2 FA 78 3D C4 AA E8 AB 74 44
61 87 EE EC 39 71 F8 FA 5D 6B E7 DB 4E 3D C2 9B

122. A1 B7 EE 94 17 7C 7B D8 1B 26 A0 00 38 EC 3C F8
31 A7 51 BC A3 C8 9C 27 FE 19 22 E2 8D 4E 8D 24
91 1E E4 63 2E BD D2 FA 78 3D C4 AA E8 AB 74 44
61 87 EE EC 39 71 F8 FA 5D 9F E7 DB 4E 3D C2 9B

123. A1 B7 EE 94 17 7C 7B D8 1B 26 A0 00 38 EC 3C F8
31 A7 51 BC A3 C8 9C 27 FE 19 22 E2 8D 4E 8D 24
91 1E E4 63 2E BD D2 FA 78 3D C4 AA E8 AB 74 44
61 87 EE EC 39 71 F8 FA 5D 9F 07 DB 4E 3D C2 9B

124. A1 B7 EE 94 17 7C 7B D8 1B 26 A0 00 38 EC 3C F8
31 A7 51 BC A3 C8 9C 27 FE 19 22 E2 8D 4E 8D 24
91 1E E4 63 2E BD D2 FA 78 3D C4 AA E8 AB 74 44
61 87 EE EC 39 71 F8 FA 5D 9F 07 32 4E 3D C2 9B

125. A1 B7 EE 94 17 7C 7B D8 1B 26 A0 00 38 EC 3C F8
31 A7 51 BC A3 C8 9C 27 FE 19 22 E2 8D 4E 8D 24
91 1E E4 63 2E BD D2 FA 78 3D C4 AA E8 AB 74 44
61 87 EE EC 39 71 F8 FA 5D 9F 07 32 04 3D C2 9B

126. A1 B7 EE 94 17 7C 7B D8 1B 26 A0 00 38 EC 3C F8
31 A7 51 BC A3 C8 9C 27 FE 19 22 E2 8D 4E 8D 24
91 1E E4 63 2E BD D2 FA 78 3D C4 AA E8 AB 74 44
61 87 EE EC 39 71 F8 FA 5D 9F 07 32 04 B2 C2 9B

127. A1 B7 EE 94 17 7C 7B D8 1B 26 A0 00 38 EC 3C F8
31 A7 51 BC A3 C8 9C 27 FE 19 22 E2 8D 4E 8D 24
91 1E E4 63 2E BD D2 FA 78 3D C4 AA E8 AB 74 44
61 87 EE EC 39 71 F8 FA 5D 9F 07 32 04 B2 C6 9B

128. A1 B7 EE 94 17 7C 7B D8 1B 26 A0 00 38 EC 3C F8
31 A7 51 BC A3 C8 9C 27 FE 19 22 E2 8D 4E 8D 24
91 1E E4 63 2E BD D2 FA 78 3D C4 AA E8 AB 74 44
61 87 EE EC 39 71 F8 FA 5D 9F 07 32 04 B2 C6 A9

129. F7 B7 EE 94 17 7C 7B D8 1B 26 A0 00 38 EC 3C F8
31 A7 51 BC A3 C8 9C 27 FE 19 22 E2 8D 4E 8D 24
91 1E E4 63 2E BD D2 FA 78 3D C4 AA E8 AB 74 44
61 87 EE EC 39 71 F8 FA 5D 9F 07 32 04 B2 C6 A9

130. F7 33 EE 94 17 7C 7B D8 1B 26 A0 00 38 EC 3C F8
31 A7 51 BC A3 C8 9C 27 FE 19 22 E2 8D 4E 8D 24
91 1E E4 63 2E BD D2 FA 78 3D C4 AA E8 AB 74 44
61 87 EE EC 39 71 F8 FA 5D 9F 07 32 04 B2 C6 A9

131. F7 33 49 94 17 7C 7B D8 1B 26 A0 00 38 EC 3C F8
31 A7 51 BC A3 C8 9C 27 FE 19 22 E2 8D 4E 8D 24
91 1E E4 63 2E BD D2 FA 78 3D C4 AA E8 AB 74 44
61 87 EE EC 39 71 F8 FA 5D 9F 07 32 04 B2 C6 A9

132. F7 33 49 F3 17 7C 7B D8 1B 26 A0 00 38 EC 3C F8
31 A7 51 BC A3 C8 9C 27 FE 19 22 E2 8D 4E 8D 24
91 1E E4 63 2E BD D2 FA 78 3D C4 AA E8 AB 74 44
61 87 EE EC 39 71 F8 FA 5D 9F 07 32 04 B2 C6 A9

133. F7 33 49 F3 8E 7C 7B D8 1B 26 A0 00 38 EC 3C F8
31 A7 51 BC A3 C8 9C 27 FE 19 22 E2 8D 4E 8D 24
91 1E E4 63 2E BD D2 FA 78 3D C4 AA E8 AB 74 44
61 87 EE EC 39 71 F8 FA 5D 9F 07 32 04 B2 C6 A9

134. F7 33 49 F3 8E E4 7B D8 1B 26 A0 00 38 EC 3C F8
31 A7 51 BC A3 C8 9C 27 FE 19 22 E2 8D 4E 8D 24
91 1E E4 63 2E BD D2 FA 78 3D C4 AA E8 AB 74 44
61 87 EE EC 39 71 F8 FA 5D 9F 07 32 04 B2 C6 A9

135. F7 33 49 F3 8E E4 0D D8 1B 26 A0 00 38 EC 3C F8
31 A7 51 BC A3 C8 9C 27 FE 19 22 E2 8D 4E 8D 24
91 1E E4 63 2E BD D2 FA 78 3D C4 AA E8 AB 74 44
61 87 EE EC 39 71 F8 FA 5D 9F 07 32 04 B2 C6 A9

136. F7 33 49 F3 8E E4 0D DD 1B 26 A0 00 38 EC 3C F8
31 A7 51 BC A3 C8 9C 27 FE 19 22 E2 8D 4E 8D 24
91 1E E4 63 2E BD D2 FA 78 3D C4 AA E8 AB 74 44
61 87 EE EC 39 71 F8 FA 5D 9F 07 32 04 B2 C6 A9

137. F7 33 49 F3 8E E4 0D DD 23 26 A0 00 38 EC 3C F8
31 A7 51 BC A3 C8 9C 27 FE 19 22 E2 8D 4E 8D 24
91 1E E4 63 2E BD D2 FA 78 3D C4 AA E8 AB 74 44
61 87 EE EC 39 71 F8 FA 5D 9F 07 32 04 B2 C6 A9

138. F7 33 49 F3 8E E4 0D DD 23 E5 A0 00 38 EC 3C F8
31 A7 51 BC A3 C8 9C 27 FE 19 22 E2 8D 4E 8D 24
91 1E E4 63 2E BD D2 FA 78 3D C4 AA E8 AB 74 44
61 87 EE EC 39 71 F8 FA 5D 9F 07 32 04 B2 C6 A9

139. F7 33 49 F3 8E E4 0D DD 23 E5 70 00 38 EC 3C F8
31 A7 51 BC A3 C8 9C 27 FE 19 22 E2 8D 4E 8D 24
91 1E E4 63 2E BD D2 FA 78 3D C4 AA E8 AB 74 44
61 87 EE EC 39 71 F8 FA 5D 9F 07 32 04 B2 C6 A9

140. F7 33 49 F3 8E E4 0D DD 23 E5 70 21 38 EC 3C F8
31 A7 51 BC A3 C8 9C 27 FE 19 22 E2 8D 4E 8D 24
91 1E E4 63 2E BD D2 FA 78 3D C4 AA E8 AB 74 44
61 87 EE EC 39 71 F8 FA 5D 9F 07 32 04 B2 C6 A9

141. F7 33 49 F3 8E E4 0D DD 23 E5 70 21 C1 EC 3C F8
31 A7 51 BC A3 C8 9C 27 FE 19 22 E2 8D 4E 8D 24
91 1E E4 63 2E BD D2 FA 78 3D C4 AA E8 AB 74 44
61 87 EE EC 39 71 F8 FA 5D 9F 07 32 04 B2 C6 A9

142. F7 33 49 F3 8E E4 0D DD 23 E5 70 21 C1 84 3C F8
31 A7 51 BC A3 C8 9C 27 FE 19 22 E2 8D 4E 8D 24
91 1E E4 63 2E BD D2 FA 78 3D C4 AA E8 AB 74 44
61 87 EE EC 39 71 F8 FA 5D 9F 07 32 04 B2 C6 A9

143. F7 33 49 F3 8E E4 0D DD 23 E5 70 21 C1 84 83 F8
31 A7 51 BC A3 C8 9C 27 FE 19 22 E2 8D 4E 8D 24
91 1E E4 63 2E BD D2 FA 78 3D C4 AA E8 AB 74 44
61 87 EE EC 39 71 F8 FA 5D 9F 07 32 04 B2 C6 A9

144. F7 33 49 F3 8E E4 0D DD 23 E5 70 21 C1 84 83 1F
31 A7 51 BC A3 C8 9C 27 FE 19 22 E2 8D 4E 8D 24
91 1E E4 63 2E BD D2 FA 78 3D C4 AA E8 AB 74 44
61 87 EE EC 39 71 F8 FA 5D 9F 07 32 04 B2 C6 A9

145. F7 33 49 F3 8E E4 0D DD 23 E5 70 21 C1 84 83 1F
EC A7 51 BC A3 C8 9C 27 FE 19 22 E2 8D 4E 8D 24
91 1E E4 63 2E BD D2 FA 78 3D C4 AA E8 AB 74 44
61 87 EE EC 39 71 F8 FA 5D 9F 07 32 04 B2 C6 A9

146. F7 33 49 F3 8E E4 0D DD 23 E5 70 21 C1 84 83 1F
EC 99 51 BC A3 C8 9C 27 FE 19 22 E2 8D 4E 8D 24
91 1E E4 63 2E BD D2 FA 78 3D C4 AA E8 AB 74 44
61 87 EE EC 39 71 F8 FA 5D 9F 07 32 04 B2 C6 A9

147. F7 33 49 F3 8E E4 0D DD 23 E5 70 21 C1 84 83 1F
EC 99 C4 BC A3 C8 9C 27 FE 19 22 E2 8D 4E 8D 24
91 1E E4 63 2E BD D2 FA 78 3D C4 AA E8 AB 74 44
61 87 EE EC 39 71 F8 FA 5D 9F 07 32 04 B2 C6 A9

148. F7 33 49 F3 8E E4 0D DD 23 E5 70 21 C1 84 83 1F
EC 99 C4 59 A3 C8 9C 27 FE 19 22 E2 8D 4E 8D 24
91 1E E4 63 2E BD D2 FA 78 3D C4 AA E8 AB 74 44
61 87 EE EC 39 71 F8 FA 5D 9F 07 32 04 B2 C6 A9

149. F7 33 49 F3 8E E4 0D DD 23 E5 70 21 C1 84 83 1F
EC 99 C4 59 E5 C8 9C 27 FE 19 22 E2 8D 4E 8D 24
91 1E E4 63 2E BD D2 FA 78 3D C4 AA E8 AB 74 44
61 87 EE EC 39 71 F8 FA 5D 9F 07 32 04 B2 C6 A9

150. F7 33 49 F3 8E E4 0D DD 23 E5 70 21 C1 84 83 1F
EC 99 C4 59 E5 B7 9C 27 FE 19 22 E2 8D 4E 8D 24
91 1E E4 63 2E BD D2 FA 78 3D C4 AA E8 AB 74 44
61 87 EE EC 39 71 F8 FA 5D 9F 07 32 04 B2 C6 A9

151. F7 33 49 F3 8E E4 0D DD 23 E5 70 21 C1 84 83 1F
EC 99 C4 59 E5 B7 D7 27 FE 19 22 E2 8D 4E 8D 24
91 1E E4 63 2E BD D2 FA 78 3D C4 AA E8 AB 74 44
61 87 EE EC 39 71 F8 FA 5D 9F 07 32 04 B2 C6 A9

152. F7 33 49 F3 8E E4 0D DD 23 E5 70 21 C1 84 83 1F
EC 99 C4 59 E5 B7 D7 DE FE 19 22 E2 8D 4E 8D 24
91 1E E4 63 2E BD D2 FA 78 3D C4 AA E8 AB 74 44
61 87 EE EC 39 71 F8 FA 5D 9F 07 32 04 B2 C6 A9

153. F7 33 49 F3 8E E4 0D DD 23 E5 70 21 C1 84 83 1F
EC 99 C4 59 E5 B7 D7 DE 41 19 22 E2 8D 4E 8D 24
91 1E E4 63 2E BD D2 FA 78 3D C4 AA E8 AB 74 44
61 87 EE EC 39 71 F8 FA 5D 9F 07 32 04 B2 C6 A9

154. F7 33 49 F3 8E E4 0D DD 23 E5 70 21 C1 84 83 1F
EC 99 C4 59 E5 B7 D7 DE 41 BD 22 E2 8D 4E 8D 24
91 1E E4 63 2E BD D2 FA 78 3D C4 AA E8 AB 74 44
61 87 EE EC 39 71 F8 FA 5D 9F 07 32 04 B2 C6 A9

155. F7 33 49 F3 8E E4 0D DD 23 E5 70 21 C1 84 83 1F
EC 99 C4 59 E5 B7 D7 DE 41 BD FA E2 8D 4E 8D 24
91 1E E4 63 2E BD D2 FA 78 3D C4 AA E8 AB 74 44
61 87 EE EC 39 71 F8 FA 5D 9F 07 32 04 B2 C6 A9

156. F7 33 49 F3 8E E4 0D DD 23 E5 70 21 C1 84 83 1F
EC 99 C4 59 E5 B7 D7 DE 41 BD FA 43 8D 4E 8D 24
91 1E E4 63 2E BD D2 FA 78 3D C4 AA E8 AB 74 44
61 87 EE EC 39 71 F8 FA 5D 9F 07 32 04 B2 C6 A9

157. F7 33 49 F3 8E E4 0D DD 23 E5 70 21 C1 84 83 1F
EC 99 C4 59 E5 B7 D7 DE 41 BD FA 43 CD 4E 8D 24
91 1E E4 63 2E BD D2 FA 78 3D C4 AA E8 AB 74 44
61 87 EE EC 39 71 F8 FA 5D 9F 07 32 04 B2 C6 A9

158. F7 33 49 F3 8E E4 0D DD 23 E5 70 21 C1 84 83 1F
EC 99 C4 59 E5 B7 D7 DE 41 BD FA 43 CD 18 8D 24
91 1E E4 63 2E BD D2 FA 78 3D C4 AA E8 AB 74 44
61 87 EE EC 39 71 F8 FA 5D 9F 07 32 04 B2 C6 A9

159. F7 33 49 F3 8E E4 0D DD 23 E5 70 21 C1 84 83 1F
EC 99 C4 59 E5 B7 D7 DE 41 BD FA 43 CD 18 63 24
91 1E E4 63 2E BD D2 FA 78 3D C4 AA E8 AB 74 44
61 87 EE EC 39 71 F8 FA 5D 9F 07 32 04 B2 C6 A9

160. F7 33 49 F3 8E E4 0D DD 23 E5 70 21 C1 84 83 1F

EC 99 C4 59 E5 B7 D7 DE 41 BD FA 43 CD 18 63 EC
91 1E E4 63 2E BD D2 FA 78 3D C4 AA E8 AB 74 44
61 87 EE EC 39 71 F8 FA 5D 9F 07 32 04 B2 C6 A9

161. F7 33 49 F3 8E E4 0D DD 23 E5 70 21 C1 84 83 1F
EC 99 C4 59 E5 B7 D7 DE 41 BD FA 43 CD 18 63 EC
40 1E E4 63 2E BD D2 FA 78 3D C4 AA E8 AB 74 44
61 87 EE EC 39 71 F8 FA 5D 9F 07 32 04 B2 C6 A9

162. F7 33 49 F3 8E E4 0D DD 23 E5 70 21 C1 84 83 1F
EC 99 C4 59 E5 B7 D7 DE 41 BD FA 43 CD 18 63 EC
40 F0 E4 63 2E BD D2 FA 78 3D C4 AA E8 AB 74 44
61 87 EE EC 39 71 F8 FA 5D 9F 07 32 04 B2 C6 A9

163. F7 33 49 F3 8E E4 0D DD 23 E5 70 21 C1 84 83 1F
EC 99 C4 59 E5 B7 D7 DE 41 BD FA 43 CD 18 63 EC
40 F0 14 63 2E BD D2 FA 78 3D C4 AA E8 AB 74 44
61 87 EE EC 39 71 F8 FA 5D 9F 07 32 04 B2 C6 A9

164. F7 33 49 F3 8E E4 0D DD 23 E5 70 21 C1 84 83 1F
EC 99 C4 59 E5 B7 D7 DE 41 BD FA 43 CD 18 63 EC
40 F0 14 06 2E BD D2 FA 78 3D C4 AA E8 AB 74 44
61 87 EE EC 39 71 F8 FA 5D 9F 07 32 04 B2 C6 A9

165. F7 33 49 F3 8E E4 0D DD 23 E5 70 21 C1 84 83 1F
EC 99 C4 59 E5 B7 D7 DE 41 BD FA 43 CD 18 63 EC
40 F0 14 06 49 BD D2 FA 78 3D C4 AA E8 AB 74 44
61 87 EE EC 39 71 F8 FA 5D 9F 07 32 04 B2 C6 A9

166. F7 33 49 F3 8E E4 0D DD 23 E5 70 21 C1 84 83 1F
EC 99 C4 59 E5 B7 D7 DE 41 BD FA 43 CD 18 63 EC
40 F0 14 06 49 00 D2 FA 78 3D C4 AA E8 AB 74 44
61 87 EE EC 39 71 F8 FA 5D 9F 07 32 04 B2 C6 A9

167. F7 33 49 F3 8E E4 0D DD 23 E5 70 21 C1 84 83 1F
EC 99 C4 59 E5 B7 D7 DE 41 BD FA 43 CD 18 63 EC
40 F0 14 06 49 00 7B FA 78 3D C4 AA E8 AB 74 44
61 87 EE EC 39 71 F8 FA 5D 9F 07 32 04 B2 C6 A9

168. F7 33 49 F3 8E E4 0D DD 23 E5 70 21 C1 84 83 1F
EC 99 C4 59 E5 B7 D7 DE 41 BD FA 43 CD 18 63 EC
40 F0 14 06 49 00 7B 1F 78 3D C4 AA E8 AB 74 44
61 87 EE EC 39 71 F8 FA 5D 9F 07 32 04 B2 C6 A9

169. F7 33 49 F3 8E E4 0D DD 23 E5 70 21 C1 84 83 1F
EC 99 C4 59 E5 B7 D7 DE 41 BD FA 43 CD 18 63 EC
40 F0 14 06 49 00 7B 1F B8 3D C4 AA E8 AB 74 44
61 87 EE EC 39 71 F8 FA 5D 9F 07 32 04 B2 C6 A9

170. F7 33 49 F3 8E E4 0D DD 23 E5 70 21 C1 84 83 1F
EC 99 C4 59 E5 B7 D7 DE 41 BD FA 43 CD 18 63 EC
40 F0 14 06 49 00 7B 1F B8 72 C4 AA E8 AB 74 44
61 87 EE EC 39 71 F8 FA 5D 9F 07 32 04 B2 C6 A9

171. F7 33 49 F3 8E E4 0D DD 23 E5 70 21 C1 84 83 1F
EC 99 C4 59 E5 B7 D7 DE 41 BD FA 43 CD 18 63 EC
40 F0 14 06 49 00 7B 1F B8 72 BA AA E8 AB 74 44
61 87 EE EC 39 71 F8 FA 5D 9F 07 32 04 B2 C6 A9

172. F7 33 49 F3 8E E4 0D DD 23 E5 70 21 C1 84 83 1F
EC 99 C4 59 E5 B7 D7 DE 41 BD FA 43 CD 18 63 EC
40 F0 14 06 49 00 7B 1F B8 72 BA 0E E8 AB 74 44
61 87 EE EC 39 71 F8 FA 5D 9F 07 32 04 B2 C6 A9

173. F7 33 49 F3 8E E4 0D DD 23 E5 70 21 C1 84 83 1F
EC 99 C4 59 E5 B7 D7 DE 41 BD FA 43 CD 18 63 EC

40 F0 14 06 49 00 7B 1F B8 72 BA 0E 67 AB 74 44
61 87 EE EC 39 71 F8 FA 5D 9F 07 32 04 B2 C6 A9

174. F7 33 49 F3 8E E4 0D DD 23 E5 70 21 C1 84 83 1F
EC 99 C4 59 E5 B7 D7 DE 41 BD FA 43 CD 18 63 EC
40 F0 14 06 49 00 7B 1F B8 72 BA 0E 67 2C 74 44
61 87 EE EC 39 71 F8 FA 5D 9F 07 32 04 B2 C6 A9

175. F7 33 49 F3 8E E4 0D DD 23 E5 70 21 C1 84 83 1F
EC 99 C4 59 E5 B7 D7 DE 41 BD FA 43 CD 18 63 EC
40 F0 14 06 49 00 7B 1F B8 72 BA 0E 67 2C 2C 44
61 87 EE EC 39 71 F8 FA 5D 9F 07 32 04 B2 C6 A9

176. F7 33 49 F3 8E E4 0D DD 23 E5 70 21 C1 84 83 1F
EC 99 C4 59 E5 B7 D7 DE 41 BD FA 43 CD 18 63 EC
40 F0 14 06 49 00 7B 1F B8 72 BA 0E 67 2C 2C 83
61 87 EE EC 39 71 F8 FA 5D 9F 07 32 04 B2 C6 A9

177. F7 33 49 F3 8E E4 0D DD 23 E5 70 21 C1 84 83 1F
EC 99 C4 59 E5 B7 D7 DE 41 BD FA 43 CD 18 63 EC
40 F0 14 06 49 00 7B 1F B8 72 BA 0E 67 2C 2C 83
32 87 EE EC 39 71 F8 FA 5D 9F 07 32 04 B2 C6 A9

178. F7 33 49 F3 8E E4 0D DD 23 E5 70 21 C1 84 83 1F
EC 99 C4 59 E5 B7 D7 DE 41 BD FA 43 CD 18 63 EC
40 F0 14 06 49 00 7B 1F B8 72 BA 0E 67 2C 2C 83
32 2E EE EC 39 71 F8 FA 5D 9F 07 32 04 B2 C6 A9

179. F7 33 49 F3 8E E4 0D DD 23 E5 70 21 C1 84 83 1F
EC 99 C4 59 E5 B7 D7 DE 41 BD FA 43 CD 18 63 EC
40 F0 14 06 49 00 7B 1F B8 72 BA 0E 67 2C 2C 83
32 2E 69 EC 39 71 F8 FA 5D 9F 07 32 04 B2 C6 A9

180. F7 33 49 F3 8E E4 0D DD 23 E5 70 21 C1 84 83 1F
EC 99 C4 59 E5 B7 D7 DE 41 BD FA 43 CD 18 63 EC
40 F0 14 06 49 00 7B 1F B8 72 BA 0E 67 2C 2C 83
32 2E 69 84 39 71 F8 FA 5D 9F 07 32 04 B2 C6 A9

181. F7 33 49 F3 8E E4 0D DD 23 E5 70 21 C1 84 83 1F
EC 99 C4 59 E5 B7 D7 DE 41 BD FA 43 CD 18 63 EC
40 F0 14 06 49 00 7B 1F B8 72 BA 0E 67 2C 2C 83
32 2E 69 84 16 71 F8 FA 5D 9F 07 32 04 B2 C6 A9

182. F7 33 49 F3 8E E4 0D DD 23 E5 70 21 C1 84 83 1F
EC 99 C4 59 E5 B7 D7 DE 41 BD FA 43 CD 18 63 EC
40 F0 14 06 49 00 7B 1F B8 72 BA 0E 67 2C 2C 83
32 2E 69 84 16 93 F8 FA 5D 9F 07 32 04 B2 C6 A9

183. F7 33 49 F3 8E E4 0D DD 23 E5 70 21 C1 84 83 1F
EC 99 C4 59 E5 B7 D7 DE 41 BD FA 43 CD 18 63 EC
40 F0 14 06 49 00 7B 1F B8 72 BA 0E 67 2C 2C 83
32 2E 69 84 16 93 6F FA 5D 9F 07 32 04 B2 C6 A9

184. F7 33 49 F3 8E E4 0D DD 23 E5 70 21 C1 84 83 1F
EC 99 C4 59 E5 B7 D7 DE 41 BD FA 43 CD 18 63 EC
40 F0 14 06 49 00 7B 1F B8 72 BA 0E 67 2C 2C 83
32 2E 69 84 16 93 6F E5 5D 9F 07 32 04 B2 C6 A9

185. F7 33 49 F3 8E E4 0D DD 23 E5 70 21 C1 84 83 1F
EC 99 C4 59 E5 B7 D7 DE 41 BD FA 43 CD 18 63 EC
40 F0 14 06 49 00 7B 1F B8 72 BA 0E 67 2C 2C 83
32 2E 69 84 16 93 6F E5 B5 9F 07 32 04 B2 C6 A9

186. F7 33 49 F3 8E E4 0D DD 23 E5 70 21 C1 84 83 1F
EC 99 C4 59 E5 B7 D7 DE 41 BD FA 43 CD 18 63 EC
40 F0 14 06 49 00 7B 1F B8 72 BA 0E 67 2C 2C 83

32 2E 69 84 16 93 6F E5 B5 41 07 32 04 B2 C6 A9

187. F7 33 49 F3 8E E4 0D DD 23 E5 70 21 C1 84 83 1F
EC 99 C4 59 E5 B7 D7 DE 41 BD FA 43 CD 18 63 EC
40 F0 14 06 49 00 7B 1F B8 72 BA 0E 67 2C 2C 83
32 2E 69 84 16 93 6F E5 B5 41 08 32 04 B2 C6 A9

188. F7 33 49 F3 8E E4 0D DD 23 E5 70 21 C1 84 83 1F
EC 99 C4 59 E5 B7 D7 DE 41 BD FA 43 CD 18 63 EC
40 F0 14 06 49 00 7B 1F B8 72 BA 0E 67 2C 2C 83
32 2E 69 84 16 93 6F E5 B5 41 08 7F 04 B2 C6 A9

189. F7 33 49 F3 8E E4 0D DD 23 E5 70 21 C1 84 83 1F
EC 99 C4 59 E5 B7 D7 DE 41 BD FA 43 CD 18 63 EC
40 F0 14 06 49 00 7B 1F B8 72 BA 0E 67 2C 2C 83
32 2E 69 84 16 93 6F E5 B5 41 08 7F C1 B2 C6 A9

190. F7 33 49 F3 8E E4 0D DD 23 E5 70 21 C1 84 83 1F
EC 99 C4 59 E5 B7 D7 DE 41 BD FA 43 CD 18 63 EC
40 F0 14 06 49 00 7B 1F B8 72 BA 0E 67 2C 2C 83
32 2E 69 84 16 93 6F E5 B5 41 08 7F C1 D7 C6 A9

191. F7 33 49 F3 8E E4 0D DD 23 E5 70 21 C1 84 83 1F
EC 99 C4 59 E5 B7 D7 DE 41 BD FA 43 CD 18 63 EC
40 F0 14 06 49 00 7B 1F B8 72 BA 0E 67 2C 2C 83
32 2E 69 84 16 93 6F E5 B5 41 08 7F C1 D7 70 A9

192. F7 33 49 F3 8E E4 0D DD 23 E5 70 21 C1 84 83 1F
EC 99 C4 59 E5 B7 D7 DE 41 BD FA 43 CD 18 63 EC
40 F0 14 06 49 00 7B 1F B8 72 BA 0E 67 2C 2C 83
32 2E 69 84 16 93 6F E5 B5 41 08 7F C1 D7 70 C5

193. BC 33 49 F3 8E E4 0D DD 23 E5 70 21 C1 84 83 1F
EC 99 C4 59 E5 B7 D7 DE 41 BD FA 43 CD 18 63 EC
40 F0 14 06 49 00 7B 1F B8 72 BA 0E 67 2C 2C 83
32 2E 69 84 16 93 6F E5 B5 41 08 7F C1 D7 70 C5

194. BC 59 49 F3 8E E4 0D DD 23 E5 70 21 C1 84 83 1F
EC 99 C4 59 E5 B7 D7 DE 41 BD FA 43 CD 18 63 EC
40 F0 14 06 49 00 7B 1F B8 72 BA 0E 67 2C 2C 83
32 2E 69 84 16 93 6F E5 B5 41 08 7F C1 D7 70 C5

195. BC 59 1F F3 8E E4 0D DD 23 E5 70 21 C1 84 83 1F
EC 99 C4 59 E5 B7 D7 DE 41 BD FA 43 CD 18 63 EC
40 F0 14 06 49 00 7B 1F B8 72 BA 0E 67 2C 2C 83
32 2E 69 84 16 93 6F E5 B5 41 08 7F C1 D7 70 C5

196. BC 59 1F B3 8E E4 0D DD 23 E5 70 21 C1 84 83 1F
EC 99 C4 59 E5 B7 D7 DE 41 BD FA 43 CD 18 63 EC
40 F0 14 06 49 00 7B 1F B8 72 BA 0E 67 2C 2C 83
32 2E 69 84 16 93 6F E5 B5 41 08 7F C1 D7 70 C5

197. BC 59 1F B3 2D E4 0D DD 23 E5 70 21 C1 84 83 1F
EC 99 C4 59 E5 B7 D7 DE 41 BD FA 43 CD 18 63 EC
40 F0 14 06 49 00 7B 1F B8 72 BA 0E 67 2C 2C 83
32 2E 69 84 16 93 6F E5 B5 41 08 7F C1 D7 70 C5

198. BC 59 1F B3 2D 74 0D DD 23 E5 70 21 C1 84 83 1F
EC 99 C4 59 E5 B7 D7 DE 41 BD FA 43 CD 18 63 EC
40 F0 14 06 49 00 7B 1F B8 72 BA 0E 67 2C 2C 83
32 2E 69 84 16 93 6F E5 B5 41 08 7F C1 D7 70 C5

199. BC 59 1F B3 2D 74 72 DD 23 E5 70 21 C1 84 83 1F
EC 99 C4 59 E5 B7 D7 DE 41 BD FA 43 CD 18 63 EC
40 F0 14 06 49 00 7B 1F B8 72 BA 0E 67 2C 2C 83
32 2E 69 84 16 93 6F E5 B5 41 08 7F C1 D7 70 C5

200.
BC 59 1F B3 2D 74 72 05 23 E5 70 21 C1 84 83 1F
EC 99 C4 59 E5 B7 D7 DE 41 BD FA 43 CD 18 63 EC
40 F0 14 06 49 00 7B 1F B8 72 BA 0E 67 2C 2C 83
32 2E 69 84 16 93 6F E5 B5 41 08 7F C1 D7 70 C5

201.
BC 59 1F B3 2D 74 72 05 33 E5 70 21 C1 84 83 1F
EC 99 C4 59 E5 B7 D7 DE 41 BD FA 43 CD 18 63 EC
40 F0 14 06 49 00 7B 1F B8 72 BA 0E 67 2C 2C 83
32 2E 69 84 16 93 6F E5 B5 41 08 7F C1 D7 70 C5

202.
BC 59 1F B3 2D 74 72 05 33 2A 70 21 C1 84 83 1F
EC 99 C4 59 E5 B7 D7 DE 41 BD FA 43 CD 18 63 EC
40 F0 14 06 49 00 7B 1F B8 72 BA 0E 67 2C 2C 83
32 2E 69 84 16 93 6F E5 B5 41 08 7F C1 D7 70 C5

203.
BC 59 1F B3 2D 74 72 05 33 2A 63 21 C1 84 83 1F
EC 99 C4 59 E5 B7 D7 DE 41 BD FA 43 CD 18 63 EC
40 F0 14 06 49 00 7B 1F B8 72 BA 0E 67 2C 2C 83
32 2E 69 84 16 93 6F E5 B5 41 08 7F C1 D7 70 C5

204.
BC 59 1F B3 2D 74 72 05 33 2A 63 AB C1 84 83 1F
EC 99 C4 59 E5 B7 D7 DE 41 BD FA 43 CD 18 63 EC
40 F0 14 06 49 00 7B 1F B8 72 BA 0E 67 2C 2C 83
32 2E 69 84 16 93 6F E5 B5 41 08 7F C1 D7 70 C5

205.
BC 59 1F B3 2D 74 72 05 33 2A 63 AB 26 84 83 1F
EC 99 C4 59 E5 B7 D7 DE 41 BD FA 43 CD 18 63 EC
40 F0 14 06 49 00 7B 1F B8 72 BA 0E 67 2C 2C 83
32 2E 69 84 16 93 6F E5 B5 41 08 7F C1 D7 70 C5

206.
BC 59 1F B3 2D 74 72 05 33 2A 63 AB 26 D4 83 1F
EC 99 C4 59 E5 B7 D7 DE 41 BD FA 43 CD 18 63 EC
40 F0 14 06 49 00 7B 1F B8 72 BA 0E 67 2C 2C 83
32 2E 69 84 16 93 6F E5 B5 41 08 7F C1 D7 70 C5

207.
BC 59 1F B3 2D 74 72 05 33 2A 63 AB 26 D4 50 1F
EC 99 C4 59 E5 B7 D7 DE 41 BD FA 43 CD 18 63 EC
40 F0 14 06 49 00 7B 1F B8 72 BA 0E 67 2C 2C 83
32 2E 69 84 16 93 6F E5 B5 41 08 7F C1 D7 70 C5

208.
BC 59 1F B3 2D 74 72 05 33 2A 63 AB 26 D4 50 71
EC 99 C4 59 E5 B7 D7 DE 41 BD FA 43 CD 18 63 EC
40 F0 14 06 49 00 7B 1F B8 72 BA 0E 67 2C 2C 83
32 2E 69 84 16 93 6F E5 B5 41 08 7F C1 D7 70 C5

209.
BC 59 1F B3 2D 74 72 05 33 2A 63 AB 26 D4 50 71
87 99 C4 59 E5 B7 D7 DE 41 BD FA 43 CD 18 63 EC
40 F0 14 06 49 00 7B 1F B8 72 BA 0E 67 2C 2C 83
32 2E 69 84 16 93 6F E5 B5 41 08 7F C1 D7 70 C5

210.
BC 59 1F B3 2D 74 72 05 33 2A 63 AB 26 D4 50 71
87 E7 C4 59 E5 B7 D7 DE 41 BD FA 43 CD 18 63 EC
40 F0 14 06 49 00 7B 1F B8 72 BA 0E 67 2C 2C 83
32 2E 69 84 16 93 6F E5 B5 41 08 7F C1 D7 70 C5

211.
BC 59 1F B3 2D 74 72 05 33 2A 63 AB 26 D4 50 71
87 E7 F0 59 E5 B7 D7 DE 41 BD FA 43 CD 18 63 EC
40 F0 14 06 49 00 7B 1F B8 72 BA 0E 67 2C 2C 83
32 2E 69 84 16 93 6F E5 B5 41 08 7F C1 D7 70 C5

212.
BC 59 1F B3 2D 74 72 05 33 2A 63 AB 26 D4 50 71
87 E7 F0 5A E5 B7 D7 DE 41 BD FA 43 CD 18 63 EC
40 F0 14 06 49 00 7B 1F B8 72 BA 0E 67 2C 2C 83
32 2E 69 84 16 93 6F E5 B5 41 08 7F C1 D7 70 C5

213. BC 59 1F B3 2D 74 72 05 33 2A 63 AB 26 D4 50 71
87 E7 F0 5A F8 B7 D7 DE 41 BD FA 43 CD 18 63 EC
40 F0 14 06 49 00 7B 1F B8 72 BA 0E 67 2C 2C 83
32 2E 69 84 16 93 6F E5 B5 41 08 7F C1 D7 70 C5

214. BC 59 1F B3 2D 74 72 05 33 2A 63 AB 26 D4 50 71
87 E7 F0 5A F8 2C D7 DE 41 BD FA 43 CD 18 63 EC
40 F0 14 06 49 00 7B 1F B8 72 BA 0E 67 2C 2C 83
32 2E 69 84 16 93 6F E5 B5 41 08 7F C1 D7 70 C5

215. BC 59 1F B3 2D 74 72 05 33 2A 63 AB 26 D4 50 71
87 E7 F0 5A F8 2C 68 DE 41 BD FA 43 CD 18 63 EC
40 F0 14 06 49 00 7B 1F B8 72 BA 0E 67 2C 2C 83
32 2E 69 84 16 93 6F E5 B5 41 08 7F C1 D7 70 C5

216. BC 59 1F B3 2D 74 72 05 33 2A 63 AB 26 D4 50 71
87 E7 F0 5A F8 2C 68 3F 41 BD FA 43 CD 18 63 EC
40 F0 14 06 49 00 7B 1F B8 72 BA 0E 67 2C 2C 83
32 2E 69 84 16 93 6F E5 B5 41 08 7F C1 D7 70 C5

217. BC 59 1F B3 2D 74 72 05 33 2A 63 AB 26 D4 50 71
87 E7 F0 5A F8 2C 68 3F 5A BD FA 43 CD 18 63 EC
40 F0 14 06 49 00 7B 1F B8 72 BA 0E 67 2C 2C 83
32 2E 69 84 16 93 6F E5 B5 41 08 7F C1 D7 70 C5

218. BC 59 1F B3 2D 74 72 05 33 2A 63 AB 26 D4 50 71
87 E7 F0 5A F8 2C 68 3F 5A B4 FA 43 CD 18 63 EC
40 F0 14 06 49 00 7B 1F B8 72 BA 0E 67 2C 2C 83
32 2E 69 84 16 93 6F E5 B5 41 08 7F C1 D7 70 C5

219. BC 59 1F B3 2D 74 72 05 33 2A 63 AB 26 D4 50 71
87 E7 F0 5A F8 2C 68 3F 5A B4 C3 43 CD 18 63 EC
40 F0 14 06 49 00 7B 1F B8 72 BA 0E 67 2C 2C 83
32 2E 69 84 16 93 6F E5 B5 41 08 7F C1 D7 70 C5

220. BC 59 1F B3 2D 74 72 05 33 2A 63 AB 26 D4 50 71
87 E7 F0 5A F8 2C 68 3F 5A B4 C3 9C CD 18 63 EC
40 F0 14 06 49 00 7B 1F B8 72 BA 0E 67 2C 2C 83
32 2E 69 84 16 93 6F E5 B5 41 08 7F C1 D7 70 C5

221. BC 59 1F B3 2D 74 72 05 33 2A 63 AB 26 D4 50 71
87 E7 F0 5A F8 2C 68 3F 5A B4 C3 9C 14 18 63 EC
40 F0 14 06 49 00 7B 1F B8 72 BA 0E 67 2C 2C 83
32 2E 69 84 16 93 6F E5 B5 41 08 7F C1 D7 70 C5

222. BC 59 1F B3 2D 74 72 05 33 2A 63 AB 26 D4 50 71
87 E7 F0 5A F8 2C 68 3F 5A B4 C3 9C 14 53 63 EC
40 F0 14 06 49 00 7B 1F B8 72 BA 0E 67 2C 2C 83
32 2E 69 84 16 93 6F E5 B5 41 08 7F C1 D7 70 C5

223. BC 59 1F B3 2D 74 72 05 33 2A 63 AB 26 D4 50 71
87 E7 F0 5A F8 2C 68 3F 5A B4 C3 9C 14 53 37 EC
40 F0 14 06 49 00 7B 1F B8 72 BA 0E 67 2C 2C 83
32 2E 69 84 16 93 6F E5 B5 41 08 7F C1 D7 70 C5

224. BC 59 1F B3 2D 74 72 05 33 2A 63 AB 26 D4 50 71
87 E7 F0 5A F8 2C 68 3F 5A B4 C3 9C 14 53 37 FE
40 F0 14 06 49 00 7B 1F B8 72 BA 0E 67 2C 2C 83
32 2E 69 84 16 93 6F E5 B5 41 08 7F C1 D7 70 C5

225. BC 59 1F B3 2D 74 72 05 33 2A 63 AB 26 D4 50 71
87 E7 F0 5A F8 2C 68 3F 5A B4 C3 9C 14 53 37 FE
1C F0 14 06 49 00 7B 1F B8 72 BA 0E 67 2C 2C 83
32 2E 69 84 16 93 6F E5 B5 41 08 7F C1 D7 70 C5

226. BC 59 1F B3 2D 74 72 05 33 2A 63 AB 26 D4 50 71

87 E7 F0 5A F8 2C 68 3F 5A B4 C3 9C 14 53 37 FE
1C 9C 14 06 49 00 7B 1F B8 72 BA 0E 67 2C 2C 83
32 2E 69 84 16 93 6F E5 B5 41 08 7F C1 D7 70 C5

227. BC 59 1F B3 2D 74 72 05 33 2A 63 AB 26 D4 50 71
87 E7 F0 5A F8 2C 68 3F 5A B4 C3 9C 14 53 37 FE
1C 9C 12 06 49 00 7B 1F B8 72 BA 0E 67 2C 2C 83
32 2E 69 84 16 93 6F E5 B5 41 08 7F C1 D7 70 C5

228. BC 59 1F B3 2D 74 72 05 33 2A 63 AB 26 D4 50 71
87 E7 F0 5A F8 2C 68 3F 5A B4 C3 9C 14 53 37 FE
1C 9C 12 1E 49 00 7B 1F B8 72 BA 0E 67 2C 2C 83
32 2E 69 84 16 93 6F E5 B5 41 08 7F C1 D7 70 C5

229. BC 59 1F B3 2D 74 72 05 33 2A 63 AB 26 D4 50 71
87 E7 F0 5A F8 2C 68 3F 5A B4 C3 9C 14 53 37 FE
1C 9C 12 1E C1 00 7B 1F B8 72 BA 0E 67 2C 2C 83
32 2E 69 84 16 93 6F E5 B5 41 08 7F C1 D7 70 C5

230. BC 59 1F B3 2D 74 72 05 33 2A 63 AB 26 D4 50 71
87 E7 F0 5A F8 2C 68 3F 5A B4 C3 9C 14 53 37 FE
1C 9C 12 1E C1 B7 7B 1F B8 72 BA 0E 67 2C 2C 83
32 2E 69 84 16 93 6F E5 B5 41 08 7F C1 D7 70 C5

231. BC 59 1F B3 2D 74 72 05 33 2A 63 AB 26 D4 50 71
87 E7 F0 5A F8 2C 68 3F 5A B4 C3 9C 14 53 37 FE
1C 9C 12 1E C1 B7 7A 1F B8 72 BA 0E 67 2C 2C 83
32 2E 69 84 16 93 6F E5 B5 41 08 7F C1 D7 70 C5

232. BC 59 1F B3 2D 74 72 05 33 2A 63 AB 26 D4 50 71
87 E7 F0 5A F8 2C 68 3F 5A B4 C3 9C 14 53 37 FE
1C 9C 12 1E C1 B7 7A 9F B8 72 BA 0E 67 2C 2C 83
32 2E 69 84 16 93 6F E5 B5 41 08 7F C1 D7 70 C5

233. BC 59 1F B3 2D 74 72 05 33 2A 63 AB 26 D4 50 71
87 E7 F0 5A F8 2C 68 3F 5A B4 C3 9C 14 53 37 FE
1C 9C 12 1E C1 B7 7A 9F 55 72 BA 0E 67 2C 2C 83
32 2E 69 84 16 93 6F E5 B5 41 08 7F C1 D7 70 C5

234. BC 59 1F B3 2D 74 72 05 33 2A 63 AB 26 D4 50 71
87 E7 F0 5A F8 2C 68 3F 5A B4 C3 9C 14 53 37 FE
1C 9C 12 1E C1 B7 7A 9F 55 11 BA 0E 67 2C 2C 83
32 2E 69 84 16 93 6F E5 B5 41 08 7F C1 D7 70 C5

235. BC 59 1F B3 2D 74 72 05 33 2A 63 AB 26 D4 50 71
87 E7 F0 5A F8 2C 68 3F 5A B4 C3 9C 14 53 37 FE
1C 9C 12 1E C1 B7 7A 9F 55 11 2D 0E 67 2C 2C 83
32 2E 69 84 16 93 6F E5 B5 41 08 7F C1 D7 70 C5

236. BC 59 1F B3 2D 74 72 05 33 2A 63 AB 26 D4 50 71
87 E7 F0 5A F8 2C 68 3F 5A B4 C3 9C 14 53 37 FE
1C 9C 12 1E C1 B7 7A 9F 55 11 2D A2 67 2C 2C 83
32 2E 69 84 16 93 6F E5 B5 41 08 7F C1 D7 70 C5

237. BC 59 1F B3 2D 74 72 05 33 2A 63 AB 26 D4 50 71
87 E7 F0 5A F8 2C 68 3F 5A B4 C3 9C 14 53 37 FE
1C 9C 12 1E C1 B7 7A 9F 55 11 2D A2 DA 2C 2C 83
32 2E 69 84 16 93 6F E5 B5 41 08 7F C1 D7 70 C5

238. BC 59 1F B3 2D 74 72 05 33 2A 63 AB 26 D4 50 71
87 E7 F0 5A F8 2C 68 3F 5A B4 C3 9C 14 53 37 FE
1C 9C 12 1E C1 B7 7A 9F 55 11 2D A2 DA 1B 2C 83
32 2E 69 84 16 93 6F E5 B5 41 08 7F C1 D7 70 C5

239. BC 59 1F B3 2D 74 72 05 33 2A 63 AB 26 D4 50 71
87 E7 F0 5A F8 2C 68 3F 5A B4 C3 9C 14 53 37 FE

	1C	9C	12	1E	C1	B7	7A	9F	55	11	2D	A2	DA	1B	78	83
	32	2E	69	84	16	93	6F	E5	B5	41	08	7F	C1	D7	70	C5
240.	BC	59	1F	B3	2D	74	72	05	33	2A	63	AB	26	D4	50	71
	87	E7	F0	5A	F8	2C	68	3F	5A	B4	C3	9C	14	53	37	FE
	1C	9C	12	1E	C1	B7	7A	9F	55	11	2D	A2	DA	1B	78	94
	32	2E	69	84	16	93	6F	E5	B5	41	08	7F	C1	D7	70	C5
241.	BC	59	1F	B3	2D	74	72	05	33	2A	63	AB	26	D4	50	71
	87	E7	F0	5A	F8	2C	68	3F	5A	B4	C3	9C	14	53	37	FE
	1C	9C	12	1E	C1	B7	7A	9F	55	11	2D	A2	DA	1B	78	94
	90	2E	69	84	16	93	6F	E5	B5	41	08	7F	C1	D7	70	C5
242.	BC	59	1F	B3	2D	74	72	05	33	2A	63	AB	26	D4	50	71
	87	E7	F0	5A	F8	2C	68	3F	5A	B4	C3	9C	14	53	37	FE
	1C	9C	12	1E	C1	B7	7A	9F	55	11	2D	A2	DA	1B	78	94
	90	2D	69	84	16	93	6F	E5	B5	41	08	7F	C1	D7	70	C5
243.	BC	59	1F	B3	2D	74	72	05	33	2A	63	AB	26	D4	50	71
	87	E7	F0	5A	F8	2C	68	3F	5A	B4	C3	9C	14	53	37	FE
	1C	9C	12	1E	C1	B7	7A	9F	55	11	2D	A2	DA	1B	78	94
	90	2D	29	84	16	93	6F	E5	B5	41	08	7F	C1	D7	70	C5
244.	BC	59	1F	B3	2D	74	72	05	33	2A	63	AB	26	D4	50	71
	87	E7	F0	5A	F8	2C	68	3F	5A	B4	C3	9C	14	53	37	FE
	1C	9C	12	1E	C1	B7	7A	9F	55	11	2D	A2	DA	1B	78	94
	90	2D	29	DC	16	93	6F	E5	B5	41	08	7F	C1	D7	70	C5
245.	BC	59	1F	B3	2D	74	72	05	33	2A	63	AB	26	D4	50	71
	87	E7	F0	5A	F8	2C	68	3F	5A	B4	C3	9C	14	53	37	FE
	1C	9C	12	1E	C1	B7	7A	9F	55	11	2D	A2	DA	1B	78	94
	90	2D	29	DC	4C	93	6F	E5	B5	41	08	7F	C1	D7	70	C5
246.	BC	59	1F	B3	2D	74	72	05	33	2A	63	AB	26	D4	50	71
	87	E7	F0	5A	F8	2C	68	3F	5A	B4	C3	9C	14	53	37	FE
	1C	9C	12	1E	C1	B7	7A	9F	55	11	2D	A2	DA	1B	78	94
	90	2D	29	DC	4C	38	6F	E5	B5	41	08	7F	C1	D7	70	C5
247.	BC	59	1F	B3	2D	74	72	05	33	2A	63	AB	26	D4	50	71
	87	E7	F0	5A	F8	2C	68	3F	5A	B4	C3	9C	14	53	37	FE
	1C	9C	12	1E	C1	B7	7A	9F	55	11	2D	A2	DA	1B	78	94
	90	2D	29	DC	4C	38	87	E5	B5	41	08	7F	C1	D7	70	C5
248.	BC	59	1F	B3	2D	74	72	05	33	2A	63	AB	26	D4	50	71
	87	E7	F0	5A	F8	2C	68	3F	5A	B4	C3	9C	14	53	37	FE
	1C	9C	12	1E	C1	B7	7A	9F	55	11	2D	A2	DA	1B	78	94
	90	2D	29	DC	4C	38	87	D8	B5	41	08	7F	C1	D7	70	C5
249.	BC	59	1F	B3	2D	74	72	05	33	2A	63	AB	26	D4	50	71
	87	E7	F0	5A	F8	2C	68	3F	5A	B4	C3	9C	14	53	37	FE
	1C	9C	12	1E	C1	B7	7A	9F	55	11	2D	A2	DA	1B	78	94
	90	2D	29	DC	4C	38	87	D8	5C	41	08	7F	C1	D7	70	C5
250.	BC	59	1F	B3	2D	74	72	05	33	2A	63	AB	26	D4	50	71
	87	E7	F0	5A	F8	2C	68	3F	5A	B4	C3	9C	14	53	37	FE
	1C	9C	12	1E	C1	B7	7A	9F	55	11	2D	A2	DA	1B	78	94
	90	2D	29	DC	4C	38	87	D8	5C	1C	08	7F	C1	D7	70	C5
251.	BC	59	1F	B3	2D	74	72	05	33	2A	63	AB	26	D4	50	71
	87	E7	F0	5A	F8	2C	68	3F	5A	B4	C3	9C	14	53	37	FE
	1C	9C	12	1E	C1	B7	7A	9F	55	11	2D	A2	DA	1B	78	94
	90	2D	29	DC	4C	38	87	D8	5C	1C	58	7F	C1	D7	70	C5
252.	BC	59	1F	B3	2D	74	72	05	33	2A	63	AB	26	D4	50	71
	87	E7	F0	5A	F8	2C	68	3F	5A	B4	C3	9C	14	53	37	FE
	1C	9C	12	1E	C1	B7	7A	9F	55	11	2D	A2	DA	1B	78	94

90 2D 29 DC 4C 38 87 D8 5C 1C 58 02 C1 D7 70 C5

253. BC 59 1F B3 2D 74 72 05 33 2A 63 AB 26 D4 50 71
87 E7 F0 5A F8 2C 68 3F 5A B4 C3 9C 14 53 37 FE
1C 9C 12 1E C1 B7 7A 9F 55 11 2D A2 DA 1B 78 94
90 2D 29 DC 4C 38 87 D8 5C 1C 58 02 32 D7 70 C5

254. BC 59 1F B3 2D 74 72 05 33 2A 63 AB 26 D4 50 71
87 E7 F0 5A F8 2C 68 3F 5A B4 C3 9C 14 53 37 FE
1C 9C 12 1E C1 B7 7A 9F 55 11 2D A2 DA 1B 78 94
90 2D 29 DC 4C 38 87 D8 5C 1C 58 02 32 C8 70 C5

255. BC 59 1F B3 2D 74 72 05 33 2A 63 AB 26 D4 50 71
87 E7 F0 5A F8 2C 68 3F 5A B4 C3 9C 14 53 37 FE
1C 9C 12 1E C1 B7 7A 9F 55 11 2D A2 DA 1B 78 94
90 2D 29 DC 4C 38 87 D8 5C 1C 58 02 32 C8 CB C5

256. BC 59 1F B3 2D 74 72 05 33 2A 63 AB 26 D4 50 71
87 E7 F0 5A F8 2C 68 3F 5A B4 C3 9C 14 53 37 FE
1C 9C 12 1E C1 B7 7A 9F 55 11 2D A2 DA 1B 78 94
90 2D 29 DC 4C 38 87 D8 5C 1C 58 02 32 C8 CB C7

257. 74 59 1F B3 2D 74 72 05 33 2A 63 AB 26 D4 50 71
87 E7 F0 5A F8 2C 68 3F 5A B4 C3 9C 14 53 37 FE
1C 9C 12 1E C1 B7 7A 9F 55 11 2D A2 DA 1B 78 94
90 2D 29 DC 4C 38 87 D8 5C 1C 58 02 32 C8 CB C7

258. 74 09 1F B3 2D 74 72 05 33 2A 63 AB 26 D4 50 71
87 E7 F0 5A F8 2C 68 3F 5A B4 C3 9C 14 53 37 FE
1C 9C 12 1E C1 B7 7A 9F 55 11 2D A2 DA 1B 78 94
90 2D 29 DC 4C 38 87 D8 5C 1C 58 02 32 C8 CB C7

259. 74 09 D4 B3 2D 74 72 05 33 2A 63 AB 26 D4 50 71
87 E7 F0 5A F8 2C 68 3F 5A B4 C3 9C 14 53 37 FE
1C 9C 12 1E C1 B7 7A 9F 55 11 2D A2 DA 1B 78 94
90 2D 29 DC 4C 38 87 D8 5C 1C 58 02 32 C8 CB C7

260. 74 09 D4 7E 2D 74 72 05 33 2A 63 AB 26 D4 50 71
87 E7 F0 5A F8 2C 68 3F 5A B4 C3 9C 14 53 37 FE
1C 9C 12 1E C1 B7 7A 9F 55 11 2D A2 DA 1B 78 94
90 2D 29 DC 4C 38 87 D8 5C 1C 58 02 32 C8 CB C7

261. 74 09 D4 7E BC 74 72 05 33 2A 63 AB 26 D4 50 71
87 E7 F0 5A F8 2C 68 3F 5A B4 C3 9C 14 53 37 FE
1C 9C 12 1E C1 B7 7A 9F 55 11 2D A2 DA 1B 78 94
90 2D 29 DC 4C 38 87 D8 5C 1C 58 02 32 C8 CB C7

262. 74 09 D4 7E BC 97 72 05 33 2A 63 AB 26 D4 50 71
87 E7 F0 5A F8 2C 68 3F 5A B4 C3 9C 14 53 37 FE
1C 9C 12 1E C1 B7 7A 9F 55 11 2D A2 DA 1B 78 94
90 2D 29 DC 4C 38 87 D8 5C 1C 58 02 32 C8 CB C7

263. 74 09 D4 7E BC 97 3B 05 33 2A 63 AB 26 D4 50 71
87 E7 F0 5A F8 2C 68 3F 5A B4 C3 9C 14 53 37 FE
1C 9C 12 1E C1 B7 7A 9F 55 11 2D A2 DA 1B 78 94
90 2D 29 DC 4C 38 87 D8 5C 1C 58 02 32 C8 CB C7

264. 74 09 D4 7E BC 97 3B FE 33 2A 63 AB 26 D4 50 71
87 E7 F0 5A F8 2C 68 3F 5A B4 C3 9C 14 53 37 FE
1C 9C 12 1E C1 B7 7A 9F 55 11 2D A2 DA 1B 78 94
90 2D 29 DC 4C 38 87 D8 5C 1C 58 02 32 C8 CB C7

265. 74 09 D4 7E BC 97 3B FE E5 2A 63 AB 26 D4 50 71
87 E7 F0 5A F8 2C 68 3F 5A B4 C3 9C 14 53 37 FE
1C 9C 12 1E C1 B7 7A 9F 55 11 2D A2 DA 1B 78 94
90 2D 29 DC 4C 38 87 D8 5C 1C 58 02 32 C8 CB C7

266. 74 09 D4 7E BC 97 3B FE E5 7F 63 AB 26 D4 50 71
87 E7 F0 5A F8 2C 68 3F 5A B4 C3 9C 14 53 37 FE
1C 9C 12 1E C1 B7 7A 9F 55 11 2D A2 DA 1B 78 94
90 2D 29 DC 4C 38 87 D8 5C 1C 58 02 32 C8 CB C7

267. 74 09 D4 7E BC 97 3B FE E5 7F 7D AB 26 D4 50 71
87 E7 F0 5A F8 2C 68 3F 5A B4 C3 9C 14 53 37 FE
1C 9C 12 1E C1 B7 7A 9F 55 11 2D A2 DA 1B 78 94
90 2D 29 DC 4C 38 87 D8 5C 1C 58 02 32 C8 CB C7

268. 74 09 D4 7E BC 97 3B FE E5 7F 7D 82 26 D4 50 71
87 E7 F0 5A F8 2C 68 3F 5A B4 C3 9C 14 53 37 FE
1C 9C 12 1E C1 B7 7A 9F 55 11 2D A2 DA 1B 78 94
90 2D 29 DC 4C 38 87 D8 5C 1C 58 02 32 C8 CB C7

Message digest:

74 09 D4 7E BC 97 3B FE E5 7F 7D 82 26 D4 50 71
87 E7 F0 5A F8 2C 68 3F 5A B4 C3 9C 14 53 37 FE
1C 9C 12 1E C1 B7 7A 9F 55 11 2D A2 DA 1B 78 94
90 2D 29 DC 4C 38 87 D8 5C 1C 58 02 32 C8 CB C7

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:

- for case n = 224 28 bytes;
- for case n = 256 32 bytes;
- for case n = 384 48 bytes;
- for case n = 512 64 bytes.

In addition, algorithm need 2 bytes for work with messages, that have remain bits, i.e. length in bits is not multiple 8: one byte – for remain bits, another – for remain bits number.

Total memory requirements:

n = 224	290 bytes
n = 256	294 bytes
n = 384	310 bytes
n = 512	326 bytes

This memory requirements same for 8-bits, 16-bits, 32-bits and 64-bits processors.

9.2 Computation Efficiency

Except preprocessing stage, all another algorithm's stages perform only SR steps. In each SR step algorithm use only following operations with bytes:

1. Addition two bytes on the module 256.
2. Subtraction two bytes on the module 256.
3. Get SR point value: get element from SR state using SR point as address.
4. Substitution for byte: get element from substitution table using byte as address.
5. Move one byte.
6. Compare two bytes.

Each of operations 1 – 6 will be called *elementary operation*.
Note that operation

7. Increase byte on module N

can be performed using elementary operations:

Addition 1 to byte on the module 256;
Compare result with N;
Replacement result on zero if compare result – success.

Assume Increase byte on module N as two elementary operations.

Then one SR step perform:

- 4 elementary operations (type 3) for calculate y_{p1},y_{p2},y_{p3},y_{p4};
- 4 elementary operations (type 1, 2 and 5) for calculate $y_{p1} - y_{p2} - y_{p3} + y_{p4}$;
- 1 elementary operation (type 4) for calculate $\pi(y_{p1} - y_{p2} - y_{p3} + y_{p4})$;
- 1 elementary operation (type 1) for calculate $\pi(y_{p1} - y_{p2} - y_{p3} + y_{p4}) + x$;
- 1 elementary operation (type 5) for replace byte in SR state;
- 8 elementary operations (type 8) for increase SR points.

Total, during one SR step algorithm perform 19 elementary operations.
Note, that during pre-hash calculations, for each message byte algorithm perform 19 elementary operations for first step and 18 elementary operations for steps number 2 – 4 (see 6).

For final hash computation necessary 4*N steps or 19*4*N elementary operations. There are following values:

n = 224	2128
n = 256	2432
n = 384	3648
n = 512	4864

For pre-hash computation for message length in bytes L necessary 19*L + 3*18*L = 73*L elementary operations. Table below demonstrate number of elementary operations Q, that are necessary for calculate message digest for different hash length.

	n	L	Q
1	224	1000	75128
2	256	1000	75432
3	384	1000	76648
4	512	1000	77864

Following data compare MCSSHA-3 speed with another hash algorithms SHA-224, SHA-256, SHA-384, SHA-512 speed. The source codes for this algorithms were copied from OpenSSL web site (http://www.openssl.org/source).

1) 32-bits OS
MS Windows Vista OS, 32-bits, Genuine Intel Core 2 CPU T2500 @ 2.00 GHz 2.00 GHz.

```
##################
SHA-224 speed test
Number of tests = 1000
Text length = 100000
Time: 2,613 sec.

##################
MCSSHA-3 speed test
Language: C
HashBitLen = 224
Number of tests = 1000
Text length = 100000
Time: 4,132 sec.

##################
SHA-256 speed test
Number of tests = 1000
Text length = 100000
Time: 2,599 sec.

##################
MCSSHA-3 speed test
Language: C
HashBitLen = 256
Number of tests = 1000
Text length = 100000
Time: 3,004 sec.

##################
SHA-384 speed test
Number of tests = 1000
Text length = 100000
Time: 4,783 sec.

##################
MCSSHA-3 speed test
Language: C
HashBitLen = 384
Number of tests = 1000
Text length = 100000
Time: 4,193 sec.

##################
SHA-512 speed test
Number of tests = 1000
Text length = 100000
Time: 6,038 sec.

##################
MCSSHA-3 speed test
Language: C
HashBitLen = 512
Number of tests = 1000
Text length = 100000
Time: 3,721 sec.
```

2) 64-bits OS
MS Windows Server 2003 R2, Enterprise x64 Edition, Service Pack 1, AMD Athlon 64 Processor, 3200+, 2.01 GHz.

```
##################
SHA-224 speed test
Number of tests = 1000
Text length = 100000
Time: 2.61 sec.

##################
MCSSHA-3 speed test
Language: C
HashBitLen = 224
Number of tests = 1000
Text length = 100000
Time: 7.032 sec.

##################
SHA-256 speed test
Number of tests = 1000
Text length = 100000
Time: 2.61 sec.

##################
MCSSHA-3 speed test
Language: C
HashBitLen = 256
Number of tests = 1000
Text length = 100000
Time: 5.063 sec.

##################
SHA-384 speed test
Number of tests = 1000
Text length = 100000
Time: 3.875 sec.

##################
MCSSHA-3 speed test
Language: C
HashBitLen = 384
Number of tests = 1000
Text length = 100000
Time: 7.031 sec.

##################
SHA-512 speed test
Number of tests = 1000
Text length = 100000
Time: 3.875 sec.

##################
MCSSHA-3 speed test
Language: C
HashBitLen = 512
Number of tests = 1000
Text length = 100000
Time: 5.344 sec.
```

The algorithm MCSSHA-3 can be realized by means of language Assembly. In this case may be some prize in speed due to optimization of performance of some operations. Below results of tests of speed of algorithm MCSSHA-3 are resulted at its realization on C and Assembly.

1) 32-bits OS
MS Windows Vista OS, 32-bits, Genuine Intel Core 2 CPU T2500 @ 2.00 GHz 2.00 GHz.

```
##################
MCSSHA-3 speed test
Language: C
HashBitLen = 224
Number of tests = 10000
```

Text length = 10000
Time: 4,642 sec.

##################
MCSSHA-3 speed test
Language: Assembly
HashBitLen = 224
Number of tests = 10000
Text length = 10000
Time: 6,94 sec.

##################
MCSSHA-3 speed test
Language: C
HashBitLen = 256
Number of tests = 10000
Text length = 10000
Time: 2,929 sec.

##################
MCSSHA-3 speed test
Language: Assembly
HashBitLen = 256
Number of tests = 10000
Text length = 10000
Time: 6,328 sec.

##################
MCSSHA-3 speed test
Language: C
HashBitLen = 384
Number of tests = 10000
Text length = 10000
Time: 4,662 sec.

##################
MCSSHA-3 speed test
Language: Assembly
HashBitLen = 384
Number of tests = 10000
Text length = 10000
Time: 7,044 sec.

##################
MCSSHA-3 speed test
Language: C
HashBitLen = 512
Number of tests = 10000
Text length = 10000
Time: 3,017 sec.

##################
MCSSHA-3 speed test
Language: Assembly
HashBitLen = 512
Number of tests = 10000
Text length = 10000
Time: 6,366 sec.

2) 64-bits OS
MS Windows Server 2003 R2, Enterprise x64 Edition, Service Pack 1, AMD Athlon 64 Processor, 3200+, 2.01 GHz.

##################
MCSSHA-3 speed test
Language: C
HashBitLen = 224
Number of tests = 10000
Text length = 10000
Time: 6.906 sec.

##################

MCSSHA-3 speed test
Language: Assembly
HashBitLen = 224
Number of tests = 10000
Text length = 10000
Time: 5.234 sec.

##################
MCSSHA-3 speed test
Language: C
HashBitLen = 256
Number of tests = 10000
Text length = 10000
Time: 4.985 sec.

##################
MCSSHA-3 speed test
Language: Assembly
HashBitLen = 256
Number of tests = 10000
Text length = 10000
Time: 5.266 sec.

##################
MCSSHA-3 speed test
Language: C
HashBitLen = 384
Number of tests = 10000
Text length = 10000
Time: 6.906 sec.

##################
MCSSHA-3 speed test
Language: Assembly
HashBitLen = 384
Number of tests = 10000
Text length = 10000
Time: 5.25 sec.

##################
MCSSHA-3 speed test
Language: C
HashBitLen = 512
Number of tests = 10000
Text length = 10000
Time: 5.234 sec.

##################
MCSSHA-3 speed test
Language: Assembly
HashBitLen = 512
Number of tests = 10000
Text length = 10000
Time: 5.297 sec.

Comparison of hash speed with MS Base Smart Card Crypto Provider.

In this section we compare hash speed MCSSHA-3 algorithm and SHA-256, SHA-384, SHA-512 algorithms, which are realized in Microsoft Base Smart Card Crypto Provider for 32-bits OS (MS CSP). MCSSHA-3 algorithm realized in Nets IDSafe Crypto Service Provider (Nets CSP). During this tests message digest calculated 100000 times for text “abc”.

32-bits OS.

MCSSHA-3 (224 bits)
Testing time: 0.468000

SHA-256
Testing time: 0.468000

MCSSHA-3 (256 bits)

Testing time: 0.483000

SHA-384
Testing time: 0.842000

MCSSHA-3 (384 bits)
Testing time: 0.671000

SHA-512
Testing time: 0.842000

MCSSHA-3 (512 bits)
Testing time: 0.734000

64-bits OS.

MCSSHA-3 (224 bits)
Testing time: 0.500000

MCSSHA-3 (256 bits)
Testing time: 0.469000

MCSSHA-3 (384 bits)
Testing time: 0.735000

MCSSHA-3 (512 bits)
Testing time: 0.765000

9.3 HMAC support.

MCSSHA-3 algorithm have construction to support HMAC as a pseudo random function. This construction similar to construction used in OpenSSL functions to support HMAC for SHA-256, SHA-384 and SHA-512. Following data allow to compare HMAC speed for known algorithms SHA-256, SHA-384, SHA-512 and MCSSHA-3. For MCSSHA-3 was used Nets CSP, for SHA-256, SHA-384, SHA-512 - MS CSP. During this tests HMAC calculated 10000 times for text length 10 bytes, encrypt key – for 3DES.

32-bits OS.

MCSSHA-3 (224 bits)
Testing time: 0.671000

SHA-256
Testing time: 0.514000

MCSSHA-3 (256 bits)
Testing time: 0.640000

SHA-384
Testing time: 0.717000

MCSSHA-3 (384 bits)
Testing time: 0.702000

SHA-512
Testing time: 0.718000

MCSSHA-3 (512 bits)
Testing time: 0.717000

64-bits OS.

MCSSHA-3 (224 bits)

Testing time: 1.750000

MCSSHA-3 (256 bits)
Testing time: 1.688000

MCSSHA-3 (384 bits)
Testing time: 1.796000

MCSSHA-3 (512 bits)
Testing time: 1.796000

10. CRYPTOGRAPHY ANALYSIS

10.1 Mathematical bases of algorithm MCSSHA-3.

Basis of the algorithm MCSSHA-3 consist transformations, which are carried out using regular shift-register with length n and elements from Z/256. All operations ("+" and " –") with shift-register elements performs in Z/256. Figure 1 shows such register.

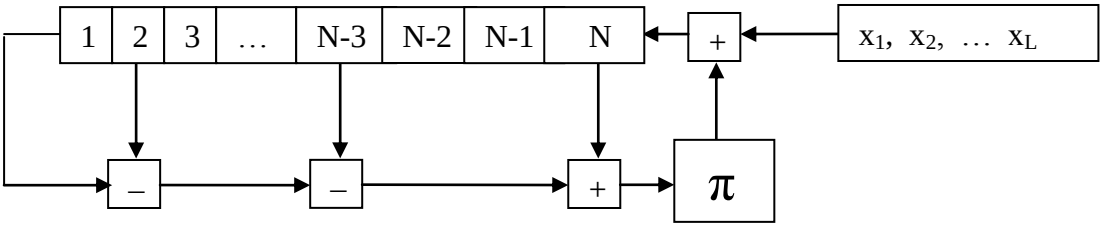

Figure 1.

where N = hashbitlen/8,
hashbitlen – hash length (in bits), 224, 256, 384 or 512,

π - substitution from symmetric group S_{256},
$x_1, x_2, \ldots x_L$ – input sequence in bytes, i.e from Z/256.
Shift-registry elements are bytes, i.e. elements from Z/256, *shift-registry state(SR state)* is vector $(y_i,y_{i+1},\ldots,y_{i+N-1})$,
where any value $y_i,y_{i+1}, \ldots, y_{i+N-1}$ is byte, i.e. element from Z/256.
If $(y_i,y_{i+1}, \ldots, y_{i+N-1})$ – SR state before i-step of work, than after i-step of work it will be $(y_{i+1},y_{i+2}, \ldots, y_{i+N})$, where

$$y_{i+N} = \pi(y_i - y_{i+1} - y_{i+N-4} + y_{i+N-1}) + x_i.$$

The values 0,1,N-4,N-1 for which we calculate argument for substitution π, in feature will be called *shift-registry points (SR points).*

10.1.1 Logarithmic substitution π.

For creation of necessary cryptographic reliability of transformation, substitution should provide "avalanche effect" duplication of distinctions of the text of the message. Such "avalanche effect " is defined by a matrix of transitive probabilities nonzero bigram P(π), i. e. a matrix of the size 255x255 in which on crossing of i-th row and j-th column there is p_{ij} - number of solutions of the system:

$$\begin{aligned} x - y &= i \\ \pi(x) - \pi(y) &= j \end{aligned} \qquad (10.1)$$

in Z/256 for each $i,j \neq 0$.
The "avalanche effect " that will be better, than less zero the matrix P(π) will contain. It is easy to prove, that the number of zero in this matrix cannot be less, than 253.

Let's notice, that $p_{ij} = p_{(256-i)(256-j)}$. For each solution (x_1,y_1) of the system (10.1) there is 1-1 response for solution $(x_2,y_2)=(y_1,x_1)$ of the system

$x-y = 256-i$

$\pi(x) - \pi(y) = 256-j$

if (10.1) multiply with –1.

From (10.1) it's clear that number of solutions (10.1) is same as number of values y, for which

$\pi(y+i) - \pi(y) = j$ (10.2)

If for each solution (x_1,y_1) of the system (10.1) set 1-1 response pair $(x_2,y_2) = (\pi^{-1}(x_1),\pi^{-1}(y_1))$, so this pair will be solution of the system

$x-y = j$ (10.3)

$\pi^{-1}(x) - \pi^{-1}(y) = i$

Hence, number of solutions (10.1) will be same as number of values y, for which

$\pi^{-1}(y+j) - \pi^{-1}(y) = i$ (10.4)

From (10.2) it's clear that the sum of all elements p_{ij} in row i for any i is 256. Similarly, from (10.4) it's clear, that sum of all elements p_{ij} in column j for any j is equal 256.

Because size of $P(\pi)$ is equal 255x255 and the sum of all elements p_{ij} in row i for any i is 256, so this means that if matrix $P(\pi)$ doesn't contain zeros => for any row all elements equal 1 except one element, that is 2. Similarly, for any column all elements equal 1 except one element, that is 2.

If for some y

$\pi(y+128) - \pi(y) = 128,$ (10.5)

as 256–128 = 128 means that (10.5) will be true for $y_1 = y+128$. This means, that $p_{(128)(128)}$ can't be odd.

Let's some row i doesn't contain zeros. This means, that among values $j_0,j_1,\ldots,j_{255}$,where

$j_k = \pi(k+i)- \pi(k)$ (10.6)

there are all non-zero elements from Z/256, and only one element present exactly 2 times.

Let's sum (10.6) for all k from 0 to 255. Because π - substitution, this means that right part must be zero => sum of all j_k must be zero too.

But among values $j_0,j_1,\ldots,j_{255}$ there are all non-zero elements from Z/256, and only one element present 2 times. Because sum (mod 256) of all non-zero elements of the Z/256 is 128*255 = 128, this means, that element 128 present two times.

So, because $p_{ij} = p_{(256-i)(256-j)}$ for any i should be

$p_{i128} = p_{(256-i)128} = 2$

and for $i\neq128$ in 128 column as minimum 2 element equals 2. This means that total number of zeros in $P(\pi)$ can't be less than 256-3 = 253. In this case in matrix exactly two non-zero rows, symmetrized from each other, and in an average line with number 128 exactly one zero value in the middle: p(128)(128) = 0.

The example of the substitutions possessing minimally possible number of zero in a matrix $P(\boldsymbol{\pi})$ is known – this is logarithmic substitutions, i.e.

$$\pi(x) = \log_\theta(\theta^{x+r} \oplus \rho) \text{ if } \theta^{x+r} \oplus \rho \neq 0,$$
$$\pi(x) = \log_\theta \rho \text{ if } \theta^{x+r} \oplus \rho = 0. \quad (10.7)$$

Here:

θ – primitive element of the GF(257) field,

ρ – non-zero element of the GF(257) field,

r – any element of the Z/256 ring.

Here and in the further we have two types of operations:

"+" and "-" – operations in Z/256.

"$\oplus$" and "$\ominus$" – operations in GF(257).

Element x_0 for which $\theta^{x+r} \oplus \rho = 0$, let's name *exclusive point* of logarithmic substitution.

Theorem 1.1.1.

Let's π – logarithmic substitution, $x_1 \neq x_2$, $x_1, x_2 \in Z/256$, i – any element from Z/256, $i \neq 0$.
Then if any of points x_1+i, x_1, x_2+i, x_2 is not exclusive => $\pi(x_1+i) - \pi(x_1) \neq \pi(x_2+i) - \pi(x_2)$.

Proof.

Let's $\pi(x_1+i) - \pi(x_1) = \pi(x_2+i) - \pi(x_2)$, => $\theta^{\pi(x1+i) - \pi(x1)} = \theta^{\pi(x2+i) - \pi(x2)}$ =>
$(\theta^{x1+i+r} \oplus \rho)(\theta^{x2+r} \oplus \rho) = (\theta^{x2+i+r} \oplus \rho)(\theta^{x1+r} \oplus \rho)$,
because all points is not exclusive.
This means $\rho\,(\theta^{x1+i+r} \oplus \theta^{x2+r}) = \rho(\theta^{x2+i+r} \oplus \theta^{x1+r})$
Because ρ - is non-zero, so
$\theta^{x1+r}(\theta^{i} \ominus 1) = \theta^{x2+r}(\theta^{i} \ominus 1)$
Because i – any non-zero element from Z/256, θ - primitive element from GF(257), so $\theta^i \neq 1$, => $x_1 = x_2$. ■

Theorem 1.1.2.

Let's π – logarithmic substitution.
Then for any non-zero $i \in Z/256\backslash\{0\}$ from a condition, that any of points x, x+i is not exclusive out follows, that
$\pi(x+i) - \pi(x) \neq i$.

Proof.

Let's $\pi(x+i) - \pi(x) = i$. Then $\theta^{\pi(x+i) - \pi(x)} = \theta^i$, => $\theta^{x+r+i} \oplus \rho = \theta^i(\theta^{x+r} \oplus \rho)$, so, $\rho = \rho\theta^i$ => i=0. ■

Let's see exclusive point x_0.
For any non-zero $i \in Z/256\backslash\{0\}$ let's see transformation Z/256 in Z/256 type:
$\mu_i(x) = \pi(x+i) - \pi(x)$,
where π - logarithmic substitution. Then from theorem 1.1.1 => number of different values in $\{\mu_i(x), x \in Z/256\backslash\{x_0, x_0-i\}\}$ is equal 254. From theorem 1.1.2 => this is exactly $\{Z/256\backslash\{0,i\}\}$. In particular, for any $i \neq 128$ exists x, $x \in Z/256\backslash\{x_0, x_0-i\}$, than $\mu_i(x) = 128$.

Theorem 1.1.3.

Let'a π – logarithmic substitution.
Then if for some $i \neq 128$ in row i of matrix $P(\pi)$ it's true $p_{(i)(128)} > 1$, then this row doesn't contain zeroes.

Proof.

From theorem 1.1.2 it's enough to proof that $p_{ii} \neq 0$. Condition $p(i)(128) > 1$means, that or $\mu_i(x_0) = 128$, or $\mu_i(x_0-i) = 128$. Let's $\mu \in \{\mu_i(x_0), \mu_i(x_0-i)\}$ and $\mu \neq 128$. Let's sum $\mu_i(x)$ for all $x \in Z/256$, than:
$128*255 - i + \mu + 128 = 0$ => $\mu = i$ => $p_{ii} \neq 0$. ■

Let's see $p_{(128)(128)}$. It's can't be odd => $p_{(128)(128)} = 0$ or $p_{(128)(128)} = 2$.
Let's $p_{(128)(128)} = 2$. From theorem 1.1.2 for any non-exclusive point $\pi(x+128) - \pi(x) \neq 128$. This means, that $\pi(x_0+128) - \pi(x_0) = 128$ and $\pi(x_0) - \pi(x_0+128) = 128$ => $2\pi(x_0) = 2\pi(x_0+128)$. This is impossible, because π – substitution => $p_{(128)(128)} = 0$.

So, we can find as minimum one row i, for which $p_{(128),i} \geq 2$, and according theorem 1.1.3 this row doesn't contain zeroes. The common number of zero in such matrix, in view of its already mentioned symmetry, will be equal 253. This is minimally possible quantity of zero.

Substitution π in MCSSHA-3 are logarithmic substitution with $\theta = 3$, $\rho = 1$, r=0.

10.2 Strategy of possible cryptographic attacks.

According 4Aii [1]

If a construct is specified for the use of the candidate algorithm in a randomized hashing scheme, the construct must, with overwhelming probability, provide *n* bits of security against the following attack:
The attacker chooses a message, *M1*. The specified construct is then used on *M1* with a randomization value *r1* that has been randomly chosen without the attacker's control after the attacker has supplied *M1*. Given *r1*, the attacker then attempts to find a second message *M2* and randomization value *r2* that yield the same randomized hash value.

According 4Aiii[1]

NIST expects the SHA-3 algorithm of message digest size *n* to meet the following security requirements at a minimum. These requirements are believed to be satisfiable by fairly standard hash algorithm constructions; any result that shows that the candidate algorithm does not meet these requirements will be considered to be a serious attack.

- Collision resistance of approximately *n*/2 bits,
- Preimage resistance of approximately *n* bits,
- Second-preimage resistance of approximately *n*-*k* bits for any message shorter than 2*k* bits,
- Resistance to length-extension attacks, and
- Any *m*-bit hash function specified by taking a fixed subset of the candidate function's output bits is expected to meet the above requirements with *m* replacing *n*. (Note that an attacker can choose the *m*-bit subset specifically to allow a limited number of precomputed message digests to collide, but once the subset has been chosen, finding additional violations of the above properties is expected to be as hard as described above.)

10.2.1 Birthday attack method.

This is well-known method (see, for example, http://en.wikipedia.org/wiki/Birthday_attack) Birthday attack on a message digest of size n bits produce a collision with a workfactor approximately $2^{n/2}$ if assume that message digest chosen randomly or pseudorandomly. For algorithm MCSSHA-3 there are bases to assume, that message digest will be casual and equiprobable by virtue of described above properties of logarithmic substitution.

10.2.2 Method of "capture" SR states during pre-hash computation.

The goal of this method is construction of some false message, such that the SR states for false and true messages will be identical during pre-hash computation. In this case false message "capture" SR state for true message and then it's easy to create false message with the same message digest like message digest for true message.

During hash update transformations, message (length L) to be hashed is used in input sequence for registry transformations.
Let's δ_m – transformation with vectors $(y_1,y_2,\ldots,y_N)$, that

$$\delta_m(y_1,y_2,\ldots,y_N) = (y_2,y_3,\ldots,y_{N+1})$$

where

$$y_{N+1} = \pi(y_1 - y_2 - y_{N-3} + y_N) + m.$$

It's clear, that transformation δ_m is regular, i.e. δ_m is substitution from symmetric group $S(256^N)$. Note, that inverse transformation δ_m^{-1} for δ_m will be

$$\delta_m^{-1}(y_2,y_3,\ldots,y_{N+1}) = (y_1,y_2,\ldots,y_N)$$

where

$$y_1 = \pi^{-1}(y_{N+1} - m) + y_2 + y_{N-3} - y_N$$

and π^{-1} – inverse substitution for π.

Lets

$$M = m(1),m(2), \dots , m(L)$$

message from L bytes.

Pre-hash computation calculate SR state Y from initial SR state Y_0 using message-depended substitution δ_M from $S(256^N)$, where

$$Y = \delta_M(Y_0)$$

$$\delta_M = (\delta_0)^3\, \delta_{m(L)}\, (\delta_0)^3 \dots \delta_{m(2)}\, (\delta_0)^3\, \delta_{m(1)} \qquad (10.8)$$

Here and in future we will use notation from substitution's groups: multiplication $\delta_y\, \delta_x$ means that first applied substitution δ_x, second - δ_y.

In (10.8) δ_0 - substitution, that not depended from text bytes, i.e. δ_m where m=0 and

$$y_{N+1} = \pi(y_1 - y_2 - y_{N-3} + y_N) \qquad (10.9)$$

and $(\delta_0)^3 = \delta_0\, \delta_0\, \delta_0$ – 3-time multiplication of the substitution δ_0.

Let's $Y_0 = (y_0,y_1,...,y_{N-1})$ – initial SR state, $y_N,y_{N+1},...,y_{N+4L-1}$ – values of SR states, where

$y_{N+i} = \pi(y_i - y_{i+1} - y_{N+i-4} + y_{N+i-1}) + m(j)$, where $j = i/4 + 1$ if $i(\mathrm{mod}4)=0$ (10.10)

$y_{N+i} = \pi(y_i - y_{i+1} - y_{N+i-4} + y_{N+i-1})$ if $i(\mathrm{mod}4)\neq 0$ (10.11)

Values $y_N,y_{N+1},...,y_{N+4L-1}$ in future will be called *intermediate values* for message M.

Let's

$M1=(m1_1,m1_2,...,m1_{L1})$ from L1 bytes and
$M2=(m2_1,m2_2,...,m2_{L2})$ from L2 bytes

two different messages,

$y_N,y_{N+1},...,y_{N+4L1-1}$ and
$z_N,z_{N+1},...,z_{N+4L2-1}$

intermediate values for M1 and M2,
$\delta_{M1}(Y_0)$ and $\delta_{M2}(Y_0)$ – SR-states for this messages after pre-hash computation.

Let's M1 – fixed true message, and M2 – false message, that we try to create for capture M1.
Let's assume that for M1 and M2

$$\delta_{M1}(Y_0) = \delta_{M2}(Y_0)$$

i.e. message M2 can “capture” SR state for message M1.

In this case if

$$Y = \delta_0^{-3}\, \delta_{M1}\, (Y_0)$$
$$Z = \delta_0^{-3}\, \delta_{M2}\, (Y_0)$$

then Y = Z too.

If message M2 can capture M1, then number of steps for M2, when M2 first time capture M1, will be called *critical* and pointed as *t*. In this case

$$(y_t, y_{t+1}, ..., y_{t+N-1}) = (z_t, z_{t+1}, ..., z_{t+N-1}) \qquad (10.12)$$

Differently, critical number is number of factors in substitution’s multiplication:

$$\delta_{m2(L2)}\, (\delta_0)^3 \ldots\, \delta_{m2(2)}\, (\delta_0)^3\, \delta_{m2(1)}$$

It’s clear, that (t-1)(mod 4) = 0 and t = 4*L2 - 3.

Note, that (t+N-1)(mod 4) = 0, and for calculate value z_{t+N-1} we use (10.10). This means, that for any SR states for 1 step before capture

$$(y_{t-1}, y_t, ..., y_{t+N-2}),\ (z_{t-1}, z_t, ..., z_{t+N-2})$$

for false message M2 we can find value $m2_{L2}$ such that will be $y_{t+N-1} = z_{t+N-1}$.

For SR states for 2 steps before capture

$$(y_{t-2}, y_{t-1}, ..., y_{t+N-3}),\ (z_{t-2}, z_{t-1}, ..., z_{t+N-3})$$

must be

$$y_{t-2} - y_{t-1} = z_{t-2} - z_{t-1}$$

because (t+N-2)(mod 4) ≠ 0 and for calculate value z_{t+N-2} we use (10.11).

Same way, for SR states for 3 steps before capture

$$(y_{t-3}, y_{t-2}, ..., y_{t+N-4}),\ (z_{t-3}, z_{t-2}, ..., z_{t+N-4})$$

must be

$$y_{t-3} - y_{t-2} = z_{t-3} - z_{t-2}$$
$$y_{t-2} - y_{t-1} = z_{t-2} - z_{t-1}$$

and for SR states for 4 steps before capture

$$(y_{t-4}, y_{t-3}, ..., y_{t+N-5}),\ (z_{t-4}, z_{t-3}, ..., z_{t+N-5})$$

must be

$$y_{t-4} - y_{t-3} = z_{t-4} - z_{t-3}$$
$$y_{t-3} - y_{t-2} = z_{t-3} - z_{t-2}$$
$$y_{t-2} - y_{t-1} = z_{t-2} - z_{t-1}$$

Same ways we can get conditions for SR states for 8 steps before capture

$$(y_{t-8},y_{t-7},\ldots,y_{t+N-9}),\ (z_{t-8},z_{t-7},\ldots,z_{t+N-9})$$

must be

$$y_{t-8} - y_{t-7} = z_{t-8} - z_{t-7}$$
$$y_{t-7} - y_{t-6} = z_{t-7} - z_{t-6}$$
$$y_{t-6} - y_{t-5} = z_{t-6} - z_{t-5}$$

$$y_{t-4} - y_{t-3} = z_{t-4} - z_{t-3}$$
$$y_{t-3} - y_{t-2} = z_{t-3} - z_{t-2}$$
$$y_{t-2} - y_{t-1} = z_{t-2} - z_{t-1}$$

Because each of N = 28, 32, 48 and 64 is multiplication of 4, let's designate N = 4p.

For SR states for 4(p-1) steps before capture

$$(y_{t-N+4},y_{t-N+5},\ldots,y_t,y_{t+1},y_{t+2},y_{t+3}),\ (z_{t-N+4},z_{t-N+5},\ldots,z_t,z_{t+1},z_{t+2},z_{t+3})$$

must be

$$y_{t-N+4} - y_{t-N+5} = z_{t-N+4} - z_{t-N+5}$$
$$y_{t-N+5} - y_{t-N+6} = z_{t-N+5} - z_{t-N+6}$$
$$y_{t-N+6} - y_{t-N+7} = z_{t-N+6} - z_{t-N+7}$$

$$y_{t-N+8} - y_{t-N+9} = z_{t-N+8} - z_{t-N+9}$$
$$y_{t-N+9} - y_{t-N+10} = z_{t-N+9} - z_{t-N+10}$$
$$y_{t-N+10} - y_{t-N+11} = z_{t-N+10} - z_{t-N+11}$$

.....

$$y_{t-4} - y_{t-3} = z_{t-4} - z_{t-3}$$
$$y_{t-3} - y_{t-2} = z_{t-3} - z_{t-2}$$
$$y_{t-2} - y_{t-1} = z_{t-2} - z_{t-1}$$

Let's fixed first j = L2 – 2p +1 values in message M2. In this case we can calculate intermediate values

$$z_N,z_{N+1},\ldots,\ z_{N+i},z_{N+i+1},z_{N+i+2},z_{N+i+3}$$

where, according (10.10) i = 4(j-1) = 4*L2 – 2N = t – 2N + 3. So, (10.13) will be

$$z_N,z_{N+1},\ldots,\ z_{t-N+3},z_{t-N+4},z_{t-N+5},z_{t-N+6} \qquad (10.13)$$

Let's test L2 – 2p +1 values in M2 so, that equalities

$$y_{t-N+4} - y_{t-N+5} = z_{t-N+4} - z_{t-N+5}$$
$$y_{t-N+5} - y_{t-N+6} = z_{t-N+5} - z_{t-N+6} \qquad (10.14)$$

were true. Because probability that (10.14) will be true is $(2^{-8})^2 = 2^{-16}$, we need to test approximately 2^{16} different variants. Event (10.14) will be called event 1 and designates μ_1. It's probability will be designates ρ_1.

Let's test value L2 – 2p +2 in M2. This value add in the set (10.13) four new members:

$$z_{t-N+7}, z_{t-N+8}, z_{t-N+9}, z_{t-N+10}$$

Because t-N+7 = 4*L2 – 3 – N + 7 = 4*L2 – N + 4 and (4*L2 – N + 4)(mod 4)=0,

so value z_{t-N+7} calculates using (10.10). In this case we can find m_j so that equality

$$y_{t-N+6} - y_{t-N+7} = z_{t-N+6} - z_{t-N+7}$$

will be true. But then event

$$y_{t-N+8} - y_{t-N+9} = z_{t-N+8} - z_{t-N+9}$$
$$y_{t-N+9} - y_{t-N+10} = z_{t-N+9} - z_{t-N+10}$$

will be with probability 2^{-16}. This event will be called event 2 and designates μ_2. It's probability will be designates ρ_2.

Same way will be tested values L2 – 2p +3, L2 – 2p +4,..., L2 – p - 1 in M2. Last byte L2 – p - 1 add in the set (10.13) four new members:

$$z_{t-5}, z_{t-4}, z_{t-3}, z_{t-2}$$

because i = 4(j-1) = 4(L2-p-2) = t-5-N => N+i = t-5;

Last event will be event number p-1 designates μ_{p-1}. It's probability will be designates ρ_{p-1}.

Note, that if to assume that events $\mu_1, \mu_2, \ldots, \mu_{p-1}$ are independent, that total probability of the all this events is $(2^{-16})^{p-1}$. This means, that we need to test approximately $(2^{16})^{p-1}$ variants of the first L2 – 2p +1 values in M2 to get SR state with $\mu_1, \mu_2, \ldots, \mu_{p-1}$ events.

Let's test byte number L2 – p. In this case appear values

$$z_{t-1}, z_t, z_{t+1}, z_{t+2}$$

Note, that (t-1)(mod 4) = 0, and according (10.10) we can select $m2_{L2-p}$ so that will be true

$$y_{t-2} - y_{t-1} = z_{t-2} - z_{t-1}$$

But then event μ_p

$$y_t = z_t$$

$$y_{t+1} = z_{t+1}$$
$$y_{t+2} = z_{t+2}$$

will be appear with probability $(2^{-8})^3 = 2^{-24}$.

For the last p bytes in M2 we select each new byte so that the first intermediate value appearing due to it was same like in true message M1. Next 3 intermediate values will be same too.

Total, if assume that events $\mu_1, \mu_2, \ldots, \mu_p$ are independent, that total probability for first random L2 – 2p +1 values in M2 to capture this way true message M1 is $(2^{-8})^{(2p+1)} = (2^{-8})^{(N+2)/2} = 2^{-(n/2+8)}$.

The work factor for this method is $2^{(n/2+8)}$.

10.2.3 Conformity of MCSSHA-3 algorithm to cryptography requirements

At an assessment of conformity of algorithm to cryptographic requirements [1], we shall assume that all possible attacks the potential malefactor will try to carry out during pre-hash computation. During final hash computation any attack available only for short messages (less than 8 bits), and it's easy to test, that all message digests for all messages less than 8 bits are different. Let's see some kind of attack from [1].

Attacker chooses a message M_1 with a randomization value r_1 that has been randomly chosen without the attacker's control.

For MCSSHA-3 randomization value r_1 is intermediate values of the SR states during pre-hash computation.

Given r_1, the attacker then attempts to find a second message M_2 and randomization value r_2 that yield the same randomized hash value.

For MCSSHA-3 this means, that attacker try to capture M_1, because for final hash computation probability to get identical message digests from different SR states before final hash stage can be estimated as 2^{-n}.

So, work factor Q for any successfully attack (insert, replace or remove some bits in M_1 and create M_2 with the same message digest) can be estimated as successfully capture message M_1 during pre-hash computation. Results 10.2.2 can be demonstrated by Table 10.1.

Table 10.1. Work factor for any successfully attack.

n	Q
224	$2^{120} \approx 10^{36}$
256	$2^{136} \approx 10^{40}$
384	$2^{200} \approx 10^{60}$
512	$2^{264} \approx 10^{79}$

10.3 Provenance of constants and tables.

10.3.1 Initial SR states.

If we use all same bits in initial SR states in this case for different short messages (length < 8 bits) will be identical message digests, because in this case SR states before final stage can be same – see (7.1).
For example, if we use SR state (0,0,...,0) as initial, we have same message digest for any message that length in bits < 8 and all bits are 0. Same effect we have for "periodical" initial SR states like 010101...01 (in bits). SR state (in byte) 0 1 2 ,...,N-1 that used in MCSSHA-3, doesn't allow to find short messages (length in bits < 8) with the same values of vectors (7.1).

10.3.2 Substitution.

This is logarithmic substitution (see 10.1) with parameters $\theta = 3$, $\rho = 1$, $r=0$.

10.3.3 SR points and delay.

This parameters used in capture SR state method. All algorithm's parameters must provide workfactor (not below $2^{n/2}$) for this method and give the basis to believe that events $\mu_1, \mu_2,...,\mu_p$ are independent.

Note, that number of SR points and delay define speed of algorithm. One step contain 19 elementary operations, so if we reduce number of points, for example, will be use 3 instead 4 SR points, there will be for one step

- 3 elementary operations (type 3) for calculate y_{p1},y_{p2},y_{p3};
- 3 elementary operations (type 1, 2 and 5) for calculate $y_{p1} - y_{p2} + y_{p3}$;
- 1 elementary operation (type 4) for calculate $\pi(y_{p1} - y_{p2} + y_{p3})$;
- 1 elementary operation (type 1) for calculate $\pi(y_{p1} - y_{p2} + y_{p3}) + x$;
- 1 elementary operation (type 5) for replace byte in SR state;
- 6 elementary operations (type 8) for increase SR points.

Total – 15 operations instead 19, approximately increase speed on 21%. But in this case appear SR points configuration like in Figure 2.

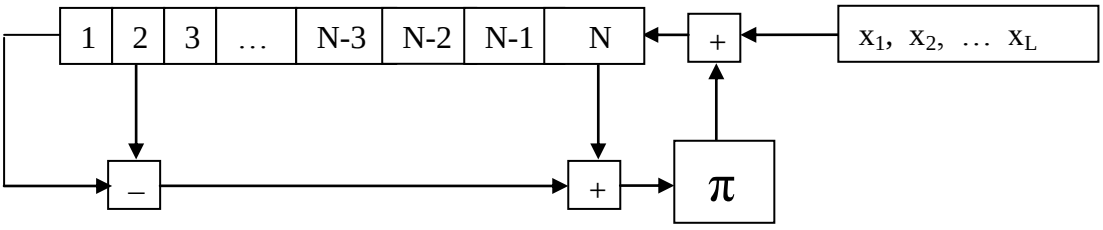

Figure 2.

This configuration can't rapidly multiple difference from one byte of the text. For example, if M1 and M2 have same first j bytes, then bytes j+1 are different, then all intermediate values

$$y_N, y_{N+1}, \ldots, y_{N+i}, y_{N+i+1}, y_{N+i+2}, y_{N+i+3}$$
$$z_N, z_{N+1}, \ldots, z_{N+i}, z_{N+i+1}, z_{N+i+2}, z_{N+i+3}$$

where i = 4(j-1), will be identical.

Then all values

$$y_{N+i+4}, y_{N+i+5}, y_{N+i+6}, y_{N+i+7}$$
$$z_{N+i+4}, z_{N+i+5}, z_{N+i+6}, z_{N+i+7}$$

will be different.
But then, because N+i+8 multiply 4, we can find, according (10.10) value $m2_{j+1}$ so that z_{N+i+8} will be same like y_{N+i+8}. In this case we have long set of the next identical intermediate values and potential dangerous to apply capture method with very small workfactor. Additional SR point prevents this dangerous phenomenon.

Let's try to decrease parameter Δ, i.e. delay of the algorithm. For example, use Δ = 2 instead 3. In this case we can increase speed approximately on 25%.

For Δ = 2 we have

$$y_{N+i} = \pi(y_i - y_{i+1} - y_{N+i-4} + y_{N+i-1}) + m(j), \text{ where } j = i/3 + 1 \qquad \text{if } i(\text{mod } 3)=0 \qquad (10.15)$$

$$y_{N+i} = \pi(y_i - y_{i+1} - y_{N+i-4} + y_{N+i-1}) \qquad \text{if } i(\text{mod } 3)\neq 0 \qquad (10.16)$$

and for critical step t will be rightly (t-1)(mod 3) = 0 and t = 3*L2 - 2.

In this case any event μ_i have probability approximately 2^{-8}, total we have N/3 events and workfactor for capture method will be approximately $2^{n/3}$.

So in MCSSHA-3 we use Δ = 3.

Appendix A. KAT and MCT tests.

Series of Known Answer Tests (KATs) and Monte Carlo Tests (MCTs) for MCSSHA-3 algorithm

ShortMsgKAT_224.txt
Algorithm Name: MCSSHA-3
Principal Submitter: Mikhail Maslennikov

Len = 0
Msg = 00
MD = 86E0035B2FA878EBB39BC5F8146743C32D86DB0CED3AAB1F7D8BA203

Len = 1
Msg = 00
MD = 11E97DE1655578152C1108BB9E971BE532DC6776162BD8F68A48531B

Len = 2
Msg = C0
MD = 80A1FEC9BFC7EED47EBA36859FD8A3B292C6C6B0C2EF526771F5BF7C

Len = 3
Msg = C0
MD = 40ACE688C8B1BB067ECD2851A01B57EC8B6149695E6CF60AA963B102

Len = 4
Msg = 80
MD = A9532DA075701F8BC2C15FC34D3D30F660B05F6FDD1446C7D2E3EC51

Len = 5
Msg = 48
MD = 5D03FE473D145FEAAC966D26CF7F5AE473755932B6BE5E4A16DE98E5

LongMsgKAT_224.txt
Algorithm Name: MCSSHA-3
Principal Submitter: Mikhail Maslennikov

Len = 2048
Msg =
724627916C50338643E6996F07877EAFD96BDF01DA7E991D4155B9BE1295EA7D21C9391
F4C4A41C75F77E5D27389253393725F1427F57914B273AB862B9E31DABCE506E55872052
0D33352D119F699E784F9E548FF91BC35CA147042128709820D69A8287EA3257857615EB
0321270E94B84F446942765CE882B191FAEE7E1C87E0F0BD4E0CD8A927703524B559B76
9CA4ECE1F6DBF313FDCF67C572EC4185C1A88E86EC11B6454B371980020F19633B6B95
BD280E4FBCB0161E1A82470320CEC6ECFA25AC73D09F1536F286D3F9DACAFB2CD1D
0CE72D64D197F5C7520B3CCB2FD74EB72664BA93853EF41EABF52F015DD591500D018
DD162815CC993595B195
MD = DDCACC0E5F097E777BD26541861D57FC4DF119B5413EF7D136A6922D
Len = 2111

Msg =
919FE5E7F35F64A7487649E564771DBBF10AE204ECC2181312D1A79FB579297C94F0DB9
EAAE9E009A4F02057AF2C973C5DAFA7B60154371A5D2C8E992FB6429176F8424B1A866
BC1D1BED00438E97FAB42040DCACDEF7CA9FC2033059B8898BB40CCFB2634B051797
BDF3B915C503EC81839AD01E0F4F2F871EFF2008D40011730BE7A47888E7955A806876B
E120CB0F3A139A3620154ECC6482A70F5629F6A9D3341BE6FBBF48E5AA0C53589A04F0
57DD44268AFFCABF75ADFC549F73F454264D46A98CCA80E3000C7446853DD5B430C93
44E87E3230555B09FB3E7E64B5AD3989293AC0FEEC0E75F909696F028A5525D26DDEA5
D2B2C813FB3613DFF38CE23209285CC77C60860
MD = D6C90D8D290D1AD8A0BCB6FB992C2714673B049F65206FE9786660E6

ExtremelyLongMsgKAT_224.txt
Algorithm Name: MCSSHA-3
Principal Submitter: Mikhail Maslennikov

Repeat = 16777216
Text = abcdefghbcdefghicdefghijdefghijkefghijklfghijklmghijklmnhijklmno
MD = A32032EB485B675831C14DE90D8D3A037E9AF5A37B3C14B8102144AD

MonteCarlo_224.txt
Algorithm Name: MCSSHA-3
Principal Submitter: Mikhail Maslennikov

Seed =
6CD4C0C5CB2CA2A0F1D1AECEBAC03B52E64EA03D1A1654372936545B92BBC5484A5
9DB74BB60F9C40CEB1A5AA35A6FAFE80349E14C253A4E8B1D77612DDD81ACE926AE
8B0AF6E53176DBFFCC2A6B88C6BD765F939D3D178A9BDE9EF3AA131C61E31C1E42C
DFAF4B4DCDE579A37E150EFBEF5555B4C1CB40439D835A724E2FAE7

j = 0
MD = 2F2281B6FB5C043171106384C0FDCFD5816AB0A630D2A923B1631016

j = 1
MD = 4196BCF2431FEE0F8BDC27C2A87012C14813381059985FD4C6CA4356

j = 2
MD = 843E74CC513BBC7F314B55BF53DB8C3DCD15BA01DAA524EAC42DCA48

j = 3
MD = A5E2BF4473AF8BE51EFFE06362B4DB31E12D722162C14F731A3B7244

j = 4
MD = F252B4DDC218D91F2E916423605EEB29D5590D16EC0F6CD952D1F923

j = 5
MD = 64A2965F1A8225BC91FCAC11A4A1ADBD9ED18CC1CBA765776D3B0894

ShortMsgKAT_256.txt
Algorithm Name: MCSSHA-3
Principal Submitter: Mikhail Maslennikov

Len = 0
Msg = 00
MD = 98860DB896BDF160B8C085213F72DA607CE6A75D2C6814B706A4A75AAE6AA10F

Len = 1
Msg = 00
MD = D05A6A971044B95E2A74A282785D6BC096C00193B84F2D93C24B6E0E6B77EA42

Len = 2
Msg = C0
MD = 03A443E0BD6AD35927295867B82E7857478AD650C47E787636E07C04DA96B7D1

Len = 3
Msg = C0
MD = 89F4F1F449355389724954CF8304B299651BF4580BB56FCC878C99314541C5A9

Len = 4
Msg = 80
MD =
7B1B65E4C0135655CCD98EEFDA6CFAD6B7E4D88EDCD51C09C50DD95AE4BC3E03

Len = 5
Msg = 48
MD = D9A1DD6FA10C3DD9B94608AC3503247E4B5E22259C8272152C4076B44005168D

LongMsgKAT_256.txt
Algorithm Name: MCSSHA-3
Principal Submitter: Mikhail Maslennikov

Len = 2048
Msg =
724627916C50338643E6996F07877EAFD96BDF01DA7E991D4155B9BE1295EA7D21C9391
F4C4A41C75F77E5D27389253393725F1427F57914B273AB862B9E31DABCE506E55872052
0D33352D119F699E784F9E548FF91BC35CA147042128709820D69A8287EA3257857615EB
0321270E94B84F446942765CE882B191FAEE7E1C87E0F0BD4E0CD8A927703524B559B76
9CA4ECE1F6DBF313FDCF67C572EC4185C1A88E86EC11B6454B371980020F19633B6B95
BD280E4FBCB0161E1A82470320CEC6ECFA25AC73D09F1536F286D3F9DACAFB2CD1D
0CE72D64D197F5C7520B3CCB2FD74EB72664BA93853EF41EABF52F015DD591500D018
DD162815CC993595B195
MD = 228315E72AEDE65807547779E196A2453BC181A885B4CBDCB165D842B8573A88
Len = 2111
Msg =
919FE5E7F35F64A7487649E564771DBBF10AE204ECC2181312D1A79FB579297C94F0DB9
EAAE9E009A4F02057AF2C973C5DAFA7B60154371A5D2C8E992FB6429176F8424B1A866
BC1D1BED00438E97FAB42040DCACDEF7CA9FC2033059B8898BB40CCFB2634B051797
BDF3B915C503EC81839AD01E0F4F2F871EFF2008D40011730BE7A47888E7955A806876B
E120CB0F3A139A3620154ECC6482A70F5629F6A9D3341BE6FBBF48E5AA0C53589A04F0
57DD44268AFFCABF75ADFC549F73F454264D46A98CCA80E3000C7446853DD5B430C93
44E87E3230555B09FB3E7E64B5AD3989293AC0FEEC0E75F909696F028A5525D26DDEA5
D2B2C813FB3613DFF38CE23209285CC77C60860
MD = 367516F7D9C2B7313394FB2B38E3BDAC4402F9DB746972D94BDB47105E27FE7E

ExtremelyLongMsgKAT_256.txt
Algorithm Name: MCSSHA-3
Principal Submitter: Mikhail Maslennikov

Repeat = 16777216
Text = abcdefghbcdefghicdefghijdefghijkefghijklfghijklmghijklmnhijklmno

MD = 71C42F8E4F83C5FFA2728ACB8C12461542FB46462357447E234AFF17CCEF42E0

MonteCarlo_256.txt
Algorithm Name: MCSSHA-3
Principal Submitter: Mikhail Maslennikov

Seed =
6CD4C0C5CB2CA2A0F1D1AECEBAC03B52E64EA03D1A1654372936545B92BBC5484A5
9DB74BB60F9C40CEB1A5AA35A6FAFE80349E14C253A4E8B1D77612DDD81ACE926AE
8B0AF6E53176DBFFCC2A6B88C6BD765F939D3D178A9BDE9EF3AA131C61E31C1E42C
DFAF4B4DCDE579A37E150EFBEF5555B4C1CB40439D835A724E2FAE7

j = 0
MD =
204FCBFDA2CD7BA4A78DA2F7033D4107C868BB9DF4D6D54246ECE2AD1049358F

j = 1
MD = BF5A4297538272A6DD7DA6F156E5018B8D49AADD3487C62582F21B97E44F5776

j = 2
MD = 5D718D07AC6566437AD8373F6562649F9A2E392E75528CFE468809E08AD71A44

j = 3
MD = EBAF11DDC9777C1580EA16CF951286892F4B115551E792474B47D29C192F67CB

j = 4
MD = D7C381B947ECA8469877AC1DBD31A5A02DC184764D41431796AFD396928BA49E

j = 5
MD =
5C65BA4AC9E8DFD88B6F3AED33CB83E82C4FF7D88D399183B59046B2BAB2451A

ShortMsgKAT_384.txt
Algorithm Name: MCSSHA-3
Principal Submitter: Mikhail Maslennikov

Len = 0
Msg = 00
MD =
8C5F0A85FE328244123A409C5A1E137655E0CB5EFBE8480975C5A8DB33B7353E3F52335
A130626AD5235E93B5A0F3277

Len = 1
Msg = 00
MD =
E3E9D497C2328FEFFE122053B7E4A7E6DEE3BBD33AF564D81E7DCA39A720016A9D7F
85E60BD990BA326954B8BA893D3D

Len = 2
Msg = C0
MD =
C7594B4671DB41BF78678210BCBA8865E9C9332DBA4C8346EC51286C6169049F0E05434
E50AA53B12321BBAC8CD02ACB

Len = 3
Msg = C0
MD =
AA60679261DEF2B4B2735A3F27A71FB75D82983325868BAB207B1F324D736018BBA9E4
146AF609DAE5396B60E313D4F5

Len = 4
Msg = 80
MD =
3B258DCA91A730292533ADEF94C6DF2F4776636D506A1F5B188F0C9698F1D1A8717BE7
494FE1F5DE7DD192DE50C25430

Len = 5
Msg = 48
MD =
2217AD827A2E1684ADBB94F399748D1B65143FD895F3310D729CFD5EF24AC8AD6769D
0CDB2387261A77AA8272CCA8AED

LongMsgKAT_384.txt
Algorithm Name: MCSSHA-3
Principal Submitter: Mikhail Maslennikov

Len = 2048
Msg =
724627916C50338643E6996F07877EAFD96BDF01DA7E991D4155B9BE1295EA7D21C9391
F4C4A41C75F77E5D27389253393725F1427F57914B273AB862B9E31DABCE506E55872052
0D33352D119F699E784F9E548FF91BC35CA147042128709820D69A8287EA3257857615EB
0321270E94B84F446942765CE882B191FAEE7E1C87E0F0BD4E0CD8A927703524B559B76
9CA4ECE1F6DBF313FDCF67C572EC4185C1A88E86EC11B6454B371980020F19633B6B95
BD280E4FBCB0161E1A82470320CEC6ECFA25AC73D09F1536F286D3F9DACAFB2CD1D
0CE72D64D197F5C7520B3CCB2FD74EB72664BA93853EF41EABF52F015DD591500D018
DD162815CC993595B195
MD =
89CEBCF5DC36F47AB0016A1D446F3E387671BBB6685AD6443D3682B0B4BB195CCB865
A48F216B57318420E0B1E039E54
Len = 2111
Msg =
919FE5E7F35F64A7487649E564771DBBF10AE204ECC2181312D1A79FB579297C94F0DB9
EAAE9E009A4F02057AF2C973C5DAFA7B60154371A5D2C8E992FB6429176F8424B1A866
BC1D1BED00438E97FAB42040DCACDEF7CA9FC2033059B8898BB40CCFB2634B051797
BDF3B915C503EC81839AD01E0F4F2F871EFF2008D40011730BE7A47888E7955A806876B
E120CB0F3A139A3620154ECC6482A70F5629F6A9D3341BE6FBBF48E5AA0C53589A04F0
57DD44268AFFCABF75ADFC549F73F454264D46A98CCA80E3000C7446853DD5B430C93
44E87E3230555B09FB3E7E64B5AD3989293AC0FEEC0E75F909696F028A5525D26DDEA5
D2B2C813FB3613DFF38CE23209285CC77C60860
MD =
57ED47B1083189BC5C6F4967AEF3DC540ED6BE9E1628875F752210403B3D22884A566B3
0E0E98DB06749AF58008AD93C

ExtremelyLongMsgKAT_384.txt
Algorithm Name: MCSSHA-3
Principal Submitter: Mikhail Maslennikov

Repeat = 16777216

Text = abcdefghbcdefghicdefghijdefghijkefghijklfghijklmghijklmnhijklmno
MD =
AC3526A591907EAB436B186A7A8945327F253180F1A6EEE7F4CECCFFA7810772ED8AC
9AEF267D3314AABE76AEA573C74

MonteCarlo_384.txt
Algorithm Name: MCSSHA-3
Principal Submitter: Mikhail Maslennikov

Seed =
6CD4C0C5CB2CA2A0F1D1AECEBAC03B52E64EA03D1A1654372936545B92BBC5484A5
9DB74BB60F9C40CEB1A5AA35A6FAFE80349E14C253A4E8B1D77612DDD81ACE926AE
8B0AF6E53176DBFFCC2A6B88C6BD765F939D3D178A9BDE9EF3AA131C61E31C1E42C
DFAF4B4DCDE579A37E150EFBEF5555B4C1CB40439D835A724E2FAE7

j = 0
MD =
3DF084520F2A6A91A110E1E682E18A4CFB8CDCD20D987C1605611484E30440CECFE045
C0151DEDD610C50D60D9183058

j = 1
MD =
02E57E6E078C9AC5F53EF0345F1281FA83BD9132C79842890B52AF2B1B085FF7E47017D
74E2D84ED684CF435372E53DB

j = 2
MD =
7743D0A8383B0829E48F6B61153F3FC63B3EAB7FCE2567AF3AEBBEF8A839DA3C262C3
3501FC222EEFDF216AE0467F129

j = 3
MD =
1DA59DA9DC05ACC3460A143A3B60A92AD57FFA0310AB1E3C3EBE66ACF6A0604896B
D5055BAF7A43DD6D43283C3BB73EA

j = 4
MD =
AF1B892D8DBC065AB6D34E9E79016EDC857980E5B4EDB0419928C50D0D347FB9709D
C601B8A6BDD650E7C5E453B6EFA6

j = 5
MD =
386012AB72FBF4B58B19A0A7D1EE58A894F2D5AD8DFA1FD2F3563596B7478E8BA974F
2EE7BA9CC1DAC7DC9612A8C6345

ShortMsgKAT_512.txt
Algorithm Name: MCSSHA-3
Principal Submitter: Mikhail Maslennikov

Len = 0
Msg = 00
MD =
476C3369A04E9162F2E906EDEBAE1146252BC3F95EB072DAE1811393C20221364FA1845
711EFEBC0F5AE4A28CB1D4D087F30808510697EF8792B7E20FDA3B402

Len = 1
Msg = 00
MD =
E253707870AF9D6574AC450CF0EE56DE30F925201869FB88C51CA4AEB4C46673CF815F
E84E66A92F08D7F9FCD3DD49D36E03CA4B3A5DDFBE0AD275E9196E17AB

Len = 2
Msg = C0
MD =
7223D4B55CDB938B0D862C0D54B398876ACDE6299077EB7E1842F30A8103DD285C227
D9152CBD75AD6912B34C5EA2FE8BA608851954DEB3023AE749D72A4F106

Len = 3
Msg = C0
MD =
683D8C08BEFA4FF960AC434F9487D7B2FA143773D1D4C466924620E3B754ECB8557A90
E35860965CCCC1CB0CC8205863C5329DC75AD6A0101469D601B8DA0C30

Len = 4
Msg = 80
MD =
07A47CD8DF2AF283B188847DBB4CBF534D6A619DD0862C1841CAAC39F6602AED502B
77CD837B67F03BAFE46944BD0BA08D47C6DD490040FA6D4E49EBF590FC24

Len = 5
Msg = 48
MD =
3734FD420BF21A5C426F0C8D08054ACB357A4E7634968B622D60BF3C2B44796B6314994
F65DFA8913521DAA6A4D7D277D4524A003C9BFD0ACDE075AAB279AC67

LongMsgKAT_512.txt
Algorithm Name: MCSSHA-3
Principal Submitter: Mikhail Maslennikov

Len = 2048
Msg =
724627916C50338643E6996F07877EAFD96BDF01DA7E991D4155B9BE1295EA7D21C9391
F4C4A41C75F77E5D27389253393725F1427F57914B273AB862B9E31DABCE506E55872052
0D33352D119F699E784F9E548FF91BC35CA147042128709820D69A8287EA3257857615EB
0321270E94B84F446942765CE882B191FAEE7E1C87E0F0BD4E0CD8A927703524B559B76
9CA4ECE1F6DBF313FDCF67C572EC4185C1A88E86EC11B6454B371980020F19633B6B95
BD280E4FBCB0161E1A82470320CEC6ECFA25AC73D09F1536F286D3F9DACAFB2CD1D
0CE72D64D197F5C7520B3CCB2FD74EB72664BA93853EF41EABF52F015DD591500D018
DD162815CC993595B195
MD =
34F5025A75AC3CFAFE29CD5B25706336F407B7F262FD1F1F48EAE65E52D766BB0F3C55
44596B64D69EBEFA4EC15534BD4DFB8488765F5602DFECB4DC48B29804
Len = 2111
Msg =
919FE5E7F35F64A7487649E564771DBBF10AE204ECC2181312D1A79FB579297C94F0DB9
EAAE9E009A4F02057AF2C973C5DAFA7B60154371A5D2C8E992FB6429176F8424B1A866
BC1D1BED00438E97FAB42040DCACDEF7CA9FC2033059B8898BB40CCFB2634B051797

BDF3B915C503EC81839AD01E0F4F2F871EFF2008D40011730BE7A47888E7955A806876B
E120CB0F3A139A3620154ECC6482A70F5629F6A9D3341BE6FBBF48E5AA0C53589A04F0
57DD44268AFFCABF75ADFC549F73F454264D46A98CCA80E3000C7446853DD5B430C93
44E87E3230555B09FB3E7E64B5AD3989293AC0FEEC0E75F909696F028A5525D26DDEA5
D2B2C813FB3613DFF38CE23209285CC77C60860
MD =
2D1DDCA7B721A38AE06E7F2B92F796A7D62F448DF4B58EEBA4F0EA215DFF287F311B
ACA16A8549D0CCEF52EF9EBF1B498C4B2BA5561951341B91CFD3D4CA357C

ExtremelyLongMsgKAT_512.txt
Algorithm Name: MCSSHA-3
Principal Submitter: Mikhail Maslennikov

Repeat = 16777216
Text = abcdefghbcdefghicdefghijdefghijkefghijklfghijklmghijklmnhijklmno
MD =
4F6E8BE35461A12C2996195C5C0BEBF335CACD75EB18AA3DAC958A2C934D8A2F6A85
B4A75E71B52BF70E608DF382234E711561C995F2E63C77DA7325A32171B4

MonteCarlo_512.txt
Algorithm Name: MCSSHA-3
Principal Submitter: Mikhail Maslennikov

Seed =
6CD4C0C5CB2CA2A0F1D1AECEBAC03B52E64EA03D1A1654372936545B92BBC5484A5
9DB74BB60F9C40CEB1A5AA35A6FAFE80349E14C253A4E8B1D77612DDD81ACE926AE
8B0AF6E53176DBFFCC2A6B88C6BD765F939D3D178A9BDE9EF3AA131C61E31C1E42C
DFAF4B4DCDE579A37E150EFBEF5555B4C1CB40439D835A724E2FAE7

j = 0
MD =
4E6A8DD366E2909B50BED07AC43F233415F11B25920BE1AF61C08D7AB1A76C82CA94
B5096656EFE1CA8B574605CAF943360E1432460D8373F49FF5B3CCD80A03

j = 1
MD =
E64E4FA3DD9747A441D83034DE930B6AA848840080951BAB06C6D687C374D694026C91
D609217DE651E8B299B8C4C01B50482DAC4C67A58EAC61EBF7A6128F3B

j = 2
MD =
12AD51A203B2972E0227BF10D7E64CD81A915D8708A356D2860B889F8F591E05384ED5
989E609AFEB8743506DC50C56B369C41F1D49E3F589640EF74067C3F90

j = 3
MD =
DFF1977BFA611DF2373B0C58C1442A89CDA8F597E782FFE12DC71E0E443BF8F549844E
C371E93100432E9C7EEF81AD82E1D8E6551B086EC320ED54C6046483EB

j = 4
MD =
DE9D225F64C90D61394EAEB8F67AA067759928EB714751596A6B3A40D51D6D02BE003
B6C963271FAF1BF5290E3CCCAEBE037B3B47B3953953FA1F070C7C806E4

j = 5
MD =
B424B647F4A57FBAC61534529732B5982489A46CE8020C7C7ED08E6F401589DD9436344
8E761C47ED7A578AE48158E63C8A8F69CEB746928528AEC51FDD06D7A

Appendix B. Literature.

[1] Announcing Request for Candidate Algorithm Nominations for a New Cryptographic Hash Algorithm (SHA–3) Family. DEPARTMENT OF COMMERCE. National Institute of Standards and Technology.[Docket No.: 070911510–7512–01]