FINAL
DRAFT

INTERNATIONAL
STANDARD

**ISO/IEC
FDIS
10118-3**

ISO/IEC JTC **1**/SC **27**

Secretariat: DIN

Voting begins on:
2017-09-15

Voting terminates on:
2017-11-10

Information technology — Security techniques — Hash-functions —

Part 3:
Dedicated hash-functions

Technologie de l'information — Techniques de sécurité — Fonctions de brouillage —

Partie 3: Fonctions de brouillage dédiées

Reference number
ISO/IEC FDIS 10118-3:2017(E)

ISO copyright office
Ch. de Blandonnet 8 • CP 401
CH-1214 Vernier, Geneva, Switzerland
Tel. +41 22 749 01 11
Fax +41 22 749 09 47
copyright@iso.org
www.iso.org

Contents

Page

Foreword

ISO (the International Organization for Standardization) and IEC (the International Electrotechnical Commission) form the specialized system for worldwide standardization. National bodies that are members of ISO or IEC participate in the development of International Standards through technical committees established by the respective organization to deal with particular fields of technical activity. ISO and IEC technical committees collaborate in fields of mutual interest. Other international organizations, governmental and non-governmental, in liaison with ISO and IEC, also take part in the work. In the field of information technology, ISO and IEC have established a joint technical committee, ISO/IEC JTC 1.

The procedures used to develop this document and those intended for its further maintenance are described in the ISO/IEC Directives, Part 1. In particular, the different approval criteria needed for the different types of document should be noted. This document was drafted in accordance with the editorial rules of the ISO/IEC Directives, Part 2 (see www.iso.org/directives).

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. ISO and IEC shall not be held responsible for identifying any or all such patent rights. Details of any patent rights identified during the development of the document will be in the Introduction and/or on the ISO list of patent declarations received (see www.iso.org/patents).

Any trade name used in this document is information given for the convenience of users and does not constitute an endorsement.

For an explanation on the voluntary nature of standards, the meaning of ISO specific terms and expressions related to conformity assessment, as well as information about ISO's adherence to the World Trade Organization (WTO) principles in the Technical Barriers to Trade (TBT) see the following URL: www.iso.org/iso/foreword.html.

This document was prepared by Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 27, *IT Security techniques*.

This fourth edition cancels and replaces the third edition (ISO/IEC 10118-3:2004), which has been technically revised. It also incorporates the Amendment ISO/IEC 10118-3:2004/Amd1:2006 and Technical Corrigendum ISO/IEC 10118-3:2004/Cor1:2011.

The main changes compared to the previous edition are as follows:

— SHA-3, STREEBOG and SM3 hash functions have been included;

— SHA-3 extendable-output functions have been included;

— caution notes for hash-functions with short hash-codes have been added.

A list of all parts in the ISO/IEC 10118 series can be found on the ISO website.

Information technology — Security techniques — Hash-functions —

Part 3: Dedicated hash-functions

1 Scope

This document specifies dedicated hash-functions, i.e. specially designed hash-functions. The hash-functions in this document are based on the iterative use of a round-function. Distinct round-functions are specified, giving rise to distinct dedicated hash-functions.

The use of Dedicated Hash-Functions 1, 2 and 3 in new digital signature implementations is deprecated.

NOTE As a result of their short hash-code length and/or cryptanalytic results, Dedicated Hash-Functions 1, 2 and 3 do not provide a sufficient level of collision resistance for future digital signature applications and they are therefore, only used for legacy applications. However, for applications where collision resistance is not required, such as in hash-functions as specified in ISO/IEC 9797-2, or in key derivation functions specified in ISO/IEC 11770-6, their use is not deprecated.

Numerical examples for dedicated hash-functions specified in this document are given in Annex B as additional information. For information purposes, SHA-3 extendable-output functions are specified in Annex C.

2 Normative references

There are no normative references in this document.

3 Terms and definitions

For the purposes of this document, the following terms and definitions apply.

ISO and IEC maintain terminological databases for use in standardization at the following addresses:

— IEC Electropedia: available at https://www.electropedia.org/

— ISO Online browsing platform: available at https://www.iso.org/obp

3.1
block
bit string of length L_1, i.e., the length of the first input to the round-function

3.2
word
string of bits

3.3
circulant matrix
matrix with the property that each row, apart from the first, consists of the right cyclic shift by one position of the row immediately above it

3.4
abelian group
group (G, *) such that $a*b = b*a$ for every a and b in G

3.5
field
set of elements S and a pair of operations (+,*) defined on S such that: (i) $a*(b + c) = a*b + a*c$ for every a, b and c in S, (ii) S together with + forms an abelian group (with identity element 0) and (iii) S excluding 0 together with * forms an abelian group

4 Symbols

4.1 Symbols specified in ISO/IEC 10118-1

B_i	byte
D	data
H	hash-code
IV	initializing value
L_1	length (in bits) of the first of the two input strings to the round-function Φ
L_2	length (in bits) of the second of the two input strings to the round-function Φ, of the output string from the round-function Φ and of the IV
L_X	length (in bits) of a bit string X
$X \oplus Y$	bitwise exclusive-or of bit strings X and Y (where $L_X = L_Y$)
$X \mid\mid Y$	concatenation of strings of bits X and Y in the indicated order
Φ	a round-function, i.e. if X, Y are bit strings of lengths L_1 and L_2 respectively, then $\Phi(X, Y)$ is the string obtained by applying Φ to X and Y

4.2 Symbols specific to this document

A^i	sequence of constant matrices used in the specification of the round-function defined in Clause 16
A^n	concatenation of n instances of the word A
a_i, a'_i	sequences of indices used in specifications of a round-function
C_i, C'_i	constant words used in the round-functions
C''	8 × 8 circulant matrix with entries chosen from GF(2^8) used in the specification of the round-function in Clause 16
c_0	function taking a string of 64 elements of GF(2^8) as input and giving an 8 × 8 matrix with entries from GF(2^8) as output, used in specifying the round-function defined in Clause 16
c_1, c_2, c_3	functions taking an 8 × 8 matrix of elements of GF(2^8) as input and giving an 8 × 8 matrix with entries from GF(2^8) as output, used in the specification of the round-function defined in Clause 16

c_4	function taking two 8 × 8 matrices of elements of GF(2^8) as input and giving an 8 × 8 matrix with entries from GF(2^8) as output, used in the specification of the round-function defined in Clause 16
D_i	a block derived from the data string after the padding process
d_i, e_i, f_i, g_i	functions taking either one or three words as input and producing a single word as output, used in specifying round-functions
H_i	a string of L_2 bits which is used in the hashing operation to store an intermediate result
Int_n	an inverse mapping to the mapping Vec_n, i.e. $\mathrm{Int}_n = \mathrm{Vec}_n^{-1}$
GF(2^8)	a field defined as GF(2)[x] / $p_8(x)$ where $p_8(x) = x^8 + x^4 + x^3 + x^2 + 1$. The elements of the field are 8-bit strings
M	an 8 × 8 matrix whose entries are chosen from GF(2^8)
q	number of blocks in the data string after the padding and splitting processes
$R^n()$	operation of right shift by n bits, i.e. if A is a word and n is a non-negative integer then $R^n(A)$ denotes the word obtained by right-shifting the contents of A by n positions
$S^n()$	operation of "circular left shift" by n bit positions, i.e. if A is a word and n is a non-negative integer then $S^n(A)$ denotes the word obtained by left-shifting the contents of A by n places in a cyclic fashion
$S'^n()$	operation of "circular right shift" by n bit positions, i.e. if A is a word and n is a non-negative integer then $S'^n(A)$ denotes the word obtained by right-shifting the contents of A by n places in a cyclic fashion
s	a function, which replaces an element $x \in$ GF(2^8) with another element $s[x] \in$ GF(2^8)
t_i, t'_i	shift-values used in specifying a round-function
Vec_n	a bijective mapping from Z_{2^n} to the set of n-bit words, which maps an integer from Z_{2^n} to its binary representation (i.e. for any integer $z = z_0 + 2z_1 + ... + 2^{n-1}z_{n-1}$ of the ring Z_{2^n}, where $z_j \in \{0,1\}$, $j = 0,..., n-1$, by definition $\mathrm{Vec}_n(z) = (z_{n-1}\|...\|z_1\|z_0)$
W, X_i, X'_i, Y_i, Z_i	words used to store the results of intermediate computations
W', X'', K_i, Y', Z'	matrices with entries chosen from GF(2^8) used to store the results of intermediate computations
Z_{2^n}	set of non-zero integers less than 2^n, together with the operations of addition and multiplication modulo 2^n
Λ	bitwise logical AND operation on bit strings, i.e. if A, B are words then $A \Lambda B$ is the word equal to bitwise logical AND of A and B
V	bitwise logical OR operation on bit strings, i.e. if A, B are words then $A \mathrm{V} B$ is the word equal to bitwise logical OR of A and B
¬	bitwise logical NOT operation on a bit string, i.e. if A is a word then $\neg A$ is the word equal to the bitwise logical NOT of A
⊎	addition modulo 2^w operation, where w is the number of bits in a word; i.e. if A and B are w–bit words, then A ⊎ B is the word obtained by treating A and B as the binary representations of integers and computing their sum modulo 2^w, where the result is constrained to lie between 0 and $2^w - 1$ inclusive. The value of w is 32 for Dedicated Hash-Functions 1 to 4, defined in Clauses 7 to 10, 64 for Dedicated Hash-Functions 5 and 6,

defined in Clauses 11 and 12 and 512 for Dedicated Hash-Functions 11 and 12, defined in Clauses 17 and 18

· multiplication operation of 8 × 8 matrices with entries chosen from GF(2^8); i.e. if A and B are such matrices, then A·B is the matrix obtained by multiplying A and B in the following way. Treat each entry of either A or B as the binary polynomial representation of an integer (for example, the binary polynomial representation of integer 89 (hexadecimal) is $x^7 + x^3 + 1$); treat the multiplication of two of the entries as the remainder when multiplication of the two polynomials is divided by a polynomial $p_8(x)$, where $p_8(x) = x^8 + x^4 + x^3 + x^2 + 1$; and treat the sum operation as the operation $\oplus$

:= a symbol denoting the "set equal to" operation used in procedural specifications of round-functions, where it indicates that the value of the variable (e.g. word or matrix) on the left side of the symbol should be set equal to the value of the expression on the right side of the symbol

5 Requirements

Users who wish to employ a hash-function from this document shall select

— one of the dedicated hash-functions specified below, and

— the length L_H of the hash-code H.

NOTE 1 All the hash-functions defined in this document take a bit string as input and give a bit string as output; this is independent of the internal byte-ordering convention used within each hash-function.

NOTE 2 The choice of L_H affects the security of the hash-function. All of the hash-functions specified in this document are believed to be collision-resistant hash-functions in environments where performing $2^{LH/2}$ hash-code computation is deemed to be computationally infeasible.

6 Models for dedicated hash-functions

6.1 Use of models

The 17 dedicated hash-functions specified in this document are defined using two different models. Dedicated Hash-Functions 1 to 12 and 17 are defined using the general round-function-based model defined in ISO/IEC 10118-1, which is further described in 6.2. Dedicated Hash-Functions 13 to 16 use the sponge construction model as defined in 6.3.

6.2 Round-function model

Dedicated Hash-Functions 1 to 12 and 17 specified in this document are based on the general model for hash-functions given in ISO/IEC 10118-1.

In the specifications of the hash-functions in this document, it is assumed that the padded data string input to the hash-function is in the form of a sequence of bytes. If the padded data string is in the form of a sequence of $8n$ bits, $x_0, x_1, \ldots, x_{8n-1}$, then it shall be interpreted as a sequence of n bytes, $B_0, B_1, \ldots, B_{n-1}$, in the following way. Each group of eight consecutive bits is considered as a byte, the first bit of a group being the most significant bit of that byte. Hence,

$$B_i = 2^7 x_{8i} + 2^6 x_{8i+1} + \ldots + x_{8i+7}$$

for every i ($0 \le i < n$).

The output transformation for the hash-functions specified in this document is defined so that the hash-code H is derived by taking the leftmost L_H bits of the final L_2-bit output string H_q.

Identifiers are defined for each of the 17 dedicated hash-functions specified in this document. The hash-function identifiers for the dedicated hash-functions specified in Clauses 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22 and 23 are equal to 31, 32, 33, 34, 35, 36, 37, 38, 39, 3A, 3B, 3C, 3D, 3E, 3F, 40 and 41 (hexadecimal), respectively. The hash-function identifiers are also used in the OSI object identifiers assigned in Annex A.

6.3 Sponge model

In 6.3, a permutation-based hash-function with sponge construction is specified.

A permutation-based hash-function with sponge construction is defined by a padding method, a permutation and a set of parameters.

The sponge construction[4] is a framework for specifying functions on a binary data with arbitrary output length. The construction employs the following three components:

— an underlying function on fixed-length strings, denoted by *f*;

— a parameter called the rate, denoted by *r*;

— a padding rule, denoted by pad.

The function that the construction produces from these components is called a sponge function, denoted by SPONGE[*f*, pad, *r*]. A sponge function takes two inputs, a bit string, *N*, and the bit length, *d*, of the output string, SPONGE[*f*, pad, *r*](*N*, *d*).

NOTE For further details on the rationale of the sponge construction framework, see Reference [5].

The function, *f*, maps strings of a single, fixed length, *b*, to strings of the same length. *b* is called the width of *f*. When the underlying function, *f*, is invertible, i.e. a permutation, it is a permutation-based hash-function with sponge construction.

The rate, *r*, is a positive integer that is strictly less than the width *b*. The capacity, *c*, is the positive integer $b - r$. Thus, $r + c = b$.

In the padding rule, pad is a function that produces padding, i.e. a string with an appropriate length to append to another string. In general, given a positive integer *x* and a non-negative integer *m*, the output pad(*x*, *m*) is a string with the property that $m + \text{len}[\text{pad}(x, m)]$ is a positive multiple of *x*. Within the sponge construction, $x = r$ and $m = \text{len}(N)$, so that the padded input string can be partitioned into a sequence of *r*-bit strings.

Given these three components, *f*, *pad* and *r*, as described above, the SPONGE[*f*, pad, *r*] function on (*N*, *d*) is specified by SPONGE[*f*, pad, *r*](*N*, *d*). The width *b* is determined by the choice of *f*.

SPONGE[*f*, pad, *r*](*N*, *d*)

Input: string *N*, non-negative integer *d*

Output: string *Z*, such that $\text{len}(Z) = d$

Steps:

a) Let $P = N \,||\, \text{pad}[r, \text{len}(N)]$.

b) Let $q = \text{len}(P)/r$.

c) Let $c = b - r$.

d) Let $P_0, \ldots, P_{q-1}$ be the unique sequence of strings of length *r*, such that $P = P_0 \,||\, \ldots \,||\, P_{q-1}$.

e) Let $S = 0^b$.

f) For i from 0 to $q-1$, let $S = f[S \oplus (P_i \,||\, 0^c)]$.

g) Let Z be the empty string.

h) Let $Z = Z \,||\, Trunc_r(S)$.

i) If $d \leq |Z|$, then return $Trunc_d(Z)$; else, continue.

j) Let $S = f(S)$ and continue with step h).

Note that the input d determines the number of bits that SPONGE[f, pad, r](N, d) returns, but it does not affect their values. In principle, the output can be regarded as an infinite string, whose computation, in practice, is halted after the desired number of output bits is produced.

The parameters of a sponge construction include

— b, the width,

— r, rate,

— c, capacity, such that $b = r + c$, and

— d, output length.

Here, if notations specified in ISO/IEC 10118-1:2016, Clause 3 are used, r can be considered as L_1, which is the length of a block of input data (message), while b can be considered as L_2, which is the output length of the function f. Furthermore, the relation between function f and the round-function Φ as defined in ISO/IEC 10118-1:2016, Clause 3 can be represented as $\Phi(P_i, S_{i-1}) = f[S_{i-1} \oplus (P_i \,||\, 0^c)]$, where $P_i = D_i$ is the ith data block, while $S_{i-1} = H_{i-1}$ is the output of the previous execution. The squeezing stage is considered the output transformation.

7 Dedicated Hash-Function 1 (RIPEMD-160)

7.1 General

In Clause 7, a padding method, an initializing value and a round-function for use in the general model for hash-functions described in ISO/IEC 10118-1 are specified. The padding method, initializing value and round-function specified here, when used in the above general model, together define Dedicated Hash-Function 1. This dedicated hash-function can be applied to all data strings, D, containing at most $2^{64}-1$ bits.

The ISO/IEC hash-function identifier for Dedicated Hash-Function 1 is equal to 31 (hexadecimal).

NOTE 1 Dedicated Hash-Function 1 defined in Clause 7 is commonly called RIPEMD-160[6].

NOTE 2 As a result of a short hash-code length and/or cryptanalytic results, Dedicated Hash-Function 1 does not provide a sufficient level of collision resistance for future digital signature applications and it is, therefore, only used for legacy applications. However, for applications where collision resistance is not required, such as in hash-functions as specified in ISO/IEC 9797 or in key derivation functions specified in ISO/IEC 11770-6, its use is not deprecated.

7.2 Parameters, functions and constants

7.2.1 Parameters

For this hash-function, $L_1 = 512$, $L_2 = 160$ and L_H is up to 160.

7.2.2 Byte ordering convention

In the specification of the round-function of Clause 7, it is assumed that the block input to the round-function is in the form of a sequence of 32-bit words, each 512-bit block being made up of 16 such words. A sequence of 64 bytes, B_0, B_1, …, B_{63}, shall be interpreted as a sequence of 16 words, Z_0, Z_1, …, Z_{15}, in the following way. Each group of four consecutive bytes is considered as a word, the first byte of a word being the least significant byte of that word. Hence,

$$Z_i = 2^{24}B_{4i+3} + 2^{16}B_{4i+2} + 2^{8}B_{4i+1} + B_{4i}, \qquad (0 \le i \le 15).$$

To convert the hash-code from a sequence of words to a byte-sequence, the inverse process shall be followed.

NOTE The byte-ordering specified here is different from that of 9.2.2.

7.2.3 Functions

To facilitate software implementation, the round-function Φ is described in terms of operations on 32-bit words. A sequence of functions g_0, g_1, …, g_{79} is used in this round-function, where each function g_i, $0 \le i \le 79$, takes three words, X_0, X_1 and X_2, as input and produces a single word as output.

The functions g_i are defined as follows:

$$\begin{aligned}
g_i(X_0,X_1,X_2) &= X_0 \oplus X_1 \oplus X_2, && (0 \le i \le 15);\\
g_i(X_0,X_1,X_2) &= (X_0 \wedge X_1) \vee (\neg X_0 \wedge X_2), && (16 \le i \le 31);\\
g_i(X_0,X_1,X_2) &= (X_0 \vee \neg X_1) \oplus X_2, && (32 \le i \le 47);\\
g_i(X_0,X_1,X_2) &= (X_0 \wedge X_2) \vee (X_1 \wedge \neg X_2), && (48 \le i \le 63);\\
g_i(X_0,X_1,X_2) &= X_0 \oplus (X_1 \vee \neg X_2), && (64 \le i \le 79).
\end{aligned}$$

7.2.4 Constants

Two sequences of constant words, C_0, C_1, …, C_{79} and C'_0, C'_1, …, C'_{79}, are used in this round-function. In a hexadecimal representation (where the most significant bit corresponds to the left-most bit), these are defined as follows:

$$\begin{aligned}
C_i &= 00000000, && (0 \le i \le 15);\\
C_i &= 5A827999, && (16 \le i \le 31);\\
C_i &= 6ED9EBA1, && (32 \le i \le 47);\\
C_i &= 8F1BBCDC, && (48 \le i \le 63);\\
C_i &= A953FD4E, && (64 \le i \le 79).
\end{aligned}$$

$$\begin{aligned}
C'_i &= 50A28BE6, && (0 \le i \le 15);\\
C'_i &= 5C4DD124, && (16 \le i \le 31);\\
C'_i &= 6D703EF3, && (32 \le i \le 47);\\
C'_i &= 7A6D76E9, && (48 \le i \le 63);\\
C'_i &= 00000000, && (64 \le i \le 79).
\end{aligned}$$

Two sequences of 80 shift-values are used in this round-function, where each shift-value is between 5 and 15. These sequences are denoted by (t_0, t_1, …, t_{79}) and (t'_0, t'_1, …, t'_{79}). Two additional sequences of 80 indices are used in this round-function, where each value in the sequence is between 0 and 15. These sequences are denoted as (a_0, a_1, …, a_{79}) and (a'_0, a'_1, …, a'_{79}). All four sequences are defined in Table 1.

Table 1 — Sequences for Hash-Function 1

i	0	1	2	3	4	5	6	7
t_i	11	14	15	12	5	8	7	9
t'_i	8	9	9	11	13	15	15	5
a_i	0	1	2	3	4	5	6	7
a'_i	5	14	7	0	9	2	11	4

i	8	9	10	11	12	13	14	15
t_i	11	13	14	15	6	7	9	8
t'_i	7	7	8	11	14	14	12	6
a_i	8	9	10	11	12	13	14	15
a'_i	13	6	15	8	1	10	3	12

i	16	17	18	19	20	21	22	23
t_i	7	6	8	13	11	9	7	15
t'_i	9	13	15	7	12	8	9	11
a_i	7	4	13	1	10	6	15	3
a'_i	6	11	3	7	0	13	5	10

i	24	25	26	27	28	29	30	31
t_i	7	12	15	9	11	7	13	12
t'_i	7	7	12	7	6	15	13	11
a_i	12	0	9	5	2	14	11	8
a'_i	14	15	8	12	4	9	1	2

i	32	33	34	35	36	37	38	39
t_i	11	13	6	7	14	9	13	15
t'_i	9	7	15	11	8	6	6	14
a_i	3	10	14	4	9	15	8	1
a'_i	15	5	1	3	7	14	6	9

i	40	41	42	43	44	45	46	47
t_i	14	8	13	6	5	12	7	5
t'_i	12	13	5	14	13	13	7	5
a_i	2	7	0	6	13	11	5	12

a'_i	11	8	12	2	10	0	4	13

i	48	49	50	51	52	53	54	55
t_i	11	12	14	15	14	15	9	8
t'_i	15	5	8	11	14	14	6	14
a_i	1	9	11	10	0	8	12	4
a'_i	8	6	4	1	3	11	15	0

i	56	57	58	59	60	61	62	63
t_i	9	14	5	6	8	6	5	12
t'_i	6	9	12	9	12	5	15	8
a_i	13	3	7	15	14	5	6	2
a'_i	5	12	2	13	9	7	10	14

i	64	65	66	67	68	69	70	71
t_i	9	15	5	11	6	8	13	12
t'_i	8	5	12	9	12	5	14	6
a_i	4	0	5	9	7	12	2	10
a'_i	12	15	10	4	1	5	8	7

i	72	73	74	75	76	77	78	79
t_i	5	12	13	14	11	8	5	6
t'_i	8	13	6	5	15	13	11	11
a_i	14	1	3	8	11	6	15	13
a'_i	6	2	13	14	0	3	9	11

7.2.5 Initializing value

For this round-function, the initializing value, *IV*, shall always be the following 160-bit string, represented here as a sequence of five words, Y_0, Y_1, Y_2, Y_3 and Y_4, in a hexadecimal representation, where Y_0 represents the left-most 32 of the 160 bits:

Y_0 = 67452301;
Y_1 = EFCDAB89;
Y_2 = 98BADCFE;
Y_3 = 10325476;
Y_4 = C3D2E1F0.

7.3 Padding method

The data string D needs to be padded to make it contain a number of bits which is an integer multiple of 512. The padding procedure operates as follows.

a) D is concatenated with a single "1" bit.

b) The result of the previous step is concatenated with between zero and 511 "0" bits such that the length (in bits) of the resultant string is congruent to 448 modulo 512. More explicitly, if the original length of D is L_D and letting r be the remainder when L_D is divided by 512, then the number of concatenated zeros is equal to either $447 - r$ (if $r \leq 447$) or $959 - r$ (if $r > 447$). The result will be a bit string whose length will be 64 bits short of an integer multiple of 512 bits.

c) Divide the 64-bit binary representation of L_D into two 32-bit strings, one representing the "most significant half" of L_D and the other the "least significant half". Now concatenate the string resulting from the previous step with these two 32-bit strings, with the "least significant half" preceding the "most significant half".

In the description of the round-function which follows, each 512-bit data block D_i, $1 \leq i \leq q$, is treated as a sequence of 16 words, $Z_0, Z_1, \ldots, Z_{15}$, where Z_0 corresponds to the left-most 32 bits of D_i.

NOTE The concatenation of the two 32-bit strings of L_D in step c) is such that these two 32-bit strings are used directly as the words Z_{14} and Z_{15} of the last data block; based on the byte ordering convention in 7.2.2, the least significant byte of L_D is the leftmost byte and the most significant byte of L_D is the rightmost byte.

7.4 Description of the round-function

The round-function Φ operates as follows.

NOTE In this description, the symbols $W, X_0, X_1, X_2, X_3, X_4, X'_0, X'_1, X'_2, X'_3$ and X'_4 are used to denote 11 distinct words which contain values required in the computations.

a) Suppose the 512-bit (first) input to Φ is contained in $Z_0, Z_1, \ldots, Z_{15}$, where Z_0 contains the left-most 32 of the 512 bits. Suppose also that the 160-bit (second) input to Φ is contained in five words, Y_0, Y_1, Y_2, Y_3 and Y_4.

b) Let $X_0 := Y_0$, $X_1 := Y_1$, $X_2 := Y_2$, $X_3 := Y_3$ and $X_4 := Y_4$.

c) Let $X'_0 := Y_0$, $X'_1 := Y_1$, $X'_2 := Y_2$, $X'_3 := Y_3$ and $X'_4 := Y_4$.

d) For $i := 0$ to 79, do the following four steps in the order specified:

   1) $W := S^{ti}[X_0 \uplus g_i(X_1, X_2, X_3) \uplus Z_{ai} \uplus C_i] \uplus X_4$;

   2) $X_0 := X_4$; $X_4 := X_3$; $X_3 := S^{10}(X_2)$; $X_2 := X_1$; $X_1 := W$;

   3) $W := S^{t'i}[X'_0 \uplus g_{79-i}(X'_1, X'_2, X'_3) \uplus Z_{a'i} \uplus C'_i] \uplus X'_4$;

   4) $X'_0 := X'_4$; $X'_4 := X'_3$; $X'_3 := S^{10}(X'_2)$; $X'_2 := X'_1$; $X'_1 := W$.

e) Let $W := Y_0$, $Y_0 := Y_1 \uplus X_2 \uplus X'_3$, $Y_1 := Y_2 \uplus X_3 \uplus X'_4$, $Y_2 := Y_3 \uplus X_4 \uplus X'_0$, $Y_3 := Y_4 \uplus X_0 \uplus X'_1$ and $Y_4 := W \uplus X_1 \uplus X'_2$.

f) The five words, Y_0, Y_1, Y_2, Y_3 and Y_4, represent the output of the round-function Φ. After the final iteration of the round-function, the five words, Y_0, Y_1, Y_2, Y_3 and Y_4, shall be converted to a sequence of 20 bytes using the inverse of the procedure specified in 7.1.2 and where Y_0 shall yield the first

four bytes, Y_1 the next four bytes and so on. Thus, the first (left-most) byte will correspond to the least significant byte of Y_0 and the 20th (right-most) byte will correspond to the most significant byte of Y_4. The 20 bytes shall be converted to a string of 160 bits using the inverse of the procedure specified in Clause 6, i.e. the first (left-most) bit will correspond to the most significant bit of the first (left-most) byte and the 160th (right-most) bit will correspond to the least significant bit of the 20th (right-most) byte.

Figure 1 shows steps 1) and 2) of item d) of the round-function Φ in Dedicated Hash-Function 1 (RIPEMD-160) [the other half, i.e. steps 3) and 4) is similar]. In the round-function Φ, steps 1) to 4) of item d) are used 80 times (i = 0, …, 79).

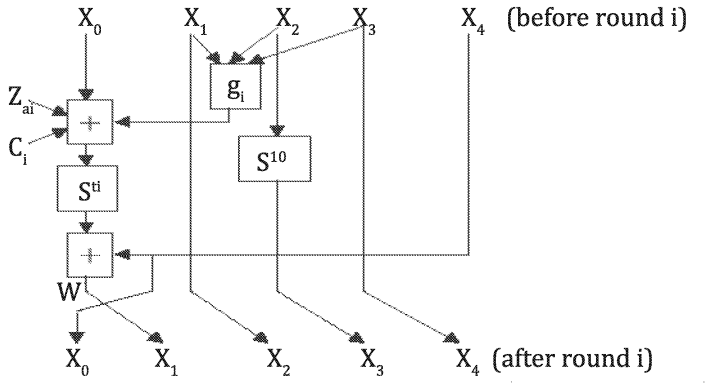

Figure 1 — Part of the round-function in Dedicated Hash-Function 1

8 Dedicated Hash-Function 2 (RIPEMD-128)

8.1 General

In Clause 8, a padding method, an initializing value and a round-function for use in the general model for hash-functions described in ISO/IEC 10118-1 are specified. The padding method, initializing value and round-function specified here, when used in the above general model, together define Dedicated Hash-Function 2. This dedicated hash-function can be applied to all data strings, D, containing at most $2^{64}-1$ bits.

The ISO/IEC hash-function identifier for Dedicated Hash-Function 2 is equal to 32 (hexadecimal).

NOTE 1 Dedicated Hash-Function 2 defined in Clause 8 is commonly called RIPEMD-128[6]. This hash-function is only used in applications where a hash-code containing 128 bits or less is considered adequately secure.

NOTE 2 As a result of a short hash-code length and/or cryptanalytic results, Dedicated Hash-Function 2 does not provide a sufficient level of collision resistance for future digital signature applications and it is, therefore, only used for legacy applications. However, for applications where collision resistance is not required, such as in hash-functions as specified in ISO/IEC 9797 or in key derivation functions specified in ISO/IEC 11770-6, its use is not deprecated.

8.2 Parameters, functions and constants

8.2.1 Parameters

For this hash-function, L_1 = 512, L_2 = 128 and L_H is up to 128.

8.2.2 Byte ordering convention

The byte ordering convention for this hash-function is the same as that for the hash-function of Clause 7.

8.2.3 Functions

To facilitate software implementation, the round-function Φ is described in terms of operations on 32-bit words. A sequence of functions, g_0, g_1, ..., g_{63}, is used in this round-function, where each function g_i, $0 \le i \le 63$, takes three words, X_0, X_1 and X_2, as input and produces a single word as output.

The functions g_i are defined to be the same as the first 64 of the functions defined in 7.2.3.

8.2.4 Constants

Two sequences of constant words, C_0, C_1, ..., C_{63} and C'_0, C'_1, ..., C'_{63}, are used in this round-function. In a hexadecimal representation (where the most significant bit corresponds to the left-most bit), these are defined as follows:

C_i = 00000000, $(0 \le i \le 15)$;
C_i = 5A827999, $(16 \le i \le 31)$;
C_i = 6ED9EBA1, $(32 \le i \le 47)$;
C_i = 8F1BBCDC, $(48 \le i \le 63)$.

C'_i = 50A28BE6, $(0 \le i \le 15)$;
C'_i = 5C4DD124, $(16 \le i \le 31)$;
C'_i = 6D703EF3, $(32 \le i \le 47)$;
C'_i = 00000000, $(48 \le i \le 63)$.

Two sequences of 64 shift-values are also used in this round-function, where each shift-value is between 5 and 15. These sequences are denoted by (t_0, t_1, ..., t_{63}) and (t'_0,t'_1, ..., t'_{63}) and they are defined to be equal to the first 64 values of the corresponding sequences defined in 7.2.4.

Finally, two further sequences of 64 indices are used in this round-function, where each value in the sequence is between 0 and 15. These sequences are denoted by (a_0, a_1, ..., a_{63}) and (a'_0, a'_1, ..., a'_{63}) and they are defined to be equal to the first 64 values of the corresponding sequences defined in 7.2.4.

8.2.5 Initializing value

For this hash-function, the initializing value, *IV*, shall always be the following 128-bit string, represented here as a sequence of four words, Y_0, Y_1, Y_2 and Y_3, in a hexadecimal representation, where Y_0 represents the left-most 32 of the 128 bits:

Y_0 = 67452301;
Y_1 = EFCDAB89;
Y_2 = 98BADCFE;
Y_3 = 10325476.

8.3 Padding method

The padding method to be used with this hash-function shall be the same as the padding method defined in 7.3.

8.4 Description of the round-function

The round-function Φ operates as follows.

NOTE In this description, the symbols W, X_0, X_1, X_2, X_3, X'_0, X'_1, X'_2 and X'_3 are used to denote nine distinct words which contain values required in the computations.

a) Suppose the 512-bit (first) input to Φ is contained in Z_0, Z_1, …, Z_{15}, where Z_0 contains the left-most 32 of the 512 bits. Suppose also that the 128-bit (second) input to Φ is contained in four words, Y_0, Y_1, Y_2 and Y_3.

b) Let $X_0 := Y_0$, $X_1 := Y_1$, $X_2 := Y_2$ and $X_3 := Y_3$.

c) Let $X'_0 := Y_0$, $X'_1 := Y_1$, $X'_2 := Y_2$ and $X'_3 := Y_3$.

d) For $i := 0$ to 63, do the following four steps in the order specified:

   1) $W := S^{ti}[X_0 \uplus g_i(X_1, X_2, X_3) \uplus Z_{ai} \uplus C_i]$;

   2) $X_0 := X_3$; $X_3 := X_2$; $X_2 := X_1$; $X_1 := W$;

   3) $W := S^{t'i}[X'_0 \uplus g_{63-i}(X'_1, X'_2, X'_3) \uplus Z_{a'i} \uplus C'_i]$;

   4) $X'_0 := X'_3$; $X'_3 := X'_2$; $X'_2 := X'_1$; $X'_1 := W$.

e) Let $W := Y_0$, $Y_0 := Y_1 \uplus X_2 \uplus X'_3$, $Y_1 := Y_2 \uplus X_3 \uplus X'_0$, $Y_2 := Y_3 \uplus X_0 \uplus X'_1$ and $Y_3 := W \uplus X_1 \uplus X'_2$.

f) The four words, Y_0, Y_1, Y_2 and Y_3, represent the output of the round-function Φ. After the final iteration of the round-function, the four words, Y_0, Y_1, Y_2 and Y_3, shall be converted to a sequence of 16 bytes using the inverse of the procedure specified in 7.2.2 and where Y_0 shall yield the first four bytes, Y_1 the next four bytes and so on. Thus, the first (left-most) byte will correspond to the least significant byte of Y_0 and the 16th (right-most) byte will correspond to the most significant byte of Y_3. The 16 bytes shall be converted to a string of 128 bits using the inverse of the procedure specified in Clause 6, i.e. the first (left-most) bit will correspond to the most significant bit of the first (left-most) byte and the 128th (right-most) bit will correspond to the least significant bit of the 16th (right-most) byte.

Figure 2 shows steps 1) and 2) of item d) of the round-function Φ in Dedicated Hash-Function 2 (RIPEMD-128) [the other half, i.e. steps 3) and 4) is similar]. In the round-function Φ, steps 1) to 4) of item d) are used 64 times (i = 0, …, 63).

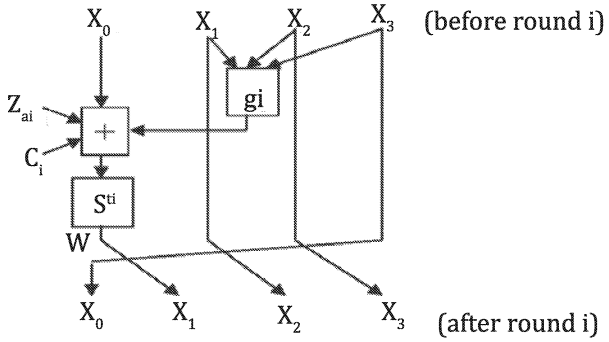

Figure 2 — Part of the round-function in Dedicated Hash-Function 2

9 Dedicated Hash-Function 3 (SHA-1)

9.1 General

In Clause 9, a padding method, an initializing value and a round-function for use in the general model for hash-functions described in ISO/IEC 10118-1 are specified. The padding method, initializing value and round-function specified here, when used in the above general model, together define the Dedicated Hash-Function 3. This dedicated hash-function can be applied to all data strings, D, containing at most $2^{64}-1$ bits.

The ISO/IEC hash-function identifier for Dedicated Hash-Function 3 is equal to 33 (hexadecimal).

NOTE 1 Dedicated Hash-Function 3 defined in Clause 9 is commonly called SHA-1[1].

NOTE 2 As a result of a short hash-code length and/or cryptanalytic results, Dedicated Hash-Function 3 does not provide a sufficient level of collision resistance for future digital signature applications and it is, therefore, only used for legacy applications. However, for applications where collision resistance is not required, such as in hash-functions as specified in ISO/IEC 9797 or in key derivation functions specified in ISO/IEC 11770-6, its use is not deprecated.

9.2 Parameters, functions and constants

9.2.1 Parameters

For this hash-function, $L_1 = 512$, $L_2 = 160$ and L_H is up to 160.

9.2.2 Byte ordering convention

In the specification of the round-function of Clause 9, it is assumed that the block input to the round-function is in the form of a sequence of 32-bit words, each 512-bit block made up of 16 such words. A sequence of 64 bytes, $B_0, B_1, \ldots, B_{63}$, shall be interpreted as a sequence of 16 words, $Z_0, Z_1, \ldots, Z_{15}$, in the following way, where each group of four consecutive bytes is considered as a word, the first byte of a word being the most significant byte of that word. Hence,

$$Z_i = 2^{24}B_{4i} + 2^{16}B_{4i+1} + 2^{8}B_{4i+2} + B_{4i+3}, \qquad (0 \le i \le 15).$$

To convert the hash-code from a sequence of words to a sequence of bytes, the inverse process shall be followed.

NOTE The byte-ordering specified here is different from that of 7.2.2.

9.2.3 Functions

To facilitate software implementation, the round-function Φ is described in terms of operations on 32-bit words. A sequence of functions, $f_0, f_1, \ldots, f_{79}$, is used in this round-function, where each function, f_i, $0 \le i \le 79$, takes three words, X_0, X_1 and X_2, as input and produces a single word as output.

The functions f_i are defined as follows:

$$f_i(X_0, X_1, X_2) = (X_0 \wedge X_1) \vee (\neg X_0 \wedge X_2), \qquad (0 \le i \le 19);$$
$$f_i(X_0, X_1, X_2) = X_0 \oplus X_1 \oplus X_2, \qquad (20 \le i \le 39);$$
$$f_i(X_0, X_1, X_2) = (X_0 \wedge X_1) \vee (X_0 \wedge X_2) \vee (X_1 \wedge X_2), \qquad (40 \le i \le 59);$$
$$f_i(X_0, X_1, X_2) = X_0 \oplus X_1 \oplus X_2, \qquad (60 \le i \le 79).$$

9.2.4 Constants

A sequence of constant words, C_0, C_1, …, C_{79}, is used in this round-function. In a hexadecimal representation (where the most significant bit corresponds to the left-most bit), these are defined as follows:

C_i = 5A827999, $(0 \le i \le 19)$;
C_i = 6ED9EBA1, $(20 \le i \le 39)$;
C_i = 8F1BBCDC, $(40 \le i \le 59)$;
C_i = CA62C1D6, $(60 \le i \le 79)$.

9.2.5 Initializing value

For this round-function the initializing value, *IV*, shall always be the following 160-bit string, represented here as a sequence of five words, Y_0, Y_1, Y_2, Y_3 and Y_4, in a hexadecimal representation, where Y_0 represents the left-most 32 of the 160 bits:

Y_0 = 67452301;
Y_1 = EFCDAB89;
Y_2 = 98BADCFE;
Y_3 = 10325476;
Y_4 = C3D2E1F0.

9.3 Padding method

The data string *D* needs to be padded to make it contain a number of bits which is an integer multiple of 512. The padding procedure operates as follows.

a) *D* is concatenated with a single "1" bit.

b) The result of the previous step is concatenated with between zero and 511 "0" bits, such that the length (in bits) of the resultant string is congruent to 448 modulo 512. More explicitly, if the original length of *D* is L_D and letting *r* be the remainder when L_D is divided by 512, then the number of concatenated zeros is equal to either $447 - r$ (if $r \le 447$) or $959 - r$ (if $r > 447$). The result will be a bit string whose length will be 64 bits short of an integer multiple of 512 bits.

c) Concatenate the string resulting from the previous step with the 64-bit binary representation of L_D, most significant bit first.

In the description of the round-function which follows, each 512-bit data block D_i, $1 \le i \le q$, is treated as a sequence of 16 words, Z_0, Z_1, …, Z_{15}, where Z_0 corresponds to the left-most 32 bits of D_i.

NOTE The concatenation of the 64-bit string of L_D in step c) is such that the most significant 32-bit string and the least significant 32-bit string of L_D are used respectively as the words Z_{14} and Z_{15} of the last data block. Based on the byte ordering convention in 9.2.2, the most significant byte of L_D is the leftmost byte and the least significant byte of L_D is the rightmost byte.

9.4 Description of the round-function

The round-function Φ operates as follows.

NOTE In this description, the symbols *W*, X_0, X_1, X_2, X_3, X_4, Z_0, Z_1, …, Z_{79} are used to denote 86 distinct words which contain values required in the computations.

a) Suppose the 512-bit (first) input to Φ is contained in Z_0, Z_1, …, Z_{15}, where Z_0 contains the left-most 32 of the 512 bits. Suppose also that the 160-bit (second) input to Φ is contained in five words, Y_0, Y_1, Y_2, Y_3 and Y_4.

b) For i = 16 to 79, let Z_i: = $S^1(Z_{i-3} \oplus Z_{i-8} \oplus Z_{i-14} \oplus Z_{i-16})$.

c) Let X_0: = Y_0, X_1: = Y_1, X_2: = Y_2, X_3: = Y_3 and X_4: = Y_4.

d) For i = 0 to 79, do the following two steps:

   1) W: = $S^5(X_0) \uplus f_i(X_1, X_2, X_3) \uplus X_4 \uplus Z_i \uplus C_i$;

   2) X_4: = X_3; X_3: = X_2; X_2: = $S^{30}(X_1)$; X_1: = X_0; X_0: = W.

e) Let Y_0:= $Y_0 \uplus X_0$, Y_1:= $Y_1 \uplus X_1$, Y_2:= $Y_2 \uplus X_2$, Y_3:= $Y_3 \uplus X_3$ and Y_4:= $Y_4 \uplus X_4$.

f) The five words, Y_0, Y_1, Y_2, Y_3 and Y_4, represent the output of the round-function Φ. After the final iteration of the round-function, the five words, Y_0, Y_1, Y_2, Y_3 and Y_4, shall be converted to a sequence of 20 bytes using the inverse of the procedure specified in 9.2.2 and where Y_0 shall yield the first four bytes, Y_1 the next four bytes and so on. Thus, the first (left-most) byte will correspond to the most significant byte of Y_0 and the 20th (right-most) byte will correspond to the least significant byte of Y_4. The 20 bytes shall be converted to a string of 160 bits using the inverse of the procedure specified in Clause 6, i.e. the first (left-most) bit will correspond to the most significant bit of the first (left-most) byte and the 160th (right-most) bit will correspond to the least significant bit of the 20th (right-most) byte.

Figure 3 shows steps 1) and 2) of item d) of the round-function Φ in Dedicated Hash-Function 3 (SHA-1). In the round-function Φ, steps 1) and 2) of item d) are used 80 times (i = 0, …, 79).

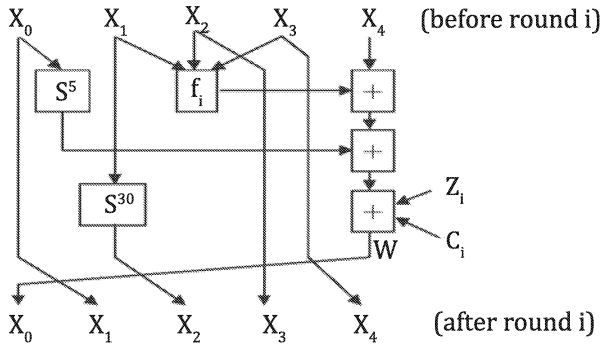

Figure 3 — Part of the round-function in Dedicated Hash-Function 3

10 Dedicated Hash-Function 4 (SHA-256)

10.1 General

In Clause 10, a padding method, an initializing value and a round-function for use in the general model for hash-functions described in ISO/IEC 10118-1 are specified. The padding method, initializing value and round-function specified here, when used in the above general model, together define Dedicated Hash-Function 4. This dedicated hash-function can be applied to all data strings, D, containing at most $2^{64}-1$ bits.

The ISO/IEC hash-function identifier for Dedicated Hash-Function 4 is equal to 34 (hexadecimal).

NOTE Dedicated Hash-Function 4 defined in Clause 10 is commonly called SHA-256[1].

10.2 Parameters, functions and constants

10.2.1 Parameters

For this hash-function, $L_1 = 512$, $L_2 = 256$ and L_H is up to 256.

10.2.2 Byte ordering convention

The byte ordering convention to be used with this hash-function shall be the same as the byte ordering convention defined in 9.2.2.

10.2.3 Functions

To facilitate software implementation, the round-function Φ is described in terms of operations on 32-bit words. A sequence of functions, e_0, e_1, e_2, e_3, e_4 and e_5, is used in this round-function, where e_0 and e_1 each takes three words, X_0, X_1 and X_2, as input; e_2, e_3, e_4 and e_5 each takes one word X_0 as input and each of these six functions produces a single 32-bit word as output.

The functions e_0, e_1, e_2, e_3, e_4 and e_5 are defined as follows:

$$e_0(X_0, X_1, X_2) = (X_0 \wedge X_1) \oplus (\neg X_0 \wedge X_2);$$
$$e_1(X_0, X_1, X_2) = (X_0 \wedge X_1) \oplus (X_0 \wedge X_2) \oplus (X_1 \wedge X_2);$$

$$e_2(X_0) = S'^{2}(X_0) \oplus S'^{13}(X_0) \oplus S'^{22}(X_0);$$
$$e_3(X_0) = S'^{6}(X_0) \oplus S'^{11}(X_0) \oplus S'^{25}(X_0);$$
$$e_4(X_0) = S'^{7}(X_0) \oplus S'^{18}(X_0) \oplus R^{3}(X_0);$$
$$e_5(X_0) = S'^{17}(X_0) \oplus S'^{19}(X_0) \oplus R^{10}(X_0).$$

10.2.4 Constants

A sequence of constant words, C_0, C_1, …, C_{63}, is used in this round-function. In a hexadecimal representation (where the most significant bit corresponds to the left-most bit), these are defined as follows, where the words are listed in the order C_0, C_1, …, C_{63}.

```
428a2f98  71374491  b5c0fbcf  e9b5dba5  3956c25b  59f111f1  923f82a4  ab1c5ed5
d807aa98  12835b01  243185be  550c7dc3  72be5d74  80deb1fe  9bdc06a7  c19bf174
e49b69c1  efbe4786  0fc19dc6  240ca1cc  2de92c6f  4a7484aa  5cb0a9dc  76f988da
983e5152  a831c66d  b00327c8  bf597fc7  c6e00bf3  d5a79147  06ca6351  14292967
27b70a85  2e1b2138  4d2c6dfc  53380d13  650a7354  766a0abb  81c2c92e  92722c85
a2bfe8a1  a81a664b  c24b8b70  c76c51a3  d192e819  d6990624  f40e3585  106aa070
19a4c116  1e376c08  2748774c  34b0bcb5  391c0cb3  4ed8aa4a  5b9cca4f  682e6ff3
748f82ee  78a5636f  84c87814  8cc70208  90befffa  a4506ceb  bef9a3f7  c67178f2
```

NOTE These values are the first 32 bits of the fractional parts of the cube roots of the first 64 primes.

10.2.5 Initializing value

For this round-function, the initializing value, IV, shall always be the following 256-bit string, represented here as a sequence of eight words, Y_0, Y_1, Y_2, Y_3, Y_4, Y_5, Y_6 and Y_7, in a hexadecimal representation, where Y_0 represents the left-most 32 of the 256 bits:

Y_0 = 6a09e667;
Y_1 = bb67ae85;
Y_2 = 3c6ef372;
Y_3 = a54ff53a;
Y_4 = 510e527f;
Y_5 = 9b05688c;
Y_6 = 1f83d9ab;
Y_7 = 5be0cd19.

NOTE These values are obtained by taking the fractional parts of the square roots of the first eight primes.

10.3 Padding method

The padding method to be used with this hash-function shall be the same as the padding method defined in 9.3.

10.4 Description of the round-function

The round-function Φ operates as follows.

NOTE In this description, the symbols W_1, W_2, X_0, X_1, X_2, X_3, X_4, X_5, X_6, X_7, Z_0, Z_1, …, Z_{63} are used to denote 74 distinct words which contain values required in the computations.

a) Suppose the 512-bit (first) input to Φ is contained in Z_0, Z_1, …, Z_{15}, where Z_0 contains the left-most 32 of the 512 bits. Suppose also that the 256-bit (second) input to Φ is contained in eight words, Y_0, Y_1, Y_2, Y_3, Y_4, Y_5, Y_6 and Y_7.

b) For i = 16 to 63, let Z_i: = $e_5(Z_{i-2}) \uplus Z_{i-7} \uplus e_4(Z_{i-15}) \uplus Z_{i-16}$.

c) Let X_0: = Y_0, X_1: = Y_1, X_2: = Y_2, X_3: = Y_3, X_4: = Y_4, X_5: = Y_5, X_6: = Y_6 and X_7: = Y_7.

d) For i = 0 to 63, do the following three steps:

   1) W_1: = $X_7 \uplus e_3(X_4) \uplus e_0(X_4, X_5, X_6) \uplus C_i \uplus Z_i$;

   2) W_2: = $e_2(X_0) \uplus e_1(X_0, X_1, X_2)$;

   3) X_7: = X_6; X_6: = X_5; X_5: = X_4; X_4: = $X_3 \uplus W_1$; X_3: = X_2; X_2: = X_1; X_1: = X_0; X_0: = $W_1 \uplus W_2$.

e) Let Y_0: = $Y_0 \uplus X_0$, Y_1: = $Y_1 \uplus X_1$, Y_2: = $Y_2 \uplus X_2$, Y_3: = $Y_3 \uplus X_3$, Y_4: = $Y_4 \uplus X_4$, Y_5: = $Y_5 \uplus X_5$, Y_6: = $Y_6 \uplus X_6$ and Y_7: = $Y_7 \uplus X_7$.

f) The eight words, Y_0, Y_1, Y_2, Y_3, Y_4, Y_5, Y_6 and Y_7, represent the output of the round-function Φ. After the final iteration of the round-function, the eight words, Y_0, Y_1, Y_2, Y_3, Y_4, Y_5, Y_6 and Y_7, shall be converted to a sequence of 32 bytes using the inverse of the procedure specified in 10.2.2 and where Y_0 shall yield the first four bytes, Y_1 the next four bytes and so on. Thus, the first (left-most) byte will correspond to the most significant byte of Y_0 and the 32nd (right-most) byte will correspond to the least significant byte of Y_7. The 32 bytes shall be converted to a string of 256 bits using the inverse of the procedure specified in Clause 6, i.e. the first (left-most) bit will correspond to the most significant bit of the first (left-most) byte and the 256th (right-most) bit will correspond to the least significant bit of the 32nd (right-most) byte.

Figure 4 shows steps 1), 2) and 3) of item d) of the round-function Φ in Dedicated Hash-Function 4 (SHA-256). In the round-function Φ, steps 1), 2) and 3) of item d) are used 64 times (i = 0, …, 63).

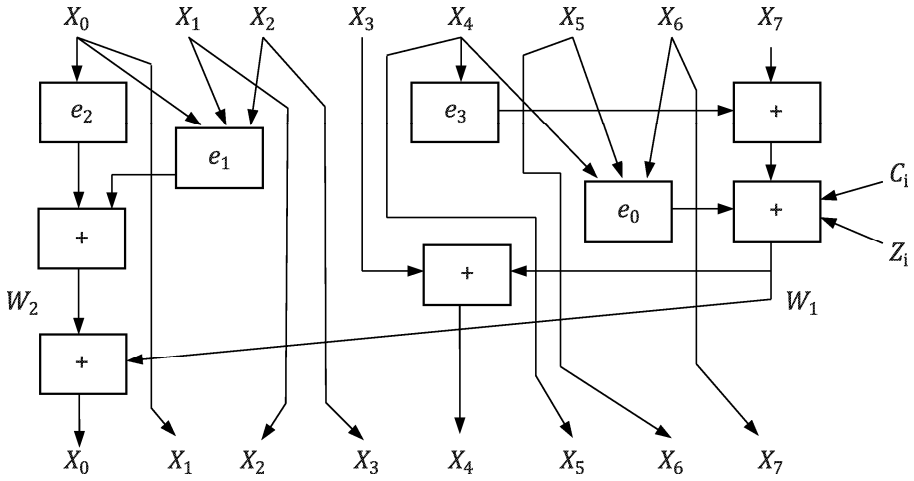

Figure 4 — Part of the round-function in Dedicated Hash-Function 4

11 Dedicated Hash-Function 5 (SHA-512)

11.1 General

In Clause 11, a padding method, an initializing value and a round-function for use in the general model for hash-functions described in ISO/IEC 10118-1 are specified. The padding method, initializing value and round-function specified here, when used in the above general model, together define Dedicated Hash-Function 5. This dedicated hash-function can be applied to all data strings, D, containing at most $2^{128}-1$ bits.

The ISO/IEC hash-function identifier for Dedicated Hash-Function 5 is equal to 35 (hexadecimal).

NOTE Dedicated Hash-Function 5 defined in Clause 11 is commonly called SHA-512[1].

11.2 Parameters, functions and constants

11.2.1 Parameters

For this hash-function, $L_1 = 1\,024$, $L_2 = 512$ and L_H is up to 512.

11.2.2 Byte ordering convention

In the specification of the round-function of Clause 11, it is assumed that the block input to the round-function is in the form of a sequence of 64-bit words, each 1 024-bit block is made up of 16 such words. A sequence of 128 bytes, B_0, B_1, …, B_{127}, shall be interpreted as a sequence of 16 words, Z_0, Z_1, …, Z_{15}, in the following way. Each group of eight consecutive bytes is considered a word, where the first byte of a word is the most significant byte of that word. Hence,

$$Z_i = 2^{56}B_{8i} + 2^{48}B_{8i+1} + 2^{40}B_{8i+2} + 2^{32}B_{8i+3} + 2^{24}B_{8i+4} + 2^{16}B_{8i+5} + 2^{8}B_{8i+6} + B_{8i+7}, \qquad (0 \le i \le 15).$$

To convert the hash-code from a sequence of words to a sequence of bytes, the inverse process shall be followed.

11.2.3 Functions

To facilitate software implementation, the round-function Φ is described in terms of operations on 64-bit words. A sequence of functions, d_0, d_1, d_2, d_3, d_4 and d_5, is used in this round-function, where d_0 and d_1

each takes three 64-bit words, X_0, X_1 and X_2, as input; d_2, d_3, d_4 and d_5 each takes one 64-bit word X_0 as input and each of these six functions produces a single 64-bit word as output.

The functions d_0, d_1, d_2, d_3, d_4 and d_5 are defined as follows:

$$d_0(X_0, X_1, X_2) = (X_0 \wedge X_1) \oplus (\neg X_0 \wedge X_2);$$
$$d_1(X_0, X_1, X_2) = (X_0 \wedge X_1) \oplus (X_0 \wedge X_2) \oplus (X_1 \wedge X_2);$$

$$d_2(X_0) = S'^{28}(X_0) \oplus S'^{34}(X_0) \oplus S'^{39}(X_0);$$
$$d_3(X_0) = S'^{14}(X_0) \oplus S'^{18}(X_0) \oplus S'^{41}(X_0);$$
$$d_4(X_0) = S'^{1}(X_0) \oplus S'^{8}(X_0) \oplus R^{7}(X_0);$$
$$d_5(X_0) = S'^{19}(X_0) \oplus S'^{61}(X_0) \oplus R^{6}(X_0).$$

11.2.4 Constants

A sequence of constant words, C_0, C_1, …, C_{79}, is used in this round-function. In a hexadecimal representation (where the most significant bit corresponds to the left-most bit), these are defined as follows, where the words are listed in the order C_0, C_1, …, C_{79}.

```
428a2f98d728ae22   7137449123ef65cd   b5c0fbcfec4d3b2f   e9b5dba58189dbbc
3956c25bf348b538   59f111f1b605d019   923f82a4af194f9b   ab1c5ed5da6d8118
d807aa98a3030242   12835b0145706fbe   243185be4ee4b28c   550c7dc3d5ffb4e2
72be5d74f27b896f   80deb1fe3b1696b1   9bdc06a725c71235   c19bf174cf692694
e49b69c19ef14ad2   efbe4786384f25e3   0fc19dc68b8cd5b5   240ca1cc77ac9c65
2de92c6f592b0275   4a7484aa6ea6e483   5cb0a9dcbd41fbd4   76f988da831153b5
983e5152ee66dfab   a831c66d2db43210   b00327c898fb213f   bf597fc7beef0ee4
c6e00bf33da88fc2   d5a79147930aa725   06ca6351e003826f   142929670a0e6e70
27b70a8546d22ffc   2e1b21385c26c926   4d2c6dfc5ac42aed   53380d139d95b3df
650a73548baf63de   766a0abb3c77b2a8   81c2c92e47edaee6   92722c851482353b
a2bfe8a14cf10364   a81a664bbc423001   c24b8b70d0f89791   c76c51a30654be30
d192e819d6ef5218   d69906245565a910   f40e35855771202a   106aa07032bbd1b8
19a4c116b8d2d0c8   1e376c085141ab53   2748774cdf8eeb99   34b0bcb5e19b48a8
391c0cb3c5c95a63   4ed8aa4ae3418acb   5b9cca4f7763e373   682e6ff3d6b2b8a3
748f82ee5defb2fc   78a5636f43172f60   84c87814a1f0ab72   8cc702081a6439ec
90befffa23631e28   a4506cebde82bde9   bef9a3f7b2c67915   c67178f2e372532b
ca273eceea26619c   d186b8c721c0c207   eada7dd6cde0eb1e   f57d4f7fee6ed178
06f067aa72176fba   0a637dc5a2c898a6   113f9804bef90dae   1b710b35131c471b
28db77f523047d84   32caab7b40c72493   3c9ebe0a15c9bebc   431d67c49c100d4c
4cc5d4becb3e42b6   597f299cfc657e2a   5fcb6fab3ad6faec   6c44198c4a475817
```

NOTE These values are the first 64 bits of the fractional parts of the cube roots of the first 80 primes.

11.2.5 Initializing value

For this round-function, the initializing value, IV, shall always be the following 512-bit string, represented here as a sequence of eight words, Y_0, Y_1, Y_2, Y_3, Y_4, Y_5, Y_6 and Y_7, in a hexadecimal representation, where Y_0 represents the left-most 64 of the 512 bits:

Y_0 = 6a09e667f3bcc908;
Y_1 = bb67ae8584caa73b;
Y_2 = 3c6ef372fe94f82b;
Y_3 = a54ff53a5f1d36f1;
Y_4 = 510e527fade682d1;
Y_5 = 9b05688c2b3e6c1f;
Y_6 = 1f83d9abfb41bd6b;
Y_7 = 5be0cd19137e2179.

NOTE These values are obtained by taking the fractional parts of the square roots of the first eight primes.

11.3 Padding method

The data string D needs to be padded to make it contain a number of bits which is an integer multiple of 1 024. The padding procedure is as follows.

a) D is concatenated with a single "1" bit.

b) The result of the previous step is concatenated with between zero and 1 023 "0" bits, such that the length (in bits) of the resultant string is congruent to 896 modulo 1 024. More explicitly, if the original length of D is L_D, and letting r be the remainder when L_D is divided by 1 024, then the number of concatenated zeros is equal to either $895 - r$ (if $r \leq 895$) or $1\,919 - r$ (if $r > 895$). The result will be a bit string whose length will be 128 bits short of an integer multiple of 1 024 bits.

c) Concatenate the string resulting from the previous step with the 128-bit binary representation of L_D, most significant bit first.

In the description of the round-function which follows, each 1 024-bit data block D_i, $1 \leq i \leq q$, is treated as a sequence of 16 words, $Z_0, Z_1, \ldots, Z_{15}$, where Z_0 corresponds to the left-most 64 bits of D_i.

NOTE The concatenation of the 128-bit string of L_D in step c) is such that the most significant 64-bit string and the least significant 64-bit string of L_D are used respectively as the words Z_{14} and Z_{15} of the last data block. Based on the byte ordering convention in 11.2.2, the most significant byte of L_D is the left-most byte and the least significant byte of L_D is the right-most byte.

11.4 Description of the round-function

The round-function Φ operates as follows.

NOTE In this description, the symbols W_1, W_2, X_0, X_1, X_2, X_3, X_4, X_5, X_6, X_7, Z_0, Z_1, …, Z_{79} are used to denote 90 distinct words which contain values required in the computations.

a) Suppose the 1 024-bit (first) input to Φ is contained in $Z_0, Z_1, \ldots, Z_{15}$, where Z_0 contains the left-most 64 of the 1 024 bits. Suppose also that the 512-bit (second) input to Φ is contained in eight words, $Y_0, Y_1, Y_2, Y_3, Y_4, Y_5, Y_6$ and Y_7.

b) For i = 16 to 79, let $Z_i := d_5(Z_{i-2}) \uplus Z_{i-7} \uplus d_4(Z_{i-15}) \uplus Z_{i-16}$.

c) Let $X_0 := Y_0$, $X_1 := Y_1$, $X_2 := Y_2$, $X_3 := Y_3$, $X_4 := Y_4$, $X_5 := Y_5$, $X_6 := Y_6$ and $X_7 := Y_7$.

d) For i = 0 to 79, do the following three steps:

1) $W_1 := X_7 \uplus d_3(X_4) \uplus d_0(X_4, X_5, X_6) \uplus C_i \uplus Z_i$;

2) $W_2 := d_2(X_0) \uplus d_1(X_0, X_1, X_2)$;

3) $X_7 := X_6$; $X_6 := X_5$; $X_5 := X_4$; $X_4 := X_3 \uplus W_1$; $X_3 := X_2$; $X_2 := X_1$; $X_1 := X_0$; $X_0 := W_1 \uplus W_2$.

e) Let $Y_0 := Y_0 \uplus X_0$, $Y_1 := Y_1 \uplus X_1$, $Y_2 := Y_2 \uplus X_2$, $Y_3 := Y_3 \uplus X_3$, $Y_4 := Y_4 \uplus X_4$, $Y_5 := Y_5 \uplus X_5$, $Y_6 := Y_6 \uplus X_6$ and $Y_7 := Y_7 \uplus X_7$.

f) The eight words, Y_0, Y_1, Y_2, Y_3, Y_4, Y_5, Y_6 and Y_7, represent the output of the round-function Φ. After the final iteration of the round-function, the eight words, Y_0, Y_1, Y_2, Y_3, Y_4, Y_5, Y_6 and Y_7, shall be converted to a sequence of 64 bytes using the inverse of the procedure specified in 11.2.2 and where Y_0 shall yield the first eight bytes, Y_1 the next eight bytes and so on. Thus, the first (left-most) byte will correspond to the most significant byte of Y_0 and the 64th (right-most) byte will correspond to the least significant byte of Y_7. The 64 bytes shall be converted to a string of 512 bits using the inverse of the procedure specified in Clause 6, i.e. the first (left-most) bit will correspond to the most significant bit of the first (left-most) byte and the 512th (right-most) bit will correspond to the least significant bit of the 64th (right-most) byte.

Figure 5 shows steps 1), 2) and 3) of item d) of the round-function Φ in Dedicated Hash-Function 5 (SHA-512). In the round-function Φ, steps 1), 2) and 3) of item d) are used 80 times (i = 0, ..., 79).

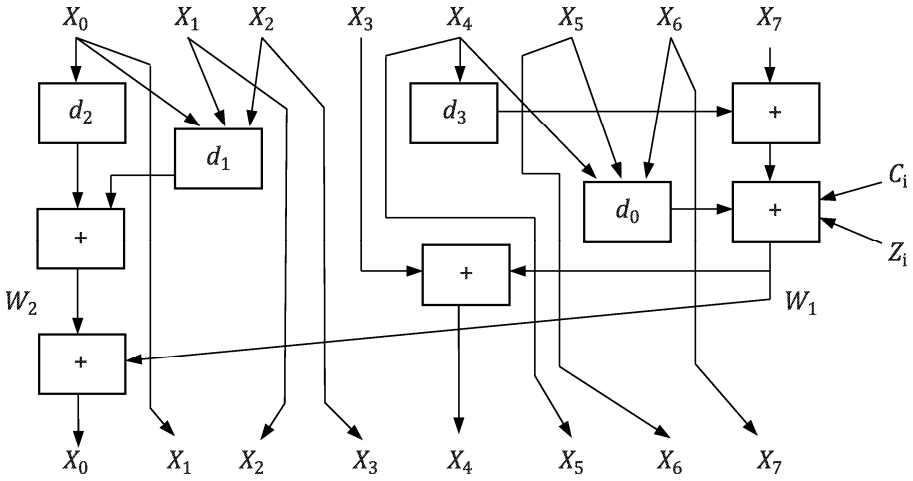

Figure 5 — Part of the round-function in Dedicated Hash-Function 5

12 Dedicated Hash-Function 6 (SHA-384)

12.1 General

In Clause 12, a padding method, an initializing value and a round-function for use in the general model for hash-functions described in ISO/IEC 10118-1 are specified. The padding method, initializing value and round-function specified here, when used in the above general model, together define Dedicated Hash-Function 6. This dedicated hash-function can be applied to all data strings, D, containing at most $2^{128}-1$ bits.

The ISO/IEC hash-function identifier for Dedicated Hash-Function 6 is equal to 36 (hexadecimal).

NOTE Dedicated Hash-Function 6 defined in Clause 12 is commonly called SHA-384[1].

12.2 Parameters, functions and constants

12.2.1 Parameters

For this hash-function, L_1 = 1 024, L_2 = 512 and L_H = 384.

12.2.2 Byte ordering convention

The byte ordering convention for this hash-function is the same as that for the hash-function of Clause 11.

12.2.3 Functions

The functions for this hash-function are the same as that for the hash-function of Clause 11.

12.2.4 Constants

The constants for this hash-function are the same as that for the hash-function of Clause 11.

12.2.5 Initializing value

For this round-function, the initializing value, *IV*, shall always be the following 512-bit string, represented here as a sequence of eight words, Y_0, Y_1, Y_2, Y_3, Y_4, Y_5, Y_6 and Y_7, in a hexadecimal representation, where Y_0 represents the left-most 64 of the 512 bits:

Y_0 = CBBB9D5DC1059ED8;
Y_1 = 629A292A367CD507;
Y_2 = 9159015A3070DD17;
Y_3 = 152FECD8F70E5939;
Y_4 = 67332667FFC00B31;
Y_5 = 8EB44A8768581511;
Y_6 = DB0C2E0D64F98FA7;
Y_7 = 47B5481DBEFA4FA4.

NOTE These values are obtained by taking the fractional parts of the square roots of the 9th to the 16th primes.

12.3 Padding method

The padding method to be used with this hash-function shall be the same as the padding method defined in Clause 11.

12.4 Description of the round-function

The round-function to be used with this hash-function shall be the same as the round-function defined in Clause 11.

The final 384-bit hash is obtained by truncating the SHA-512-based hash output to its left-most 384 bits.

13 Dedicated Hash-Function 7 (WHIRLPOOL)

13.1 General

In Clause 13, a padding method, an initializing value and a round-function for use in the general model for hash-functions described in ISO/IEC 10118-1 are specified. The padding method, initializing value

and round-function specified here, when used in the above general model, together define Dedicated Hash-Function 7. This dedicated hash-function can be applied to all data strings, D, containing at most $2^{256}-1$ bits.

The ISO/IEC hash-function identifier for Dedicated Hash-Function 7 is equal to 37 (hexadecimal).

NOTE Dedicated Hash-Function 7 defined in Clause 13 is commonly called WHIRLPOOL[3].

13.2 Parameters, functions and constants

13.2.1 Parameters

For this hash-function, $L_1 = 512$, $L_2 = 512$ and L_H is up to 512.

13.2.2 Byte ordering convention

In the specification of the round-function of Clause 13, it is assumed that the block input to the round-function is in the form of a matrix M [where all matrices here are 8×8 matrices with entries chosen from GF(2^8)], each 512-bit block being made up of such a matrix. A sequence of 64 bytes, $B = (B_0, B_1, \ldots, B_{63})$, shall be interpreted as a matrix M in the following way. The entry in the first row and the first column of the matrix shall be the left-most byte (where the left-most byte corresponds to the most significant byte) of the sequence B (i.e. B_0), the entry in the first row and the second column of the matrix shall be the second left-most byte of B (i.e. B_1), …, and the entry in the eighth row and the eighth column of the matrix shall be the right-most byte of B (i.e. B_{63}). This is performed using function c_0 specified in 13.2.3.

To convert the hash-code from such a matrix to a sequence of bytes, the inverse process of the function c_0 shall be followed.

13.2.3 Functions

To facilitate software implementation, the round-function Φ is described in terms of operations on a matrix M. A sequence of functions, c_0, c_1, c_2, c_3 and c_4, is used in this round-function. They are defined as follows.

a) Function c_0 takes a 64-byte sequence, $B = (B_0, B_1, \ldots, B_{63})$ as input and produces a matrix $Z' = (z'_{ij})$ as output where

$$z'_{ij} = B_{8i+j} \qquad (0 \le i, j \le 7).$$

This means that $Z' = c_0(B)$, if and only if, $z'_{ij} = B_{8i+j}$ $(0 \le i, j \le 7)$.

b) Function c_1 takes a matrix $X'' = (x''_{ij})$ as input and produces another matrix $W' = (w'_{ij})$ as output where

$$w'_{ij} = s[x''_{ij}], \qquad (0 \le i, j \le 7),$$

and where s is a function defined below. This means $W' = c_1(X'')$, if and only if, $w'_{ij} = s[x''_{ij}]$ $(0 \le i, j \le 7)$.

The function s replaces an element $x \in$ GF(2^8) with another element $s[x] \in$ GF(2^8). As specified in Table 2, the elements in the first column are the "most significant half" of x and the elements in the first row are the "least significant half" of x. For instance, if $x = 01010110 = 56$ (hexadecimal), $s[x] = 49$ (hexadecimal) = 01001001.

Table 2 — Values of the *s*-box

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

c) Function c_2 takes a matrix $X'' = (x''_{ij})$ as input and produces another matrix $W' = (w'_{ij})$ as output where

$$w'_{ij} = x''_{(i - j) \bmod 8,j}, \qquad (0 \le i, j \le 7).$$

This means that $W' = c_2(X'')$, if and only if, $w'_{ij} = x''_{(i - j) \bmod 8,j}$ $(0 \le i, j \le 7)$.

d) Function c_3 takes a matrix X'' as input and produces another matrix W' as output where

$$W' = X'' \cdot C'',$$

and where C'' is an 8 × 8 circulant matrix with entries chosen from GF(2^8), as specified below:

$$C'' = \begin{bmatrix} 01 & 01 & 04 & 01 & 08 & 05 & 02 & 09 \\ 09 & 01 & 01 & 04 & 01 & 08 & 05 & 02 \\ 02 & 09 & 01 & 01 & 04 & 01 & 08 & 05 \\ 05 & 02 & 09 & 01 & 01 & 04 & 01 & 08 \\ 08 & 05 & 02 & 09 & 01 & 01 & 04 & 01 \\ 01 & 08 & 05 & 02 & 09 & 01 & 01 & 04 \\ 04 & 01 & 08 & 05 & 02 & 09 & 01 & 01 \\ 01 & 04 & 01 & 08 & 05 & 02 & 09 & 01 \end{bmatrix}$$

This means that $W' = c_3(X'')$ if and only if $W' = X'' \cdot C''$.

e) Function c_4 takes two matrices $X'' = (x''_{ij})$ and $Y' = (y'_{ij})$ as input and produces a single matrix $W' = (w'_{ij})$ as output where

$$w'_{ij} = x''_{ij} \oplus y'_{ij}, \qquad (0 \le i, j \le 7).$$

This means that $W' = c_4(X'', Y')$, if and only if, $w'_{ij} = x''_{ij} \oplus y'_{ij}$ $(0 \le i, j \le 7)$.

13.2.4 Constants

A sequence of constant matrices, $A^r = (A^r_{ij})$ $(0 < r \le 10)$, is used in this round-function. The round constant for the rth round is a matrix, defined as:

$$A^r_{0j} = s[8(r - 1) + j], \qquad (0 \le j \le 7),$$
$$A^r_{ij} = 0, \qquad (1 \le i \le 7, 0 \le j \le 7).$$

13.2.5 Initializing value

The initializing value, *IV*, is a string of 512 "0" bits.

NOTE 512 "0" bits for the initial value is represented by a matrix Y' with entries in GF(2^8).

13.3 Padding method

The data string D needs to be padded to make it contain a number of bits which is an integer multiple of 512. The padding procedure is as follows.

a) D is concatenated with a single "1" bit.

b) The result of the previous step is concatenated with between zero and 511 "0" bits, such that the length (in bits) of the resultant string is an odd multiple of 256.

c) If the original length of D is L_D, concatenate the string resulting from the previous step with the 256-bit binary representation of L_D, most significant bit first.

In the description of the round-function which follows, each 512-bit data block D_i, $1 \le i \le q$, is treated as a matrix $Z' = (z'_{ij})$ $(0 \le i, j \le 7)$, as specified in 13.2.3, where z'_{00} corresponds to the left-most 8 bits of D_i and z'_{77} corresponds to the right-most 8 bits of D_i.

NOTE The concatenation of the 256-bit string of L_D in step c) is such that the 256-bit string is used directly as the second half of the last data matrix. Based on the byte ordering convention in 13.2.2, the most significant byte of L_D is the entry in the fifth row and the first column and the least significant byte of L_D is the entry in the eighth row and the eighth column.

13.4 Description of the round-function

The round-function Φ operates as follows.

NOTE In this description, the symbols W', X'', K_0, K_1, …, K_{10} are used to denote 13 distinct matrices, each with entries chosen from GF(2^8), which contain values required in the computations.

a) Suppose the 512-bit (first) input to Φ is contained in a matrix Z' with entries chosen from GF(2^8) which is formed by using the byte ordering convention specified in 13.2.2. Suppose also that the 512-bit (second) input to Φ is contained in a matrix Y' with entries chosen from GF(2^8).

b) Let $K_0 := Y'$ and for $i = 1$ to 10, let $K_i := c_4\langle c_3\{c_2[c_1(K_{i-1})]\}, A^i\rangle$.

NOTE This step expands the matrix Y' onto a sequence of round keys K_0, …, K_{10}.

c) Let X'': = $c_4(Z', K_0)$ and for j = 1 to 10, do the following two steps:

1) W': = c_4<c_3{c_2[c_1(X'')]}, K_j>;

2) X'': = W'.

d) Let Y':= $W' \oplus K_0 \oplus Z'$.

The matrix Y' represents the output of the round-function Φ. After the final iteration of the round-function, the matrix Y' shall be converted to a sequence of 64 bytes using the inverse of the procedure specified in 16.2.2 and where the entry in the first row and the first column of the matrix shall yield the first byte, the entry in the first row and the second column of the matrix the next byte, …, the entry in the eighth row and the eighth column of the matrix the last byte. The 64 bytes shall be converted to a string of 512 bits using the inverse of the procedure specified in Clause 6, i.e. the first (left-most) bit will correspond to the most significant bit of the first (left-most) byte and the 512th (right-most) bit will correspond to the least significant bit of the 64th (right-most) byte.

Figure 6 shows steps 1) and 2) of item c) of the round-function Φ in Dedicated Hash-Function 7 (WHIRLPOOL). In the round-function Φ, the steps shown in Figure 6 are used 10 times (j = 1, …, 10).

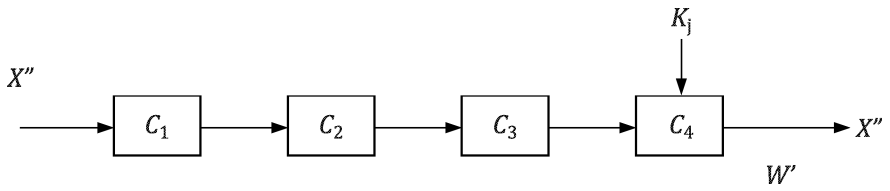

Figure 6 — Part of the round-function in Dedicated Hash-Function 7

14 Dedicated Hash-Function 8 (SHA-224)

14.1 General

In Clause 14, a padding method, an initializing value and a round-function for use in the general model for hash-functions described in ISO/IEC 10118-1 are specified. The padding method, initializing value and round-function specified here, when used in the above general model, together define Dedicated Hash-Function 8. This dedicated hash-function can be applied to all data strings, D, containing at most $2^{64}-1$ bits.

The ISO/IEC hash-function identifier for Dedicated Hash-Function 8 is equal to 38 (hexadecimal).

NOTE Dedicated Hash-Function 8 defined in Clause 14 is commonly called SHA-224[1].

14.2 Parameters, functions and constants

14.2.1 Parameters

For this hash-function, L_1 = 512, L_2 = 256 and L_H = 224.

14.2.2 Byte ordering convention

The byte ordering convention for this hash-function is the same as that for the hash-function of Clause 10.

14.2.3 Functions

The functions for this hash-function are the same as those for the hash-function of Clause 10.

14.2.4 Constants

The constants for this hash-function are the same as those for the hash-function of Clause 10.

14.2.5 Initializing value

For this round-function, the initializing value, *IV*, shall always be the following 256-bit string, represented here as a sequence of eight words, Y_0, Y_1, Y_2, Y_3, Y_4, Y_5, Y_6 and Y_7, in a hexadecimal representation, where Y_0 represents the left-most 32 of the 256 bits:

Y_0 = C1059ED8
Y_1 = 367CD507
Y_2 = 3070DD17
Y_3 = f70E5939
Y_4 = FFC00B31
Y_5 = 68581511
Y_6 = 64F98FA7
Y_7 = BEFA4FA4

NOTE These values are the low order 32-bits of the values specified in 12.2.5.

14.3 Padding method

The padding method to be used with this hash-function shall be the same as the padding method defined in 10.3.

14.4 Description of the round-function

The round-function to be used with this hash-function shall be the same as the round-function defined in 10.4.

The final 224-bit hash is obtained by truncating the SHA-256-based hash output to its left-most 224 bits.

15 Dedicated Hash-Function 9 (SHA-512/224)

15.1 General

In Clause 15, a padding method, an initializing value and a round-function for use in the general model for hash-functions described in ISO/IEC 10118-1 are specified. The padding method, initializing value and round-function specified here, when used in the above general model, together define Dedicated Hash-Function 9. This dedicated hash-function can be applied to all data strings, *D*, containing at most $2^{128}-1$ bits.

The ISO/IEC hash-function identifier for Dedicated Hash-Function 9 is equal to 39 (hexadecimal).

NOTE Dedicated Hash-Function 9 defined in Clause 15 is commonly called SHA-512/224[1].

15.2 Parameters, functions and constants

15.2.1 Parameters

For this hash-function, L_1 = 1 024, L_2 = 512 and L_H is up to 224.

15.2.2 Byte ordering convention

The byte ordering convention for this hash-function is the same as that for the hash-function of Clause 11.

15.2.3 Functions

The functions for this hash-function are the same as that for the hash-function of Clause 11.

15.2.4 Constants

The constants for this hash-function are the same as that for the hash-function of Clause 11.

15.2.5 Initializing value

For this round-function, the initializing value, *IV*, shall always be the following 512-bit string, represented here as a sequence of eight words, Y_0, Y_1, Y_2, Y_3, Y_4, Y_5, Y_6 and Y_7, in a hexadecimal representation, where Y_0 represents the left-most 64 of the 512 bits:

Y_0 = 8C3D37C819544DA2
Y_1 = 73E1996689DCD4D6
Y_2 = 1DFAB7AE32FF9C82
Y_3 = 679DD514582F9FCF
Y_4 = 0F6D2B697BD44DA8
Y_5 = 77E36F7304C48942
Y_6 = 3F9D85A86A1D36C8
Y_7 = 1112E6AD91D692A1

15.3 Padding method

The padding method to be used with this hash-function shall be the same as the padding method defined in Clause 11.

15.4 Description of the round-function

The round-function to be used with this hash-function shall be the same as the round-function defined in Clause 11. The final 224-bit hash is obtained by truncating the SHA-512-based hash output to its left-most 224 bits.

16 Dedicated Hash-Function 10 (SHA-512/256)

16.1 General

In Clause 16, a padding method, an initializing value and a round-function for use in the general model for hash-functions described in ISO/IEC 10118-1 are specified. The padding method, initializing value and round-function specified here, when used in the above general model, together define Dedicated Hash-Function 10. This dedicated hash-function can be applied to all data strings, *D*, containing at most $2^{128}-1$ bits.

The ISO/IEC hash-function identifier for Dedicated Hash-Function 10 is equal to 3A (hexadecimal).

NOTE Dedicated Hash-Function 10 defined in Clause 16 is commonly called SHA-512/256[1].

16.2 Parameters, functions and constants

16.2.1 Parameters

For this hash-function, L_1 = 1 024, L_2 = 512 and L_H is up to 256.

16.2.2 Byte ordering convention

The byte ordering convention for this hash-function is the same as that for the hash-function of Clause 11.

16.2.3 Functions

The functions for this hash-function are the same as that for the hash-function of Clause 11.

16.2.4 Constants

The constants for this hash-function are the same as that for the hash-function of Clause 11.

16.2.5 Initializing value

For this round-function the initializing value, *IV*, shall always be the following 512-bit string, represented here as a sequence of eight words, Y_0, Y_1, Y_2, Y_3, Y_4, Y_5, Y_6 and Y_7, in a hexadecimal representation, where Y_0 represents the left-most 64 of the 512 bits:

Y_0 = 22312194FC2BF72C
Y_1 = 9F555FA3C84C64C2
Y_2 = 2393B86B6F53B151
Y_3 = 963877195940EABD
Y_4 = 96283EE2A88EFFE3
Y_5 = BE5E1E2553863992
Y_6 = 2B0199FC2C85B8AA
Y_7 = 0EB72DDC81C52CA2

16.3 Padding method

The padding method to be used with this hash-function shall be the same as the padding method defined in Clause 11.

16.4 Description of the round-function

The round-function to be used with this hash-function shall be the same as the round-function defined in Clause 11. The final 256-bit hash is obtained by truncating the SHA-512-based hash output to its left-most 256 bits.

17 Dedicated Hash-Function 11 (STREEBOG-512)

17.1 General

In Clause 17, a padding method, an initializing value and a round-function for use in the general model for hash-functions described in ISO/IEC 10118-1 are specified. The padding method, initializing value and round-function specified here, when used in the above general model, together define Dedicated Hash-Function 11. This dedicated hash-function can be applied to all data strings, *D*, containing at most $2^{512}-1$ bits.

The ISO/IEC hash-function identifier for Dedicated Hash-Function 11 is equal to 3B (hexadecimal).

NOTE Dedicated Hash-Function 11 defined in Clause 17 is one of the functions specified in GOST R 34.11–2012, the national standard of the Russian Federation, commonly called STREEBOG[2].

17.2 Parameters, functions and constants

17.2.1 Parameters

For this hash-function, $L_1 = 512$, $L_2 = 512$ and $L_H = 512$.

17.2.2 Byte ordering convention

In the specification of the round-function of Clause 17, it is assumed that the block input to the round-function is in the form of a sequence of 512 bits. A sequence of 64 bytes, B_0, …, B_{63}, shall be interpreted as a sequence of consecutive bits in the following way. Each byte is considered as an 8-bit sequence, the most significant bit of the byte shall be the first bit of the sequence. Each 512-bit block is treated as a number in the following format:

$$Z = B_0 + B_1 2^8 + ... + B_{63} 2^{504}.$$

To convert the hash-code from a sequence of bits to a sequence of bytes, the inverse process shall be followed.

17.2.3 Functions

17.2.3.1 General

To calculate the hash-code H of the data string D, functions X, S, P, L and MSB_n are used. They are defined in the following subclauses.

17.2.3.2 Function *X*

Function $X[k]$ takes a 512-bit word as input and for the given 512-bit word, produces a 512-bit word as output, where $X[k](a) = k \oplus a$.

17.2.3.3 Function *S*

Function S takes a 512-bit word as input, produces a 512-bit word as output and is defined as

$$S(a) = S(a_{63} \,||\, \ldots \,||\, a_0) = \pi(a_{63}) \,||\, \ldots \,||\, \pi(a_0),$$

where $a = a_{63} \,||\, \ldots \,||\, a_0$, a_i, $i = 0, \ldots, 63$ are 8-bit words and π denotes a function from the set of octet strings to itself. π is defined as

$$\pi = \text{Vec}_8 \pi' \text{Int}_8,$$

where $\pi' : Z_{2^8} \rightarrow Z_{2^8}$.

The function π' is defined by the array $\pi' = [\pi'(0), \pi'(1), ..., \pi'(255)]$:

π' = (252, 238, 221, 17, 207, 110, 49, 22, 251, 196, 250, 218, 35, 197, 4, 77, 233, 119, 240, 219, 147, 46, 153, 186, 23, 54, 241, 187, 20, 205, 95, 193, 249, 24, 101, 90, 226, 92, 239, 33, 129, 28, 60, 66, 139, 1, 142, 79, 5, 132, 2, 174, 227, 106, 143, 160, 6, 11, 237, 152, 127, 212, 211, 31, 235, 52, 44, 81, 234, 200, 72, 171, 242, 42, 104, 162, 253, 58, 206, 204, 181, 112, 14, 86, 8, 12, 118, 18, 191, 114, 19, 71, 156, 183, 93, 135, 21, 161, 150, 41, 16, 123, 154, 199, 243, 145, 120, 111, 157, 158, 178, 177, 50, 117, 25, 61, 255, 53, 138, 126, 109, 84, 198, 128, 195, 189, 13, 87, 223, 245, 36, 169, 62, 168, 67, 201, 215, 121, 214, 246, 124, 34, 185, 3, 224, 15, 236, 222, 122, 148, 176, 188, 220, 232, 40, 80, 78, 51, 10, 74, 167, 151, 96, 115, 30, 0, 98, 68, 26, 184, 56, 130, 100, 159, 38, 65, 173, 69, 70, 146, 39, 94, 85, 47, 140, 163, 165, 125, 105, 213, 149, 59, 7, 88, 179, 64, 134, 172, 29, 247, 48, 55, 107, 228, 136, 217, 231, 137, 225, 27, 131, 73, 76, 63, 248, 254, 141, 83, 170, 144, 202, 216, 133, 97, 32, 113, 103, 164, 45, 43, 9, 91, 203, 155, 37, 208, 190, 229, 108, 82, 89, 166, 116, 210, 230, 244, 180, 192, 209, 102, 175, 194, 57, 75, 99, 182).

17.2.3.4 Function *P*

Function *P* takes a 512-bit word as input, produces a 512-bit word as output and is defined as

$$P(a) = P(a_{63} \| ... \| a_0) = a_{\tau(63)} \| ... \| a_{\tau(0)},$$

where $a = a_{63} \| ... \| a_0$, a_i, $i = 0,..., 63$ are 8-bit words and τ is a permutation of the set {0, 1, ..., 63} given by the array $\tau = [\tau(0), \tau(1), ..., \tau(63)]$:

τ = (0, 8, 16, 24, 32, 40, 48, 56, 1, 9, 17, 25, 33, 41, 49, 57, 2, 10, 18, 26, 34, 42, 50, 58, 3, 11, 19, 27, 35, 43, 51, 59, 4, 12, 20, 28, 36, 44, 52, 60, 5, 13, 21, 29, 37, 45, 53, 61, 6, 14, 22, 30, 38, 46, 54, 62, 7, 15, 23, 31, 39, 47, 55, 63).

17.2.3.5 Function *L*

Function *L* takes a 512-bit word as input, produces a 512-bit word as output and is defined as

$$L(a) = L(a_7 \| ... \| a_0) = l(a_7) \| ... \| l(a_0),$$

where $a = a_7 \| ... \| a_0$, a_i, $i = 0, ..., 7$, are 64-bit words and l is a function equal to right multiplication by the matrix A, given below, over the field GF(2). The matrix rows are expressed sequentially in hexadecimal notation. The row with number j, $j = 0, ..., 63$, (specified in the form $a_{j,15}, ..., a_{j,0}$, where $a_{j,i} \in Z_{16}$, $i = 0, ..., 15$), is $\mathrm{Vec}_4(a_{j,15}) \| ... \| \mathrm{Vec}_4(a_{j,0})$.

8e20faa72ba0b470	47107ddd9b505a38	ad08b0e0c3282d1c	d8045870ef14980e
6c022c38f90a4c07	3601161cf205268d	1b8e0b0e798c13c8	83478b07b2468764
a011d380818e8f40	5086e740ce47c920	2843fd2067adea10	14aff010bdd87508
0ad97808d06cb404	05e23c0468365a02	8c711e02341b2d01	46b60f011a83988e
90dab52a387ae76f	486dd4151c3dfdb9	24b86a840e90f0d2	125c354207487869
092e94218d243cba	8a174a9ec8121e5d	4585254f64090fa0	accc9ca9328a8950
9d4df05d5f661451	c0a878a0a1330aa6	60543c50de970553	302a1e286fc58ca7
18150f14b9ec46dd	0c84890ad27623e0	0642ca05693b9f70	0321658cba93c138
86275df09ce8aaa8	439da0784e745554	afc0503c273aa42a	d960281e9d1d5215
e230140fc0802984	71180a8960409a42	b60c05ca30204d21	5b068c651810a89e
456c34887a3805b9	ac361a443d1c8cd2	561b0d22900e4669	2b838811480723ba
9bcf4486248d9f5d	c3e9224312c8c1a0	effa11af0964ee50	f97d86d98a327728

e4fa2054a80b329c	727d102a548b194e	39b008152acb8227	9258048415eb419d
492c024284fbaec0	aa16012142f35760	550b8e9e21f7a530	a48b474f9ef5dc18
70a6a56e2440598e	3853dc371220a247	1ca76e95091051ad	0edd37c48a08a6d8
07e095624504536c	8d70c431ac02a736	c83862965601dd1b	641c314b2b8ee083

Each row of the given table contains four rows of the matrix A. So, the line with number i, $i = 0, ..., 15$, specifies the rows of the matrix A with numbers $4i + j$, $j = 0, ..., 3$, in the following left-to-right order: $4i + 0$, $4i + 1$, $4i + 2$, $4i + 3$.

The product of the 64-bit word $b = b_{63}, ..., b_0$ and the matrix A is a 64-bit word c:

$$c = b_{63}[\mathrm{Vec}_4(a_{0,15}) \| \ldots \| \mathrm{Vec}_4(a_{0,0})] \oplus \ldots \oplus b_0[\mathrm{Vec}_4(a_{63,15}) \| \ldots \| \mathrm{Vec}_4(a_{63,0})],$$

where

$$b_i\left[\mathrm{Vec}_4(a_{63-i,15})\|\ldots\|\mathrm{Vec}_4(a_{63-i,0})\right] = \left\{\begin{array}{c} 0^{64}, \text{if } b_i = 0, \\ \left[\mathrm{Vec}_4(a_{63-i,15})\|\ldots\|\mathrm{Vec}_4(a_{63-i,0})\right] \end{array}\right\}, \text{if } b_i = 1,$$

for all $i = 0, \ldots, 63$.

17.2.3.6 Truncation function

Function MSB_n maps the word $z_{k-1} \| \ldots \| z_1 \| z_0$, $k \geq n$ to the word $z_{k-1} \| \ldots \| z_{k-n+1} \| z_{k-n}$.

17.2.4 Constants

Round constants are expressed in hexadecimal notation. The constant value specified in the form $a_{127}, \ldots, a_0$ (where $a_i \in Z_{16}$, $i = 0, \ldots, 127$) is $\mathrm{Vec}_4(a_{127}) \| \ldots \| \mathrm{Vec}_4(a_0)$:

```
C1 = b1085bda1ecadae9ebcb2f81c0657c1f2f6a76432e45d016714eb88d7585c4fc
  4b7ce09192676901a2422a08a460d31505767436cc744d23dd806559f2a64507;
C2 = 6fa3b58aa99d2f1a4fe39d460f70b5d7f3feea720a232b9861d55e0f16b50131
  9ab5176b12d699585cb561c2db0aa7ca55dda21bd7cbcd56e679047021b19bb7;
C3 = f574dcac2bce2fc70a39fc286a3d843506f15e5f529c1f8bf2ea7514b1297b7b
  d3e20fe490359eb1c1c93a376062db09c2b6f443867adb31991e96f50aba0ab2;
C4 = ef1fdfb3e81566d2f948e1a05d71e4dd488e857e335c3c7d9d721cad685e353f
  a9d72c82ed03d675d8b71333935203be3453eaa193e837f1220cbebc84e3d12e;
C5 = 4bea6bacad4747999a3f410c6ca923637f151c1f1686104a359e35d7800fffbd
  bfcd1747253af5a3dfff00b723271a167a56a27ea9ea63f5601758fd7c6cfe57;
C6 = ae4faeae1d3ad3d96fa4c33b7a3039c02d66c4f95142a46c187f9ab49af08ec6
  cffaa6b71c9ab7b40af21f66c2bec6b6bf71c57236904f35fa68407a46647d6e;
C7 = f4c70e16eeaac5ec51ac86febf240954399ec6c7e6bf87c9d3473e33197a93c9
  0992abc52d822c3706476983284a05043517454ca23c4af38886564d3a14d493;
C8 = 9b1f5b424d93c9a703e7aa020c6e41414eb7f8719c36de1e89b4443b4ddbc49a
  f4892bcb929b069069d18d2bd1a5c42f36acc2355951a8d9a47f0dd4bf02e71e;
C9 = 378f5a541631229b944c9ad8ec165fde3a7d3a1b258942243cd955b7e00d0984
  800a440bdbb2ceb17b2b8a9aa6079c540e38dc92cb1f2a607261445183235adb;
C10 = abbedea680056f52382ae548b2e4f3f38941e71cff8a78db1fffe18a1b336103
  9fe76702af69334b7a1e6c303b7652f43698fad1153bb6c374b4c7fb98459ced;
C11 = 7bcd9ed0efc889fb3002c6cd635afe94d8fa6bbbebab07612001802114846679
  8a1d71efea48b9caefbacd1d7d476e98dea2594ac06fd85d6bcaa4cd81f32d1b;
C12 = 378ee767f11631bad21380b00449b17acda43c32bcdf1d77f82012d430219f9b
  5d80ef9d1891cc86e71da4aa88e12852faf417d5d9b21b9948bc924af11bd720.
```

17.2.5 Initializing value

The initializing value, IV, is equal to 0^{512}.

17.3 Padding method

The data string, D, needs to be padded to make it contain a number of bits which is an integer multiple of 512. The padding procedure is as follows:

a) D is concatenated with a single "1" bit (bit placed to the left).

b) The result of the previous step is concatenated with between zero and 511 "0" bits (placed to the left) such that the length (in bits) of the resultant string is a multiple of 512.

c) If the original length of D is L_D, concatenate the string resulting from the previous step with the 512-bit binary representation of L_D.

d) If the data after step b) of padding could be expressed in the form D_0, D_1, …, D_k, where D_i are 512-bit words and k is a positive integer, calculate the value $\Sigma = D_0 \uplus D_1 \uplus \ldots \uplus D_k$ and concatenate the string resulting from the previous step with value Σ.

17.4 Description of the round-function

The round-function Φ operates as follows. Note that in Clause 17, the symbols h, m and N are used to denote three distinct 512-bit words which contain values required in the computations. The hash-code value of the data string D is calculated using an iterative procedure. Each iteration is performed using a round-function that transforms two 512-bit words to a 512-bit word and is calculated as:

$$\Phi(h, m) = g_N(h, m) = E[LPS(h \oplus N), m] \oplus h \oplus m,$$

where $E(K, m) = X[K_{13}]LPSX[K_{12}]\ldots LPSX[K_2]LPSX[K_1](m)$ and where N denotes a 512-bit word calculated during the iterative procedure.

The values $K_i \in V_{512}$, i = 1, …, 13 are calculated as follows:

$K_1 = K$;

$K_i = LPS(K_{i-1} \oplus C_{i-1})$, i =2, …, 13.

For brevity, instead of $g_{0^{512}}$, the notation g_0 is used.

The hash-function operates as follows. The input for calculating the hash-code is the data string, D (to be hashed), and the initializing value, IV.

The padding method described in 17.3 is accomplished within the algorithm that follows, i.e. that the padding does not actually have to be done prior to running the algorithm.

The algorithm for calculating the hash-code consists of the following stages.

a) Stage 1

Assign initial values to the following variables:

1) $h := IV$;

2) $N := 0^{512}$;

3) $\Sigma := 0^{512}$;

4) Go to Stage 2.

b) Stage 2

1) Check the condition: $L_D < 512$.

   If it is true, then go to Stage 3.

   Else, perform the following calculations:

   i) Let m be the right-most 512 bits of the message D (so that $D = D' \,||\, m$). Then perform the following calculations:

      — $h := g_N(h, m)$.

      — $N := \mathrm{Vec}_{512}[\mathrm{Int}_{512}(N) \boxplus 512]$.

      — $\Sigma := \mathrm{Vec}_{512}[\mathrm{Int}_{512}(\Sigma) \boxplus \mathrm{Int}_{512}(m)]$.

      — $D := D'$.

   ii) Go to 1).

c) Stage 3

   1) $m := 0^{511-L_D} \,||\, 1 \,||\, D$.

   2) $h := g_N(h, m)$.

   3) $N := \mathrm{Vec}_{512}[\mathrm{Int}_{512}(N) \boxplus L_D]$.

   4) $\Sigma := \mathrm{Vec}_{512}[\mathrm{Int}_{512}(\Sigma) \boxplus \mathrm{Int}_{512}(m)]$.

   5) $h := g_0(h, N)$.

   6) $h := g_0(h, \Sigma)$.

   7) End of the algorithm.

   The value of the variable h [obtained in step 6)] is the hash-code *H.*

18 Dedicated Hash-Function 12 (STREEBOG-256)

18.1 General

In Clause 18, a padding method, an initializing value and a round-function for use in the general model for hash-functions described in ISO/IEC 10118-1 are specified. The padding method, initializing value and round-function specified here, when used in the above general model, together define the Dedicated Hash-Function 12. This dedicated hash-function can be applied to all data strings, D, containing at most $2^{512}-1$ bits.

The ISO/IEC hash-function identifier for Dedicated Hash-Function 12 is equal to 3C (hexadecimal).

NOTE Dedicated Hash-Function 12 defined in Clause 18 is one of the functions specified in GOST R 34.11–2012, the national standard of the Russian Federation, commonly called STREEBOG[2].

18.2 Parameters, functions and constants

18.2.1 Parameters

For this hash-function, $L_1 = 512$, $L_2 = 512$ and $L_H = 256$.

18.2.2 Byte ordering convention

The byte ordering convention for this hash-function is the same as that for the hash-function of Clause 17.

18.2.3 Functions

The functions for this hash-function are the same as those for the hash-function of Clause 17.

18.2.4 Constants

The constants for this hash-function are the same as those for the hash-function of Clause 17.

18.2.5 Initializing value

The initializing value, *IV*, equals $(000\ 000\ 01)^{64}$.

18.3 Padding method

The padding method to be used with this hash-function shall be the same as the padding method defined in Clause 17.

18.4 Description of the round-function

The round-function to be used with this hash-function shall be the same as the round-function defined in Clause 17. The final 256-bit hash is obtained by truncating the STREEBOG-512-based hash output to its most significant 256 bits.

19 Dedicated Hash-Function 13 (SHA3-224)

19.1 General

The ISO/IEC hash-function identifier for Dedicated Hash-Function 13 is equal to 3D (hexadecimal).

19.2 Parameters, functions and constants

19.2.1 Parameters

For this hash-function, $L_1 = r = 1\ 152$, $L_2 = b = 1\ 600$, $c = b - r = 448$, $d = 224$, L_H is up to 224.

19.2.2 Byte ordering convention

Each data input D to the round-function Φ is a block of 1 152 bits that is XORed into the part of the state. The permutation f is then applied to the state. Because the step mappings that comprise the permutation are defined on the array form of the state, it is convenient to regard D as a sequence of 64-bit words that are XORed directly into the state array. For this purpose, when D is represented as a sequence of 144 bytes, $B_0, B_1, \ldots, B_{143}$, then D shall be interpreted as a sequence of 18 lane words, $Z_0, Z_1, \ldots, Z_{17}$, as follows:

$$Z_i = 2^{56}B_{8i+7} + 2^{48}B_{8i+6} + 2^{40}B_{8i+5} + 2^{32}B_{8i+4} + 2^{24}B_{8i+3} + 2^{16}B_{8i+2} + 2^{8}B_{8i+1} + B_{8i},$$

for $0 \le i \le 17$.

Hence, each group of eight consecutive bytes is a word and the bytes of the word are arranged in increasing order of significance, so that the first byte in the group becomes the least significant byte of the word.

Under this interpretation, D is XORed with the state array as follows:

If j and k are the elements of {0, 1, 2, 3, 4} such that (j, k) is the unique pair for which $i = 5k + j$, then for $0 \le i \le 17$, $Lane'(j, k) = Z_i \oplus Lane(j, k)$, where $Lane'(j, k)$ is the updated value of the lane.

19.2.3 Functions

19.2.3.1 General

In 19.2.3.8, the KECCAK-p permutations are specified. A KECCAK-p permutation is determined by two parameters. First, the fixed length of the strings that are permuted, called the *width* of the permutation, is denoted as b. Second, the number of iterations of an internal transformation, called a *round*, is denoted as n_r. For the Dedicated Hash-Functions 13, 14, 15 and 16, $b = 1\,600$ and $n_r = 24$. However, in some of the examples, in particular when a figure is used to illustrate the operations, smaller values of b are used.

A round of a KECCAK-p permutation, denoted by *Rnd*, consists of a sequence of five transformations called *step mappings*. The permutation is specified in terms of an array of values for b (= 1 600) bits that is repeatedly updated, called the *state*. The state is initially set to the input values of the permutation.

NOTE The term round is used differently from the term specified in ISO/IEC 10118-1, where a round is a function used to process one single input data block to the hash-function. For the Dedicated Hash-Functions 13, 14, 15 and 16, to process one single data block, the round-function is iterated n_r (= 24) times. That is, each execution of round-function Φ, as it is named in ISO/IEC 10118-1, iterates *Rnd* 24 times.

The notation and terminology for the state are described in 19.2.3.2 to 19.2.3.6. The step mappings are specified in 19.2.3.7. The KECCAK-p permutations, including the round-function *Rnd*, are specified in 19.2.3.8.

19.2.3.2 State

The input and output states of the permutation are comprised of b bit strings. To represent the step mappings, a state is represented as a $5 \times 5 \times w$ array of bits, where $w = b/25$. For $b = 1\,600$, $w = 64$. If S denotes a string that represents the state, then its bits are indexed from 0 to $b-1$, so that

$$S = S[0] \,||\, S[1] \,||\, \ldots \,||\, S[b\text{-}2] \,||\, S[b-1].$$

If **A** denotes a $5 \times 5 \times w$ array of bits that represents the state, then its indices are the integer triples (x, y, z) for which $0 \le x < 5$, $0 \le y < 5$ and $0 \le z < w$. The bit that corresponds to (x, y, z) is denoted by $\mathbf{A}[x, y, z]$. A *state array* is a representation of the state by a three-dimensional array that is indexed in this manner.

19.2.3.3 Parts of the state array

The two-dimensional sub-arrays are called sheets, planes and slices; and the single-dimensional sub-arrays are called rows, columns and lanes.

The algebraic definitions of these sub-arrays are as follows.

Column For a state array, a sub-array of 5 bits with constant x and z coordinates.

Lane For a state array of a KECCAK-p permutation with width b, a sub-array of $b/25$ bits with constant x and y coordinates.

Plane For a state array of a KECCAK-*p* permutation with width *b*, a sub-array of *b*/5 bits with constant *y* coordinate.

Row For a state array, a sub-array of 5 bits with constant *y* and *z* coordinates.

Sheet For a state array of a KECCAK-*p* permutation with width *b*, a sub-array of *b*/5 bits with a constant *x* coordinate.

Slice For a state array, a sub-array of 25 bits with a constant *z* coordinate.

19.2.3.4 Converting strings to state arrays

Let *S* denote a string of *b* bits that represents the state for the KECCAK-*p* permutation. The corresponding state array, denoted by **A**, is defined as follows.

For all triples (x, y, z), such that $0 \le x < 5$, $0 \le y < 5$ and $0 \le z < w$,

$\mathbf{A}[x, y, z] = S[w(5y + x) + z]$.

For $b = 1\,600$ and $w = 64$,

$\mathbf{A}[0, 0, 0] = S[0]$ $\mathbf{A}[1, 0, 0] = S[64]$ $\mathbf{A}[4, 0, 0] = S[256]$

$\mathbf{A}[0, 0, 1] = S[1]$ $\mathbf{A}[1, 0, 1] = S[65]$ $\mathbf{A}[4, 0, 1] = S[257]$

$\mathbf{A}[0, 0, 2] = S[2]$ $\mathbf{A}[1, 0, 2] = S[66]$ $\mathbf{A}[4, 0, 2] = S[258]$

⋮ ⋮ … ⋮

$\mathbf{A}[0, 0, 61] = S[61]$ $\mathbf{A}[1, 0, 61] = S[125]$ $\mathbf{A}[4, 0, 61] = S[317]$

$\mathbf{A}[0, 0, 62] = S[62]$ $\mathbf{A}[1, 0, 62] = S[126]$ $\mathbf{A}[4, 0, 62] = S[318]$

$\mathbf{A}[0, 0, 63] = S[63]$ $\mathbf{A}[1, 0, 63] = S[127]$ $\mathbf{A}[4, 0, 63] = S[319]$

and

$\mathbf{A}[0, 1, 0] = S[320]$ $\mathbf{A}[1, 1, 0] = S[384]$ $\mathbf{A}[4, 1, 0] = S[576]$

$\mathbf{A}[0, 1, 1] = S[321]$ $\mathbf{A}[1, 1, 1] = S[385]$ $\mathbf{A}[4, 1, 1] = S[577]$

$\mathbf{A}[0, 1, 2] = S[322]$ $\mathbf{A}[1, 1, 2] = S[386]$ $\mathbf{A}[4, 1, 2] = S[578]$

⋮ ⋮ … ⋮

$\mathbf{A}[0, 1, 61] = S[381]$ $\mathbf{A}[1, 1, 61] = S[445]$ $\mathbf{A}[4, 1, 61] = S[637]$

$\mathbf{A}[0, 1, 62] = S[382]$ $\mathbf{A}[1, 1, 62] = S[446]$ $\mathbf{A}[4, 1, 62] = S[638]$

$\mathbf{A}[0, 1, 63] = S[383]$ $\mathbf{A}[1, 1, 63] = S[447]$ $\mathbf{A}[4, 1, 63] = S[639]$

and

$\mathbf{A}[0, 2, 0] = S[640]$ $\mathbf{A}[1, 2, 0] = S[704]$ $\mathbf{A}[4, 2, 0] = S[896]$

$\mathbf{A}[0, 2, 1] = S[641]$ $\mathbf{A}[1, 2, 1] = S[705]$ $\mathbf{A}[4, 2, 1] = S[897]$

$\mathbf{A}[0, 2, 2] = S[642]$ $\mathbf{A}[1, 2, 2] = S[706]$ $\mathbf{A}[4, 2, 2] = S[898]$

⋮ ⋮ … ⋮

A[0, 2, 61] = *S* [701] **A**[1, 2, 61] = *S* [765] **A**[4, 2, 61] = *S* [957]

A[0, 2, 62] = *S* [702] **A**[1, 2, 62] = *S* [766] **A**[4, 2, 62] = *S* [958]

A[0, 2, 63] = *S* [703] **A**[1, 2, 63] = *S* [767] **A**[4, 2, 63] = *S* [959]

etc.

19.2.3.5 Converting state arrays to strings

Let **A** denote a state array. The corresponding string representation, denoted by *S*, can be constructed from the lanes and planes of **A**, as follows:

For each pair of integers (i, j), such that $0 \le i < 5$ and $0 \le j < 5$, define the string *Lane* (i, j) by using

Lane (i, j) = **A**$[i, j, 0]$ || **A**$[i, j, 1]$ || **A**$[i, j, 2]$ || … || **A**$[i, j, w\text{-}2]$ || **A**$[i, j, w-1]$.

For b = 1 600 and w = 64,

Lane (0, 0) = **A**[0, 0, 0] || **A**[0, 0, 1] || **A**[0, 0, 2] || … || **A**[0, 0, 62] || **A**[0, 0, 63]

Lane (1, 0) = **A**[1, 0, 0] || **A**[1, 0, 1] || **A**[1, 0, 2] || … || **A**[1, 0, 62] || **A**[1, 0, 63]

Lane (2, 0) = **A**[2, 0, 0] || **A**[2, 0, 1] || **A**[2, 0, 2] || … || **A**[2, 0, 62] || **A**[2, 0, 63]

etc.

For each integer, j, such that $0 \le j < 5$, define the string *Plane* (j) by using

Plane (j) = *Lane* $(0, j)$ || *Lane* $(1, j)$ || *Lane* $(2, j)$ || *Lane* $(3, j)$ || *Lane* $(4, j)$.

Then,

S = *Plane* (0) || *Plane* (1) || *Plane* (2) || *Plane* (3) || *Plane* (4).

For b = 1 600 and w = 64,

S = **A**[0, 0, 0] || **A**[0, 0, 1] || **A**[0, 0, 2] || … || **A**[0, 0, 62] || **A**[0, 0, 63]

|| **A**[1, 0, 0] || **A**[1, 0, 1] || **A**[1, 0, 2] || … || **A**[1, 0, 62] || **A**[1, 0, 63]

|| **A**[2, 0, 0] || **A**[2, 0, 1] || **A**[2, 0, 2] || … || **A**[2, 0, 62] || **A**[2, 0, 63]

|| **A**[3, 0, 0] || **A**[3, 0, 1] || **A**[3, 0, 2] || … || **A**[3, 0, 62] || **A**[3, 0, 63]

|| **A**[4, 0, 0] || **A**[4, 0, 1] || **A**[4, 0, 2] || … || **A**[4, 0, 62] || **A**[4, 0, 63]

|| **A**[0, 1, 0] || **A**[0, 1, 1] || **A**[0, 1, 2] || … || **A**[0, 1, 62] || **A**[0, 1, 63]

|| **A**[1, 1, 0] || **A**[1, 1, 1] || **A**[1, 1, 2] || … || **A**[1, 1, 62] || **A**[1, 1, 63]

|| **A**[2, 1, 0] || **A**[2, 1, 1] || **A**[2, 1, 2] || … || **A**[2, 1, 62] || **A**[2, 1, 63]

|| **A**[3, 1, 0] || **A**[3, 1, 1] || **A**[3, 1, 2] || … || **A**[3, 1, 62] || **A**[3, 1, 63]

|| **A**[4, 1, 0] || **A**[4, 1, 1] || **A**[4, 1, 2] || … || **A**[4, 1, 62] || **A**[4, 1, 63]

⋮

|| **A**[0, 4, 0] || **A**[0, 4, 1] || **A**[0, 4, 2] || … || **A**[0, 4, 62] || **A**[0, 4, 63]

|| **A**[1, 4, 0] || **A**[1, 4, 1] || **A**[1, 4, 2] || … || **A**[1, 4, 62] || **A**[1, 4, 63]

|| **A**[2, 4, 0] || **A**[2, 4, 1] || **A**[2, 4, 2] || … || **A**[2, 4, 62] || **A**[2, 4, 63]

|| **A**[3, 4, 0] || **A**[3, 4, 1] || **A**[3, 4, 2] || … || **A**[3, 4, 62] || **A**[3, 4, 63]

|| **A**[4, 4, 0] || **A**[4, 4, 1] || **A**[4, 4, 2] || … || **A**[4, 4, 62] || **A**[4, 4, 63].

19.2.3.6 Labelling convention for the state array

In the diagrams of the state that accompany the specifications of the step mappings, the lane that corresponds to the coordinates $(x, y) = (0, 0)$ is depicted at the centre of the slices.

19.2.3.7 Step mappings

19.2.3.7.1 General

The five step mappings that comprise a round of KECCAK-p are denoted by θ, ρ, π, χ and ι. Specifications for these functions are given in 19.2.3.7.2 to 19.2.3.7.6.

The algorithm for each step mapping takes a state array, denoted by **A**, as an input and returns an updated state array, denoted by **A′**, as the output.

The ι mapping has a second input: an integer called the *round index*, denoted by i_r, which is defined within Algorithm 5 for KECCAK-p, in 19.2.3.7.6. The other step mappings do not depend on the *round index*.

19.2.3.7.2 Specification of θ

Algorithm 1: θ(**A**)

Input: state array **A**

Output: state array **A′**

Steps:

a) For all pairs (x, z), such that $0 \le x < 5$ and $0 \le z < w$, let

$$C[x, z] = \mathbf{A}[x, 0, z] \oplus \mathbf{A}[x, 1, z] \oplus \mathbf{A}[x, 2, z] \oplus \mathbf{A}[x, 3, z] \oplus \mathbf{A}[x, 4, z].$$

b) For all pairs (x, z), such that $0 \le x < 5$ and $0 \le z < w$ let

$$D[x, z] = C[(x-1) \bmod 5, z] \oplus C[(x+1) \bmod 5, (z - 1) \bmod w].$$

c) For all triples (x, y, z), such that $0 \le x < 5$, $0 \le y < 5$ and $0 \le z < w$, let

$$\mathbf{A}'[x, y, z] = \mathbf{A}[x, y, z] \oplus D[x, z].$$

The effect of θ is to XOR each bit in the state with the parities of two columns in the array. In particular, for the bit $\mathbf{A}[x_0, y_0, z_0]$, the x-coordinate of one of the columns is $(x_0 - 1) \bmod 5$, with the same z-coordinate, z_0, while the x-coordinate of the other column is $(x_0 + 1) \bmod 5$, with z-coordinate $(z_0 - 1) \bmod w$.

19.2.3.7.3 Specification of ρ

Algorithm 2: ρ(**A**)

Input: state array **A**

Output: state array **A′**

Steps:

a) For all z such that $0 \le z < w$, let **A′** [0, 0, z] = **A** [0, 0, z].

b) Let $(x, y) = (1, 0)$.

c) For t from 0 to 23:

   1) for all z such that $0 \le z < w$, let **A′** $[x, y, z]$ = **A** $\{x, y, [z - (t + 1)(t + 2)/2] \bmod w\}$;

   2) let $(x, y) = [y, (2x + 3y) \bmod 5]$.

d) Return **A′**.

19.2.3.7.4 Specification of π

Algorithm 3: π(**A**)

Input: state array **A**

Output: state array **A′**

Steps:

a) For all triples (x, y, z) such that $0 \le x < 5$, $0 \le y < 5$ and $0 \le z < w$, let

   A′ $[x, y, z]$ = **A** $[(x + 3y) \bmod 5, x, z]$.

b) Return **A′**.

19.2.3.7.5 Specification of χ

Algorithm 4: χ(**A**)

Input: state array **A**

Output: state array **A′**

Steps:

a) For all triples (x, y, z) such that $0 \le x < 5$, $0 \le y < 5$ and $0 \le z < w$, let

   A′ $[x, y, z]$ = **A** $[x, y, z] \oplus <\{$**A** $[(x+1) \bmod 5, y, z] \oplus 1\}$ ^ **A** $[(x+2) \bmod 5, y, z]>$.

b) Return **A′**.

The dot in the right side of the assignment for step a) indicates integer multiplication, which, in this case, is equivalent to the intended Boolean "AND" operation.

19.2.3.7.6 Specification of ι

The ι mapping is parameterized by the round index, i_r, whose values are specified in step b) of Algorithm 7 for computing KECCAK-p, in 19.2.3.8. Within the specification of ι in Algorithm 6, this

parameter determines $l + 1$ bits of a lane value called the *round constant*, denoted by *RC*, where $l = \log(w)$. When $w = 64$, $l = 6$. Each of these 7 bits is generated by a function that is based on a linear feedback shift register. This function, denoted by *rc*, is specified in Algorithm 5.

Algorithm 5: $rc(t)$

Input: integer t

Output: bit $rc(t)$

Steps:

a) If $t \bmod 255 = 0$, return 1.

b) Let $R = 10000000$.

c) For i from 1 to $t \bmod 255$, let:

1) $R = 0 \,||\, R$;

2) $R[0] = R[0] \oplus R[8]$;

3) $R[6] = R[6] \oplus R[8]$;

4) $R[3] = R[3] \oplus R[8]$;

5) $R[2] = R[2] \oplus R[8]$;

6) $R = Trunc_8[R]$.

d) Return $R[0]$.

In Algorithm 6, *RC* is a w-bit binary string and denoted as $RC[0], RC[1], ..., RC[w-1]$.

Algorithm 6: $\iota(\mathbf{A}, i_r)$

Input: state array $\mathbf{A}$; round index i_r

Output: state array $\mathbf{A'}$

Steps:

a) For all triples (x, y, z), such that $0 \le x < 5$, $0 \le y < 5$ and $0 \le z < w$, let $\mathbf{A'}[x, y, z] = \mathbf{A}[x, y, z]$.

b) Let $RC = 0^w$.

c) For j from 0 to 6, let $RC[2_j - 1] = rc(j + 7i_r)$.

d) For all z, such that $0 \le z < w$, let $\mathbf{A'}[0, 0, z] = \mathbf{A'}[0, 0, z] \oplus RC[z]$.

e) Return $\mathbf{A'}$.

The effect of ι is to modify some of the bits of *Lane* (0, 0) in a manner that depends on the round index i_r. The other 24 lanes are not affected by ι.

19.2.3.8 KECCAK-*p*

Given a state array $\mathbf{A}$ and a round index i_r, the round-function *Rnd* is the transformation that results from applying the step mappings θ, ρ, π, χ and ι, in that order, i.e.:

$$Rnd(\mathbf{A}, i_r) = \iota(\chi<\pi\{\rho[\theta(\mathbf{A})]\}>, i_r).$$

The KECCAK-*p* permutation consists of 24 iterations of *Rnd*, as specified in Algorithm 7.

Algorithm 7: KECCAK-*p* (*S*)

Input: string *S* of length 1 600 bits

Output: string *S* of length1 600 bits

Steps:

a) Convert *S* into a state array, **A**, as described in 19.2.3.4.

b) For i_r from 0 to 23, let **A** = *Rnd*(**A**, i_r).

c) Convert **A** into a string, *S*′ of length *b*, as described in 19.2.3.5.

d) Return *S*′.

19.3 Padding method

The data, a binary string *M*, will be padded with "01" before applying the padding method pad10*1(*x*, *m*), specified below with *x* = 1 152.

pad10*1(*x*, *m*)

Input: positive integer *x*; non-negative integer *m*

Output: string *P*, such that *m* + len(*P*) is a positive multiple of *x*

Steps:

a) Let *j* = (–*m* – 2) mod *x*.

b) Return *P* = 1 || 0_j || 1.

Thus, the asterisk in "pad10*1" indicates that the "0" bit is either omitted or repeated as necessary, in order to produce an output string of the desired length.

That is, the padded data is *P* = *M* || 01 || 10*1, such that the length of *P* is a multiple of 1 152.

19.4 Description of a round-function

The round-function for Dedicated Hash-Function 13 is the permutation KECCAK-*p* specified in 19.2.3.8. Notice that KECCAK-*p* is considered as *Φ* as defined in ISO/IEC 10118-1. However, for each execution of KECCAK-*p*, it iterates the *Rnd* function 24 times. That is, it executes

$$Rnd(\mathbf{A}, i_r) = \iota(\chi<\pi\{\rho\{\theta(\mathbf{A})]\}>, i_r),$$

for i_r = 0, 1, ..., 23.

19.5 Output transformation

In step h) of SPONGE[*f*, pad, *r*](*N*, *d*), because *r* = 1 152, *d* = 224 and *r* > *d*, the $Trunc_r(S)$ will be further truncated to *d* bits.

20 Dedicated Hash-Function 14 (SHA3-256)

20.1 General

In Clause 20, a permutation-based hash-function with sponge construction SHA3-256 is specified. The description of permutation-based hash-function with sponge construction is given in Clause 19.

The ISO/IEC hash-function identifier for Dedicated Hash-Function 14 is equal to 3E (hexadecimal).

20.2 Parameters, functions and constants

20.2.1 Parameters

For this hash-function, $L_1 = r = 1\,088$, $L_2 = b = 1\,600$, $c = b - r = 512$, $d = 256$, L_H is up to 256.

20.2.2 Byte ordering convention

Each data input D to the round-function Φ is a block of 1 088 bits that is XORed into the part of the state. The permutation f is then applied to the state. Because the step mappings that comprise the permutation are defined on the array form of the state, it is convenient to regard D as a sequence of 64-bit words that are XORed directly into the state array. For this purpose, when D is represented as a sequence of 136 bytes, B_0, B_1, …, B_{135}, then D shall be interpreted as a sequence of 17 lane words, Z_0, Z_1, …, Z_{16}, as follows:

$$Z_i = 2^{56}B_{8i+7} + 2^{48}B_{8i+6} + 2^{40}B_{8i+5} + 2^{32}B_{8i+4} + 2^{24}B_{8i+3} + 2^{16}B_{8i+2} + 2^{8}B_{8i+1} + B_{8i},$$

for $0 \le i \le 16$.

Hence, each group of eight consecutive bytes is a word and the bytes of the word are arranged in increasing order of significance, so that the first byte in the group becomes the least significant byte of the word.

Under this interpretation, D is XORed with the state array as follows.

If j and k are the elements of {0, 1, 2, 3, 4} such that (j, k) is the unique pair for which $i = 5k + j$, then for $0 \le i \le 16$, $Lane'(j, k) = Z_i \oplus \text{Lane}(j, k)$, where $Lane'(j, k)$ is the updated value of the lane.

20.2.3 Functions

The functions, including the function *Rnd* and step mappings, for the Dedicated Hash-Function 14 are the same as Dedicated Hash-Function 13 and is specified in Clause 19.

20.2.4 Constants

The constants used for the mapping ρ are the offsets defined in Clause 19.

20.2.5 Initializing value

The initializing value is a 1 600-bit all-zero string

20.3 Padding method

The data M will be padded with "01" before applying the padding method pad10*1(x, m) specified in Clause 19, with $x = 1\,088$.

That is, the padded data is $P = M \,||\, 01 \,||\, 10^*1$, such that the length of P is a multiple of 1 088.

20.4 Description of round-function

The round-function for Dedicated Hash-Function 14 is the permutation KECCAK-*p* specified in Clause 19. Notice that KECCAK-*p* is considered as Φ as defined in ISO/IEC 10118-1. However, for each execution of KECCAK-*p*, it iterates the *Rnd* function 24 times. That is, it executes

$$Rnd(\mathbf{A}, i_r) = \iota(\chi<\pi\{\rho[\theta(\mathbf{A})]\}>, i_r),$$

for $i_r = 0, 1, ..., 23$.

20.5 Output transformation

In step h) of SPONGE[*f*, pad, *r*](*N*, *d*) specified in Clause 19, because $r = 1\ 088$, $d = 256$ and $r > d$, the $Trunc_r(S)$ will be further truncated to *d* bits.

21 Dedicated Hash-Function 15 (SHA3-384)

21.1 General

In Clause 21, a permutation-based hash-function with sponge construction SHA3-384 is specified. The description of permutation-based hash-function with sponge construction is given in Clause 19.

The ISO/IEC hash-function identifier for Dedicated Hash-Function 15 is equal to 3F (hexadecimal).

21.2 Parameters, functions and constants

21.2.1 Parameters

For this hash-function, $L_1 = r = 832$, $L_2 = b = 1\ 600$, $c = b - r = 768$, $d = 384$, L_H is up to 384.

21.2.2 Byte ordering convention

Each data input *D* to the round-function Φ is a block of 832 bits that is XORed into the part of the state; the permutation *f* is then applied to the state. Because the step mappings that comprise the permutation are defined on the array form of the state, it is convenient to regard *D* as a sequence of 64-bit words that are XORed directly into the state array. For this purpose, when *D* is represented as a sequence of 104 bytes, $B_0, B_1, \ldots, B_{103}$, then *D* shall be interpreted as a sequence of 13 lane words, $Z_0, Z_1, \ldots, Z_{12}$, as follows:

$$Z_i = 2^{56}B_{8i+7} + 2^{48}B_{8i+6} + 2^{40}B_{8i+5} + 2^{32}B_{8i+4} + 2^{24}B_{8i+3} + 2^{16}B_{8i+2} + 2^{8}B_{8i+1} + B_{8i},$$

for $0 \le i \le 12$.

Hence, each group of eight consecutive bytes is a word and the bytes of the word are arranged in increasing order of significance, so that the first byte in the group becomes the least significant byte of the word.

Under this interpretation, *D* is XORed with the state array as follows.

If *j* and *k* are the elements of {0, 1, 2, 3, 4} such that (*j, k*) is the unique pair for which $i = 5k + j$, then for $0 \le i \le 12$, $Lane'(j, k) = Z_i \oplus Lane(j, k)$, where $Lane'(j, k)$ is the updated value of the lane.

21.2.3 Functions

The functions, including the function *Rnd* and step mappings, for the Dedicated Hash-Function 15 are the same as Dedicated Hash-Function 13 and is specified in Clause 19.

21.2.4 Constants

The constants used for the mapping ρ are the offsets defined in Clause 19.

21.2.5 Initializing value

The initializing value is a 1 600-bit all-zero string.

21.3 Padding method

The data M will be padded with "01" before applying the padding method pad10*1(x, m) specified in Clause 19, with x = 832.

That is, the padded data is $P = M \,||\, 01 \,||\, 10^*1$, such that the length of P is a multiple of 832.

21.4 Description of round-function

The round-function for Dedicated Hash-Function 15 is the permutation KECCAK-p specified in Clause 19. Notice that KECCAK-p is considered as Φ as defined in ISO/IEC 10118-1. However, for each execution of KECCAK-p, it iterates the *Rnd* function 24 times. That is, it executes

$$Rnd(\mathbf{A}, i_r) = \iota(\chi<\pi\{\rho\{\theta(\mathbf{A})\}\}>, i_r),$$

for i_r = 0, 1, ..., 23.

21.5 Output transformation

In step h) of SPONGE[f, pad, r](N, d) specified in Clause 19, because r = 832, d = 384 and $r > d$, the $Trunc_r(S)$ will be further truncated to d bits.

22 Dedicated Hash-Function 16 (SHA3-512)

22.1 General

In Clause 22, a permutation-based hash-function with sponge construction SHA3-512 is specified. The description of permutation-based hash-function with sponge construction is given in Clause 19.

The ISO/IEC hash-function identifier for Dedicated Hash-Function 16 is equal to 40 (hexadecimal).

22.2 Parameters, functions and constants

22.2.1 Parameters

For this hash-function, $L_1 = r$ = 576, $L_2 = b$ = 1 600, $c = b - r$ = 1 024, d = 512, L_H is up to 512.

22.2.2 Byte ordering convention

Each data input D to the round-function Φ is a block of 576 bits that is XORed into the part of the state. The permutation f is then applied to the state. Because the step mappings that comprise the permutation are defined on the array form of the state, it is convenient to regard D as a sequence of 64-bit words that are XORed directly into the state array. For this purpose, when D is represented as a sequence of 72 bytes, B_0, B_1, …, B_{71}, then D shall be interpreted as a sequence of 9 lane words, Z_0, Z_1, …, Z_8, as follows:

$$Z_i = 2^{56}B_{8i+7} + 2^{48}B_{8i+6} + 2^{40}B_{8i+5} + 2^{32}B_{8i+4} + 2^{24}B_{8i+3} + 2^{16}B_{8i+2} + 2^{8}B_{8i+1} + B_{8i},$$

for $0 \le i \le 8$.

Hence, each group of eight consecutive bytes is a word and the bytes of the word are arranged in increasing order of significance, so that the first byte in the group becomes the least significant byte of the word.

Under this interpretation, D is XORed with the state array as follows.

If j and k are the elements of {0, 1, 2, 3, 4} such that (j, k) is the unique pair for which $i = 5k + j$, then for $0 \le i \le 8$, $Lane'(j, k) = Z_i \oplus Lane(j, k)$, where $Lane'(j, k)$ is the updated value of the lane.

22.2.3 Functions

The functions, including the function *Rnd* and step mappings, for the Dedicated Hash-Function 16 are the same as Dedicated Hash-Function 13 and is specified in Clause 19.

22.2.4 Constants

The constants used for the mapping ρ are the offsets defined in Clause 19.

22.2.5 Initializing value

The initializing value is a 1 600-bit all-zero string.

22.3 Padding method

The data M will be padded with "01" before applying the padding method pad10*1(x, m) specified in Clause 19, with $x = 576$.

That is, the padded data is $P = M \,||\, 01 \,||\, 10^*1$, such that the length of P is a multiple of 576.

22.4 Description of round-function

The round-function for Dedicated Hash-Function 16 is the permutation KECCAK-p specified in Clause 19. Notice that KECCAK-p is considered as ϕ as defined in ISO/IEC 10118-1. However, for each execution of KECCAK-p, it iterates the *Rnd* function 24 times. That is, it executes

$$Rnd(\mathbf{A}, i_r) = \iota(\chi<\pi\{\rho[\theta(\mathbf{A})]\}>, i_r),$$

for $i_r = 0, 1, ..., 23$.

22.5 Output transformation

In step h) of SPONGE[f, pad, r](N, d) specified in Clause 19, because $r = 576$, $d = 512$ and $r > d$, the $Trunc_r(S)$ will be further truncated to d bits.

23 Dedicated Hash-Function 17 (SM3)

23.1 General

In Clause 23, a padding method, an initializing value and a round-function for use in the general model for hash-functions described in ISO/IEC 10118-1 are specified. The padding method, initializing value and round-function specified here, when used in the above general model, together define Dedicated Hash-Function 17. This dedicated hash-function can be applied to all data strings, D, containing at most $2^{64}-1$ bits.

The ISO/IEC hash-function identifier for Dedicated Hash-Function 17 is equal to 11 (hexadecimal).

NOTE Dedicated Hash-Function 17 defined in Clause 23 is commonly called SM3[7] [8].

23.2 Parameters, functions and constants

23.2.1 Parameters

For this hash-function, $L_1 = 512$, $L_2 = 256$ and L_H is up to 256.

23.2.2 Byte ordering convention

The byte ordering convention to be used with this hash-function shall be the same as the byte ordering convention defined in 9.2.2.

23.2.3 Functions

To facilitate software implementation, the round-function Φ is described in terms of operations on 32-bit words.

Two sequences of functions $b_0, b_1, \ldots, b_{63}$ and $b'_0, b'_1, \ldots, b'_{63}$ are used in this round-function, where each takes three words, X_0, X_1 and X_2, as input and produces a single word as output. Two functions, P_0 and P_1, are also used in this round-function, where each takes one word, X_0, as input and produces a single word as output.

The functions $b_0, b_1, \ldots, b_{63}, b'_0, b'_1, \ldots, b'_{63}, P_0, P_1$ are defined as follows:

$$b_i(X_0, X_1, X_2) = \begin{cases} X_0 \oplus X_1 \oplus X_2, & 0 \le i \le 15, \\ (X_0 \wedge X_1) \vee (X_0 \wedge X_2) \vee (X_1 \wedge X_2), & 16 \le i \le 63, \end{cases}$$

$$b'_i(X_0, X_1, X_2) = \begin{cases} X_0 \oplus X_1 \oplus X_2, & 0 \le i \le 15, \\ (X_0 \wedge X_1) \vee (\neg X_0 \wedge X_2), & 16 \le i \le 63, \end{cases}$$

$$P_0(X_0) = X_0 \oplus S^9(X_0) \oplus S^{17}(X_0),$$

$$P_1(X_0) = X_0 \oplus S^{15}(X_0) \oplus S^{23}(X_0).$$

23.2.4 Constants

A sequence of constant words, $C_0, C_1, \ldots, C_{63}$, is used in this round-function. In a hexadecimal representation (the most significant bit corresponds to the left-most bit), these are defined as follows:

$$C_i = \begin{cases} 79cc4519 & 0 \le i \le 15, \\ 7a879d8a & 16 \le i \le 63. \end{cases}$$

23.2.5 Initializing value

For this round-function the initializing value, *IV*, shall always be the following 256-bit string, represented here as a sequence of eight words, $Y_0, Y_1, \ldots, Y_7$, in a hexadecimal representation, where Y_0 represents the left-most 32 of the 256 bits.

Y_0 = 7380166*f*;
Y_1 = 4914*b*2*b*9;
Y_2 = 172442*d*7;
Y_3 = *da*8*a*0600;
Y_4 = *a*96*f*30*bc*;
Y_5 = 163138*aa*;
Y_6 = *e*38*dee*4*d*;
Y_7 = *b*0*fb*0*e*4*e*.

23.3 Padding method

The padding method to be used with this hash-function shall be the same as the padding method defined in 9.3.

23.4 Description of the round-function

The round-function Φ operates as follows.

NOTE In this description, the symbols W_1, W_2, W_3, W_4, X_0, X_1, X_2, X_3, X_4, X_5, X_6, X_7, Z_0, Z_1, …, Z_{67}, Z'_0, Z'_1, …, Z'_{63} are used to denote 144 distinct words which contain values required in the computations.

a) Suppose the 512-bit (first) input to Φ is contained in Z_0, Z_1, …, Z_{15}, where Z_0 contains the left-most 32 of the 512 bits. Suppose also that the 256-bit (second) input to Φ is contained in eight words, Y_0, Y_1, …, Y_7.

b) For i = 16 to 67, let $Z_i := P_1[Z_{i-16} \oplus Z_{i-9} \oplus S^{15}(Z_{i-3})] \oplus S^7(Z_{i-13}) \oplus Z_{i-6}$.

c) For i = 0 to 63, let $Z'_i := Z_i \oplus Z_{i+4}$.

d) Let $X_0 := Y_0$, $X_1 := Y_1$, $X_2 := Y_2$, $X_3 := Y_3$, $X_4 := Y_4$, $X_5 := Y_5$, $X_6 := Y_6$, $X_7 := Y_7$.

e) For i = 0 to 63, do the following five steps:

   1) $W_1 := S^7[S^{12}(X_0) \uplus X_4 \uplus S^i(C_i)]$;

   2) $W_2 := W_1 \oplus S^{12}(X_0)$;

   3) $W_3 := b_i(X_0, X_1, X_2) \uplus X_3 \uplus W_2 \uplus Z'_i$;

   4) $W_4 := b'_i(X_4, X_5, X_6) \uplus X_7 \uplus W_1 \uplus Z_i$;

   5) $X_7 := X_6$, $X_6 := S^{19}(X_5)$, $X_5 := X_4$, $X_4 := P_0(W_4)$, $X_3 := X_2$, $X_2 := S^9(X_1)$, $X_1 := X_0$, $X_0 := W_3$;

f) Let $Y_0 := Y_0 \oplus X_0$, $Y_1 := Y_1 \oplus X_1$, $Y_2 := Y_2 \oplus X_2$, $Y_3 := Y_3 \oplus X_3$, $Y_4 := Y_4 \oplus X_4$, $Y_5 := Y_5 \oplus X_5$, $Y_6 := Y_6 \oplus X_6$ and $Y_7 := Y_7 \oplus X_7$.

g) The eight words, Y_0, Y_1, …, Y_7, represent the output of the round-function Φ. After the final iteration of the round-function, the eight words, Y_0, Y_1, …, Y_7, shall be converted to a sequence of 32 bytes using the inverse of the procedure specified in Clause 9, where Y_0 shall yield the first four bytes, Y_1 the next four bytes and so on. Thus, the first (left-most) byte will correspond to the most significant byte of Y_0 and the 32nd (right-most) byte will correspond to the least significant byte of Y_7. The 32 bytes shall be converted to a string of 256 bits using the inverse of the procedure specified in Clause 6, i.e. the first (left-most) bit will correspond to the most significant bit of the first (left-most) byte and the 256th (right-most) bit will correspond to the least significant bit of the 32nd (right-most) byte.

Figure 7 shows steps 1), 2), 3), 4) and 5) of item e) of the round-function Φ in SM3. In the round-function Φ, steps 1), 2), 3), 4) and 5) of item e) are used 64 times (i = 0, 1, …, 63).

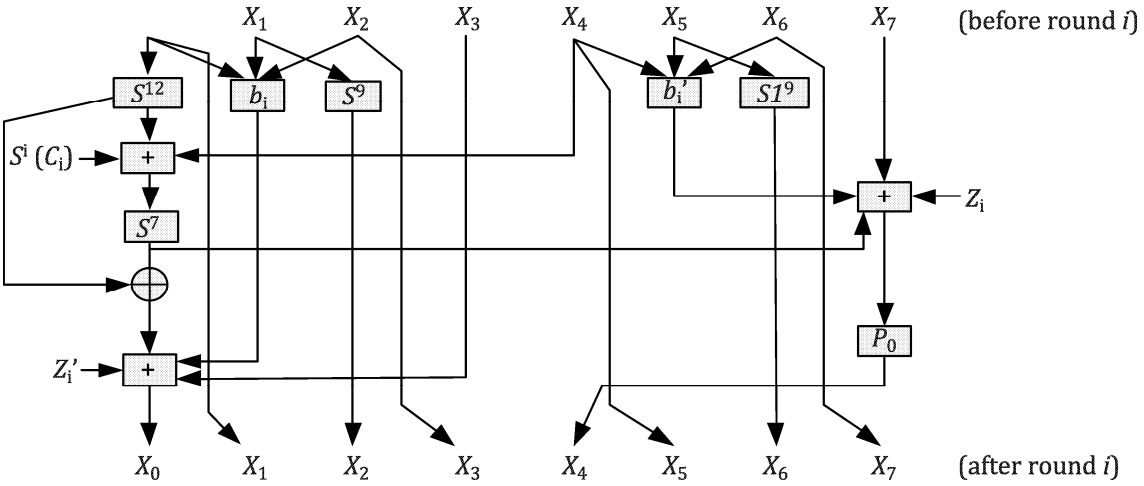

Figure 7 — Part of the round-function in Dedicated Hash-Function 17

Annex A
(normative)

Object identifiers

Annex A lists the object identifiers assigned to the dedicated hash-functions specified in this document.

```
--
-- Draft object identifiers of ISO/IEC 10118-3
-- Based on ISO/IEC JTC 1/SC 27 N XXXX XXXX-XX-XX
--

DedicatedHashFunctions {
iso(1) standard(0) hash-functions(10118) part(3)
asn1-module(1) dedicated-hash-functions(0) }
DEFINITIONS EXPLICIT TAGS ::= BEGIN

-- EXPORTS All; --

-- IMPORTS None; --

OID ::= OBJECT IDENTIFIER  -- alias

-- Synonyms --

id-dhf OID ::= {
iso(1) standard(0) hash-functions(10118) part3(3) algorithm(0) }

-- Assignments --

id-dhf-ripemd160 OID ::= { id-dhf ripemd160(49) }

id-dhf-ripemd128 OID ::= { id-dhf ripemd128(50) }

id-dhf-whirlpool OID ::= { id-dhf whirlpool(55) }

id-dhf-streebog512 OID ::= { id-dhf streebog512 (59) }

id-dhf-streebog256 OID ::= { id-dhf streebog256 (60) }

id-sha3-224 OID ::= { id-dhf hashAlgs7 (61) }

id-sha3-256 OID ::= { id-dhf hashAlgs8 (62) }

id-sha3-384 OID ::= { id-dhf hashAlgs9 (63) }

id-sha3-512 OID ::= { id-dhf hashAlgs10 (64) }

id-dhf-SM3 OID ::= { id-dhf sm3 (65) }

id-shake128 OID ::= { id-dhf hashAlgs11 (66) }

id-shake256 OID ::= { id-dhf hashAlgs12 (67) }


-- note: assign any new OIDs above 68

-- FIPS 180-1 and FIPS 180-2 Secure Hash Algorithm --
```

```
id-sha1 OID ::= {
iso(1) identified-organization(3) oiw(14) secsig(3)
algorithm(2) 26
}

sha2Algorithm OID ::= {
joint-iso-itu-t(2) country(16) us(840) organization(1) gov(101)
csor(3) nistAlgorithm(4) hashAlgs(2)
}

id-sha256 OID ::= { sha2Algorithm sha256(1) }

id-sha384 OID ::= { sha2Algorithm sha384(2) }

id-sha512 OID ::= { sha2Algorithm sha512(3) }

HashFunctions ::= SEQUENCE {
algorithm   ALGORITHM.&id({HashFunctionAlgs}),
parameters  ALGORITHM.&Type({HashFunctionAlgs}{@algorithm}) OPTIONAL
}

HashFunctionAlgs ALGORITHM ::= {
dhf-ripemd160  |
dhf-ripemd128  |
dhf-whirlpool  |
dhf-streebog256   |
dhf-streebog512   |
sha3-224 |
sha3-256 |
sha3-384 |
sha3-512 |
dhf-sm3 |
shake128 |
shake256 |
SHA-Algorithms,

...  -- Expect additional algorithms --
}

dhf-ripemd160 ALGORITHM ::= {
OID id-dhf-ripemd160  PARMS NullParms
}

dhf-ripemd128 ALGORITHM ::= {
OID id-dhf-ripemd128  PARMS NullParms
}

dhf-whirlpool ALGORITHM ::= {
OID id-dhf-whirlpool  PARMS NullParms
}

dhf-streebog256 ALGORITHM ::= {
OID id-dhf-streebog256  PARMS NullParms
}

dhf-streebog512 ALGORITHM ::= {
OID id-dhf-streebog512  PARMS NullParms
}

dhf-sha3-224 ALGORITHM ::= {
OID id-dhf-sha3-224 PARMS NullParms
}
```

```
dhf-sha3-256 ALGORITHM ::= {
OID id-dhf-sha3-256 PARMS NullParms
}

dhf-sha3-384 ALGORITHM ::= {
OID id-dhf-sha3-384 PARMS NullParms
}

dhf-sha3-512 ALGORITHM ::= {
OID id-dhf-sha3-512 PARMS NullParms
}

dhf-SM3 ALGORITHM ::= {
OID id-dhf-sm3  PARMS NullParms
}

dhf-shake128 ALGORITHM ::= {
OID id-dhf-shake128 PARMS NullParms
}

dhf-shake256 ALGORITHM ::= {
OID id-dhf-shake256 PARMS NullParms
}


SHA-Algorithms ALGORITHM ::= {

-- The parameters associated with id-sha1, id-sha256, id-sha384,  --
-- and id-sha512 should be omitted, but if present, should have    --
-- a value of ASN.1 type NULL. This is to align with the original --
-- NIST definitions (which did not have parameters) and certain   --
-- existing implementations (which have them). For these SHA     --
-- algorithms, implementations should accept AlgorithmIdentifier   --
-- values with NULL parameters and with the optional parameters   --
-- component not present.                                         --

sha-1    |
sha-256  |
sha-384  |
sha-512,

...  -- Expect additional algorithms --
}

sha-1 ALGORITHM ::= {
OID id-sha1  PARMS NullParms
}

sha-256 ALGORITHM ::= {
OID id-sha256 PARMS NullParms
}

sha-384 ALGORITHM ::= {
OID id-sha384 PARMS NullParms
}

sha-512 ALGORITHM ::= {
OID id-sha512 PARMS NullParms
}

NullParms ::= NULL

-- Cryptographic algorithm identification --
```

```
ALGORITHM ::= CLASS {
&id    OBJECT IDENTIFIER  UNIQUE,
&Type  OPTIONAL
}
WITH SYNTAX { OID &id [PARMS &Type] }

END  -- DedicatedHashFunctions --
```

Annex B
(informative)

Numerical examples

B.1 General

This annex gives numerical examples for the computation of Dedicated Hash-Functions 1 to 17. For each of the hash-functions, intermediate values derived during the hash-function's operation are given for some examples.

Throughout this annex, it is referred to as ASCII coding of data strings, which is equivalent to coding using ISO 646.

B.2 Dedicated Hash-Function 1 (RIPEMD-160)

NOTE Reference [4] contains a pseudocode description of Dedicated Hash-Function 1.

B.2.1 Example 1

In this example, the data string is the empty string, i.e., the string of length zero.

The hash-code is the following 160-bit string.

```
9C 11 85 A5 C5 E9 FC 54 61 28 08 97 7E E8 F5 48 B2 25 8D 31
```

B.2.2 Example 2

In this example, the data string consists of a single byte, namely the ASCII-coded version of the letter "a".

The hash-code is the following 160-bit string.

```
0B DC 9D 2D 25 6B 3E E9 DA AE 34 7B E6 F4 DC 83 5A 46 7F FE
```

B.2.3 Example 3

In this example, the data string is the 3-byte string consisting of the ASCII-coded version of "abc". This is equivalent to the bit string "01100001 01100010 01100011".

After the padding process, the single 16-word block derived from the data string is as follows.

```
80636261  00000000  00000000  00000000  00000000  00000000  00000000  00000000
00000000  00000000  00000000  00000000  00000000  00000000  00000018  00000000
```

The following are (hexadecimal representations of) the successive values of the variables X_0, X_1, X_2, X_3, X_4, X'_0, X'_1, X'_2, X'_3 and X'_4.

```
67452301, EFCDAB89, 98BADCFE, 10325476, C3D2E1F0, 67452301, EFCDAB89, 98BADCFE, 10325476, C3D2E1F0
C3D2E1F0, 3115FC67, EFCDAB89, EB73FA62, 10325476, C3D2E1F0, DDD63FB8, EFCDAB89, EB73FA62, 10325476
10325476, B41192D5, 3115FC67, 36AE27BF, EB73FA62, 10325476, 322E7AE3, DDD63FB8, 36AE27BF, EB73FA62
EB73FA62, 3A35DC50, B41192D5, 57F19CC4, 36AE27BF, EB73FA62, 883EE903, 322E7AE3, 58FEE377, 36AE27BF
36AE27BF, D3786413, 3A35DC50, 464B56D0, 57F19CC4, 36AE27BF, 92B2B79B, 883EE903, B9EB8CC8, 58FEE377
57F19CC4, 0E946720, D3786413, D77140E8, 464B56D0, 58FEE377, F9091FF2, 92B2B79B, FBA40E20, B9EB8CC8
464B56D0, D52BF632, 0E946720, E1904F4D, D77140E8, B9EB8CC8, E5B09992, F9091FF2, CADE6E4A, FBA40E20
D77140E8, 150BD8A8, D52BF632, 519C803A, E1904F4D, FBA40E20, 8B2D9FB3, E5B09992, 247FCBE4, CADE6E4A
E1904F4D, 3D6F601F, 150BD8A8, AFD8CB54, 519C803A, CADE6E4A, E755F422, 8B2D9FB3, C2664B96, 247FCBE4
```

519C803A, B7B60384, 3D6F601F, 2F62A054, AFD8CB54, 247FCBE4, 5922D09E, E755F422, B67ECE2C, C2664B96
AFD8CB54, B85A0A3F, B7B60384, BD807CF5, 2F62A054, C2664B96, CF24E72C, 5922D09E, 57D08B9D, B67ECE2C
2F62A054, 7F8B38E5, B85A0A3F, D80E12DE, BD807CF5, B67ECE2C, CA6A1C75, CF24E72C, 8B427964, 57D08B9D
BD807CF5, 9DACA495, 7F8B38E5, 6828FEE1, D80E12DE, 57D08B9D, 227F6D84, CA6A1C75, 939CB33C, 8B427964
D80E12DE, BC05F46F, 9DACA495, 2CE395FE, 6828FEE1, 8B427964, 5D801685, 227F6D84, A871D729, 939CB33C
6828FEE1, 1494F053, BC05F46F, B2925676, 2CE395FE, 939CB33C, B3C3F4D5, 5D801685, FDB61089, A871D729
2CE395FE, 85861D02, 1494F053, 17D1BEF0, B2925676, A871D729, 3D16242D, B3C3F4D5, 005A1576, FDB61089
B2925676, 597BF629, 85861D02, 53C14C52, 17D1BEF0, FDB61089, FF459078, 3D16242D, 0FD356CF, 005A1576
17D1BEF0, 6347EF78, 597BF629, 18740A16, 53C14C52, 005A1576, 927E40A8, FF459078, 5890B4F4, 0FD356CF
53C14C52, 45C8FA44, 6347EF78, EFD8A565, 18740A16, 0FD356CF, ACBB994E, 927E40A8, 1641E3FD, 5890B4F4
18740A16, AD2956AF, 45C8FA44, 1FBDE18D, EFD8A565, 5890B4F4, AD30AD24, ACBB994E, F902A249, 1641E3FD
EFD8A565, 5EAF16B7, AD2956AF, 23E91117, 1FBDE18D, 1641E3FD, 6261732E, AD30AD24, EE653AB2, F902A249
1FBDE18D, 41730D4B, 5EAF16B7, A55ABEB4, 23E91117, F902A249, 45ED27AF, 6261732E, C2B492B4, EE653AB2
23E91117, FC0CCBD3, 41730D4B, BC5ADD7A, A55ABEB4, EE653AB2, 243C5668, 45ED27AF, 85CCB989, C2B492B4
A55ABEB4, 042ECC93, FC0CCBD3, CC352D05, BC5ADD7A, C2B492B4, 82F89BD1, 243C5668, B49EBD17, 85CCB989
BC5ADD7A, 4D4D4377, 042ECC93, 332F4FF0, CC352D05, 85CCB989, 5FC74686, 82F89BD1, F159A090, B49EBD17
CC352D05, 5207002B, 4D4D4377, BB324C10, 332F4FF0, B49EBD17, B2720031, 5FC74686, E26F460B, F159A090
332F4FF0, 388278F5, 5207002B, 350DDD35, BB324C10, F159A090, 58A100F8, B2720031, 1D1A197F, E26F460B
BB324C10, 62879D70, 388278F5, 1C00AD48, 350DDD35, E26F460B, 5992068B, 58A100F8, C800C6C9, 1D1A197F
350DDD35, A30A1FD9, 62879D70, 09E3D4E2, 1C00AD48, 1D1A197F, CC290DCA, 5992068B, 8403E162, C800C6C9
1C00AD48, BDA2B31B, A30A1FD9, 1E75C18A, 09E3D4E2, C800C6C9, 863D625E, CC290DCA, 481A2D66, 8403E162
09E3D4E2, F7211DEE, BDA2B31B, 287F668C, 1E75C18A, 8403E162, 6061B5A5, 863D625E, A4372B30, 481A2D66
1E75C18A, B6A665C6, F7211DEE, 8ACC6EF6, 287F668C, 481A2D66, AA98ADB5, 6061B5A5, F5897A18, A4372B30
287F668C, 2D30FA02, B6A665C6, 8477BBDC, 8ACC6EF6, A4372B30, 2999255A, AA98ADB5, 86D69581, F5897A18
8ACC6EF6, C76D12F9, 2D30FA02, 99971ADA, 8477BBDC, F5897A18, 98237631, 2999255A, 62B6D6AA, 86D69581
8477BBDC, 516F84DF, C76D12F9, C3E808B4, 99971ADA, 86D69581, 6C472A90, 98237631, 649568A6, 62B6D6AA
99971ADA, F3FA5B05, 516F84DF, B44BE71D, C3E808B4, 62B6D6AA, 2EAD5672, 6C472A90, 8DD8C660, 649568A6
C3E808B4, D539625E, F3FA5B05, BE137D45, B44BE71D, 649568A6, C5CB48BA, 2EAD5672, 1CAA41B1, 8DD8C660
B44BE71D, D8500C99, D539625E, E96C17CF, BE137D45, 8DD8C660, 05286DFB, C5CB48BA, B559C8BA, 1CAA41B1
BE137D45, 7ECDE5B2, D8500C99, E5897B54, E96C17CF, 1CAA41B1, 88396DD2, 05286DFB, 2D22EB17, B559C8BA
E96C17CF, 681D30B9, 7ECDE5B2, 40326761, E5897B54, B559C8BA, 333F2212, 88396DD2, A1B7EC14, 2D22EB17
E5897B54, 960F7BFD, 681D30B9, 3796C9FB, 40326761, 2D22EB17, C699295B, 333F2212, E5B74A20, A1B7EC14
40326761, 6770E498, 960F7BFD, 74C2E5A0, 3796C9FB, A1B7EC14, BFD68874, C699295B, FC8848CC, E5B74A20
3796C9FB, 75EB06C5, 6770E498, 3DEFF658, 74C2E5A0, E5B74A20, BDDF3474, BFD68874, 64A56F1A, FC8848CC
74C2E5A0, 14FA827A, 75EB06C5, C392619D, 3DEFF658, FC8848CC, 8CBC87E9, BDDF3474, 5A21D2FF, 64A56F1A
3DEFF658, 804B0068, 14FA827A, AC1B15D7, C392619D, 64A56F1A, CDDA6EBF, 8CBC87E9, 7CD1D2F7, 5A21D2FF
C392619D, 475BA81B, 804B0068, EA09E853, AC1B15D7, 5A21D2FF, 656C7DA3, CDDA6EBF, F21FA632, 7CD1D2F7
AC1B15D7, D26BC25D, 475BA81B, 2C01A201, EA09E853, 7CD1D2F7, 76D66CA3, 656C7DA3, 69BAFF37, F21FA632
EA09E853, DBC5A2CB, D26BC25D, 6EA06D1D, 2C01A201, F21FA632, C9B17F72, 76D66CA3, B1F68D95, 69BAFF37
2C01A201, 77367F5E, DBC5A2CB, AF097749, 6EA06D1D, 69BAFF37, 65A60151, C9B17F72, 59B28DDB, B1F68D95
6EA06D1D, 8155A6B4, 77367F5E, 168B2F6F, AF097749, B1F68D95, 33F3AC81, 65A60151, C5FDCB26, 59B28DDB
AF097749, C90C4D38, 8155A6B4, D9FD79DC, 168B2F6F, 59B28DDB, 9BFB827D, 33F3AC81, 98054596, C5FDCB26
168B2F6F, 9762713B, C90C4D38, 569AD205, D9FD79DC, C5FDCB26, DDC8130E, 9BFB827D, CEB204CF, 98054596
D9FD79DC, 7EBF9C32, 9762713B, 3134E324, 569AD205, 98054596, C24C2C79, DDC8130E, EE09F66F, CEB204CF
569AD205, 20EFFA01, 7EBF9C32, 89C4EE5D, 3134E324, CEB204CF, F255847E, C24C2C79, 204C3B77, EE09F66F
3134E324, 75B7117F, 20EFFA01, FE70C9FA, 89C4EE5D, EE09F66F, DCD63949, F255847E, 30B1E709, 204C3B77
89C4EE5D, A96BE4C7, 75B7117F, BFE80483, FE70C9FA, 204C3B77, 5B99238D, DCD63949, 5611FBC9, 30B1E709
FE70C9FA, 5E3201FC, A96BE4C7, DC45FDD6, BFE80483, 30B1E709, B43484F4, 5B99238D, 58E52773, 5611FBC9
BFE80483, 2CF95A98, 5E3201FC, AF931EA5, DC45FDD6, 5611FBC9, 52325A09, B43484F4, 648E356E, 58E52773
DC45FDD6, 1393F0C3, 2CF95A98, C807F178, AF931EA5, 58E52773, D015577D, 52325A09, D213D2D0, 648E356E
AF931EA5, BB49CCF7, 1393F0C3, E56A60B3, C807F178, 648E356E, BB9C87C4, D015577D, C9682548, D213D2D0
C807F178, 6A330EB4, BB49CCF7, 4FC30C4E, E56A60B3, D213D2D0, B1BB1A2E, BB9C87C4, 555DF740, C9682548
E56A60B3, 14E58204, 6A330EB4, 2733DEED, 4FC30C4E, C9682548, AC77F96D, B1BB1A2E, 721F12EE, 555DF740
4FC30C4E, 79AAF53E, 14E58204, CC3AD1A8, 2733DEED, 555DF740, 1774D326, AC77F96D, EC68BAC6, 721F12EE
2733DEED, 210769B3, 79AAF53E, 96081053, CC3AD1A8, 721F12EE, A625F112, 1774D326, DFE5B6B1, EC68BAC6
CC3AD1A8, F44B53A7, 210769B3, ABD4F9E6, 96081053, EC68BAC6, 5DCA4D12, A625F112, D34C985D, DFE5B6B1
96081053, 7C1E3640, F44B53A7, 1DA6CC84, ABD4F9E6, DFE5B6B1, EBC4D9C6, 5DCA4D12, 97C44A98, D34C985D
ABD4F9E6, 06B59EE8, 7C1E3640, 2D4E9FD1, 1DA6CC84, D34C985D, 095F37FD, EBC4D9C6, 29344977, 97C44A98
1DA6CC84, C422C3CD, 06B59EE8, 78D901F0, 2D4E9FD1, 97C44A98, 5BBEE487, 095F37FD, 13671BAF, 29344977
2D4E9FD1, AD864025, C422C3CD, D67BA01A, 78D901F0, 29344977, BF5B2529, 5BBEE487, 7CDFF425, 13671BAF
78D901F0, 29A83BB5, AD864025, 8B0F3710, D67BA01A, 13671BAF, FB5747C5, BF5B2529, FB921D6E, 7CDFF425
D67BA01A, 626E3910, 29A83BB5, 190096B6, 8B0F3710, 7CDFF425, DD935A5F, FB5747C5, 6C94A6FD, FB921D6E
8B0F3710, A719D8BC, 626E3910, A0EED4A6, 190096B6, FB921D6E, 27754F3A, DD935A5F, 5D1F17ED, 6C94A6FD
190096B6, BA84C782, A719D8BC, B8E44189, A0EED4A6, 6C94A6FD, 4F5CA4A5, 27754F3A, 4D697F76, 5D1F17ED
A0EED4A6, 9F6887A9, BA84C782, 6762F29C, B8E44189, 5D1F17ED, 325AFE7E, 4F5CA4A5, D53CE89D, 4D697F76
B8E44189, 3A88288C, 9F6887A9, 131E0AEA, 6762F29C, 4D697F76, 86AFE021, 325AFE7E, 7292953D, D53CE89D
6762F29C, AB23F78F, 3A88288C, A21EA67D, 131E0AEA, D53CE89D, C97F9EA1, 86AFE021, 6BF9F8C9, 7292953D
131E0AEA, 7299044A, AB23F78F, 20A230EA, A21EA67D, 7292953D, 9F60751C, C97F9EA1, BF80861A, 6BF9F8C9
A21EA67D, 6A3F10CF, 7299044A, 8FDE3EAC, 20A230EA, 6BF9F8C9, 1E9CE713, 9F60751C, FE7A8725, BF80861A

```
20A230EA, 1A1B904D, 6A3F10CF, 641129CA, 8FDE3EAC, BF80861A, C13F038A, 1E9CE713, 81D4727D, FE7A8725
8FDE3EAC, 0B2CDC01, 1A1B904D, FC433DA8, 641129CA, FE7A8725, BF627814, C13F038A, 739C4C7A, 81D4727D
641129CA, D563BFDC, 0B2CDC01, 6E413468, FC433DA8, 81D4727D, 5FCCBADE, BF627814, FC0E2B04, 739C4C7A
```

The hash-code is the following 160-bit string.

```
8E B2 08 F7 E0 5D 98 7A 9B 04 4A 8E 98 C6 B0 87 F1 5A 0B FC
```

B.2.4 Example 4

In this example, the data string is the 14-byte string consisting of the ASCII-coded version of

```
"message digest"
```

The hash-code is the following 160-bit string.

```
5D 06 89 EF 49 D2 FA E5 72 B8 81 B1 23 A8 5F FA 21 59 5F 36
```

B.2.5 Example 5

In this example, the data string is the 26-byte string consisting of the ASCII-coded version of

```
"abcdefghijklmnopqrstuvwxyz"
```

The hash-code is the following 160-bit string.

```
F7 1C 27 10 9C 69 2C 1B 56 BB DC EB 5B 9D 28 65 B3 70 8D BC
```

B.2.6 Example 6

In this example, the data string is the 62-byte string consisting of the ASCII-coded version of

```
"ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz0123456789"
```

The hash-code is the following 160-bit string.

```
B0 E2 0B 6E 31 16 64 02 86 ED 3A 87 A5 71 30 79 B2 1F 51 89
```

B.2.7 Example 7

In this example, the data string is the 80-byte string consisting of the ASCII-coded version of eight repetitions of

```
"1234567890"
```

The hash-code is the following 160-bit string.

```
9B 75 2E 45 57 3D 4B 39 F4 DB D3 32 3C AB 82 BF 63 32 6B FB
```

B.2.8 Example 8

In this example, the data string is the 56-byte string consisting of the ASCII-coded version of

```
"abcdbcdecdefdefgefghfghighijhijkijkljklmklmnlmnomnopnopq"
```

After the padding process, the two 16-word blocks derived from the data string are as follows.

```
64636261  65646362  66656463  67666564  68676665  69686766  6A696867  6B6A6968
6C6B6A69  6D6C6B6A  6E6D6C6B  6F6E6D6C  706F6E6D  71706F6E  00000080  00000000

00000000  00000000  00000000  00000000  00000000  00000000  00000000  00000000
00000000  00000000  00000000  00000000  00000000  00000000  000001C0  00000000
```

The following are (hexadecimal representations of) the successive values of the variables X_0, X_1, X_2, X_3, X_4, X'_0, X'_1, X'_2, X'_3 and X'_4, obtained during the processing of the first block.

```
67452301, EFCDAB89, 98BADCFE, 10325476, C3D2E1F0, 67452301, EFCDAB89, 98BADCFE, 10325476, C3D2E1F0
C3D2E1F0, 3115FB87, EFCDAB89, EB73FA62, 10325476, C3D2E1F0, 463DA521, EFCDAB89, EB73FA62, 10325476
10325476, CC21EC2E, 3115FB87, 36AE27BF, EB73FA62, 10325476, DB247A12, 463DA521, 36AE27BF, EB73FA62
EB73FA62, DFEB9B7A, CC21EC2E, 57EE1CC4, 36AE27BF, EB73FA62, 1D166A23, DB247A12, F6948518, 36AE27BF
36AE27BF, 2363912E, DFEB9B7A, 87B0BB30, 57EE1CC4, 36AE27BF, CE7A12F6, 1D166A23, 91E84B6C, F6948518
57EE1CC4, A1B60DC7, 2363912E, AE6DEB7F, 87B0BB30, F6948518, 57FF19DD, CE7A12F6, 59A88C74, 91E84B6C
87B0BB30, 96AC7C1E, A1B60DC7, 8E44B88D, AE6DEB7F, 91E84B6C, 01A9FEFA, 57FF19DD, E84BDB39, 59A88C74
AE6DEB7F, 6AE46154, 96AC7C1E, D8371E86, 8E44B88D, 59A88C74, 5D9A609C, 01A9FEFA, FC67755F, E84BDB39
8E44B88D, 3CF61F09, 6AE46154, B1F07A5A, D8371E86, E84BDB39, 030F7FE7, 5D9A609C, A7FBE806, FC67755F
D8371E86, 696F0D9A, 3CF61F09, 918551AB, B1F07A5A, FC67755F, 7456C8E3, 030F7FE7, 69827176, A7FBE806
B1F07A5A, AB957B91, 696F0D9A, D87C24F3, 918551AB, A7FBE806, F64C4453, 7456C8E3, 3DFF9C0C, 69827176
918551AB, 9FF4A064, AB957B91, BC3669A5, D87C24F3, 69827176, 22A5FE6E, F64C4453, 5B238DD1, 3DFF9C0C
D87C24F3, 912FE998, 9FF4A064, 55EE46AE, BC3669A5, 3DFF9C0C, 8D7E53E4, 22A5FE6E, 31114FD9, 5B238DD1
BC3669A5, C45F164E, 912FE998, D281927F, 55EE46AE, 5B238DD1, 695B23B7, 8D7E53E4, 97F9B88A, 31114FD9
55EE46AE, 2211A508, C45F164E, BFA66244, D281927F, 31114FD9, 6FAA776F, 695B23B7, F94F9235, 97F9B88A
D281927F, 80B1F3DE, 2211A508, 7C593B11, BFA66244, 97F9B88A, 4D94F720, 6FAA776F, 6C8EDDA5, F94F9235
BFA66244, 3AA6A8F5, 80B1F3DE, 46942088, 7C593B11, F94F9235, D81C6137, 4D94F720, A9DDBDBE, 6C8EDDA5
7C593B11, 9E4C4BF6, 3AA6A8F5, C7CF7A02, 46942088, 6C8EDDA5, B2ECCABD, D81C6137, 53DC8136, A9DDBDBE
46942088, F929216E, 9E4C4BF6, 9AA3D4EA, C7CF7A02, A9DDBDBE, A96B1820, B2ECCABD, 7184DF60, 53DC8136
C7CF7A02, D9AEEFAF, F929216E, 312FDA79, 9AA3D4EA, 53DC8136, 5A5E09B3, A96B1820, B32AF6CB, 7184DF60
9AA3D4EA, 8BB34505, D9AEEFAF, A485BBE4, 312FDA79, 7184DF60, 616711FA, 5A5E09B3, AC6082A5, B32AF6CB
312FDA79, 07067302, 8BB34505, BBBEBF66, A485BBE4, B32AF6CB, F4F47116, 616711FA, 7826CD69, AC6082A5
A485BBE4, 51997747, 07067302, CD14162E, BBBEBF66, AC6082A5, FAE97297, F4F47116, 9C47E985, 7826CD69
BBBEBF66, C213132C, 51997747, 19CC081C, CD14162E, 7826CD69, 887E5A3F, FAE97297, D1C45BD3, 9C47E985
CD14162E, 29D001F0, C213132C, 65DD1D46, 19CC081C, 9C47E985, 187068EF, 887E5A3F, A5CA5FEB, D1C45BD3
19CC081C, 2B59B58A, 29D001F0, 4C4CB308, 65DD1D46, D1C45BD3, 56C66FD3, 187068EF, F968FE21, A5CA5FEB
65DD1D46, C45681A6, 2B59B58A, 4007C0A7, 4C4CB308, A5CA5FEB, D718432A, 56C66FD3, C1A3BC61, F968FE21
4C4CB308, 2E32CA16, C45681A6, 66D628AD, 4007C0A7, F968FE21, 775BA27D, D718432A, 19BF4D5B, C1A3BC61
4007C0A7, 5C712D51, 2E32CA16, 5A069B11, 66D628AD, C1A3BC61, 6243D22F, 775BA27D, 610CAB5C, 19BF4D5B
66D628AD, 989BC126, 5C712D51, CB2858B8, 5A069B11, 19BF4D5B, 44DCD35A, 6243D22F, 6E89F5DD, 610CAB5C
5A069B11, 9EE4CA1F, 989BC126, C4B54571, CB2858B8, 610CAB5C, 8FBE3F7E, 44DCD35A, 0F48BD89, 6E89F5DD
CB2858B8, F417F849, 9EE4CA1F, 6F049A62, C4B54571, 6E89F5DD, DA718428, 8FBE3F7E, 734D6913, 0F48BD89
C4B54571, 75239882, F417F849, 93287E7B, 6F049A62, 0F48BD89, 91573E0A, DA718428, F8FDFA3E, 734D6913
6F049A62, 3AC6B69F, 75239882, 5FE127D0, 93287E7B, 734D6913, 2A5224A6, 91573E0A, C610A369, F8FDFA3E
93287E7B, 0B7C24AC, 3AC6B69F, 8E6209D4, 5FE127D0, F8FDFA3E, 8128FFB7, 2A5224A6, 5CF82A45, C610A369
5FE127D0, 2854DCE0, 0B7C24AC, 1ADA7CEB, 8E6209D4, C610A369, FF374DFD, 8128FFB7, 489298A9, 5CF82A45
8E6209D4, 267080E2, 2854DCE0, F092B02D, 1ADA7CEB, 5CF82A45, C5E0CCD7, FF374DFD, A3FEDE04, 489298A9
1ADA7CEB, 7806D96F, 267080E2, 537380A1, F092B02D, 489298A9, 31860C44, C5E0CCD7, DD37F7FC, A3FEDE04
F092B02D, 52638496, 7806D96F, C2038899, 537380A1, A3FEDE04, CEE7092B, 31860C44, 83335F17, DD37F7FC
537380A1, 59FC5CDB, 52638496, 1B65BDE0, C2038899, DD37F7FC, 46827AAE, CEE7092B, 183110C6, 83335F17
C2038899, 8AE30FBE, 59FC5CDB, 8E125949, 1B65BDE0, 83335F17, A757A907, 46827AAE, 9C24AF3B, 183110C6
1B65BDE0, 4F4AEBED, 8AE30FBE, F1736D67, 8E125949, 183110C6, E90F38FC, A757A907, 09EAB91A, 9C24AF3B
8E125949, 65BBCCCC, 4F4AEBED, 8C3EFA2B, F1736D67, 9C24AF3B, EC65CB85, E90F38FC, 5EA41E9D, 09EAB91A
F1736D67, 0B3B88C1, 65BBCCCC, 2BAFB53D, 8C3EFA2B, 09EAB91A, 54B06FBD, EC65CB85, 3CE3F3A4, 5EA41E9D
8C3EFA2B, 6DF30989, 0B3B88C1, EF333196, 2BAFB53D, 5EA41E9D, D8D6F0E3, 54B06FBD, 972E17B1, 3CE3F3A4
2BAFB53D, 156421AC, 6DF30989, EE23042C, EF333196, 3CE3F3A4, B30DA892, D8D6F0E3, C1BEF552, 972E17B1
EF333196, 6F54F9CA, 156421AC, CC2625B7, EE23042C, 972E17B1, F526A85A, B30DA892, 5BC38F63, C1BEF552
EE23042C, A5D28921, 6F54F9CA, 9086B055, CC2625B7, C1BEF552, 5F5587DB, F526A85A, 36A24ACC, 5BC38F63
CC2625B7, 2959D915, A5D28921, 53E729BD, 9086B055, 5BC38F63, 9FABAC24, 5F5587DB, 9AA16BD4, 36A24ACC
9086B055, 4EFF0384, 2959D915, 4A248697, 53E729BD, 36A24ACC, 52E4FB9B, 9FABAC24, 561F6D7D, 9AA16BD4
53E729BD, 17292945, 4EFF0384, 676454A5, 4A248697, 9AA16BD4, E13C3BDA, 52E4FB9B, AEB0927E, 561F6D7D
4A248697, 5FE71F22, 17292945, FC0E113B, 676454A5, 561F6D7D, 71244E49, E13C3BDA, 93EE6D4B, AEB0927E
676454A5, DC06A80F, 5FE71F22, A4A5145C, FC0E113B, AEB0927E, AA49234C, 71244E49, F0EF6B84, 93EE6D4B
FC0E113B, 5BD21FC5, DC06A80F, 9C7C897F, A4A5145C, 93EE6D4B, 42532D95, AA49234C, 913925C4, F0EF6B84
A4A5145C, 5587BC4F, 5BD21FC5, 1AA03F70, 9C7C897F, F0EF6B84, CDA86FD0, 42532D95, 248D32A9, 913925C4
```

```
9C7C897F, A1755F6B, 5587BC4F, 487F156F, 1AA03F70, 913925C4, 69C12F76, CDA86FD0, 4CB65509, 248D32A9
1AA03F70, 100A6B19, A1755F6B, 1EF13D56, 487F156F, 248D32A9, 44272219, 69C12F76, A1BF4336, 4CB65509
487F156F, AA2CFD07, 100A6B19, D57DAE85, 1EF13D56, 4CB65509, CBD360C3, 44272219, 04BDD9A7, A1BF4336
1EF13D56, 28246D22, AA2CFD07, 29AC6440, D57DAE85, A1BF4336, 27A64C2D, CBD360C3, 9C886510, 04BDD9A7
D57DAE85, 4909C2BD, 28246D22, B3F41EA8, 29AC6440, 04BDD9A7, CCB70B88, 27A64C2D, 4D830F2F, 9C886510
29AC6440, 9020271B, 4909C2BD, 91B488A0, B3F41EA8, 9C886510, 2020C0FC, CCB70B88, 9930B49E, 4D830F2F
B3F41EA8, A557D838, 9020271B, 270AF524, 91B488A0, 4D830F2F, 7541E108, 2020C0FC, DC2E2332, 9930B49E
91B488A0, F879D1F8, A557D838, 809C6E40, 270AF524, 9930B49E, 0A66EBF9, 7541E108, 8303F080, DC2E2332
270AF524, 39BAC08A, F879D1F8, 5F60E295, 809C6E40, DC2E2332, A0AB24D8, 0A66EBF9, 078421D5, 8303F080
809C6E40, DF212B9C, 39BAC08A, E747E3E1, 5F60E295, 8303F080, 44C068DD, A0AB24D8, 9BAFE429, 078421D5
5F60E295, 46F2CD86, DF212B9C, EB0228E6, E747E3E1, 078421D5, 3F8B3B48, 44C068DD, AC936282, 9BAFE429
E747E3E1, A17766F4, 46F2CD86, 84AE737C, EB0228E6, 9BAFE429, 873A41C4, 3F8B3B48, 01A37513, AC936282
EB0228E6, FC20AA01, A17766F4, CB36191B, 84AE737C, AC936282, A2969EB4, 873A41C4, 2CED20FE, 01A37513
84AE737C, 93A30DD9, FC20AA01, DD9BD285, CB36191B, 01A37513, 7B345F4F, A2969EB4, E907121C, 2CED20FE
CB36191B, 98554E1C, 93A30DD9, 82A807F0, DD9BD285, 2CED20FE, 07B2EA78, 7B345F4F, 5A7AD28A, E907121C
DD9BD285, 79D46BD1, 98554E1C, 8C37664E, 82A807F0, E907121C, 93451653, 07B2EA78, D17D3DEC, 5A7AD28A
82A807F0, 5FBC55DB, 79D46BD1, 55387261, 8C37664E, 5A7AD28A, AA0DF949, 93451653, CBA9E01E, D17D3DEC
8C37664E, DEF23A3B, 5FBC55DB, 51AF45E7, 55387261, D17D3DEC, 030FFB9A, AA0DF949, 14594E4D, CBA9E01E
55387261, 287DB1EB, DEF23A3B, F1576D7E, 51AF45E7, CBA9E01E, 0D9CD217, 030FFB9A, 37E526A8, 14594E4D
51AF45E7, CF955B8E, 287DB1EB, C8E8EF7B, F1576D7E, 14594E4D, BECE1BBD, 0D9CD217, 3FEE680C, 37E526A8
F1576D7E, 83B6B7E8, CF955B8E, F6C7ACA1, C8E8EF7B, 37E526A8, D97CFEEC, BECE1BBD, 73485C36, 3FEE680C
C8E8EF7B, 7943C443, 83B6B7E8, 556E3B3E, F6C7ACA1, 3FEE680C, DBEA79F5, D97CFEEC, 386EF6FB, 73485C36
F6C7ACA1, F336AA45, 7943C443, DADFA20E, 556E3B3E, 73485C36, 91704BDB, DBEA79F5, F3FBB365, 386EF6FB
556E3B3E, 2FF847D6, F336AA45, 0F110DE5, DADFA20E, 386EF6FB, 40CBA97D, 91704BDB, A9E7D76F, F3FBB365
DADFA20E, 33FE64C9, 2FF847D6, DAA917CC, 0F110DE5, F3FBB365, B0BD2456, 40CBA97D, C12F6E45, A9E7D76F
0F110DE5, 78378FE9, 33FE64C9, E11F58BF, DAA917CC, A9E7D76F, CA09D415, B0BD2456, 2EA5F503, C12F6E45
```

The following are (hexadecimal representations of) the successive values of the variables X_0, X_1, X_2, X_3, X_4, X'_0, X'_1, X'_2, X'_3 and X'_4, obtained during the processing of the second block.

```
52720555, 3B09A402, 94C343B1, 9CEDC3EA, 9039D740, 52720555, 3B09A402, 94C343B1, 9CEDC3EA, 9039D740
9039D740, 59874B6C, 3B09A402, 0D0EC653, 9CEDC3EA, 9039D740, 7FA6C9AF, 3B09A402, 0D0EC653, 9CEDC3EA
9CEDC3EA, 1D0D43D8, 59874B6C, 269008EC, 0D0EC653, 9CEDC3EA, 149F92B4, 7FA6C9AF, 269008EC, 0D0EC653
0D0EC653, EF3045D6, 1D0D43D8, 1D2DB166, 269008EC, 0D0EC653, 0E887E05, 149F92B4, 9B26BDFE, 269008EC
269008EC, 1E6BC8AD, EF3045D6, 350F6074, 1D2DB166, 269008EC, 6E8757AC, 0E887E05, 7E4AD052, 9B26BDFE
1D2DB166, 79CC70E3, 1E6BC8AD, C1175BBC, 350F6074, 9B26BDFE, 32C1290B, 6E8757AC, 21F8143A, 7E4AD052
350F6074, 13A4B937, 79CC70E3, AF22B479, C1175BBC, 7E4AD052, 8EB02C5A, 32C1290B, 1D5EB1BA, 21F8143A
C1175BBC, EE066CB9, 13A4B937, 31C38DE7, AF22B479, 21F8143A, 719EB9D9, 8EB02C5A, 04A42CCB, 1D5EB1BA
AF22B479, A08AFF93, EE066CB9, 92E4DC4E, 31C38DE7, 1D5EB1BA, 3D5B8A9A, 719EB9D9, C0B16A3A, 04A42CCB
31C38DE7, 89E27A43, A08AFF93, 19B2E7B8, 92E4DC4E, 04A42CCB, 47DEA0A3, 3D5B8A9A, 7AE765C6, C0B16A3A
92E4DC4E, 50EEC8A1, 89E27A43, 2BFE4E82, 19B2E7B8, C0B16A3A, A6AACEE1, 47DEA0A3, 6E2A68F5, 7AE765C6
19B2E7B8, 0FDE892D, 50EEC8A1, 89E90E27, 2BFE4E82, 7AE765C6, 4456D048, A6AACEE1, 7A828D1F, 6E2A68F5
2BFE4E82, 47B046C8, 0FDE892D, BB228543, 89E90E27, 6E2A68F5, 072D166E, 4456D048, AB3B869A, 7A828D1F
89E90E27, 5C8F582E, 47B046C8, 7A24B43F, BB228543, 7A828D1F, B37A11D1, 072D166E, 5B412111, AB3B869A
BB228543, 3D7F05B8, 5C8F582E, C11B211E, 7A24B43F, AB3B869A, 654CBE94, B37A11D1, B459B81C, 5B412111
7A24B43F, 962BCAF7, 3D7F05B8, 3D60B972, C11B211E, 5B412111, 6AFF9ABA, 654CBE94, E84746CD, B459B81C
C11B211E, 1A459D2E, 962BCAF7, FC16E0F5, 3D60B972, B459B81C, EE0E390E, 6AFF9ABA, 32FA5195, E84746CD
3D60B972, 1622907A, 1A459D2E, AF2BDE58, FC16E0F5, E84746CD, 569023C2, EE0E390E, FE6AE9AB, 32FA5195
FC16E0F5, B75B2E49, 1622907A, 1674B869, AF2BDE58, 32FA5195, 5C2944E8, 569023C2, 38E43BB8, FE6AE9AB
AF2BDE58, 6F16D4C4, B75B2E49, 8A41E858, 1674B869, FE6AE9AB, 103CE067, 5C2944E8, 408F095A, 38E43BB8
1674B869, 46FDEE89, 6F16D4C4, 6CB926DD, 8A41E858, 38E43BB8, AB641473, 103CE067, A513A170, 408F095A
8A41E858, E9F89F50, 46FDEE89, 5B5311BC, 6CB926DD, 408F095A, 25643DBF, AB641473, F3819C40, A513A170
6CB926DD, EC9A614C, E9F89F50, F7BA251B, 5B5311BC, A513A170, E60A5336, 25643DBF, 9051CEAD, F3819C40
5B5311BC, D525F69D, EC9A614C, E27D43A7, F7BA251B, F3819C40, FF4D318D, E60A5336, 90F6FC95, 9051CEAD
F7BA251B, EDFBF331, D525F69D, 698533B2, E27D43A7, 9051CEAD, 6D5A28DD, FF4D318D, 294CDB98, 90F6FC95
E27D43A7, 93C5E732, EDFBF331, 97DA7754, 698533B2, 90F6FC95, 855C140A, 6D5A28DD, 34C637FD, 294CDB98
698533B2, 24907FDF, 93C5E732, EFCCC7B7, 97DA7754, 294CDB98, 79C1BC35, 855C140A, 68A375B5, 34C637FD
97DA7754, E2193F3E, 24907FDF, 179CCA4F, EFCCC7B7, 34C637FD, B2D5EF34, 79C1BC35, 70502A15, 68A375B5
EFCCC7B7, D3AD6006, E2193F3E, 41FF7C92, 179CCA4F, 68A375B5, DB87209A, B2D5EF34, 06F0D5E7, 70502A15
179CCA4F, 6B8BFAB4, D3AD6006, 64FCFB88, 41FF7C92, 70502A15, 4DEC84F2, DB87209A, 57BCD2CB, 06F0D5E7
41FF7C92, 5052D6EF, 6B8BFAB4, B5801B4E, 64FCFB88, 06F0D5E7, D4F6A30D, 4DEC84F2, 1C826B6E, 57BCD2CB
64FCFB88, FF36EBC8, 5052D6EF, 2FEAD1AE, B5801B4E, 57BCD2CB, 0191C9F0, D4F6A30D, B213C937, 1C826B6E
B5801B4E, 5A010C53, FF36EBC8, 4B5BBD41, 2FEAD1AE, 1C826B6E, 20FBAB36, 0191C9F0, DA8C3753, B213C937
2FEAD1AE, 952BFB5D, 5A010C53, DBAF23FC, 4B5BBD41, B213C937, 7E796493, 20FBAB36, 4727C006, DA8C3753
4B5BBD41, FE05BEE3, 952BFB5D, 04314D68, DBAF23FC, DA8C3753, C9EABB3E, 7E796493, EEACD883, 4727C006
DBAF23FC, 2256AF69, FE05BEE3, AFED7654, 04314D68, 4727C006, B44977A5, C9EABB3E, E5924DF9, EEACD883
04314D68, 5285B0D3, 2256AF69, 16FB8FF8, AFED7654, EEACD883, 287580C6, B44977A5, AAECFB27, E5924DF9
AFED7654, 1DFB856C, 5285B0D3, 5ABDA489, 16FB8FF8, E5924DF9, 1E1DBD16, 287580C6, 25DE96D1, AAECFB27
16FB8FF8, 32974404, 1DFB856C, 16C34D4A, 5ABDA489, AAECFB27, FBEB21BA, 1E1DBD16, D60318A1, 25DE96D1
```

```
5ABDA489, 90AC71CE, 32974404, EE15B077, 16C34D4A, 25DE96D1, B74BF3E2, FBEB21BA, 76F45878, D60318A1
16C34D4A, 849CCC12, 90AC71CE, 5D1010CA, EE15B077, D60318A1, 755BEDDF, B74BF3E2, AC86EBEF, 76F45878
EE15B077, 340EBE92, 849CCC12, B1C73A42, 5D1010CA, 76F45878, 3CD099C6, 755BEDDF, 2FCF8ADD, AC86EBEF
5D1010CA, F531E5F5, 340EBE92, 73304A12, B1C73A42, AC86EBEF, A19BBAA2, 3CD099C6, 6FB77DD5, 2FCF8ADD
B1C73A42, 27528557, F531E5F5, 3AFA48D0, 73304A12, 2FCF8ADD, EFC554F1, A19BBAA2, 426718F3, 6FB77DD5
73304A12, E4AFA69F, 27528557, C797D7D4, 3AFA48D0, 6FB77DD5, F56F1485, EFC554F1, 6EEA8A86, 426718F3
3AFA48D0, E3462C93, E4AFA69F, 4A155C9D, C797D7D4, 426718F3, E0A1480A, F56F1485, 1553C7BF, 6EEA8A86
C797D7D4, 3CF5CD85, E3462C93, BE9A7F92, 4A155C9D, 6EEA8A86, 9F80007D, E0A1480A, BC5217D5, 1553C7BF
4A155C9D, B6C756F9, 3CF5CD85, 18B24F8D, BE9A7F92, 1553C7BF, 090898BE, 9F80007D, 85202B82, BC5217D5
BE9A7F92, CC2AB627, B6C756F9, D73614F3, 18B24F8D, BC5217D5, A0CD75A2, 090898BE, 0001F67E, 85202B82
18B24F8D, E5471921, CC2AB627, 1D5BE6DB, D73614F3, 85202B82, 95FE46E6, A0CD75A2, 2262F824, 0001F67E
D73614F3, E8FEFBC6, E5471921, AAD89F30, 1D5BE6DB, 0001F67E, 4B55D832, 95FE46E6, 35D68A83, 2262F824
1D5BE6DB, 788FFBE7, E8FEFBC6, 1C648795, AAD89F30, 2262F824, 681302D4, 4B55D832, F91B9A57, 35D68A83
AAD89F30, FA97F1BB, 788FFBE7, FBEF1BA3, 1C648795, 35D68A83, 860F8E32, 681302D4, 5760C92D, F91B9A57
1C648795, 2FE154B4, FA97F1BB, 3FEF9DE2, FBEF1BA3, F91B9A57, CA3DDAC0, 860F8E32, 4C0B51A0, 5760C92D
FBEF1BA3, D884695B, 2FE154B4, 5FC6EFEA, 3FEF9DE2, 5760C92D, 7E790793, CA3DDAC0, 3E38CA18, 4C0B51A0
3FEF9DE2, A09357E9, D884695B, 8552D0BF, 5FC6EFEA, 4C0B51A0, 4E0DF927, 7E790793, F76B0328, 3E38CA18
5FC6EFEA, 019B9791, A09357E9, 11A56F62, 8552D0BF, 3E38CA18, 311DFB90, 4E0DF927, E41E4DF9, F76B0328
8552D0BF, 70DB6FDF, 019B9791, 4D5FA682, 11A56F62, F76B0328, 24FA9DC7, 311DFB90, 37E49D38, E41E4DF9
11A56F62, 82F104B4, 70DB6FDF, 6E5E4406, 4D5FA682, E41E4DF9, CE45E142, 24FA9DC7, 77EE40C4, 37E49D38
4D5FA682, BFAB29F8, 82F104B4, 6DBF7DC3, 6E5E4406, 37E49D38, 9C4F267F, CE45E142, EA771C93, 77EE40C4
6E5E4406, 880198A9, BFAB29F8, C412D20B, 6DBF7DC3, 77EE40C4, 06880805, 9C4F267F, 17850B39, EA771C93
6DBF7DC3, 917C197C, 880198A9, ACA7E2FE, C412D20B, EA771C93, 7625BD09, 06880805, 3C99FE71, 17850B39
C412D20B, 03E7992A, 917C197C, 0662A620, ACA7E2FE, 17850B39, 8720C8E7, 7625BD09, 2020141A, 3C99FE71
ACA7E2FE, 824CEF7A, 03E7992A, F065F245, 0662A620, 3C99FE71, CBB7DA7A, 8720C8E7, 96F425D8, 2020141A
0662A620, AF16F218, 824CEF7A, 9E64A80F, F065F245, 2020141A, 88851068, CBB7DA7A, 83239E1C, 96F425D8
F065F245, EFC8943D, AF16F218, 33BDEA09, 9E64A80F, 96F425D8, C85C4EB8, 88851068, DF69EB2E, 83239E1C
9E64A80F, C80FF53B, EFC8943D, 5BC862BC, 33BDEA09, 83239E1C, 57BF18E2, C85C4EB8, 1441A222, DF69EB2E
33BDEA09, 28DF9E36, C80FF53B, 2250F7BF, 5BC862BC, DF69EB2E, 48932C1A, 57BF18E2, 713AE321, 1441A222
5BC862BC, 6E1D8950, 28DF9E36, 3FD4EF20, 2250F7BF, 1441A222, 15C7B0BD, 48932C1A, FC63895E, 713AE321
2250F7BF, 21EEE621, 6E1D8950, 7E78D8A3, 3FD4EF20, 713AE321, FCBC9E78, 15C7B0BD, 4CB06922, FC63895E
3FD4EF20, 561379BA, 21EEE621, 762541B8, 7E78D8A3, FC63895E, DD28EA60, FCBC9E78, 1EC2F457, 4CB06922
7E78D8A3, 4D0255C5, 561379BA, BB988487, 762541B8, 4CB06922, CF1BB810, DD28EA60, F279E3F2, 1EC2F457
762541B8, 966845EC, 4D0255C5, 4DE6E958, BB988487, 1EC2F457, 5D899D62, CF1BB810, A3A98374, F279E3F2
BB988487, D922DEB8, 966845EC, 09571534, 4DE6E958, F279E3F2, F1144141, 5D899D62, 6EE0433C, A3A98374
4DE6E958, B919B2A3, D922DEB8, A117B259, 09571534, A3A98374, 940BBA12, F1144141, 26758976, 6EE0433C
09571534, D3CF80F9, B919B2A3, 8B7AE364, A117B259, 6EE0433C, 33DDA9B5, 940BBA12, 510507C4, 26758976
A117B259, F548EA98, D3CF80F9, 66CA8EE4, 8B7AE364, 26758976, DCE0B562, 33DDA9B5, 2EE84A50, 510507C4
8B7AE364, A1D3372D, F548EA98, 3E03E74F, 66CA8EE4, 510507C4, C103FBE9, DCE0B562, 76A6D4CF, 2EE84A50
66CA8EE4, 6578D66C, A1D3372D, 23AA63D5, 3E03E74F, 2EE84A50, 832961D9, C103FBE9, 82D58B73, 76A6D4CF
3E03E74F, 57C29604, 6578D66C, 4CDCB687, 23AA63D5, 76A6D4CF, B183744E, 832961D9, 0FEFA704, 82D58B73
23AA63D5, 27F5E937, 57C29604, E359B195, 4CDCB687, 82D58B73, E710A112, B183744E, A587660C, 0FEFA704
```

The hash-code is the following 160-bit string.

```
12 A0 53 38 4A 9C 0C 88 E4 05 A0 6C 27 DC F4 9A DA 62 EB 2B
```

B.2.9 Example 9

In this example, the data string is the 1 000 000-byte string consisting of the ASCII-coded version of "a" repeated 10^6 times.

The hash-code is the following 160-bit string.

```
52 78 32 43 C1 69 7B DB E1 6D 37 F9 7F 68 F0 83 25 DC 15 28
```

B.2.10 Example 10

In this example, the data string is the 112-byte string consisting of the ASCII-coded version of

```
"abcdefghbcdefghicdefghijdefghijkefghijklfghijklmghijklmn
hijklmnoijklmnopjklmnopqklmnopqrlmnopqrsmnopqrstnopqrstu"
```

(with no line break after the first n).

The hash-code is the following 160-bit string.

```
6f 3f a3 9b 6b 50 3c 38 4f 91 9a 49 a7 aa 5c 2c 08 bd fb 45
```

B.2.11 Example 11

In this example, the data string is the 32-byte string consisting of the ASCII-coded version of

"abcdbcdecdefdefgefghfghighijhijk"

The hash-code is the following 160-bit string.

94 c2 64 11 54 04 e6 33 79 0d fc c8 7b 58 7d 36 77 06 7d 9f

B.3 Dedicated Hash-Function 2 (RIPEMD-128)

B.3.1 Example 1

In this example, the data string is the empty string, i.e., the string of length zero.

The hash-code is the following 128-bit string.

CD F2 62 13 A1 50 DC 3E CB 61 0F 18 F6 B3 8B 46

B.3.2 Example 2

In this example, the data string consists of a single byte, namely the ASCII-coded version of the letter "a".

The hash-code is the following 128-bit string.

86 BE 7A FA 33 9D 0F C7 CF C7 85 E7 2F 57 8D 33

B.3.3 Example 3

In this example, the data string is the 3-byte string consisting of the ASCII-coded version of "abc". This is equivalent to the bit string "01100001 01100010 01100011".

After the padding process, the single 16-word block derived from the data string is as follows.

```
80636261  00000000  00000000  00000000  00000000  00000000  00000000  00000000
00000000  00000000  00000000  00000000  00000000  00000000  00000018  00000000
```

The following are (hexadecimal representations of) the successive values of the variables X_0, X_1, X_2, X_3, X'_0, X'_1, X'_2 and X'_3.

```
67452301, EFCDAB89, 98BADCFE, 10325476, 67452301, EFCDAB89, 98BADCFE, 10325476
10325476, 6D431A77, EFCDAB89, 98BADCFE, 10325476, 70376F40, EFCDAB89, 98BADCFE
98BADCFE, B05D8A99, 6D431A77, EFCDAB89, 98BADCFE, 989F6BB0, 70376F40, EFCDAB89
EFCDAB89, 0C32E5C7, B05D8A99, 6D431A77, EFCDAB89, 39B14904, 989F6BB0, 70376F40
6D431A77, A20B2C0F, 0C32E5C7, B05D8A99, 70376F40, 671C03CC, 39B14904, 989F6BB0
B05D8A99, 74EBB911, A20B2C0F, 0C32E5C7, 989F6BB0, BFD55C42, 671C03CC, 39B14904
0C32E5C7, 2FFB728B, 74EBB911, A20B2C0F, 39B14904, A12F346F, BFD55C42, 671C03CC
A20B2C0F, A766AE02, 2FFB728B, 74EBB911, 671C03CC, 989C2210, A12F346F, BFD55C42
74EBB911, 03234F3D, A766AE02, 2FFB728B, BFD55C42, 0F95FBEA, 989C2210, A12F346F
2FFB728B, 52662805, 03234F3D, A766AE02, A12F346F, 068D5115, 0F95FBEA, 989C2210
A766AE02, E778A4C3, 52662805, 03234F3D, 989C2210, AFCD27FC, 068D5115, 0F95FBEA
03234F3D, 1C7F5769, E778A4C3, 52662805, 0F95FBEA, CBD1F3F8, AFCD27FC, 068D5115
52662805, 95765642, 1C7F5769, E778A4C3, 068D5115, CFFE405F, CBD1F3F8, AFCD27FC
E778A4C3, 35F37B70, 95765642, 1C7F5769, AFCD27FC, 2B55C9C3, CFFE405F, CBD1F3F8
1C7F5769, 398F8F52, 35F37B70, 95765642, CBD1F3F8, DD6A43FB, 2B55C9C3, CFFE405F
95765642, 13F3C36B, 398F8F52, 35F37B70, CFFE405F, 049B909E, DD6A43FB, 2B55C9C3
35F37B70, 058D8BB5, 13F3C36B, 398F8F52, 2B55C9C3, 3713BFFD, 049B909E, DD6A43FB
398F8F52, FCBE3664, 058D8BB5, 13F3C36B, DD6A43FB, 82ADDB53, 3713BFFD, 049B909E
13F3C36B, F7F306A6, FCBE3664, 058D8BB5, 049B909E, CC1D8105, 82ADDB53, 3713BFFD
058D8BB5, 34CC3963, F7F306A6, FCBE3664, 3713BFFD, BE09159A, CC1D8105, 82ADDB53
```

```
FCBE3664, 416E8BA0, 34CC3963, F7F306A6, 82ADDB53, 541AE568, BE09159A, CC1D8105
F7F306A6, EDE91870, 416E8BA0, 34CC3963, CC1D8105, 27D40F94, 541AE568, BE09159A
34CC3963, C352C547, EDE91870, 416E8BA0, BE09159A, 675C363A, 27D40F94, 541AE568
416E8BA0, 5D5EEE28, C352C547, EDE91870, 541AE568, 77F3A38B, 675C363A, 27D40F94
EDE91870, 6CC4BEF2, 5D5EEE28, C352C547, 27D40F94, 84D73C44, 77F3A38B, 675C363A
C352C547, E140970B, 6CC4BEF2, 5D5EEE28, 675C363A, D2958F37, 84D73C44, 77F3A38B
5D5EEE28, 79F631A9, E140970B, 6CC4BEF2, 77F3A38B, FC39C927, D2958F37, 84D73C44
6CC4BEF2, 038E0E91, 79F631A9, E140970B, 84D73C44, E3A5A4DE, FC39C927, D2958F37
E140970B, 1B942D52, 038E0E91, 79F631A9, D2958F37, 4BA3A889, E3A5A4DE, FC39C927
79F631A9, 496AECFD, 1B942D52, 038E0E91, FC39C927, A964BA74, 4BA3A889, E3A5A4DE
038E0E91, FE6CD56F, 496AECFD, 1B942D52, E3A5A4DE, 7AF9DBB0, A964BA74, 4BA3A889
1B942D52, 2E94F501, FE6CD56F, 496AECFD, 4BA3A889, 7DA68EA9, 7AF9DBB0, A964BA74
496AECFD, 584E8E58, 2E94F501, FE6CD56F, A964BA74, 9C7247E5, 7DA68EA9, 7AF9DBB0
FE6CD56F, 41A17EFA, 584E8E58, 2E94F501, 7AF9DBB0, 0130312B, 9C7247E5, 7DA68EA9
2E94F501, 8981C6CD, 41A17EFA, 584E8E58, 7DA68EA9, 90552232, 0130312B, 9C7247E5
584E8E58, 400A93E1, 8981C6CD, 41A17EFA, 9C7247E5, 99C1FBA4, 90552232, 0130312B
41A17EFA, 841F817F, 400A93E1, 8981C6CD, 0130312B, 9D481CD2, 99C1FBA4, 90552232
8981C6CD, 659379BE, 841F817F, 400A93E1, 90552232, F5AABE07, 9D481CD2, 99C1FBA4
400A93E1, AB3D9A70, 659379BE, 841F817F, 99C1FBA4, C3AFB7E6, F5AABE07, 9D481CD2
841F817F, D3D21DC8, AB3D9A70, 659379BE, 9D481CD2, 473E2B79, C3AFB7E6, F5AABE07
659379BE, 38C8D29D, D3D21DC8, AB3D9A70, F5AABE07, C4CAFF99, 473E2B79, C3AFB7E6
AB3D9A70, 738B9B0F, 38C8D29D, D3D21DC8, C3AFB7E6, A2879AA4, C4CAFF99, 473E2B79
D3D21DC8, 8528B83E, 738B9B0F, 38C8D29D, 473E2B79, 56565EDB, A2879AA4, C4CAFF99
38C8D29D, 7345AF18, 8528B83E, 738B9B0F, C4CAFF99, E7A4BD86, 56565EDB, A2879AA4
738B9B0F, FFCCC52B, 7345AF18, 8528B83E, A2879AA4, 974B9E10, E7A4BD86, 56565EDB
8528B83E, A77E902B, FFCCC52B, 7345AF18, 56565EDB, 96CC5AE1, 974B9E10, E7A4BD86
7345AF18, CB9C6C83, A77E902B, FFCCC52B, E7A4BD86, 57E6A772, 96CC5AE1, 974B9E10
FFCCC52B, 38A2DA83, CB9C6C83, A77E902B, 974B9E10, F10B6CF5, 57E6A772, 96CC5AE1
A77E902B, 487F9401, 38A2DA83, CB9C6C83, 96CC5AE1, 90426E6B, F10B6CF5, 57E6A772
CB9C6C83, C7184576, 487F9401, 38A2DA83, 57E6A772, 0066E6BE, 90426E6B, F10B6CF5
38A2DA83, 56D619B1, C7184576, 487F9401, F10B6CF5, 22D17257, 0066E6BE, 90426E6B
487F9401, 3A35A3C5, 56D619B1, C7184576, 90426E6B, 016777A4, 22D17257, 0066E6BE
C7184576, B5517538, 3A35A3C5, 56D619B1, 0066E6BE, 9A8DC5A0, 016777A4, 22D17257
56D619B1, 4609C4C2, B5517538, 3A35A3C5, 22D17257, A9C46E68, 9A8DC5A0, 016777A4
3A35A3C5, D5C2B699, 4609C4C2, B5517538, 016777A4, 13B0D540, A9C46E68, 9A8DC5A0
B5517538, 342AF741, D5C2B699, 4609C4C2, 9A8DC5A0, 983D8B08, 13B0D540, A9C46E68
4609C4C2, 38286DDA, 342AF741, D5C2B699, A9C46E68, 96084F4E, 983D8B08, 13B0D540
D5C2B699, 9BCEEC0A, 38286DDA, 342AF741, 13B0D540, D25FDBB1, 96084F4E, 983D8B08
342AF741, 5803DF3A, 9BCEEC0A, 38286DDA, 983D8B08, 35EA6FE0, D25FDBB1, 96084F4E
38286DDA, E1B026EB, 5803DF3A, 9BCEEC0A, 96084F4E, B862709F, 35EA6FE0, D25FDBB1
9BCEEC0A, 31587C22, E1B026EB, 5803DF3A, D25FDBB1, C02839EB, B862709F, 35EA6FE0
5803DF3A, 9B25E1DC, 31587C22, E1B026EB, 35EA6FE0, 00245200, C02839EB, B862709F
E1B026EB, 2205379E, 9B25E1DC, 31587C22, B862709F, CB116A95, 00245200, C02839EB
31587C22, 5E3334A3, 2205379E, 9B25E1DC, C02839EB, B90EE1BF, CB116A95, 00245200
9B25E1DC, 56F80FA9, 5E3334A3, 2205379E, 00245200, 64132D32, B90EE1BF, CB116A95
```

The hash-code is the following 128-bit string.

```
C1 4A 12 19 9C 66 E4 BA 84 63 6B 0F 69 14 4C 77
```

B.3.4 Example 4

In this example, the data string is the 14-byte string consisting of the ASCII-coded version of

```
"message digest"
```

The hash-code is the following 128-bit string.

```
9E 32 7B 3D 6E 52 30 62 AF C1 13 2D 7D F9 D1 B8
```

B.3.5 Example 5

In this example, the data string is the 26-byte string consisting of the ASCII-coded version of

"abcdefghijklmnopqrstuvwxyz"

The hash-code is the following 128-bit string.

FD 2A A6 07 F7 1D C8 F5 10 71 49 22 B3 71 83 4E

B.3.6 Example 6

In this example, the data string is the 62-byte string consisting of the ASCII-coded version of

"ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz0123456789"

The hash-code is the following 128-bit string.

D1 E9 59 EB 17 9C 91 1F AE A4 62 4C 60 C5 C7 02

B.3.7 Example 7

In this example, the data string is the 80-byte string consisting of the ASCII-coded version of eight repetitions of

"1234567890"

The hash-code is the following 128-bit string.

3F 45 EF 19 47 32 C2 DB B2 C4 A2 C7 69 79 5F A3

B.3.8 Example 8

In this example, the data string is the 56-byte string consisting of the ASCII-coded version of

"abcdbcdecdefdefgefghfghighijhijkijkljklmklmnlmnomnopnopq"

After the padding process, the two 16-word blocks derived from the data string are as follows.

```
64636261  65646362  66656463  67666564  68676665  69686766  6A696867  6B6A6968
6C6B6A69  6D6C6B6A  6E6D6C6B  6F6E6D6C  706F6E6D  71706F6E  00000080  00000000

00000000  00000000  00000000  00000000  00000000  00000000  00000000  00000000
00000000  00000000  00000000  00000000  00000000  00000000  000001C0  00000000
```

The following are (hexadecimal representations of) the successive values of the variables X_0, X_1, X_2, X_3, X'_0, X'_1, X'_2 and X'_3 obtained during the processing of the first block.

```
67452301, EFCDAB89, 98BADCFE, 10325476, 67452301, EFCDAB89, 98BADCFE, 10325476
10325476, 6D431997, EFCDAB89, 98BADCFE, 10325476, D89ED5A9, EFCDAB89, 98BADCFE
98BADCFE, C9AE23F2, 6D431997, EFCDAB89, 98BADCFE, 69B10AC1, D89ED5A9, EFCDAB89
EFCDAB89, 69A6A520, C9AE23F2, 6D431997, EFCDAB89, B661DB9C, 69B10AC1, D89ED5A9
6D431997, FB032247, 69A6A520, C9AE23F2, D89ED5A9, ABACC2AF, B661DB9C, 69B10AC1
C9AE23F2, 16C49226, FB032247, 69A6A520, 69B10AC1, D412CAD1, ABACC2AF, B661DB9C
69A6A520, 77A099B7, 16C49226, FB032247, B661DB9C, E2DEDF22, D412CAD1, ABACC2AF
FB032247, 3B9BAEB7, 77A099B7, 16C49226, ABACC2AF, CFB03688, E2DEDF22, D412CAD1
16C49226, DA61AB82, 3B9BAEB7, 77A099B7, D412CAD1, 72599389, CFB03688, E2DEDF22
77A099B7, 54C888CC, DA61AB82, 3B9BAEB7, E2DEDF22, CF3CD682, 72599389, CFB03688
3B9BAEB7, F2635347, 54C888CC, DA61AB82, CFB03688, B235784E, CF3CD682, 72599389
DA61AB82, E2CAC9B4, F2635347, 54C888CC, 72599389, 881678DF, B235784E, CF3CD682
54C888CC, 9596C718, E2CAC9B4, F2635347, CF3CD682, E815373B, 881678DF, B235784E
F2635347, 9DD54912, 9596C718, E2CAC9B4, B235784E, BD994B56, E815373B, 881678DF
```

E2CAC9B4, 2E8539A7, 9DD54912, 9596C718, 881678DF, B0055655, BD994B56, E815373B
9596C718, 2303C213, 2E8539A7, 9DD54912, E815373B, CC87EF5A, B0055655, BD994B56
9DD54912, EA79BE25, 2303C213, 2E8539A7, BD994B56, 6B24384D, CC87EF5A, B0055655
2E8539A7, 23D7CB45, EA79BE25, 2303C213, B0055655, 93E7329F, 6B24384D, CC87EF5A
2303C213, F028EF04, 23D7CB45, EA79BE25, CC87EF5A, 35B95AE7, 93E7329F, 6B24384D
EA79BE25, 48863F19, F028EF04, 23D7CB45, 6B24384D, 06C6536D, 35B95AE7, 93E7329F
23D7CB45, 514C81B6, 48863F19, F028EF04, 93E7329F, FF1C5DC7, 06C6536D, 35B95AE7
F028EF04, 6102CE67, 514C81B6, 48863F19, 35B95AE7, D0D541F1, FF1C5DC7, 06C6536D
48863F19, 330485FD, 6102CE67, 514C81B6, 06C6536D, A94C0DD9, D0D541F1, FF1C5DC7
514C81B6, 289E8C82, 330485FD, 6102CE67, FF1C5DC7, DEDC1E39, A94C0DD9, D0D541F1
6102CE67, 13CC3A1D, 289E8C82, 330485FD, D0D541F1, 12D926C0, DEDC1E39, A94C0DD9
330485FD, 40A226A6, 13CC3A1D, 289E8C82, A94C0DD9, ED7EDA63, 12D926C0, DEDC1E39
289E8C82, 70BFB1A8, 40A226A6, 13CC3A1D, DEDC1E39, 9E52219C, ED7EDA63, 12D926C0
13CC3A1D, CE1D1A37, 70BFB1A8, 40A226A6, 12D926C0, F5D22339, 9E52219C, ED7EDA63
40A226A6, EC9F7830, CE1D1A37, 70BFB1A8, ED7EDA63, 0BC5B4FC, F5D22339, 9E52219C
70BFB1A8, 3CF2D6EE, EC9F7830, CE1D1A37, 9E52219C, FCFBD391, 0BC5B4FC, F5D22339
CE1D1A37, F0C1F95C, 3CF2D6EE, EC9F7830, F5D22339, 2B6A389B, FCFBD391, 0BC5B4FC
EC9F7830, 9A351A9D, F0C1F95C, 3CF2D6EE, 0BC5B4FC, FBF85B05, 2B6A389B, FCFBD391
3CF2D6EE, 138B0685, 9A351A9D, F0C1F95C, FCFBD391, F7BBBE8B, FBF85B05, 2B6A389B
F0C1F95C, EA3574D1, 138B0685, 9A351A9D, 2B6A389B, C8592ACC, F7BBBE8B, FBF85B05
9A351A9D, 4719C849, EA3574D1, 138B0685, FBF85B05, FE2D3EFA, C8592ACC, F7BBBE8B
138B0685, 57F52A13, 4719C849, EA3574D1, F7BBBE8B, 5411CC34, FE2D3EFA, C8592ACC
EA3574D1, 4751F880, 57F52A13, 4719C849, C8592ACC, DC8ED546, 5411CC34, FE2D3EFA
4719C849, 80605BAF, 4751F880, 57F52A13, FE2D3EFA, 55C1E317, DC8ED546, 5411CC34
57F52A13, 1E53AD4A, 80605BAF, 4751F880, 5411CC34, 0B92E4F0, 55C1E317, DC8ED546
4751F880, 1ABEED79, 1E53AD4A, 80605BAF, DC8ED546, 5E192900, 0B92E4F0, 55C1E317
80605BAF, 75EACBB7, 1ABEED79, 1E53AD4A, 55C1E317, 186EB0CF, 5E192900, 0B92E4F0
1E53AD4A, 08AC1056, 75EACBB7, 1ABEED79, 0B92E4F0, 8F3A64E3, 186EB0CF, 5E192900
1ABEED79, 9BDB7A88, 08AC1056, 75EACBB7, 5E192900, 3701E7B3, 8F3A64E3, 186EB0CF
75EACBB7, ADF32F05, 9BDB7A88, 08AC1056, 186EB0CF, 6CE969E9, 3701E7B3, 8F3A64E3
08AC1056, 2277B80D, ADF32F05, 9BDB7A88, 8F3A64E3, EE7224D5, 6CE969E9, 3701E7B3
9BDB7A88, 535DBB9A, 2277B80D, ADF32F05, 3701E7B3, 3E849D0F, EE7224D5, 6CE969E9
ADF32F05, 2A494EC5, 535DBB9A, 2277B80D, 6CE969E9, DDBD8EE7, 3E849D0F, EE7224D5
2277B80D, 693C7A09, 2A494EC5, 535DBB9A, EE7224D5, C3DDAC40, DDBD8EE7, 3E849D0F
535DBB9A, 148A5796, 693C7A09, 2A494EC5, 3E849D0F, 5E0E10B9, C3DDAC40, DDBD8EE7
2A494EC5, D2932448, 148A5796, 693C7A09, DDBD8EE7, 1CCB75AF, 5E0E10B9, C3DDAC40
693C7A09, 39CA97B6, D2932448, 148A5796, C3DDAC40, 27F81499, 1CCB75AF, 5E0E10B9
148A5796, 770BCE98, 39CA97B6, D2932448, 5E0E10B9, 82843491, 27F81499, 1CCB75AF
D2932448, 8C4DC6AF, 770BCE98, 39CA97B6, 1CCB75AF, 4E4E13E9, 82843491, 27F81499
39CA97B6, 048CC517, 8C4DC6AF, 770BCE98, 27F81499, 03BD1BD9, 4E4E13E9, 82843491
770BCE98, 419960CF, 048CC517, 8C4DC6AF, 82843491, 6FA999B7, 03BD1BD9, 4E4E13E9
8C4DC6AF, 407700EE, 419960CF, 048CC517, 4E4E13E9, 37B18629, 6FA999B7, 03BD1BD9
048CC517, E60ABEC4, 407700EE, 419960CF, 03BD1BD9, 9EA44395, 37B18629, 6FA999B7
419960CF, 0E248A8B, E60ABEC4, 407700EE, 6FA999B7, F877D28C, 9EA44395, 37B18629
407700EE, 10667792, 0E248A8B, E60ABEC4, 37B18629, F63EA862, F877D28C, 9EA44395
E60ABEC4, 646BB7A8, 10667792, 0E248A8B, 9EA44395, 424072F0, F63EA862, F877D28C
0E248A8B, 625CCE22, 646BB7A8, 10667792, F877D28C, 3B7642B8, 424072F0, F63EA862
10667792, 8E0E1101, 625CCE22, 646BB7A8, F63EA862, CD620F4E, 3B7642B8, 424072F0
646BB7A8, C23D3583, 8E0E1101, 625CCE22, 424072F0, BFAA1A02, CD620F4E, 3B7642B8
625CCE22, 81DE3DC5, C23D3583, 8E0E1101, 3B7642B8, 1BA7FD36, BFAA1A02, CD620F4E
8E0E1101, D24E4181, 81DE3DC5, C23D3583, CD620F4E, E62BB2A4, 1BA7FD36, BFAA1A02

The following are (hexadecimal representations of) the successive values of the variables X_0, X_1, X_2, X_3, X'_0, X'_1, X'_2 and X'_3 obtained during the processing of the second block.

31560350, 285A21CF, 846C181B, 553B61B8, 31560350, 285A21CF, 846C181B, 553B61B8
553B61B8, 1ADDE153, 285A21CF, 846C181B, 553B61B8, 56C8C102, 285A21CF, 846C181B
846C181B, CE8FC309, 1ADDE153, 285A21CF, 846C181B, 702249A4, 56C8C102, 285A21CF
285A21CF, 0DD8403A, CE8FC309, 1ADDE153, 285A21CF, 22CB0A97, 702249A4, 56C8C102
1ADDE153, 4842F01E, 0DD8403A, CE8FC309, 56C8C102, 35B2DCDF, 22CB0A97, 702249A4
CE8FC309, BE6A9014, 4842F01E, 0DD8403A, 702249A4, D2EFFB4A, 35B2DCDF, 22CB0A97
0DD8403A, 7FE339CA, BE6A9014, 4842F01E, 22CB0A97, 59EA6C60, D2EFFB4A, 35B2DCDF
4842F01E, D1CCFD4B, 7FE339CA, BE6A9014, 35B2DCDF, 82DEA3AE, 59EA6C60, D2EFFB4A

```
BE6A9014, 108966B1, D1CCFD4B, 7FE339CA, D2EFFB4A, 4481FDE2, 82DEA3AE, 59EA6C60
7FE339CA, 899223E8, 108966B1, D1CCFD4B, 59EA6C60, 13BB8F73, 4481FDE2, 82DEA3AE
D1CCFD4B, 5E3B9917, 899223E8, 108966B1, 82DEA3AE, 946BD478, 13BB8F73, 4481FDE2
108966B1, 7666663B, 5E3B9917, 899223E8, 4481FDE2, BD0605EA, 946BD478, 13BB8F73
899223E8, A1BAD92C, 7666663B, 5E3B9917, 13BB8F73, 36F99153, BD0605EA, 946BD478
5E3B9917, DE527A04, A1BAD92C, 7666663B, 946BD478, EB4AE872, 36F99153, BD0605EA
7666663B, E52F1533, DE527A04, A1BAD92C, BD0605EA, 7C346442, EB4AE872, 36F99153
A1BAD92C, 5C3C2C22, E52F1533, DE527A04, 36F99153, AFA320AD, 7C346442, EB4AE872
DE527A04, FC1C4108, 5C3C2C22, E52F1533, EB4AE872, B4905651, AFA320AD, 7C346442
E52F1533, 0A03E84B, FC1C4108, 5C3C2C22, 7C346442, 02E94FA1, B4905651, AFA320AD
5C3C2C22, FB74BD26, 0A03E84B, FC1C4108, AFA320AD, E08D1799, 02E94FA1, B4905651
FC1C4108, C78DC5C4, FB74BD26, 0A03E84B, B4905651, 69AFAA80, E08D1799, 02E94FA1
0A03E84B, ACF60434, C78DC5C4, FB74BD26, 02E94FA1, FA665E46, 69AFAA80, E08D1799
FB74BD26, 58F751E0, ACF60434, C78DC5C4, E08D1799, 269AB7E3, FA665E46, 69AFAA80
C78DC5C4, EB75C7CB, 58F751E0, ACF60434, 69AFAA80, 0F06388B, 269AB7E3, FA665E46
ACF60434, 83C0A8B7, EB75C7CB, 58F751E0, FA665E46, FD44FBD5, 0F06388B, 269AB7E3
58F751E0, 27C87178, 83C0A8B7, EB75C7CB, 269AB7E3, DBBC0190, FD44FBD5, 0F06388B
EB75C7CB, B7B9163F, 27C87178, 83C0A8B7, 0F06388B, D0E3FC2B, DBBC0190, FD44FBD5
83C0A8B7, 0FA1C6DC, B7B9163F, 27C87178, FD44FBD5, 7D87B4BA, D0E3FC2B, DBBC0190
27C87178, 2CC60316, 0FA1C6DC, B7B9163F, DBBC0190, 68367FDB, 7D87B4BA, D0E3FC2B
B7B9163F, 08029C44, 2CC60316, 0FA1C6DC, D0E3FC2B, 53AB5439, 68367FDB, 7D87B4BA
0FA1C6DC, F693A10E, 08029C44, 2CC60316, 7D87B4BA, E78B75B5, 53AB5439, 68367FDB
2CC60316, 356224B9, F693A10E, 08029C44, 68367FDB, 830530DF, E78B75B5, 53AB5439
08029C44, 669F7869, 356224B9, F693A10E, 53AB5439, 67FCB1AC, 830530DF, E78B75B5
F693A10E, 7B70C168, 669F7869, 356224B9, E78B75B5, 757BB243, 67FCB1AC, 830530DF
356224B9, 037FB19C, 7B70C168, 669F7869, 830530DF, F0CA8878, 757BB243, 67FCB1AC
669F7869, 9B0A10B3, 037FB19C, 7B70C168, 67FCB1AC, FA10CB33, F0CA8878, 757BB243
7B70C168, 9D015956, 9B0A10B3, 037FB19C, 757BB243, 5487E56C, FA10CB33, F0CA8878
037FB19C, 6A7DE5F4, 9D015956, 9B0A10B3, F0CA8878, A5D33699, 5487E56C, FA10CB33
9B0A10B3, E522D913, 6A7DE5F4, 9D015956, FA10CB33, BEB495BC, A5D33699, 5487E56C
9D015956, 0EFD42E5, E522D913, 6A7DE5F4, 5487E56C, 05202F93, BEB495BC, A5D33699
6A7DE5F4, 7902100B, 0EFD42E5, E522D913, A5D33699, BACE7DD9, 05202F93, BEB495BC
E522D913, 1ACEFABC, 7902100B, 0EFD42E5, BEB495BC, 08D045DD, BACE7DD9, 05202F93
0EFD42E5, E07378FF, 1ACEFABC, 7902100B, 05202F93, 5448A3A0, 08D045DD, BACE7DD9
7902100B, 489C7A1A, E07378FF, 1ACEFABC, BACE7DD9, D98BE3AA, 5448A3A0, 08D045DD
1ACEFABC, C02A45A5, 489C7A1A, E07378FF, 08D045DD, 12EC982F, D98BE3AA, 5448A3A0
E07378FF, 3068DDE8, C02A45A5, 489C7A1A, 5448A3A0, 4A1EB2B2, 12EC982F, D98BE3AA
489C7A1A, D5DD5018, 3068DDE8, C02A45A5, D98BE3AA, D677AAA8, 4A1EB2B2, 12EC982F
C02A45A5, B9D75D76, D5DD5018, 3068DDE8, 12EC982F, 5AA89133, D677AAA8, 4A1EB2B2
3068DDE8, 51A9B2DD, B9D75D76, D5DD5018, 4A1EB2B2, 49BCE169, 5AA89133, D677AAA8
D5DD5018, 36F589C4, 51A9B2DD, B9D75D76, D677AAA8, CF4FA8D2, 49BCE169, 5AA89133
B9D75D76, B5C60EAF, 36F589C4, 51A9B2DD, 5AA89133, C1985969, CF4FA8D2, 49BCE169
51A9B2DD, 725DF80C, B5C60EAF, 36F589C4, 49BCE169, 427440B4, C1985969, CF4FA8D2
36F589C4, 3F7A2507, 725DF80C, B5C60EAF, CF4FA8D2, 60927896, 427440B4, C1985969
B5C60EAF, 9D539EB6, 3F7A2507, 725DF80C, C1985969, 7050ED96, 60927896, 427440B4
725DF80C, 5A249895, 9D539EB6, 3F7A2507, 427440B4, CBC74513, 7050ED96, 60927896
3F7A2507, A7CECDCD, 5A249895, 9D539EB6, 60927896, 8431C75E, CBC74513, 7050ED96
9D539EB6, F8DCD12B, A7CECDCD, 5A249895, 7050ED96, 0E3A1C68, 8431C75E, CBC74513
5A249895, 3E30DB2A, F8DCD12B, A7CECDCD, CBC74513, 62EEEC87, 0E3A1C68, 8431C75E
A7CECDCD, A25D36CE, 3E30DB2A, F8DCD12B, 8431C75E, 2B1F312D, 62EEEC87, 0E3A1C68
F8DCD12B, A92CF759, A25D36CE, 3E30DB2A, 0E3A1C68, FB124197, 2B1F312D, 62EEEC87
3E30DB2A, 0CD0BA66, A92CF759, A25D36CE, 62EEEC87, DB8A5C11, FB124197, 2B1F312D
A25D36CE, AF62D775, 0CD0BA66, A92CF759, 2B1F312D, EC3264DC, DB8A5C11, FB124197
A92CF759, 69D4E1DF, AF62D775, 0CD0BA66, FB124197, 9AA87F7C, EC3264DC, DB8A5C11
0CD0BA66, 0EE66339, 69D4E1DF, AF62D775, DB8A5C11, 04512915, 9AA87F7C, EC3264DC
AF62D775, 5C5B5FBD, 0EE66339, 69D4E1DF, EC3264DC, C763272A, 04512915, 9AA87F7C
69D4E1DF, 0D80E8CF, 5C5B5FBD, 0EE66339, 9AA87F7C, CCD7DF45, C763272A, 04512915
```

The hash-code is the following 128-bit string.

```
A1 AA 06 89 D0 FA FA 2D DC 22 E8 8B 49 13 3A 06
```

B.3.9 Example 9

In this example, the data string is the 1 000 000-byte string consisting of the ASCII-coded version of "a" repeated 10^6 times.

The hash-code is the following 128-bit string.

```
4A 7F 57 23 F9 54 EB A1 21 6C 9D 8F 63 20 43 1F
```

B.3.10 Example 10

In this example, the data string is the 112-byte string consisting of the ASCII-coded version of

```
"abcdefghbcdefghicdefghijdefghijkefghijklfghijklmghijklmn
hijklmnoijklmnopjklmnopqklmnopqrlmnopqrsmnopqrstnopqrstu"
```

(with no line break after the first n).

The hash-code is the following 128-bit string.

```
d4 ec c9 13 e1 df 77 6b f4 8d e9 d5 5b 1f 25 46
```

B.3.11 Example 11

In this example, the data string is the 32-byte string consisting of the ASCII-coded version of

```
"abcdbcdecdefdefgefghfghighijhijk"
```

The hash-code is the following 128-bit string.

```
13 fc 13 e8 ef ff 34 7d e1 93 ff 46 db ac cf d4
```

B.4 Dedicated Hash-Function 3 (SHA-1)

B.4.1 Example 1

In this example, the data string is the empty string, i.e., the string of length zero.

The hash-code is the following 160-bit string.

```
DA 39 A3 EE 5E 6B 4B 0D 32 55 BF EF 95 60 18 90 AF D8 07 09
```

B.4.2 Example 2

In this example, the data string consists of a single byte, namely the ASCII-coded version of the letter "a".

The hash-code is the following 160-bit string.

```
86 F7 E4 37 FA A5 A7 FC E1 5D 1D DC B9 EA EA EA 37 76 67 B8
```

B.4.3 Example 3

In this example, the data string is the 3-byte string consisting of the ASCII-coded version of "abc". This is equivalent to the bit string "01100001 01100010 01100011".

After the padding process, the single 16-word block derived from the data string is as follows.

```
61626380  00000000  00000000  00000000  00000000  00000000  00000000  00000000
00000000  00000000  00000000  00000000  00000000  00000000  00000000  00000018
```

The following are (hexadecimal representations of) the successive values of the variables X_0, X_1, X_2, X_3 and X_4.

```
0116FC33, 67452301, 7BF36AE2, 98BADCFE, 10325476
8990536D, 0116FC33, 59D148C0, 7BF36AE2, 98BADCFE
A1390F08, 8990536D, C045BF0C, 59D148C0, 7BF36AE2
CDD8E11B, A1390F08, 626414DB, C045BF0C, 59D148C0
CFD499DE, CDD8E11B, 284E43C2, 626414DB, C045BF0C
3FC7CA40, CFD499DE, F3763846, 284E43C2, 626414DB
993E30C1, 3FC7CA40, B3F52677, F3763846, 284E43C2
9E8C07D4, 993E30C1, 0FF1F290, B3F52677, F3763846
4B6AE328, 9E8C07D4, 664F8C30, 0FF1F290, B3F52677
8351F929, 4B6AE328, 27A301F5, 664F8C30, 0FF1F290
FBDA9E89, 8351F929, 12DAB8CA, 27A301F5, 664F8C30
63188FE4, FBDA9E89, 60D47E4A, 12DAB8CA, 27A301F5
4607B664, 63188FE4, 7EF6A7A2, 60D47E4A, 12DAB8CA
9128F695, 4607B664, 18C623F9, 7EF6A7A2, 60D47E4A
196BEE77, 9128F695, 1181ED99, 18C623F9, 7EF6A7A2
20BDD62F, 196BEE77, 644A3DA5, 1181ED99, 18C623F9
4E925823, 20BDD62F, C65AFB9D, 644A3DA5, 1181ED99
82AA6728, 4E925823, C82F758B, C65AFB9D, 644A3DA5
DC64901D, 82AA6728, D3A49608, C82F758B, C65AFB9D
FD9E1D7D, DC64901D, 20AA99CA, D3A49608, C82F758B
1A37B0CA, FD9E1D7D, 77192407, 20AA99CA, D3A49608
33A23BFC, 1A37B0CA, 7F67875F, 77192407, 20AA99CA
21283486, 33A23BFC, 868DEC32, 7F67875F, 77192407
D541F12D, 21283486, 0CE88EFF, 868DEC32, 7F67875F
C7567DC6, D541F12D, 884A0D21, 0CE88EFF, 868DEC32
48413BA4, C7567DC6, 75507C4B, 884A0D21, 0CE88EFF
BE35FBD5, 48413BA4, B1D59F71, 75507C4B, 884A0D21
4AA84D97, BE35FBD5, 12104EE9, B1D59F71, 75507C4B
8370B52E, 4AA84D97, 6F8D7EF5, 12104EE9, B1D59F71
C5FBAF5D, 8370B52E, D2AA1365, 6F8D7EF5, 12104EE9
1267B407, C5FBAF5D, A0DC2D4B, D2AA1365, 6F8D7EF5
3B845D33, 1267B407, 717EEBD7, A0DC2D4B, D2AA1365
046FAA0A, 3B845D33, C499ED01, 717EEBD7, A0DC2D4B
2C0EBC11, 046FAA0A, CEE1174C, C499ED01, 717EEBD7
21796AD4, 2C0EBC11, 811BEA82, CEE1174C, C499ED01
DCBBB0CB, 21796AD4, 4B03AF04, 811BEA82, CEE1174C
0F511FD8, DCBBB0CB, 085E5AB5, 4B03AF04, 811BEA82
DC63973F, 0F511FD8, F72EEC32, 085E5AB5, 4B03AF04
4C986405, DC63973F, 03D447F6, F72EEC32, 085E5AB5
32DE1CBA, 4C986405, F718E5CF, 03D447F6, F72EEC32
FC87DEDF, 32DE1CBA, 53261901, F718E5CF, 03D447F6
970A0D5C, FC87DEDF, 8CB7872E, 53261901, F718E5CF
7F193DC5, 970A0D5C, FF21F7B7, 8CB7872E, 53261901
EE1B1AAF, 7F193DC5, 25C28357, FF21F7B7, 8CB7872E
40F28E09, EE1B1AAF, 5FC64F71, 25C28357, FF21F7B7
1C51E1F2, 40F28E09, FB86C6AB, 5FC64F71, 25C28357
A01B846C, 1C51E1F2, 503CA382, FB86C6AB, 5FC64F71
BEAD02CA, A01B846C, 8714787C, 503CA382, FB86C6AB
BAF39337, BEAD02CA, 2806E11B, 8714787C, 503CA382
120731C5, BAF39337, AFAB40B2, 2806E11B, 8714787C
641DB2CE, 120731C5, EEBCE4CD, AFAB40B2, 2806E11B
3847AD66, 641DB2CE, 4481CC71, EEBCE4CD, AFAB40B2
E490436D, 3847AD66, 99076CB3, 4481CC71, EEBCE4CD
27E9F1D8, E490436D, 8E11EB59, 99076CB3, 4481CC71
7B71F76D, 27E9F1D8, 792410DB, 8E11EB59, 99076CB3
5E6456AF, 7B71F76D, 09FA7C76, 792410DB, 8E11EB59
C846093F, 5E6456AF, 5EDC7DDB, 09FA7C76, 792410DB
D262FF50, C846093F, D79915AB, 5EDC7DDB, 09FA7C76
09D785FD, D262FF50, F211824F, D79915AB, 5EDC7DDB
3F52DE5A, 09D785FD, 3498BFD4, F211824F, D79915AB
D756C147, 3F52DE5A, 4275E17F, 3498BFD4, F211824F
548C9CB2, D756C147, 8FD4B796, 4275E17F, 3498BFD4
B66C020B, 548C9CB2, F5D5B051, 8FD4B796, 4275E17F
```

```
6B61C9E1, B66C020B, 9523272C, F5D5B051, 8FD4B796
19DFA7AC, 6B61C9E1, ED9B0082, 9523272C, F5D5B051
101655F9, 19DFA7AC, 5AD87278, ED9B0082, 9523272C
0C3DF2B4, 101655F9, 0677E9EB, 5AD87278, ED9B0082
78DD4D2B, 0C3DF2B4, 4405957E, 0677E9EB, 5AD87278
497093C0, 78DD4D2B, 030F7CAD, 4405957E, 0677E9EB
3F2588C2, 497093C0, DE37534A, 030F7CAD, 4405957E
C199F8C7, 3F2588C2, 125C24F0, DE37534A, 030F7CAD
39859DE7, C199F8C7, 8FC96230, 125C24F0, DE37534A
EDB42DE4, 39859DE7, F0667E31, 8FC96230, 125C24F0
11793F6F, EDB42DE4, CE616779, F0667E31, 8FC96230
5EE76897, 11793F6F, 3B6D0B79, CE616779, F0667E31
63F7DAB7, 5EE76897, C45E4FDB, 3B6D0B79, CE616779
A079B7D9, 63F7DAB7, D7B9DA25, C45E4FDB, 3B6D0B79
860D21CC, A079B7D9, D8FDF6AD, D7B9DA25, C45E4FDB
5738D5E1, 860D21CC, 681E6DF6, D8FDF6AD, D7B9DA25
42541B35, 5738D5E1, 21834873, 681E6DF6, D8FDF6AD
```

The hash-code is the following 160-bit string.

```
A9 99 3E 36 47 06 81 6A BA 3E 25 71 78 50 C2 6C 9C D0 D8 9D
```

B.4.4 Example 4

In this example, the data string is the 14-byte string consisting of the ASCII-coded version of

```
"message digest"
```

The hash-code is the following 160-bit string.

```
C1 22 52 CE DA 8B E8 99 4D 5F A0 29 0A 47 23 1C 1D 16 AA E3
```

B.4.5 Example 5

In this example, the data string is the 26-byte string consisting of the ASCII-coded version of

```
"abcdefghijklmnopqrstuvwxyz"
```

The hash-code is the following 160-bit string.

```
32 D1 0C 7B 8C F9 65 70 CA 04 CE 37 F2 A1 9D 84 24 0D 3A 89
```

B.4.6 Example 6

In this example, the data string is the 62-byte string consisting of the ASCII-coded version of

```
"ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz0123456789"
```

The hash-code is the following 160-bit string.

```
76 1C 45 7B F7 3B 14 D2 7E 9E 92 65 C4 6F 4B 4D DA 11 F9 40
```

B.4.7 Example 7

In this example, the data string is the 80-byte string consisting of the ASCII-coded version of eight repetitions of

```
"1234567890"
```

The hash-code is the following 160-bit string.

```
50 AB F5 70 6A 15 09 90 A0 8B 2C 5E A4 0F A0 E5 85 55 47 32
```

B.4.8 Example 8

In this example, the data string is the 56-byte string consisting of the ASCII-coded version of

"abcdbcdecdefdefgefghfghighijhijkijkljklmklmnlmnomnopnopq"

After the padding process, the two 16-word blocks derived from the data string are as follows.

```
61626364  62636465  63646566  64656667  65666768  66676869  6768696A  68696A6B
696A6B6C  6A6B6C6D  6B6C6D6E  6C6D6E6F  6D6E6F70  6E6F7071  80000000  00000000

00000000  00000000  00000000  00000000  00000000  00000000  00000000  00000000
00000000  00000000  00000000  00000000  00000000  00000000  00000000  000001C0
```

The following are (hexadecimal representations of) the successive values of the variables X_0, X_1, X_2, X_3 and X_4 obtained during the processing of the first block.

```
0116FC17, 67452301, 7BF36AE2, 98BADCFE, 10325476
EBF3B452, 0116FC17, 59D148C0, 7BF36AE2, 98BADCFE
5109913A, EBF3B452, C045BF05, 59D148C0, 7BF36AE2
2C4F6EAC, 5109913A, BAFCED14, C045BF05, 59D148C0
33F4AE5B, 2C4F6EAC, 9442644E, BAFCED14, C045BF05
96B85189, 33F4AE5B, 0B13DBAB, 9442644E, BAFCED14
DB04CB58, 96B85189, CCFD2B96, 0B13DBAB, 9442644E
45833F0F, DB04CB58, 65AE1462, CCFD2B96, 0B13DBAB
C565C35E, 45833F0F, 36C132D6, 65AE1462, CCFD2B96
6350AFDA, C565C35E, D160CFC3, 36C132D6, 65AE1462
8993EA77, 6350AFDA, B15970D7, D160CFC3, 36C132D6
E19ECAA2, 8993EA77, 98D42BF6, B15970D7, D160CFC3
8603481E, E19ECAA2, E264FA9D, 98D42BF6, B15970D7
32F94A85, 8603481E, B867B2A8, E264FA9D, 98D42BF6
B2E7A8BE, 32F94A85, A180D207, B867B2A8, E264FA9D
42637E39, B2E7A8BE, 4CBE52A1, A180D207, B867B2A8
6B068048, 42637E39, ACB9EA2F, 4CBE52A1, A180D207
426B9C35, 6B068048, 5098DF8E, ACB9EA2F, 4CBE52A1
944B1BD1, 426B9C35, 1AC1A012, 5098DF8E, ACB9EA2F
6C445652, 944B1BD1, 509AE70D, 1AC1A012, 5098DF8E
95836DA5, 6C445652, 6512C6F4, 509AE70D, 1AC1A012
09511177, 95836DA5, 9B111594, 6512C6F4, 509AE70D
E2B92DC4, 09511177, 6560DB69, 9B111594, 6512C6F4
FD224575, E2B92DC4, C254445D, 6560DB69, 9B111594
EEB82D9A, FD224575, 38AE4B71, C254445D, 6560DB69
5A142C1A, EEB82D9A, 7F48915D, 38AE4B71, C254445D
2972F7C7, 5A142C1A, BBAE0B66, 7F48915D, 38AE4B71
D526A644, 2972F7C7, 96850B06, BBAE0B66, 7F48915D
E1122421, D526A644, CA5CBDF1, 96850B06, BBAE0B66
05B457B2, E1122421, 3549A991, CA5CBDF1, 96850B06
A9C84BEC, 05B457B2, 78448908, 3549A991, CA5CBDF1
52E31F60, A9C84BEC, 816D15EC, 78448908, 3549A991
5AF3242C, 52E31F60, 2A7212FB, 816D15EC, 78448908
31C756A9, 5AF3242C, 14B8C7D8, 2A7212FB, 816D15EC
E9AC987C, 31C756A9, 16BCC90B, 14B8C7D8, 2A7212FB
AB7C32EE, E9AC987C, 4C71D5AA, 16BCC90B, 14B8C7D8
5933FC99, AB7C32EE, 3A6B261F, 4C71D5AA, 16BCC90B
43F87AE9, 5933FC99, AADF0CBB, 3A6B261F, 4C71D5AA
24957F22, 43F87AE9, 564CFF26, AADF0CBB, 3A6B261F
ADEB7478, 24957F22, 50FE1EBA, 564CFF26, AADF0CBB
D70E5010, ADEB7478, 89255FC8, 50FE1EBA, 564CFF26
79BCFB08, D70E5010, 2B7ADD1E, 89255FC8, 50FE1EBA
F9BCB8DE, 79BCFB08, 35C39404, 2B7ADD1E, 89255FC8
```

```
633E9561, F9BCB8DE, 1E6F3EC2, 35C39404, 2B7ADD1E
98C1EA64, 633E9561, BE6F2E37, 1E6F3EC2, 35C39404
C6EA241E, 98C1EA64, 58CFA558, BE6F2E37, 1E6F3EC2
A2AD4F02, C6EA241E, 26307A99, 58CFA558, BE6F2E37
C8A69090, A2AD4F02, B1BA8907, 26307A99, 58CFA558
88341600, C8A69090, A8AB53C0, B1BA8907, 26307A99
7E846F58, 88341600, 3229A424, A8AB53C0, B1BA8907
86E358BA, 7E846F58, 220D0580, 3229A424, A8AB53C0
8D2E76C8, 86E358BA, 1FA11BD6, 220D0580, 3229A424
CE892E10, 8D2E76C8, A1B8D62E, 1FA11BD6, 220D0580
EDEA95B1, CE892E10, 234B9DB2, A1B8D62E, 1FA11BD6
36D1230A, EDEA95B1, 33A24B84, 234B9DB2, A1B8D62E
776C3910, 36D1230A, 7B7AA56C, 33A24B84, 234B9DB2
A681B723, 776C3910, 8DB448C2, 7B7AA56C, 33A24B84
AC0A794F, A681B723, 1DDB0E44, 8DB448C2, 7B7AA56C
F03D3782, AC0A794F, E9A06DC8, 1DDB0E44, 8DB448C2
9EF775C3, F03D3782, EB029E53, E9A06DC8, 1DDB0E44
36254B13, 9EF775C3, BC0F4DE0, EB029E53, E9A06DC8
4080D4DC, 36254B13, E7BDDD70, BC0F4DE0, EB029E53
2BFAF7A8, 4080D4DC, CD8952C4, E7BDDD70, BC0F4DE0
513F9CA0, 2BFAF7A8, 10203537, CD8952C4, E7BDDD70
E5895C81, 513F9CA0, 0AFEBDEA, 10203537, CD8952C4
1037D2D5, E5895C81, 144FE728, 0AFEBDEA, 10203537
14A82DA9, 1037D2D5, 79625720, 144FE728, 0AFEBDEA
6D17C9FD, 14A82DA9, 440DF4B5, 79625720, 144FE728
2C7B07BD, 6D17C9FD, 452A0B6A, 440DF4B5, 79625720
FDF6EFFF, 2C7B07BD, 5B45F27F, 452A0B6A, 440DF4B5
112B96E3, FDF6EFFF, 4B1EC1EF, 5B45F27F, 452A0B6A
84065712, 112B96E3, FF7DBBFF, 4B1EC1EF, 5B45F27F
AB89FB71, 84065712, C44AE5B8, FF7DBBFF, 4B1EC1EF
C5210E35, AB89FB71, A10195C4, C44AE5B8, FF7DBBFF
352D9F4B, C5210E35, 6AE27EDC, A10195C4, C44AE5B8
1A0E0E0A, 352D9F4B, 7148438D, 6AE27EDC, A10195C4
D0D47349, 1A0E0E0A, CD4B67D2, 7148438D, 6AE27EDC
AD38620D, D0D47349, 86838382, CD4B67D2, 7148438D
D3AD7C25, AD38620D, 74351CD2, 86838382, CD4B67D2
8CE34517, D3AD7C25, 6B4E1883, 74351CD2, 86838382
```

The following are (hexadecimal representations of) the successive values of the variables X_0, X_1, X_2, X_3 and X_4, obtained during the processing of the second block.

```
2DF257E9, F4286818, B0DEC9EB, 0408F581, 84677148
4D3DC58F, 2DF257E9, 3D0A1A06, B0DEC9EB, 0408F581
C352BB05, 4D3DC58F, 4B7C95FA, 3D0A1A06, B0DEC9EB
EEF743C6, C352BB05, D34F7163, 4B7C95FA, 3D0A1A06
41E34277, EEF743C6, 70D4AEC1, D34F7163, 4B7C95FA
5443915C, 41E34277, BBBDD0F1, 70D4AEC1, D34F7163
E7FA0377, 5443915C, D078D09D, BBBDD0F1, 70D4AEC1
C6946813, E7FA0377, 1510E457, D078D09D, BBBDD0F1
FDDE1DE1, C6946813, F9FE80DD, 1510E457, D078D09D
B8538ACA, FDDE1DE1, F1A51A04, F9FE80DD, 1510E457
6BA94F63, B8538ACA, 7F778778, F1A51A04, F9FE80DD
43A2792F, 6BA94F63, AE14E2B2, 7F778778, F1A51A04
FECD7BBF, 43A2792F, DAEA53D8, AE14E2B2, 7F778778
A2604CA8, FECD7BBF, D0E89E4B, DAEA53D8, AE14E2B2
258B0BAA, A2604CA8, FFB35EEF, D0E89E4B, DAEA53D8
D9772360, 258B0BAA, 2898132A, FFB35EEF, D0E89E4B
5507DB6E, D9772360, 8962C2EA, 2898132A, FFB35EEF
A51B58BC, 5507DB6E, 365DC8D8, 8962C2EA, 2898132A
C2EB709F, A51B58BC, 9541F6DB, 365DC8D8, 8962C2EA
D8992153, C2EB709F, 2946D62F, 9541F6DB, 365DC8D8
37482F5F, D8992153, F0BADC27, 2946D62F, 9541F6DB
EE8700BD, 37482F5F, F6264854, F0BADC27, 2946D62F
```

```
9AD594B9, EE8700BD, CDD20BD7, F6264854, F0BADC27
8FBAA5B9, 9AD594B9, 7BA1C02F, CDD20BD7, F6264854
88FB5867, 8FBAA5B9, 66B5652E, 7BA1C02F, CDD20BD7
EEC50521, 88FB5867, 63EEA96E, 66B5652E, 7BA1C02F
50BCE434, EEC50521, E23ED619, 63EEA96E, 66B5652E
5C416DAF, 50BCE434, 7BB14148, E23ED619, 63EEA96E
2429BE5F, 5C416DAF, 142F390D, 7BB14148, E23ED619
0A2FB108, 2429BE5F, D7105B6B, 142F390D, 7BB14148
17986223, 0A2FB108, C90A6F97, D7105B6B, 142F390D
8A4AF384, 17986223, 028BEC42, C90A6F97, D7105B6B
6B629993, 8A4AF384, C5E61888, 028BEC42, C90A6F97
F15F04F3, 6B629993, 2292BCE1, C5E61888, 028BEC42
295CC25B, F15F04F3, DAD8A664, 2292BCE1, C5E61888
696DA404, 295CC25B, FC57C13C, DAD8A664, 2292BCE1
CEF5AE12, 696DA404, CA573096, FC57C13C, DAD8A664
87D5B80C, CEF5AE12, 1A5B6901, CA573096, FC57C13C
84E2A5F2, 87D5B80C, B3BD6B84, 1A5B6901, CA573096
03BB6310, 84E2A5F2, 21F56E03, B3BD6B84, 1A5B6901
C2D8F75F, 03BB6310, A138A97C, 21F56E03, B3BD6B84
BFB25768, C2D8F75F, 00EED8C4, A138A97C, 21F56E03
28589152, BFB25768, F0B63DD7, 00EED8C4, A138A97C
EC1D3D61, 28589152, 2FEC95DA, F0B63DD7, 00EED8C4
3CAED7AF, EC1D3D61, 8A162454, 2FEC95DA, F0B63DD7
C3D033EA, 3CAED7AF, 7B074F58, 8A162454, 2FEC95DA
7316056A, C3D033EA, CF2BB5EB, 7B074F58, 8A162454
46F93B68, 7316056A, B0F40CFA, CF2BB5EB, 7B074F58
DC8E7F26, 46F93B68, 9CC5815A, B0F40CFA, CF2BB5EB
850D411C, DC8E7F26, 11BE4EDA, 9CC5815A, B0F40CFA
7E4672C0, 850D411C, B7239FC9, 11BE4EDA, 9CC5815A
89FBD41D, 7E4672C0, 21435047, B7239FC9, 11BE4EDA
1797E228, 89FBD41D, 1F919CB0, 21435047, B7239FC9
431D65BC, 1797E228, 627EF507, 1F919CB0, 21435047
2BDBB8CB, 431D65BC, 05E5F88A, 627EF507, 1F919CB0
6DA72E7F, 2BDBB8CB, 10C7596F, 05E5F88A, 627EF507
A8495A9B, 6DA72E7F, CAF6EE32, 10C7596F, 05E5F88A
E785655A, A8495A9B, DB69CB9F, CAF6EE32, 10C7596F
5B086C42, E785655A, EA1256A6, DB69CB9F, CAF6EE32
A65818F7, 5B086C42, B9E15956, EA1256A6, DB69CB9F
7AAB101B, A65818F7, 96C21B10, B9E15956, EA1256A6
93614C9C, 7AAB101B, E996063D, 96C21B10, B9E15956
F66D9BF4, 93614C9C, DEAAC406, E996063D, 96C21B10
D504902B, F66D9BF4, 24D85327, DEAAC406, E996063D
60A9DA62, D504902B, 3D9B66FD, 24D85327, DEAAC406
8B687819, 60A9DA62, F541240A, 3D9B66FD, 24D85327
083E90C3, 8B687819, 982A7698, F541240A, 3D9B66FD
F6226BBF, 083E90C3, 62DA1E06, 982A7698, F541240A
76C0563B, F6226BBF, C20FA430, 62DA1E06, 982A7698
989DD165, 76C0563B, FD889AEF, C20FA430, 62DA1E06
8B2C7573, 989DD165, DDB0158E, FD889AEF, C20FA430
AE1B8E7B, 8B2C7573, 66277459, DDB0158E, FD889AEF
CA1840DE, AE1B8E7B, E2CB1D5C, 66277459, DDB0158E
16F3BABB, CA1840DE, EB86E39E, E2CB1D5C, 66277459
D28D83AD, 16F3BABB, B2861037, EB86E39E, E2CB1D5C
6BC02DFE, D28D83AD, C5BCEEAE, B2861037, EB86E39E
D3A6E275, 6BC02DFE, 74A360EB, C5BCEEAE, B2861037
DA955482, D3A6E275, 9AF00B7F, 74A360EB, C5BCEEAE
58C0AAC0, DA955482, 74E9B89D, 9AF00B7F, 74A360EB
906FD62C, 58C0AAC0, B6A55520, 74E9B89D, 9AF00B7F
```

The hash-code is the following 160-bit string.

```
84 98 3E 44 1C 3B D2 6E BA AE 4A A1 F9 51 29 E5 E5 46 70 F1
```

B.4.9 Example 9

In this example, the data string is the 1 000 000-byte string consisting of the ASCII-coded version of "a" repeated 10^6 times.

The hash-code is the following 160-bit string.

```
34 AA 97 3C D4 C4 DA A4 F6 1E EB 2B DB AD 27 31 65 34 01 6F
```

B.4.10 Example 10

In this example, the data string is the 112-byte string consisting of the ASCII-coded version of

```
"abcdefghbcdefghicdefghijdefghijkefghijklfghijklmghijklmn
hijklmnoijklmnopjklmnopqklmnopqrlmnopqrsmnopqrstnopqrstu"
```

(with no line break after the first n).

The hash-code is the following 160-bit string.

```
a4 9b 24 46 a0 2c 64 5b f4 19 f9 95 b6 70 91 25 3a 04 a2 59
```

B.4.11 Example 11

In this example, the data string is the 32-byte string consisting of the ASCII-coded version of

```
"abcdbcdecdefdefgefghfghighijhijk"
```

The hash-code is the following 160-bit string.

```
37 bc 52 21 ad e3 bc 09 ca d1 5e 47 84 f3 c7 05 14 54 b1 b3
```

B.5 Dedicated Hash-Function 4 (SHA-256)

B.5.1 Example 1

In this example, the data string is the empty string, i.e., the string of length zero.

The hash-code is the following 256-bit string.

```
e3b0c442 98fc1c14 9afbf4c8 996fb924 27ae41e4 649b934c a495991b 7852b855
```

B.5.2 Example 2

In this example, the data string consists of a single byte, namely the ASCII-coded version of the letter "a".

The hash-code is the following 256-bit string.

```
ca978112 ca1bbdca fac231b3 9a23dc4d a786eff8 147c4e72 b9807785 afee48bb
```

B.5.3 Example 3

In this example, the data string is the 3-byte string consisting of the ASCII-coded version of "abc". This is equivalent to the bit string "01100001 01100010 01100011".

After the padding process, the single 16-word block derived from the data string is as follows.

```
61626380 00000000 00000000 00000000 00000000 00000000 00000000 00000000
00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000018
```

The following are (hexadecimal representations of) the successive values of the variables X_0, X_1, X_2, X_3, X_4, X_5, X_6 and X_7.

```
init:  6a09e667 bb67ae85 3c6ef372 a54ff53a 510e527f 9b05688c 1f83d9ab 5be0cd19
  0  5d6aebcd 6a09e667 bb67ae85 3c6ef372 fa2a4622 510e527f 9b05688c 1f83d9ab
  1  5a6ad9ad 5d6aebcd 6a09e667 bb67ae85 78ce7989 fa2a4622 510e527f 9b05688c
  2  c8c347a7 5a6ad9ad 5d6aebcd 6a09e667 f92939eb 78ce7989 fa2a4622 510e527f
  3  d550f666 c8c347a7 5a6ad9ad 5d6aebcd 24e00850 f92939eb 78ce7989 fa2a4622
  4  04409a6a d550f666 c8c347a7 5a6ad9ad 43ada245 24e00850 f92939eb 78ce7989
  5  2b4209f5 04409a6a d550f666 c8c347a7 714260ad 43ada245 24e00850 f92939eb
  6  e5030380 2b4209f5 04409a6a d550f666 9b27a401 714260ad 43ada245 24e00850
  7  85a07b5f e5030380 2b4209f5 04409a6a 0c657a79 9b27a401 714260ad 43ada245
  8  8e04ecb9 85a07b5f e5030380 2b4209f5 32ca2d8c 0c657a79 9b27a401 714260ad
  9  8c87346b 8e04ecb9 85a07b5f e5030380 1cc92596 32ca2d8c 0c657a79 9b27a401
 10 4798a3f4 8c87346b 8e04ecb9 85a07b5f 436b23e8 1cc92596 32ca2d8c 0c657a79
 11 f71fc5a9 4798a3f4 8c87346b 8e04ecb9 816fd6e9 436b23e8 1cc92596 32ca2d8c
 12 87912990 f71fc5a9 4798a3f4 8c87346b 1e578218 816fd6e9 436b23e8 1cc92596
 13 d932eb16 87912990 f71fc5a9 4798a3f4 745a48de 1e578218 816fd6e9 436b23e8
 14 c0645fde d932eb16 87912990 f71fc5a9 0b92f20c 745a48de 1e578218 816fd6e9
 15 b0fa238e c0645fde d932eb16 87912990 07590dcd 0b92f20c 745a48de 1e578218
 16 21da9a9b b0fa238e c0645fde d932eb16 8034229c 07590dcd 0b92f20c 745a48de
 17 c2fbd9d1 21da9a9b b0fa238e c0645fde 846ee454 8034229c 07590dcd 0b92f20c
 18 fe777bbf c2fbd9d1 21da9a9b b0fa238e cc899961 846ee454 8034229c 07590dcd
 19 e1f20c33 fe777bbf c2fbd9d1 21da9a9b b0638179 cc899961 846ee454 8034229c
 20 9dc68b63 e1f20c33 fe777bbf c2fbd9d1 8ada8930 b0638179 cc899961 846ee454
 21 c2606d6d 9dc68b63 e1f20c33 fe777bbf e1257970 8ada8930 b0638179 cc899961
 22 a7a3623f c2606d6d 9dc68b63 e1f20c33 49f5114a e1257970 8ada8930 b0638179
 23 c5d53d8d a7a3623f c2606d6d 9dc68b63 aa47c347 49f5114a e1257970 8ada8930
 24 1c2c2838 c5d53d8d a7a3623f c2606d6d 2823ef91 aa47c347 49f5114a e1257970
 25 cde8037d 1c2c2838 c5d53d8d a7a3623f 14383d8e 2823ef91 aa47c347 49f5114a
 26 b62ec4bc cde8037d 1c2c2838 c5d53d8d c74c6516 14383d8e 2823ef91 aa47c347
 27 77d37528 b62ec4bc cde8037d 1c2c2838 edffbff8 c74c6516 14383d8e 2823ef91
 28 363482c9 77d37528 b62ec4bc cde8037d 6112a3b7 edffbff8 c74c6516 14383d8e
 29 a0060b30 363482c9 77d37528 b62ec4bc ade79437 6112a3b7 edffbff8 c74c6516
 30 ea992a22 a0060b30 363482c9 77d37528 0109ab3a ade79437 6112a3b7 edffbff8
 31 73b33bf5 ea992a22 a0060b30 363482c9 ba591112 0109ab3a ade79437 6112a3b7
 32 98e12507 73b33bf5 ea992a22 a0060b30 9cd9f5f6 ba591112 0109ab3a ade79437
 33 fe604df5 98e12507 73b33bf5 ea992a22 59249dd3 9cd9f5f6 ba591112 0109ab3a
 34 a9a7738c fe604df5 98e12507 73b33bf5 085f3833 59249dd3 9cd9f5f6 ba591112
 35 65a0cfe4 a9a7738c fe604df5 98e12507 f4b002d6 085f3833 59249dd3 9cd9f5f6
 36 41a65cb1 65a0cfe4 a9a7738c fe604df5 0772a26b f4b002d6 085f3833 59249dd3
 37 34df1604 41a65cb1 65a0cfe4 a9a7738c a507a53d 0772a26b f4b002d6 085f3833
 38 6dc57a8a 34df1604 41a65cb1 65a0cfe4 f0781bc8 a507a53d 0772a26b f4b002d6
 39 79ea687a 6dc57a8a 34df1604 41a65cb1 1efbc0a0 f0781bc8 a507a53d 0772a26b
 40 d6670766 79ea687a 6dc57a8a 34df1604 26352d63 1efbc0a0 f0781bc8 a507a53d
 41 df46652f d6670766 79ea687a 6dc57a8a 838b2711 26352d63 1efbc0a0 f0781bc8
 42 17aa0dfe df46652f d6670766 79ea687a decd4715 838b2711 26352d63 1efbc0a0
 43 9d4baf93 17aa0dfe df46652f d6670766 fda24c2e decd4715 838b2711 26352d63
 44 26628815 9d4baf93 17aa0dfe df46652f a80f11f0 fda24c2e decd4715 838b2711
 45 72ab4b91 26628815 9d4baf93 17aa0dfe b7755da1 a80f11f0 fda24c2e decd4715
 46 a14c14b0 72ab4b91 26628815 9d4baf93 d57b94a9 b7755da1 a80f11f0 fda24c2e
 47 4172328d a14c14b0 72ab4b91 26628815 fecf0bc6 d57b94a9 b7755da1 a80f11f0
 48 05757ceb 4172328d a14c14b0 72ab4b91 bd714038 fecf0bc6 d57b94a9 b7755da1
 49 f11bfaa8 05757ceb 4172328d a14c14b0 6e5c390c bd714038 fecf0bc6 d57b94a9
 50 7a0508a1 f11bfaa8 05757ceb 4172328d 52f1ccf7 6e5c390c bd714038 fecf0bc6
 51 886e7a22 7a0508a1 f11bfaa8 05757ceb 49231c1e 52f1ccf7 6e5c390c bd714038
 52 101fd28f 886e7a22 7a0508a1 f11bfaa8 529e7d00 49231c1e 52f1ccf7 6e5c390c
 53 f5702fdb 101fd28f 886e7a22 7a0508a1 9f4787c3 529e7d00 49231c1e 52f1ccf7
 54 3ec45cdb f5702fdb 101fd28f 886e7a22 e50e1b4f 9f4787c3 529e7d00 49231c1e
 55 38cc9913 3ec45cdb f5702fdb 101fd28f 54cb266b e50e1b4f 9f4787c3 529e7d00
 56 fcd1887b 38cc9913 3ec45cdb f5702fdb 9b5e906c 54cb266b e50e1b4f 9f4787c3
 57 c062d46f fcd1887b 38cc9913 3ec45cdb 7e44008e 9b5e906c 54cb266b e50e1b4f
 58 ffb70472 c062d46f fcd1887b 38cc9913 6d83bfc6 7e44008e 9b5e906c 54cb266b
```

```
59 b6ae8fff ffb70472 c062d46f fcd1887b b21bad3d 6d83bfc6 7e44008e 9b5e906c
60 b85e2ce9 b6ae8fff ffb70472 c062d46f 961f4894 b21bad3d 6d83bfc6 7e44008e
61 04d24d6c b85e2ce9 b6ae8fff ffb70472 948d25b6 961f4894 b21bad3d 6d83bfc6
62 d39a2165 04d24d6c b85e2ce9 b6ae8fff fb121210 948d25b6 961f4894 b21bad3d
63 506e3058 d39a2165 04d24d6c b85e2ce9 5ef50f24 fb121210 948d25b6 961f4894
```

The following eight words, Y_0, Y_1, Y_2, Y_3, Y_4, Y_5, Y_6 and Y_7, represent the output of the final iteration of the round-function.

$$Y_0 = 6a09e667 \boxplus 506e3058 = ba7816bf$$
$$Y_1 = bb67ae85 \boxplus d39a2165 = 8f01cfea$$
$$Y_2 = 3c6ef372 \boxplus 04d24d6c = 414140de$$
$$Y_3 = a54ff53a \boxplus b85e2ce9 = 5dae2223$$
$$Y_4 = 510e527f \boxplus 5ef50f24 = b00361a3$$
$$Y_5 = 9b05688c \boxplus fb121210 = 96177a9c$$
$$Y_6 = 1f83d9ab \boxplus 948d25b6 = b410ff61$$
$$Y_7 = 5be0cd19 \boxplus 961f4894 = f20015ad$$

The hash value is the following 256-bit string.

```
ba7816bf 8f01cfea 414140de 5dae2223 b00361a3 96177a9c b410ff61 f20015ad
```

B.5.4 Example 4

In this example, the data string is the 14-byte string consisting of the ASCII-coded version of

"message digest"

The hash value is the following 256-bit string.

```
f7846f55 cf23e14e ebeab5b4 e1550cad 5b509e33 48fbc4ef a3a1413d 393cb650
```

B.5.5 Example 5

In this example, the data string is the 26-byte string consisting of the ASCII-coded version of

"abcdefghijklmnopqrstuvwxyz"

The hash value is the following 256-bit string.

```
71c480df 93d6ae2f 1efad144 7c66c952 5e316218 cf51fc8d 9ed832f2 daf18b73
```

B.5.6 Example 6

In this example, the data string is the 62-byte string consisting of the ASCII-coded version of

"ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz0123456789"

The hash value is the following 256-bit string.

```
db4bfcbd 4da0cd85 a60c3c37 d3fbd880 5c77f15f c6b1fdfe 614ee0a7 c8fdb4c0
```

B.5.7 Example 7

In this example, the data string is the 80-byte string consisting of the ASCII-coded version of eight repetitions of

"1234567890"

The hash-code is the following 256-bit string.

```
f371bc4a 311f2b00 9eef952d d83ca80e 2b60026c 8e935592 d0f9c308 453c813e
```

B.5.8 Example 8

In this example, the data string is the 56-byte string consisting of the ASCII-coded version of

"abcdbcdecdefdefgefghfghighijhijkijkljklmklmnlmnomnopnopq"

After the padding process, the following two 16-word blocks are derived from the data string.

```
61626364 62636465 63646566 64656667 65666768 66676869 6768696a 68696a6b
696a6b6c 6a6b6c6d 6b6c6d6e 6c6d6e6f 6d6e6f70 6e6f7071 80000000 00000000

00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000
00000000 00000000 00000000 00000000 00000000 00000000 00000000 000001c0
```

The following are (hexadecimal representations of) the successive values of the variables X_0, X_1, X_2, X_3, X_4, X_5, X_6 and X_7 in the first block process.

```
init:  6a09e667 bb67ae85 3c6ef372 a54ff53a 510e527f 9b05688c 1f83d9ab 5be0cd19
  0  5d6aebb1 6a09e667 bb67ae85 3c6ef372 fa2a4606 510e527f 9b05688c 1f83d9ab
  1  2f2d5fcf 5d6aebb1 6a09e667 bb67ae85 4eb1cfce fa2a4606 510e527f 9b05688c
  2  97651825 2f2d5fcf 5d6aebb1 6a09e667 62d5c49e 4eb1cfce fa2a4606 510e527f
  3  4a8d64d5 97651825 2f2d5fcf 5d6aebb1 6494841b 62d5c49e 4eb1cfce fa2a4606
  4  f921c212 4a8d64d5 97651825 2f2d5fcf 05c4f88a 6494841b 62d5c49e 4eb1cfce
  5  55c8ef48 f921c212 4a8d64d5 97651825 7ff91c94 05c4f88a 6494841b 62d5c49e
  6  485835b7 55c8ef48 f921c212 4a8d64d5 39a5b2ca 7ff91c94 05c4f88a 6494841b
  7  d237e6db 485835b7 55c8ef48 f921c212 a401d211 39a5b2ca 7ff91c94 05c4f88a
  8  359f2bce d237e6db 485835b7 55c8ef48 c09ffec4 a401d211 39a5b2ca 7ff91c94
  9  3a474b2b 359f2bce d237e6db 485835b7 9037b3b8 c09ffec4 a401d211 39a5b2ca
 10 b8e2b4cb 3a474b2b 359f2bce d237e6db 443ed29e 9037b3b8 c09ffec4 a401d211
 11 1762215c b8e2b4cb 3a474b2b 359f2bce ee1c97a8 443ed29e 9037b3b8 c09ffec4
 12 101a4861 1762215c b8e2b4cb 3a474b2b 839a0fc9 ee1c97a8 443ed29e 9037b3b8
 13 d68e6457 101a4861 1762215c b8e2b4cb 9243f8af 839a0fc9 ee1c97a8 443ed29e
 14 dd16cbb3 d68e6457 101a4861 1762215c 9162aded 9243f8af 839a0fc9 ee1c97a8
 15 c3486194 dd16cbb3 d68e6457 101a4861 1496a54f 9162aded 9243f8af 839a0fc9
 16 b9dcacb1 c3486194 dd16cbb3 d68e6457 d4f64250 1496a54f 9162aded 9243f8af
 17 046a193e b9dcacb1 c3486194 dd16cbb3 885370b6 d4f64250 1496a54f 9162aded
 18 f402f058 046a193e b9dcacb1 c3486194 6f433549 885370b6 d4f64250 1496a54f
 19 2139187b f402f058 046a193e b9dcacb1 7c304206 6f433549 885370b6 d4f64250
 20 d70ac17d 2139187b f402f058 046a193e 7cc6b262 7c304206 6f433549 885370b6
 21 1b2b66b8 d70ac17d 2139187b f402f058 d560b028 7cc6b262 7c304206 6f433549
 22 ae2e2d4f 1b2b66b8 d70ac17d 2139187b f074fc95 d560b028 7cc6b262 7c304206
 23 59fce6b9 ae2e2d4f 1b2b66b8 d70ac17d a2c7d51d f074fc95 d560b028 7cc6b262
 24 4a885065 59fce6b9 ae2e2d4f 1b2b66b8 763597fb a2c7d51d f074fc95 d560b028
 25 573221da 4a885065 59fce6b9 ae2e2d4f 36e74eb4 763597fb a2c7d51d f074fc95
 26 128661da 573221da 4a885065 59fce6b9 1162d575 36e74eb4 763597fb a2c7d51d
 27 73f858af 128661da 573221da 4a885065 e77c797f 1162d575 36e74eb4 763597fb
 28 74bcf468 73f858af 128661da 573221da 72abaecd e77c797f 1162d575 36e74eb4
 29 df7151a0 74bcf468 73f858af 128661da 7629c961 72abaecd e77c797f 1162d575
 30 eb43f3ed df7151a0 74bcf468 73f858af 0635d880 7629c961 72abaecd e77c797f
 31 5581ab07 eb43f3ed df7151a0 74bcf468 df980085 0635d880 7629c961 72abaecd
 32 9fc905c8 5581ab07 eb43f3ed df7151a0 a94d2af1 df980085 0635d880 7629c961
 33 9ce5a62f 9fc905c8 5581ab07 eb43f3ed 6ef3b6bd a94d2af1 df980085 0635d880
 34 1df8e885 9ce5a62f 9fc905c8 5581ab07 2a9e048e 6ef3b6bd a94d2af1 df980085
 35 0786dce8 1df8e885 9ce5a62f 9fc905c8 de2a21d1 2a9e048e 6ef3b6bd a94d2af1
 36 2c55d3a6 0786dce8 1df8e885 9ce5a62f b067c1af de2a21d1 2a9e048e 6ef3b6bd
 37 a985b4be 2c55d3a6 0786dce8 1df8e885 f72bf353 b067c1af de2a21d1 2a9e048e
 38 91ac9d5d a985b4be 2c55d3a6 0786dce8 68d8d590 f72bf353 b067c1af de2a21d1
 39 7e4d30b8 91ac9d5d a985b4be 2c55d3a6 9f5b9b6d 68d8d590 f72bf353 b067c1af
 40 7e056794 7e4d30b8 91ac9d5d a985b4be 423b26c0 9f5b9b6d 68d8d590 f72bf353
 41 508a16ab 7e056794 7e4d30b8 91ac9d5d 45459d97 423b26c0 9f5b9b6d 68d8d590
 42 b62c7013 508a16ab 7e056794 7e4d30b8 80a92a00 45459d97 423b26c0 9f5b9b6d
 43 167361de b62c7013 508a16ab 7e056794 41dd3844 80a92a00 45459d97 423b26c0
 44 de71e2f2 167361de b62c7013 508a16ab ff61c636 41dd3844 80a92a00 45459d97
```

```
45 18f0d19d de71e2f2 167361de b62c7013 6b88472c ff61c636 41dd3844 80a92a00
46 165be9cd 18f0d19d de71e2f2 167361de a483f080 6b88472c ff61c636 41dd3844
47 13d82741 165be9cd 18f0d19d de71e2f2 a7802a4d a483f080 6b88472c ff61c636
48 017b9d99 13d82741 165be9cd 18f0d19d aeb10b60 a7802a4d a483f080 6b88472c
49 543c99a1 017b9d99 13d82741 165be9cd 16f134b6 aeb10b60 a7802a4d a483f080
50 758ca97a 543c99a1 017b9d99 13d82741 100cf2ea 16f134b6 aeb10b60 a7802a4d
51 81c1cde0 758ca97a 543c99a1 017b9d99 5c47eb7b 100cf2ea 16f134b6 aeb10b60
52 b8d55619 81c1cde0 758ca97a 543c99a1 1c806a61 5c47eb7b 100cf2ea 16f134b6
53 1d6de87a b8d55619 81c1cde0 758ca97a 3443bed4 1c806a61 5c47eb7b 100cf2ea
54 f907b313 1d6de87a b8d55619 81c1cde0 61a41711 3443bed4 1c806a61 5c47eb7b
55 9e57c4a0 f907b313 1d6de87a b8d55619 eec13548 61a41711 3443bed4 1c806a61
56 71629856 9e57c4a0 f907b313 1d6de87a 2f6c8c4e eec13548 61a41711 3443bed4
57 7c015a2c 71629856 9e57c4a0 f907b313 cb9d3dd0 2f6c8c4e eec13548 61a41711
58 921fccb6 7c015a2c 71629856 9e57c4a0 43d8a034 cb9d3dd0 2f6c8c4e eec13548
59 e18f259a 921fccb6 7c015a2c 71629856 51e15869 43d8a034 cb9d3dd0 2f6c8c4e
60 bcfce922 e18f259a 921fccb6 7c015a2c 962d8621 51e15869 43d8a034 cb9d3dd0
61 f6f443f8 bcfce922 e18f259a 921fccb6 acc75916 962d8621 51e15869 43d8a034
62 86126910 f6f443f8 bcfce922 e18f259a 2fc08f85 acc75916 962d8621 51e15869
63 1bdc6f6f 86126910 f6f443f8 bcfce922 25d2430a 2fc08f85 acc75916 962d8621
```

The following eight words, Y_0, Y_1, Y_2, Y_3, Y_4, Y_5, Y_6 and Y_7, represent the output of the round-function in the first block process.

$$Y_0 = \text{6a09e667} \boxplus \text{1bdc6f6f} = \text{85e655d6}$$
$$Y_1 = \text{bb67ae85} \boxplus \text{86126910} = \text{417a1795}$$
$$Y_2 = \text{3c6ef372} \boxplus \text{f6f443f8} = \text{3363376a}$$
$$Y_3 = \text{a54ff53a} \boxplus \text{bcfce922} = \text{624cde5c}$$
$$Y_4 = \text{510e527f} \boxplus \text{25d2430a} = \text{76e09589}$$
$$Y_5 = \text{9b05688c} \boxplus \text{2fc08f85} = \text{cac5f811}$$
$$Y_6 = \text{1f83d9ab} \boxplus \text{acc75916} = \text{cc4b32c1}$$
$$Y_7 = \text{5be0cd19} \boxplus \text{962d8621} = \text{f20e533a}$$

The following are (hexadecimal representations of) the successive values of the variables Y_0, Y_1, Y_2, Y_3, Y_4, Y_5, Y_6 and Y_7 in the second block process.

```
init:  85e655d6 417a1795 3363376a 624cde5c 76e09589 cac5f811 cc4b32c1 f20e533a
  0  7c20c838 85e655d6 417a1795 3363376a 4670ae6e 76e09589 cac5f811 cc4b32c1
  1  7c3c0f86 7c20c838 85e655d6 417a1795 8c51be64 4670ae6e 76e09589 cac5f811
  2  fd1eebdc 7c3c0f86 7c20c838 85e655d6 af71b9ea 8c51be64 4670ae6e 76e09589
  3  f268faa9 fd1eebdc 7c3c0f86 7c20c838 e20362ef af71b9ea 8c51be64 4670ae6e
  4  185a5d79 f268faa9 fd1eebdc 7c3c0f86 8dff3001 e20362ef af71b9ea 8c51be64
  5  3eeb6c06 185a5d79 f268faa9 fd1eebdc fe20cda6 8dff3001 e20362ef af71b9ea
  6  89bba3f1 3eeb6c06 185a5d79 f268faa9 0a34df03 fe20cda6 8dff3001 e20362ef
  7  bf9a93a0 89bba3f1 3eeb6c06 185a5d79 059abdd1 0a34df03 fe20cda6 8dff3001
  8  2c096744 bf9a93a0 89bba3f1 3eeb6c06 abfa465b 059abdd1 0a34df03 fe20cda6
  9  2d964e86 2c096744 bf9a93a0 89bba3f1 aa27ed82 abfa465b 059abdd1 0a34df03
 10 5b35025b 2d964e86 2c096744 bf9a93a0 10e77723 aa27ed82 abfa465b 059abdd1
 11 5eb4ec40 5b35025b 2d964e86 2c096744 e11b4548 10e77723 aa27ed82 abfa465b
 12 35ee996d 5eb4ec40 5b35025b 2d964e86 5c24e2a2 e11b4548 10e77723 aa27ed82
 13 d74080fa 35ee996d 5eb4ec40 5b35025b 68aa893f 5c24e2a2 e11b4548 10e77723
 14 0cea5cbc d74080fa 35ee996d 5eb4ec40 60356548 68aa893f 5c24e2a2 e11b4548
 15 16a8cc79 0cea5cbc d74080fa 35ee996d 0fcb1f6f 60356548 68aa893f 5c24e2a2
 16 f16f634e 16a8cc79 0cea5cbc d74080fa 8b21cdc1 0fcb1f6f 60356548 68aa893f
 17 23dcb6c2 f16f634e 16a8cc79 0cea5cbc ca9182d3 8b21cdc1 0fcb1f6f 60356548
 18 dcff40fd 23dcb6c2 f16f634e 16a8cc79 69bf7b95 ca9182d3 8b21cdc1 0fcb1f6f
 19 76f1a2bc dcff40fd 23dcb6c2 f16f634e 0dc84bb1 69bf7b95 ca9182d3 8b21cdc1
 20 20aad899 76f1a2bc dcff40fd 23dcb6c2 cc4769f2 0dc84bb1 69bf7b95 ca9182d3
 21 d44dc81a 20aad899 76f1a2bc dcff40fd 5bace62d cc4769f2 0dc84bb1 69bf7b95
 22 f13ae55b d44dc81a 20aad899 76f1a2bc 966aa287 5bace62d cc4769f2 0dc84bb1
 23 a4195b91 f13ae55b d44dc81a 20aad899 eddbd6ed 966aa287 5bace62d cc4769f2
 24 4984fa79 a4195b91 f13ae55b d44dc81a a530d939 eddbd6ed 966aa287 5bace62d
 25 aa6cb982 4984fa79 a4195b91 f13ae55b 0b5eeea4 a530d939 eddbd6ed 966aa287
 26 9450fbbc aa6cb982 4984fa79 a4195b91 09166dda 0b5eeea4 a530d939 eddbd6ed
```

```
27 0d936bab 9450fbbc aa6cb982 4984fa79 6e495d4b 09166dda 0b5eeea4 a530d939
28 d958b529 0d936bab 9450fbbc aa6cb982 c2fa99b1 6e495d4b 09166dda 0b5eeea4
29 1cfa5eb0 d958b529 0d936bab 9450fbbc 6c49db9f c2fa99b1 6e495d4b 09166dda
30 02ef3a5f 1cfa5eb0 d958b529 0d936bab 5da10665 6c49db9f c2fa99b1 6e495d4b
31 b0eab1c5 02ef3a5f 1cfa5eb0 d958b529 f6d93952 5da10665 6c49db9f c2fa99b1
32 0bfba73c b0eab1c5 02ef3a5f 1cfa5eb0 8b99e3a9 f6d93952 5da10665 6c49db9f
33 4bd1df96 0bfba73c b0eab1c5 02ef3a5f 905e44ac 8b99e3a9 f6d93952 5da10665
34 9907f1b6 4bd1df96 0bfba73c b0eab1c5 66c3043d 905e44ac 8b99e3a9 f6d93952
35 ecde4e0d 9907f1b6 4bd1df96 0bfba73c 5dc119e6 66c3043d 905e44ac 8b99e3a9
36 2f11c939 ecde4e0d 9907f1b6 4bd1df96 fed4ce1d 5dc119e6 66c3043d 905e44ac
37 d949682b 2f11c939 ecde4e0d 9907f1b6 32d99008 fed4ce1d 5dc119e6 66c3043d
38 adca7a96 d949682b 2f11c939 ecde4e0d c6cce4ff 32d99008 fed4ce1d 5dc119e6
39 221b8a5a adca7a96 d949682b 2f11c939 0b82c5eb c6cce4ff 32d99008 fed4ce1d
40 12d97845 221b8a5a adca7a96 d949682b e4213ca2 0b82c5eb c6cce4ff 32d99008
41 2c794876 12d97845 221b8a5a adca7a96 ff6759ba e4213ca2 0b82c5eb c6cce4ff
42 8300fca2 2c794876 12d97845 221b8a5a e0e3457c ff6759ba e4213ca2 0b82c5eb
43 f2ad6322 8300fca2 2c794876 12d97845 cc48c7f3 e0e3457c ff6759ba e4213ca2
44 0f154e11 f2ad6322 8300fca2 2c794876 6f9517cb cc48c7f3 e0e3457c ff6759ba
45 104a7db4 0f154e11 f2ad6322 8300fca2 5348e8f6 6f9517cb cc48c7f3 e0e3457c
46 0b3303a7 104a7db4 0f154e11 f2ad6322 bbe1c39a 5348e8f6 6f9517cb cc48c7f3
47 d7354d5b 0b3303a7 104a7db4 0f154e11 aad55b6b bbe1c39a 5348e8f6 6f9517cb
48 b736d7a6 d7354d5b 0b3303a7 104a7db4 68f25260 aad55b6b bbe1c39a 5348e8f6
49 2748e5ec b736d7a6 d7354d5b 0b3303a7 d4b58576 68f25260 aad55b6b bbe1c39a
50 d8aabcf9 2748e5ec b736d7a6 d7354d5b 27844711 d4b58576 68f25260 aad55b6b
51 1a6bcf6a d8aabcf9 2748e5ec b736d7a6 ff5e99d0 27844711 d4b58576 68f25260
52 4eca6fa0 1a6bcf6a d8aabcf9 2748e5ec 989ed071 ff5e99d0 27844711 d4b58576
53 ec02560a 4eca6fa0 1a6bcf6a d8aabcf9 7151df8e 989ed071 ff5e99d0 27844711
54 d9f0c115 ec02560a 4eca6fa0 1a6bcf6a 624150c4 7151df8e 989ed071 ff5e99d0
55 92952710 d9f0c115 ec02560a 4eca6fa0 226806d6 624150c4 7151df8e 989ed071
56 20d4d0e4 92952710 d9f0c115 ec02560a 4e515a4d 226806d6 624150c4 7151df8e
57 4348eb1f 20d4d0e4 92952710 d9f0c115 c21eddf9 4e515a4d 226806d6 624150c4
58 286fe5f0 4348eb1f 20d4d0e4 92952710 54076664 c21eddf9 4e515a4d 226806d6
59 1c4cddd9 286fe5f0 4348eb1f 20d4d0e4 f487a853 54076664 c21eddf9 4e515a4d
60 a9f181dd 1c4cddd9 286fe5f0 4348eb1f 27ccb387 f487a853 54076664 c21eddf9
61 b25cef29 a9f181dd 1c4cddd9 286fe5f0 2aa1bb13 27ccb387 f487a853 54076664
62 908c2123 b25cef29 a9f181dd 1c4cddd9 9a392956 2aa1bb13 27ccb387 f487a853
63 9ea7148b 908c2123 b25cef29 a9f181dd 2c5c4ed0 9a392956 2aa1bb13 27ccb387
```

The following eight words, Y_0, Y_1, Y_2, Y_3, Y_4, Y_5, Y_6 and Y_7, represent the output of the final iteration of the round-function.

$$
\begin{aligned}
Y_0 &= 85e655d6 \boxplus 9ea7148b = 248d6a61 \\
Y_1 &= 417a1795 \boxplus 908c2123 = d20638b8 \\
Y_2 &= 3363376a \boxplus b25cef29 = e5c02693 \\
Y_3 &= 624cde5c \boxplus a9f181dd = 0c3e6039 \\
Y_4 &= 76e09589 \boxplus 2c5c4ed0 = a33ce459 \\
Y_5 &= cac5f811 \boxplus 9a392956 = 64ff2167 \\
Y_6 &= cc4b32c1 \boxplus 2aa1bb13 = f6ecedd4 \\
Y_7 &= f20e533a \boxplus 27ccb387 = 19db06c1
\end{aligned}
$$

The hash value for this message is

```
248d6a61 d20638b8 e5c02693 0c3e6039 a33ce459 64ff2167 f6ecedd4 19db06c1
```

B.5.9 Example 9

In this example, the data string is the 1 000 000-byte string consisting of the ASCII-coded version of “a” repeated 10^6 times.

The hash-code is the following 256-bit string.

```
cdc76e5c 9914fb92 81a1c7e2 84d73e67 f1809a48 a497200e 046d39cc c7112cd0
```

B.5.10 Example 10

In this example, the data string is the 112-byte string consisting of the ASCII-coded version of

"abcdefghbcdefghicdefghijdefghijkefghijklfghijklmghijklmn
hijklmnoijklmnopjklmnopqklmnopqrlmnopqrsmnopqrstnopqrstu"

(with no line break after the first n).

The hash-code is the following 256-bit string.

```
cf5b16a7 78af8380 036ce59e 7b049237 0b249b11 e8f07a51 afac4503 7afee9d1
```

B.5.11 Example 11

In this example, the data string is the 32-byte string consisting of the ASCII-coded version of

"abcdbcdecdefdefgefghfghighijhijk"

The hash-code is the following 256-bit string.

```
b09cbd26 3b043f00 0c5befca a40bc2f5 5a4785e0 24e5deb7 49b56061 eafb65e9
```

B.6 Dedicated Hash-Function 5 (SHA-512)

B.6.1 Example 1

In this example, the data string is the empty string, i.e. the string of length zero.

The hash-code is the following 512-bit string.

```
cf83e1357eefb8bd f1542850d66d8007 d620e4050b5715dc 83f4a921d36ce9ce
47d0d13c5d85f2b0 ff8318d2877eec2f 63b931bd47417a81 a538327af927da3e
```

B.6.2 Example 2

In this example, the data string consists of a single byte, namely the ASCII-coded version of the letter "a".

The hash-code is the following 512-bit string.

```
1f40fc92da241694 750979ee6cf582f2 d5d7d28e18335de0 5abc54d0560e0f53
02860c652bf08d56 0252aa5e74210546 f369fbbbce8c12cf c7957b2652fe9a75
```

B.6.3 Example 3

In this example, the data string is the 3-byte string consisting of the ASCII-coded version of "abc". This is equivalent to the bit string "01100001 01100010 01100011".

After the padding process, the single 16-word block derived from the data string is as follows.

```
61626380 00000000 00000000 00000000 00000000 00000000 00000000 00000000
00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000
00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000
00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000018
```

The following are (hexadecimal representations of) the successive values of the variables X_0, X_1, X_2, X_3, X_4, X_5, X_6 and X_7.

```
Init  6a09e667f3bcc908 bb67ae8584caa73b 3c6ef372fe94f82b a54ff53a5f1d36f1
   510e527fade682d1 9b05688c2b3e6c1f 1f83d9abfb41bd6b 5be0cd19137e2179
 0  f6afceb8bcfcddf5 6a09e667f3bcc908 bb67ae8584caa73b 3c6ef372fe94f82b
   58cb02347ab51f91 510e527fade682d1 9b05688c2b3e6c1f 1f83d9abfb41bd6b
 1  1320f8c9fb872cc0 f6afceb8bcfcddf5 6a09e667f3bcc908 bb67ae8584caa73b
```

```
  c3d4ebfd48650ffa 58cb02347ab51f91 510e527fade682d1 9b05688c2b3e6c1f
2  ebcffc07203d91f3 1320f8c9fb872cc0 f6afceb8bcfcddf5 6a09e667f3bcc908
  dfa9b239f2697812 c3d4ebfd48650ffa 58cb02347ab51f91 510e527fade682d1
3  5a83cb3e80050e82 ebcffc07203d91f3 1320f8c9fb872cc0 f6afceb8bcfcddf5
  0b47b4bb1928990e dfa9b239f2697812 c3d4ebfd48650ffa 58cb02347ab51f91
4  b680953951604860 5a83cb3e80050e82 ebcffc07203d91f3 1320f8c9fb872cc0
  745aca4a342ed2e2 0b47b4bb1928990e dfa9b239f2697812 c3d4ebfd48650ffa
5  af573b02403e89cd b680953951604860 5a83cb3e80050e82 ebcffc07203d91f3
  96f60209b6dc35ba 745aca4a342ed2e2 0b47b4bb1928990e dfa9b239f2697812
6  c4875b0c7abc076b af573b02403e89cd b680953951604860 5a83cb3e80050e82
  5a6c781f54dcc00c 96f60209b6dc35ba 745aca4a342ed2e2 0b47b4bb1928990e
7  8093d195e0054fa3 c4875b0c7abc076b af573b02403e89cd b680953951604860
  86f67263a0f0ec0a 5a6c781f54dcc00c 96f60209b6dc35ba 745aca4a342ed2e2
8  f1eca5544cb89225 8093d195e0054fa3 c4875b0c7abc076b af573b02403e89cd
  d0403c398fc40002 86f67263a0f0ec0a 5a6c781f54dcc00c 96f60209b6dc35ba
9  81782d4a5db48f03 f1eca5544cb89225 8093d195e0054fa3 c4875b0c7abc076b
  00091f460be46c52 d0403c398fc40002 86f67263a0f0ec0a 5a6c781f54dcc00c
10  69854c4aa0f25b59 81782d4a5db48f03 f1eca5544cb89225 8093d195e0054fa3
  d375471bde1ba3f4 00091f460be46c52 d0403c398fc40002 86f67263a0f0ec0a
11 db0a9963f80c2eaa 69854c4aa0f25b59 81782d4a5db48f03 f1eca5544cb89225
  475975b91a7a462c d375471bde1ba3f4 00091f460be46c52 d0403c398fc40002
12 5e41214388186c14 db0a9963f80c2eaa 69854c4aa0f25b59 81782d4a5db48f03
  cdf3bff2883fc9d9 475975b91a7a462c d375471bde1ba3f4 00091f460be46c52
13 44249631255d2ca0 5e41214388186c14 db0a9963f80c2eaa 69854c4aa0f25b59
  860acf9effba6f61 cdf3bff2883fc9d9 475975b91a7a462c d375471bde1ba3f4
14 fa967eed85a08028 44249631255d2ca0 5e41214388186c14 db0a9963f80c2eaa
  874bfe5f6aae9f2f 860acf9effba6f61 cdf3bff2883fc9d9 475975b91a7a462c
15 0ae07c86b1181c75 fa967eed85a08028 44249631255d2ca0 5e41214388186c14
  a77b7c035dd4c161 874bfe5f6aae9f2f 860acf9effba6f61 cdf3bff2883fc9d9
16 caf81a425d800537 0ae07c86b1181c75 fa967eed85a08028 44249631255d2ca0
  2deecc6b39d64d78 a77b7c035dd4c161 874bfe5f6aae9f2f 860acf9effba6f61
17 4725be249ad19e6b caf81a425d800537 0ae07c86b1181c75 fa967eed85a08028
  f47e8353f8047455 2deecc6b39d64d78 a77b7c035dd4c161 874bfe5f6aae9f2f
18 3c4b4104168e3edb 4725be249ad19e6b caf81a425d800537 0ae07c86b1181c75
  29695fd88d81dbd0 f47e8353f8047455 2deecc6b39d64d78 a77b7c035dd4c161
19 9a3fb4d38ab6cf06 3c4b4104168e3edb 4725be249ad19e6b caf81a425d800537
  f14998dd5f70767e 29695fd88d81dbd0 f47e8353f8047455 2deecc6b39d64d78
20 8dc5ae65569d3855 9a3fb4d38ab6cf06 3c4b4104168e3edb 4725be249ad19e6b
  4bb9e66d1145bfdc f14998dd5f70767e 29695fd88d81dbd0 f47e8353f8047455
21 da34d6673d452dcf 8dc5ae65569d3855 9a3fb4d38ab6cf06 3c4b4104168e3edb
  8e30ff09ad488753 4bb9e66d1145bfdc f14998dd5f70767e 29695fd88d81dbd0
22 3e2644567b709a78 da34d6673d452dcf 8dc5ae65569d3855 9a3fb4d38ab6cf06
  0ac2b11da8f571c6 8e30ff09ad488753 4bb9e66d1145bfdc f14998dd5f70767e
23 4f6877b58fe55484 3e2644567b709a78 da34d6673d452dcf 8dc5ae65569d3855
  c66005f87db55233 0ac2b11da8f571c6 8e30ff09ad488753 4bb9e66d1145bfdc
24 9aff71163fa3a940 4f6877b58fe55484 3e2644567b709a78 da34d6673d452dcf
  d3ecf13769180e6f c66005f87db55233 0ac2b11da8f571c6 8e30ff09ad488753
25 0bc5f791f8e6816b 9aff71163fa3a940 4f6877b58fe55484 3e2644567b709a78
  6ddf1fd7edcce336 d3ecf13769180e6f c66005f87db55233 0ac2b11da8f571c6
26 884c3bc27bc4f941 0bc5f791f8e6816b 9aff71163fa3a940 4f6877b58fe55484
  e6e48c9a8e948365 6ddf1fd7edcce336 d3ecf13769180e6f c66005f87db55233
27 eab4a9e5771b8d09 884c3bc27bc4f941 0bc5f791f8e6816b 9aff71163fa3a940
  09068a4e255a0dac e6e48c9a8e948365 6ddf1fd7edcce336 d3ecf13769180e6f
28 e62349090f47d30a eab4a9e5771b8d09 884c3bc27bc4f941 0bc5f791f8e6816b
  0fcdf99710f21584 09068a4e255a0dac e6e48c9a8e948365 6ddf1fd7edcce336
29 74bf40f869094c63 e62349090f47d30a eab4a9e5771b8d09 884c3bc27bc4f941
  f0aec2fe1437f085 0fcdf99710f21584 09068a4e255a0dac e6e48c9a8e948365
30 4c4fbbb75f1873a6 74bf40f869094c63 e62349090f47d30a eab4a9e5771b8d09
  73e025d91b9efea3 f0aec2fe1437f085 0fcdf99710f21584 09068a4e255a0dac
31 ff4d3f1f0d46a736 4c4fbbb75f1873a6 74bf40f869094c63 e62349090f47d30a
  3cd388e119e8162e 73e025d91b9efea3 f0aec2fe1437f085 0fcdf99710f21584
32 a0509015ca08c8d4 ff4d3f1f0d46a736 4c4fbbb75f1873a6 74bf40f869094c63
  e1034573654a106f 3cd388e119e8162e 73e025d91b9efea3 f0aec2fe1437f085
```

```
33 60d4e6995ed91fe6 a0509015ca08c8d4 ff4d3f1f0d46a736 4c4fbbb75f1873a6
  efabbd8bf47c041a e1034573654a106f 3cd388e119e8162e 73e025d91b9efea3
34 2c59ec7743632621 60d4e6995ed91fe6 a0509015ca08c8d4 ff4d3f1f0d46a736
  0fbae670fa780fd3 efabbd8bf47c041a e1034573654a106f 3cd388e119e8162e
35 1a081afc59fdbc2c 2c59ec7743632621 60d4e6995ed91fe6 a0509015ca08c8d4
  f098082f502b44cd 0fbae670fa780fd3 efabbd8bf47c041a e1034573654a106f
36 88df85b0bbe77514 1a081afc59fdbc2c 2c59ec7743632621 60d4e6995ed91fe6
  8fbfd0162bbf4675 f098082f502b44cd 0fbae670fa780fd3 efabbd8bf47c041a
37 002bb8e4cd989567 88df85b0bbe77514 1a081afc59fdbc2c 2c59ec7743632621
  66adcfa249ac7bbd 8fbfd0162bbf4675 f098082f502b44cd 0fbae670fa780fd3
38 b3bb8542b3376de5 002bb8e4cd989567 88df85b0bbe77514 1a081afc59fdbc2c
  b49596c20feba7de 66adcfa249ac7bbd 8fbfd0162bbf4675 f098082f502b44cd
39 8e01e125b855d225 b3bb8542b3376de5 002bb8e4cd989567 88df85b0bbe77514
  0c710a47ba6a567b b49596c20feba7de 66adcfa249ac7bbd 8fbfd0162bbf4675
40 b01521dd6a6be12c 8e01e125b855d225 b3bb8542b3376de5 002bb8e4cd989567
  169008b3a4bb170b 0c710a47ba6a567b b49596c20feba7de 66adcfa249ac7bbd
41 e96f89dd48cbd851 b01521dd6a6be12c 8e01e125b855d225 b3bb8542b3376de5
  f0996439e7b50cb1 169008b3a4bb170b 0c710a47ba6a567b b49596c20feba7de
42 bc05ba8de5d3c480 e96f89dd48cbd851 b01521dd6a6be12c 8e01e125b855d225
  639cb938e14dc190 f0996439e7b50cb1 169008b3a4bb170b 0c710a47ba6a567b
43 35d7e7f41defcbd5 bc05ba8de5d3c480 e96f89dd48cbd851 b01521dd6a6be12c
  cc5100997f5710f2 639cb938e14dc190 f0996439e7b50cb1 169008b3a4bb170b
44 c47c9d5c7ea8a234 35d7e7f41defcbd5 bc05ba8de5d3c480 e96f89dd48cbd851
  858d832ae0e8911c cc5100997f5710f2 639cb938e14dc190 f0996439e7b50cb1
45 021fbadbabab5ac6 c47c9d5c7ea8a234 35d7e7f41defcbd5 bc05ba8de5d3c480
  e95c2a57572d64d9 858d832ae0e8911c cc5100997f5710f2 639cb938e14dc190
46 f61e672694de2d67 021fbadbabab5ac6 c47c9d5c7ea8a234 35d7e7f41defcbd5
  c6bc35740d8daa9a e95c2a57572d64d9 858d832ae0e8911c cc5100997f5710f2
47 6b69fc1bb482feac f61e672694de2d67 021fbadbabab5ac6 c47c9d5c7ea8a234
  35264334c03ac8ad c6bc35740d8daa9a e95c2a57572d64d9 858d832ae0e8911c
48 571f323d96b3a047 6b69fc1bb482feac f61e672694de2d67 021fbadbabab5ac6
  271580ed6c3e5650 35264334c03ac8ad c6bc35740d8daa9a e95c2a57572d64d9
49 ca9bd862c5050918 571f323d96b3a047 6b69fc1bb482feac f61e672694de2d67
  dfe091dab182e645 271580ed6c3e5650 35264334c03ac8ad c6bc35740d8daa9a
50 813a43dd2c502043 ca9bd862c5050918 571f323d96b3a047 6b69fc1bb482feac
  07a0d8ef821c5e1a dfe091dab182e645 271580ed6c3e5650 35264334c03ac8ad
51 d43f83727325dd77 813a43dd2c502043 ca9bd862c5050918 571f323d96b3a047
  483f80a82eaee23e 07a0d8ef821c5e1a dfe091dab182e645 271580ed6c3e5650
52 03df11b32d42e203 d43f83727325dd77 813a43dd2c502043 ca9bd862c5050918
  504f94e40591cffa 483f80a82eaee23e 07a0d8ef821c5e1a dfe091dab182e645
53 d63f68037ddf06aa 03df11b32d42e203 d43f83727325dd77 813a43dd2c502043
  a6781efe1aa1ce02 504f94e40591cffa 483f80a82eaee23e 07a0d8ef821c5e1a
54 f650857b5babda4d d63f68037ddf06aa 03df11b32d42e203 d43f83727325dd77
  9ccfb31a86df0f86 a6781efe1aa1ce02 504f94e40591cffa 483f80a82eaee23e
55 63b460e42748817e f650857b5babda4d d63f68037ddf06aa 03df11b32d42e203
  c6b4dd2a9931c509 9ccfb31a86df0f86 a6781efe1aa1ce02 504f94e40591cffa
56 7a52912943d52b05 63b460e42748817e f650857b5babda4d d63f68037ddf06aa
  d2e89bbd91e00be0 c6b4dd2a9931c509 9ccfb31a86df0f86 a6781efe1aa1ce02
57 4b81c3aec976ea4b 7a52912943d52b05 63b460e42748817e f650857b5babda4d
  70505988124351ac d2e89bbd91e00be0 c6b4dd2a9931c509 9ccfb31a86df0f86
58 581ecb3355dcd9b8 4b81c3aec976ea4b 7a52912943d52b05 63b460e42748817e
  6a3c9b0f71c8bf36 70505988124351ac d2e89bbd91e00be0 c6b4dd2a9931c509
59 2c074484ef1eac8c 581ecb3355dcd9b8 4b81c3aec976ea4b 7a52912943d52b05
  4797cde4ed370692 6a3c9b0f71c8bf36 70505988124351ac d2e89bbd91e00be0
60 3857dfd2fc37d3ba 2c074484ef1eac8c 581ecb3355dcd9b8 4b81c3aec976ea4b
  a6af4e9c9f807e51 4797cde4ed370692 6a3c9b0f71c8bf36 70505988124351ac
61 cfcd928c5424e2b6 3857dfd2fc37d3ba 2c074484ef1eac8c 581ecb3355dcd9b8
  09aee5bda1644de5 a6af4e9c9f807e51 4797cde4ed370692 6a3c9b0f71c8bf36
62 a81dedbb9f19e643 cfcd928c5424e2b6 3857dfd2fc37d3ba 2c074484ef1eac8c
  84058865d60a05fa 09aee5bda1644de5 a6af4e9c9f807e51 4797cde4ed370692
63 ab44e86276478d85 a81dedbb9f19e643 cfcd928c5424e2b6 3857dfd2fc37d3ba
  cd881ee59ca6bc53 84058865d60a05fa 09aee5bda1644de5 a6af4e9c9f807e51
64 5a806d7e9821a501 ab44e86276478d85 a81dedbb9f19e643 cfcd928c5424e2b6
```

```
  aa84b086688a5c45 cd881ee59ca6bc53 84058865d60a05fa 09aee5bda1644de5
65 eeb9c21bb0102598 5a806d7e9821a501 ab44e86276478d85 a81dedbb9f19e643
  3b5fed0d6a1f96e1 aa84b086688a5c45 cd881ee59ca6bc53 84058865d60a05fa
66 46c4210ab2cc155d eeb9c21bb0102598 5a806d7e9821a501 ab44e86276478d85
  29fab5a7bff53366 3b5fed0d6a1f96e1 aa84b086688a5c45 cd881ee59ca6bc53
67 54ba35cf56a0340e 46c4210ab2cc155d eeb9c21bb0102598 5a806d7e9821a501
  1c66f46d95690bcf 29fab5a7bff53366 3b5fed0d6a1f96e1 aa84b086688a5c45
68 181839d609c79748 54ba35cf56a0340e 46c4210ab2cc155d eeb9c21bb0102598
  0ada78ba2d446140 1c66f46d95690bcf 29fab5a7bff53366 3b5fed0d6a1f96e1
69 fb6aaae5d0b6a447 181839d609c79748 54ba35cf56a0340e 46c4210ab2cc155d
  e3711cb6564d112d 0ada78ba2d446140 1c66f46d95690bcf 29fab5a7bff53366
70 7652c579cb60f19c fb6aaae5d0b6a447 181839d609c79748 54ba35cf56a0340e
  aff62c9665ff80fa e3711cb6564d112d 0ada78ba2d446140 1c66f46d95690bcf
71 f15e9664b2803575 7652c579cb60f19c fb6aaae5d0b6a447 181839d609c79748
  947c3dfafee570ef aff62c9665ff80fa e3711cb6564d112d 0ada78ba2d446140
72 358406d165aee9ab f15e9664b2803575 7652c579cb60f19c fb6aaae5d0b6a447
  8c7b5fd91a794ca0 947c3dfafee570ef aff62c9665ff80fa e3711cb6564d112d
73 20878dcd29cdfaf5 358406d165aee9ab f15e9664b2803575 7652c579cb60f19c
  054d3536539948d0 8c7b5fd91a794ca0 947c3dfafee570ef aff62c9665ff80fa
74 33d48dabb5521de2 20878dcd29cdfaf5 358406d165aee9ab f15e9664b2803575
  2ba18245b50de4cf 054d3536539948d0 8c7b5fd91a794ca0 947c3dfafee570ef
75 c8960e6be864b916 33d48dabb5521de2 20878dcd29cdfaf5 358406d165aee9ab
  995019a6ff3ba3de 2ba18245b50de4cf 054d3536539948d0 8c7b5fd91a794ca0
76 654ef9abec389ca9 c8960e6be864b916 33d48dabb5521de2 20878dcd29cdfaf5
  ceb9fc3691ce8326 995019a6ff3ba3de 2ba18245b50de4cf 054d3536539948d0
77 d67806db8b148677 654ef9abec389ca9 c8960e6be864b916 33d48dabb5521de2
  25c96a7768fb2aa3 ceb9fc3691ce8326 995019a6ff3ba3de 2ba18245b50de4cf
78 10d9c4c4295599f6 d67806db8b148677 654ef9abec389ca9 c8960e6be864b916
  9bb4d39778c07f9e 25c96a7768fb2aa3 ceb9fc3691ce8326 995019a6ff3ba3de
79 73a54f399fa4b1b2 10d9c4c4295599f6 d67806db8b148677 654ef9abec389ca9
  d08446aa79693ed7 9bb4d39778c07f9e 25c96a7768fb2aa3 ceb9fc3691ce8326
```

The following eight words, Y_0, Y_1, Y_2, Y_3, Y_4, Y_5, Y_6 and Y_7, represent the output of the final iteration of the round-function.

$$
\begin{aligned}
Y_0 &= \texttt{6a09e667f3bcc908} \boxplus \texttt{73a54f399fa4b1b2} = \texttt{ddaf35a193617aba} \\
Y_1 &= \texttt{bb67ae8584caa73b} \boxplus \texttt{10d9c4c4295599f6} = \texttt{cc417349ae204131} \\
Y_2 &= \texttt{3c6ef372fe94f82b} \boxplus \texttt{d67806db8b148677} = \texttt{12e6fa4e89a97ea2} \\
Y_3 &= \texttt{a54ff53a5f1d36f1} \boxplus \texttt{654ef9abec389ca9} = \texttt{0a9eeee64b55d39a} \\
Y_4 &= \texttt{510e527fade682d1} \boxplus \texttt{d08446aa79693ed7} = \texttt{2192992a274fc1a8} \\
Y_5 &= \texttt{9b05688c2b3e6c1f} \boxplus \texttt{9bb4d39778c07f9e} = \texttt{36ba3c23a3feebbd} \\
Y_6 &= \texttt{1f83d9abfb41bd6b} \boxplus \texttt{25c96a7768fb2aa3} = \texttt{454d4423643ce80e} \\
Y_7 &= \texttt{5be0cd19137e2179} \boxplus \texttt{ceb9fc3691ce8326} = \texttt{2a9ac94fa54ca49f}
\end{aligned}
$$

The hash value is the following 512-bit string.

```
ddaf35a193617aba cc417349ae204131 12e6fa4e89a97ea2 0a9eeee64b55d39a
2192992a274fc1a8 36ba3c23a3feebbd 454d4423643ce80e 2a9ac94fa54ca49f
```

B.6.4 Example 4

In this example, the data string is the 14-byte string consisting of the ASCII-coded version of

"message digest"

The hash-code is the following 512-bit string.

```
107dbf389d9e9f71 a3a95f6c055b9251 bc5268c2be16d6c1 3492ea45b0199f33
09e16455ab1e9611 8e8a905d5597b720 38ddb372a8982604 6de66687bb420e7c
```

B.6.5 Example 5

In this example, the data string is the 26-byte string consisting of the ASCII-coded version of

"abcdefghijklmnopqrstuvwxyz"

The hash-code is the following 512-bit string.

```
4dbff86cc2ca1bae 1e16468a05cb9881 c97f1753bce36190 34898faa1aabe429
955a1bf8ec483d74 21fe3c1646613a59 ed5441fb0f321389 f77f48a879c7b1f1
```

B.6.6 Example 6

In this example, the data string is the 62-byte string consisting of the ASCII-coded version of

"ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz0123456789"

The hash-code is the following 512-bit string.

```
1e07be23c26a86ea 37ea810c8ec78093 52515a970e9253c2 6f536cfc7a9996c4
5c8370583e0a78fa 4a90041d71a4ceab 7423f19c71b9d5a3 e01249f0bebd5894
```

B.6.7 Example 7

In this example, the data string is the 80-byte string consisting of the ASCII-coded version of eight repetitions of

"1234567890"

The hash-code is the following 512-bit string.

```
72ec1ef1124a45b0 47e8b7c75a932195 135bb61de24ec0d1 914042246e0aec3a
2354e093d76f3048 b456764346900cb1 30d2a4fd5dd16abb 5e30bcb850dee843
```

B.6.8 Example 8

In this example, the data string is the 56-byte string consisting of the ASCII-coded version of

"abcdbcdecdefdefgefghfghighijhijkijkljklmklmnlmnomnopnopq"

The hash-code is the following 512-bit string.

```
204a8fc6dda82f0a 0ced7beb8e08a416 57c16ef468b228a8 279be331a703c335
96fd15c13b1b07f9 aa1d3bea57789ca0 31ad85c7a71dd703 54ec631238ca3445
```

B.6.9 Example 9

In this example, the data string is the 1 000 000-byte string consisting of the ASCII-coded version of "a" repeated 10^6 times.

The hash-code is the following 512-bit string.

```
e718483d0ce76964 4e2e42c7bc15b463 8e1f98b13b204428 5632a803afa973eb
de0ff244877ea60a 4cb0432ce577c31b eb009c5c2c49aa2e 4eadb217ad8cc09b
```

B.6.10 Example 10

In this example, the data string is the 112-byte string consisting of the ASCII-coded version of

```
"abcdefghbcdefghicdefghijdefghijkefghijklfghijklmghijklmn
hijklmnoijklmnopjklmnopqklmnopqrlmnopqrsmnopqrstnopqrstu"
```

(with no line break after the first n).

After the padding process, the following two 16-word blocks are derived from the data string.

```
61626364 65666768 62636465 66676869 63646566 6768696a 64656667 68696a6b
65666768 696a6b6c 66676869 6a6b6c6d 6768696a 6b6c6d6e 68696a6b 6c6d6e6f
696a6b6c 6d6e6f70 6a6b6c6d 6e6f7071 6b6c6d6e 6f707172 6c6d6e6f 70717273
6d6e6f70 71727374 6e6f7071 72737475 80000000 00000000 00000000 00000000

00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000
00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000
00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000
00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000380
```

The following are (hexadecimal representations of) the successive values of the variables X_0, X_1, X_2, X_3, X_4, X_5, X_6 and X_7 in the first block process.

```
init  6a09e667f3bcc908 bb67ae8584caa73b 3c6ef372fe94f82b a54ff53a5f1d36f1
   510e527fade682d1 9b05688c2b3e6c1f 1f83d9abfb41bd6b 5be0cd19137e2179
 0  f6afce9d2263455d 6a09e667f3bcc908 bb67ae8584caa73b 3c6ef372fe94f82b
   58cb0218e01b86f9 510e527fade682d1 9b05688c2b3e6c1f 1f83d9abfb41bd6b
 1  0b7056a534ae5f62 f6afce9d2263455d 6a09e667f3bcc908 bb67ae8584caa73b
   f8c7198fe39e4c8c 58cb0218e01b86f9 510e527fade682d1 9b05688c2b3e6c1f
 2  2ca82233760c9942 0b7056a534ae5f62 f6afce9d2263455d 6a09e667f3bcc908
   303eccccd65953de f8c7198fe39e4c8c 58cb0218e01b86f9 510e527fade682d1
 3  a023f17ce52cda7b 2ca82233760c9942 0b7056a534ae5f62 f6afce9d2263455d
   ffdee5eedcc9ca42 303eccccd65953de f8c7198fe39e4c8c 58cb0218e01b86f9
 4  8f0a67d9d591a1a7 a023f17ce52cda7b 2ca82233760c9942 0b7056a534ae5f62
   cb4cfbb166505f2f ffdee5eedcc9ca42 303eccccd65953de f8c7198fe39e4c8c
 5  b466267371acc493 8f0a67d9d591a1a7 a023f17ce52cda7b 2ca82233760c9942
   73d6c84c54d399ee cb4cfbb166505f2f ffdee5eedcc9ca42 303eccccd65953de
 6  658269f1a312fccd b466267371acc493 8f0a67d9d591a1a7 a023f17ce52cda7b
   cdc40314975fb275 73d6c84c54d399ee cb4cfbb166505f2f ffdee5eedcc9ca42
 7  65e3519c5b88181b 658269f1a312fccd b466267371acc493 8f0a67d9d591a1a7
   a657850ab3970c5a cdc40314975fb275 73d6c84c54d399ee cb4cfbb166505f2f
 8  56604fbb4b6393ec 65e3519c5b88181b 658269f1a312fccd b466267371acc493
   e8b3be22fbe64df7 a657850ab3970c5a cdc40314975fb275 73d6c84c54d399ee
 9  c4562769a37d02c0 56604fbb4b6393ec 65e3519c5b88181b 658269f1a312fccd
   0062e70a1ef705c1 e8b3be22fbe64df7 a657850ab3970c5a cdc40314975fb275
10 27c0b4c9186e1736 c4562769a37d02c0 56604fbb4b6393ec 65e3519c5b88181b
   bc9740477a18ae2d 0062e70a1ef705c1 e8b3be22fbe64df7 a657850ab3970c5a
11 f17f52fb02f4eb74 27c0b4c9186e1736 c4562769a37d02c0 56604fbb4b6393ec
   be58522cb9590ee1 bc9740477a18ae2d 0062e70a1ef705c1 e8b3be22fbe64df7
12 f2c245ac903d4a35 f17f52fb02f4eb74 27c0b4c9186e1736 c4562769a37d02c0
   49d5fa3a16dcd502 be58522cb9590ee1 bc9740477a18ae2d 0062e70a1ef705c1
13 9b04175ea8090daa f2c245ac903d4a35 f17f52fb02f4eb74 27c0b4c9186e1736
   ec9c5e98ff98760d 49d5fa3a16dcd502 be58522cb9590ee1 bc9740477a18ae2d
14 481b8a6ee5e07031 9b04175ea8090daa f2c245ac903d4a35 f17f52fb02f4eb74
   e4d35b613a5ac420 ec9c5e98ff98760d 49d5fa3a16dcd502 be58522cb9590ee1
15 9356ac3ec3e51459 481b8a6ee5e07031 9b04175ea8090daa f2c245ac903d4a35
   701f17d27582443b e4d35b613a5ac420 ec9c5e98ff98760d 49d5fa3a16dcd502
16 b889ed34abd7aa37 9356ac3ec3e51459 481b8a6ee5e07031 9b04175ea8090daa
   1d05d9ba779a1a78 701f17d27582443b e4d35b613a5ac420 ec9c5e98ff98760d
17 bf537b1f3edc7381 b889ed34abd7aa37 9356ac3ec3e51459 481b8a6ee5e07031
   c362ff9cf932951d 1d05d9ba779a1a78 701f17d27582443b e4d35b613a5ac420
18 d4e44d54e8242ad8 bf537b1f3edc7381 b889ed34abd7aa37 9356ac3ec3e51459
   459e4e6888919f36 c362ff9cf932951d 1d05d9ba779a1a78 701f17d27582443b
19 05f3fba454e5de3d d4e44d54e8242ad8 bf537b1f3edc7381 b889ed34abd7aa37
   caed4b5fa322b984 459e4e6888919f36 c362ff9cf932951d 1d05d9ba779a1a78
20 cdb73772dc0248bf 05f3fba454e5de3d d4e44d54e8242ad8 bf537b1f3edc7381
   dc8049afa6acd502 caed4b5fa322b984 459e4e6888919f36 c362ff9cf932951d
21 1d47a3268ff677ed cdb73772dc0248bf 05f3fba454e5de3d d4e44d54e8242ad8
   8407818e9b28cc12 dc8049afa6acd502 caed4b5fa322b984 459e4e6888919f36
22 af4e23eb622d0df4 1d47a3268ff677ed cdb73772dc0248bf 05f3fba454e5de3d
   64b5ae5424598428 8407818e9b28cc12 dc8049afa6acd502 caed4b5fa322b984
```

```
23 be50606778de14a6 af4e23eb622d0df4 1d47a3268ff677ed cdb73772dc0248bf
  0a5d727cc92e7adb 64b5ae5424598428 8407818e9b28cc12 dc8049afa6acd502
24 821e44f6678ac478 be50606778de14a6 af4e23eb622d0df4 1d47a3268ff677ed
  f367e596d0a038a5 0a5d727cc92e7adb 64b5ae5424598428 8407818e9b28cc12
25 0c852b1359a77c18 821e44f6678ac478 be50606778de14a6 af4e23eb622d0df4
  6dec8a3396a80c3f f367e596d0a038a5 0a5d727cc92e7adb 64b5ae5424598428
26 ebb574fad4b7a7e4 0c852b1359a77c18 821e44f6678ac478 be50606778de14a6
  a241e7efc1eb6ff9 6dec8a3396a80c3f f367e596d0a038a5 0a5d727cc92e7adb
27 a092821c3cdf08da ebb574fad4b7a7e4 0c852b1359a77c18 821e44f6678ac478
  c84e849917a7c08e a241e7efc1eb6ff9 6dec8a3396a80c3f f367e596d0a038a5
28 82ba2e1a2df2a4f1 a092821c3cdf08da ebb574fad4b7a7e4 0c852b1359a77c18
  61845f6924789851 c84e849917a7c08e a241e7efc1eb6ff9 6dec8a3396a80c3f
29 1959ad991c63d06a 82ba2e1a2df2a4f1 a092821c3cdf08da ebb574fad4b7a7e4
  231faf24910a891a 61845f6924789851 c84e849917a7c08e a241e7efc1eb6ff9
30 9b32d4cacd9a625b 1959ad991c63d06a 82ba2e1a2df2a4f1 a092821c3cdf08da
  533066919d608799 231faf24910a891a 61845f6924789851 c84e849917a7c08e
31 dc55339f4d841965 9b32d4cacd9a625b 1959ad991c63d06a 82ba2e1a2df2a4f1
  e2517f359998a58d 533066919d608799 231faf24910a891a 61845f6924789851
32 fdebb1283b12514f dc55339f4d841965 9b32d4cacd9a625b 1959ad991c63d06a
  b1989170a183c661 e2517f359998a58d 533066919d608799 231faf24910a891a
33 b44c7975a83e3334 fdebb1283b12514f dc55339f4d841965 9b32d4cacd9a625b
  009ad175b8d588a4 b1989170a183c661 e2517f359998a58d 533066919d608799
34 0bac61bfc53d18b7 b44c7975a83e3334 fdebb1283b12514f dc55339f4d841965
  a7d5416d690557b8 009ad175b8d588a4 b1989170a183c661 e2517f359998a58d
35 392893c22e75856a 0bac61bfc53d18b7 b44c7975a83e3334 fdebb1283b12514f
  7a7c9eb7bc813248 a7d5416d690557b8 009ad175b8d588a4 b1989170a183c661
36 824408631432e09b 392893c22e75856a 0bac61bfc53d18b7 b44c7975a83e3334
  5e696a9fda56d6bf 7a7c9eb7bc813248 a7d5416d690557b8 009ad175b8d588a4
37 a64162f151a8c1cb 824408631432e09b 392893c22e75856a 0bac61bfc53d18b7
  0f57062401dc680b 5e696a9fda56d6bf 7a7c9eb7bc813248 a7d5416d690557b8
38 922537abad1e95a1 a64162f151a8c1cb 824408631432e09b 392893c22e75856a
  4f4c193d435ff721 0f57062401dc680b 5e696a9fda56d6bf 7a7c9eb7bc813248
39 b80591f6fbfadcde 922537abad1e95a1 a64162f151a8c1cb 824408631432e09b
  00f4407c0f37237e 4f4c193d435ff721 0f57062401dc680b 5e696a9fda56d6bf
40 08f151f4b8d0fa2e b80591f6fbfadcde 922537abad1e95a1 a64162f151a8c1cb
  ec8b96fe402094cd 00f4407c0f37237e 4f4c193d435ff721 0f57062401dc680b
41 12b5fcc2b68f65c0 08f151f4b8d0fa2e b80591f6fbfadcde 922537abad1e95a1
  d688101dfd24a148 ec8b96fe402094cd 00f4407c0f37237e 4f4c193d435ff721
42 a71bf5bd64289948 12b5fcc2b68f65c0 08f151f4b8d0fa2e b80591f6fbfadcde
  e052bfb7a6945939 d688101dfd24a148 ec8b96fe402094cd 00f4407c0f37237e
43 890c2cd670c4aea3 a71bf5bd64289948 12b5fcc2b68f65c0 08f151f4b8d0fa2e
  dd13e4edeeff00e7 e052bfb7a6945939 d688101dfd24a148 ec8b96fe402094cd
44 ca61990b43297ffc 890c2cd670c4aea3 a71bf5bd64289948 12b5fcc2b68f65c0
  139aa55c51d9ee5f dd13e4edeeff00e7 e052bfb7a6945939 d688101dfd24a148
45 7196e8fa538ba4bf ca61990b43297ffc 890c2cd670c4aea3 a71bf5bd64289948
  046735513cdd14d3 139aa55c51d9ee5f dd13e4edeeff00e7 e052bfb7a6945939
46 1f0720944dbeb6a4 7196e8fa538ba4bf ca61990b43297ffc 890c2cd670c4aea3
  a41eb7e5a27588e3 046735513cdd14d3 139aa55c51d9ee5f dd13e4edeeff00e7
47 d6d4f8608b8ab199 1f0720944dbeb6a4 7196e8fa538ba4bf ca61990b43297ffc
  24b9c216f915da60 a41eb7e5a27588e3 046735513cdd14d3 139aa55c51d9ee5f
48 88761eb67845978e d6d4f8608b8ab199 1f0720944dbeb6a4 7196e8fa538ba4bf
  9fe22e39448d50ed 24b9c216f915da60 a41eb7e5a27588e3 046735513cdd14d3
49 7d40e6be47d85702 88761eb67845978e d6d4f8608b8ab199 1f0720944dbeb6a4
  d9c900e01968c33e 9fe22e39448d50ed 24b9c216f915da60 a41eb7e5a27588e3
50 7d0d988df5768598 7d40e6be47d85702 88761eb67845978e d6d4f8608b8ab199
  2ec2e522a7c7d12c d9c900e01968c33e 9fe22e39448d50ed 24b9c216f915da60
51 48a8b60575b37f31 7d0d988df5768598 7d40e6be47d85702 88761eb67845978e
  7059f9bc8c88a373 2ec2e522a7c7d12c d9c900e01968c33e 9fe22e39448d50ed
52 6bc425af294bbf79 48a8b60575b37f31 7d0d988df5768598 7d40e6be47d85702
  6a8143b1716ee33d 7059f9bc8c88a373 2ec2e522a7c7d12c d9c900e01968c33e
53 307a456158ee8849 6bc425af294bbf79 48a8b60575b37f31 7d0d988df5768598
  4372e85c16ee4440 6a8143b1716ee33d 7059f9bc8c88a373 2ec2e522a7c7d12c
54 af36382c8fd716be 307a456158ee8849 6bc425af294bbf79 48a8b60575b37f31
```

```
  a8f8b0033187a916 4372e85c16ee4440 6a8143b1716ee33d 7059f9bc8c88a373
55 810ebee951c64ca1 af36382c8fd716be 307a456158ee8849 6bc425af294bbf79
  16a64f5997b9cca6 a8f8b0033187a916 4372e85c16ee4440 6a8143b1716ee33d
56 2dd7659f1b4d13cd 810ebee951c64ca1 af36382c8fd716be 307a456158ee8849
  5da6793bb7286a4b 16a64f5997b9cca6 a8f8b0033187a916 4372e85c16ee4440
57 5ac712acff4b98be 2dd7659f1b4d13cd 810ebee951c64ca1 af36382c8fd716be
  91f6395b301adbfd 5da6793bb7286a4b 16a64f5997b9cca6 a8f8b0033187a916
58 c1af358833cb03c0 5ac712acff4b98be 2dd7659f1b4d13cd 810ebee951c64ca1
  d4883c0c21dda190 91f6395b301adbfd 5da6793bb7286a4b 16a64f5997b9cca6
59 88a306074d388c7d c1af358833cb03c0 5ac712acff4b98be 2dd7659f1b4d13cd
  9fc52468b897f9c8 d4883c0c21dda190 91f6395b301adbfd 5da6793bb7286a4b
60 f11bfd0cf67d3040 88a306074d388c7d c1af358833cb03c0 5ac712acff4b98be
  47efb6407f74d318 9fc52468b897f9c8 d4883c0c21dda190 91f6395b301adbfd
61 1f065e7828ed4e1b f11bfd0cf67d3040 88a306074d388c7d c1af358833cb03c0
  7481899904a4ce23 47efb6407f74d318 9fc52468b897f9c8 d4883c0c21dda190
62 aebde39f2bc42ec1 1f065e7828ed4e1b f11bfd0cf67d3040 88a306074d388c7d
  62ab526ff177a988 7481899904a4ce23 47efb6407f74d318 9fc52468b897f9c8
63 d35a94706e3e5df2 aebde39f2bc42ec1 1f065e7828ed4e1b f11bfd0cf67d3040
  53f92b648d5d815c 62ab526ff177a988 7481899904a4ce23 47efb6407f74d318
64 d72d727c53e09ab9 d35a94706e3e5df2 aebde39f2bc42ec1 1f065e7828ed4e1b
  10746426ba9824f4 53f92b648d5d815c 62ab526ff177a988 7481899904a4ce23
65 3a7235e5a4051d94 d72d727c53e09ab9 d35a94706e3e5df2 aebde39f2bc42ec1
  afe455daec5c2b00 10746426ba9824f4 53f92b648d5d815c 62ab526ff177a988
66 f7f510fe73ef7e76 3a7235e5a4051d94 d72d727c53e09ab9 d35a94706e3e5df2
  f1202c0bb7c4583f afe455daec5c2b00 10746426ba9824f4 53f92b648d5d815c
67 23c2acfb393523e9 f7f510fe73ef7e76 3a7235e5a4051d94 d72d727c53e09ab9
  a0bc2a61044ac12e f1202c0bb7c4583f afe455daec5c2b00 10746426ba9824f4
68 0307d241a1ed7121 23c2acfb393523e9 f7f510fe73ef7e76 3a7235e5a4051d94
  fad5f38f1e0aea12 a0bc2a61044ac12e f1202c0bb7c4583f afe455daec5c2b00
69 191814d82f0a16fb 0307d241a1ed7121 23c2acfb393523e9 f7f510fe73ef7e76
  39d325086e66e200 fad5f38f1e0aea12 a0bc2a61044ac12e f1202c0bb7c4583f
70 0a1ed41b6da18c01 191814d82f0a16fb 0307d241a1ed7121 23c2acfb393523e9
  b3d3521e166e5df1 39d325086e66e200 fad5f38f1e0aea12 a0bc2a61044ac12e
71 8a3f07db93f6c827 0a1ed41b6da18c01 191814d82f0a16fb 0307d241a1ed7121
  6b370074be040ed7 b3d3521e166e5df1 39d325086e66e200 fad5f38f1e0aea12
72 002744d87ef80d28 8a3f07db93f6c827 0a1ed41b6da18c01 191814d82f0a16fb
  8c5a245de2d72fe6 6b370074be040ed7 b3d3521e166e5df1 39d325086e66e200
73 778dc7880a4a2aa0 002744d87ef80d28 8a3f07db93f6c827 0a1ed41b6da18c01
  45a375b466e5e342 8c5a245de2d72fe6 6b370074be040ed7 b3d3521e166e5df1
74 a3f11de5ede05b11 778dc7880a4a2aa0 002744d87ef80d28 8a3f07db93f6c827
  f5bbf52f1ab7cc05 45a375b466e5e342 8c5a245de2d72fe6 6b370074be040ed7
75 629c8ae6ecd8af4b a3f11de5ede05b11 778dc7880a4a2aa0 002744d87ef80d28
  5a8fe5919d3cf136 f5bbf52f1ab7cc05 45a375b466e5e342 8c5a245de2d72fe6
76 c9a8c1e2d063ce94 629c8ae6ecd8af4b a3f11de5ede05b11 778dc7880a4a2aa0
  aacd089bfae8faf9 5a8fe5919d3cf136 f5bbf52f1ab7cc05 45a375b466e5e342
77 c517cba6a09bb26a c9a8c1e2d063ce94 629c8ae6ecd8af4b a3f11de5ede05b11
  e1682bd33c8f8e23 aacd089bfae8faf9 5a8fe5919d3cf136 f5bbf52f1ab7cc05
78 11e3570e06e3b74e c517cba6a09bb26a c9a8c1e2d063ce94 629c8ae6ecd8af4b
  075aabbade34fd01 e1682bd33c8f8e23 aacd089bfae8faf9 5a8fe5919d3cf136
79 d90f1b1237b3a561 11e3570e06e3b74e c517cba6a09bb26a c9a8c1e2d063ce94
  867983f69d3a3ad1 075aabbade34fd01 e1682bd33c8f8e23 aacd089bfae8faf9
```

The following eight words, Y_0, Y_1, Y_2, Y_3, Y_4, Y_5, Y_6 and Y_7, represent the output of the round-function in the first block process.

$$Y_0 = 6a09e667f3bcc908 \boxplus d90f1b1237b3a561 = 4319017a2b706e69$$
$$Y_1 = bb67ae8584caa73b \boxplus 11e3570e06e3b74e = cd4b05938bae5e89$$
$$Y_2 = 3c6ef372fe94f82b \boxplus c517cba6a09bb26a = 0186bf199f30aa95$$
$$Y_3 = a54ff53a5f1d36f1 \boxplus c9a8c1e2d063ce94 = 6ef8b71d2f810585$$
$$Y_4 = 510e527fade682d1 \boxplus 867983f69d3a3ad1 = d787d6764b20bda2$$
$$Y_5 = 9b05688c2b3e6c1f \boxplus 075aabbade34fd01 = a260144709736920$$
$$Y_6 = 1f83d9abfb41bd6b \boxplus e1682bd33c8f8e23 = 00ec057f37d14b8e$$
$$Y_7 = 5be0cd19137e2179 \boxplus aacd089bfae8faf9 = 06add5b50e671c72$$

The following are (hexadecimal representations of) the successive values of the variables Y_0, Y_1, Y_2, Y_3, Y_4, Y_5, Y_6 and Y_7 in the second block process.

```
init  4319017a2b706e69 cd4b05938bae5e89 0186bf199f30aa95 6ef8b71d2f810585
   d787d6764b20bda2 a260144709736920 00ec057f37d14b8e 06add5b50e671c72
 0  b8fdb92bdfb187e8 4319017a2b706e69 cd4b05938bae5e89 0186bf199f30aa95
   1d5f4d5ad031b8e6 d787d6764b20bda2 a260144709736920 00ec057f37d14b8e
 1  6eb90718369c5cd7 b8fdb92bdfb187e8 4319017a2b706e69 cd4b05938bae5e89
   4b9b4877d987b0fe 1d5f4d5ad031b8e6 d787d6764b20bda2 a260144709736920
 2  c83451f2335d5144 6eb90718369c5cd7 b8fdb92bdfb187e8 4319017a2b706e69
   d6b67350e0781e99 4b9b4877d987b0fe 1d5f4d5ad031b8e6 d787d6764b20bda2
 3  28ec1deb2a9ee6e3 c83451f2335d5144 6eb90718369c5cd7 b8fdb92bdfb187e8
   25e3136be5999b8c d6b67350e0781e99 4b9b4877d987b0fe 1d5f4d5ad031b8e6
 4  806abd86c0479e5b 28ec1deb2a9ee6e3 c83451f2335d5144 6eb90718369c5cd7
   1b8f7670eab1cf89 25e3136be5999b8c d6b67350e0781e99 4b9b4877d987b0fe
 5  234788f8a54aed38 806abd86c0479e5b 28ec1deb2a9ee6e3 c83451f2335d5144
   4fabe51c67d5d156 1b8f7670eab1cf89 25e3136be5999b8c d6b67350e0781e99
 6  01264f18257b5e2c 234788f8a54aed38 806abd86c0479e5b 28ec1deb2a9ee6e3
   1c3506096b99de50 4fabe51c67d5d156 1b8f7670eab1cf89 25e3136be5999b8c
 7  5b14f38104dde991 01264f18257b5e2c 234788f8a54aed38 806abd86c0479e5b
   13f8bfdc4001c362 1c3506096b99de50 4fabe51c67d5d156 1b8f7670eab1cf89
 8  f522574a41b2aac6 5b14f38104dde991 01264f18257b5e2c 234788f8a54aed38
   63a5f09617622ed2 13f8bfdc4001c362 1c3506096b99de50 4fabe51c67d5d156
 9  6ec258b855afae5a f522574a41b2aac6 5b14f38104dde991 01264f18257b5e2c
   211e271d92770b36 63a5f09617622ed2 13f8bfdc4001c362 1c3506096b99de50
10 9364214ba48b416c 6ec258b855afae5a f522574a41b2aac6 5b14f38104dde991
   d64dcb6ec0fe5bac 211e271d92770b36 63a5f09617622ed2 13f8bfdc4001c362
11 082ba62147ecbbd5 9364214ba48b416c 6ec258b855afae5a f522574a41b2aac6
   34fe78473b61266e d64dcb6ec0fe5bac 211e271d92770b36 63a5f09617622ed2
12 5790f6ba82bba809 082ba62147ecbbd5 9364214ba48b416c 6ec258b855afae5a
   d491e309141dcaa3 34fe78473b61266e d64dcb6ec0fe5bac 211e271d92770b36
13 a6b8aefd086d33ce 5790f6ba82bba809 082ba62147ecbbd5 9364214ba48b416c
   044943c2992cc0f0 d491e309141dcaa3 34fe78473b61266e d64dcb6ec0fe5bac
14 bf2324a9a363abe7 a6b8aefd086d33ce 5790f6ba82bba809 082ba62147ecbbd5
   0cf5f4bde5977c54 044943c2992cc0f0 d491e309141dcaa3 34fe78473b61266e
15 00e8e32076a61aff bf2324a9a363abe7 a6b8aefd086d33ce 5790f6ba82bba809
   43bf4eb269a2650c 0cf5f4bde5977c54 044943c2992cc0f0 d491e309141dcaa3
16 f0376dff66fff4a7 00e8e32076a61aff bf2324a9a363abe7 a6b8aefd086d33ce
   69fa5896969e85b8 43bf4eb269a2650c 0cf5f4bde5977c54 044943c2992cc0f0
17 2fad194272cda857 f0376dff66fff4a7 00e8e32076a61aff bf2324a9a363abe7
   ddb519d663b7b6ec 69fa5896969e85b8 43bf4eb269a2650c 0cf5f4bde5977c54
18 9ae56936e95325ac 2fad194272cda857 f0376dff66fff4a7 00e8e32076a61aff
   04ceb04676619057 ddb519d663b7b6ec 69fa5896969e85b8 43bf4eb269a2650c
19 d94ccb853f53433b 9ae56936e95325ac 2fad194272cda857 f0376dff66fff4a7
   dcdc0f45813fb5a2 04ceb04676619057 ddb519d663b7b6ec 69fa5896969e85b8
20 837f8075d2945995 d94ccb853f53433b 9ae56936e95325ac 2fad194272cda857
   272b5f79a91419d8 dcdc0f45813fb5a2 04ceb04676619057 ddb519d663b7b6ec
21 786bde689f7aa62d 837f8075d2945995 d94ccb853f53433b 9ae56936e95325ac
   566586e69ad3f487 272b5f79a91419d8 dcdc0f45813fb5a2 04ceb04676619057
22 276457f01812aa6f 786bde689f7aa62d 837f8075d2945995 d94ccb853f53433b
   e78fb8b0dfbbc62f 566586e69ad3f487 272b5f79a91419d8 dcdc0f45813fb5a2
23 0de519f5d6c2c298 276457f01812aa6f 786bde689f7aa62d 837f8075d2945995
   5ca3e5cd1a30b954 e78fb8b0dfbbc62f 566586e69ad3f487 272b5f79a91419d8
24 54314dff825e2b22 0de519f5d6c2c298 276457f01812aa6f 786bde689f7aa62d
   b81a51e0c96ccf77 5ca3e5cd1a30b954 e78fb8b0dfbbc62f 566586e69ad3f487
25 5d3f98dd7b29c363 54314dff825e2b22 0de519f5d6c2c298 276457f01812aa6f
   95d49494f5a0d14a b81a51e0c96ccf77 5ca3e5cd1a30b954 e78fb8b0dfbbc62f
26 5e9da426aa7d4a58 5d3f98dd7b29c363 54314dff825e2b22 0de519f5d6c2c298
   d22cccad2e391cd4 95d49494f5a0d14a b81a51e0c96ccf77 5ca3e5cd1a30b954
27 3b62dd973298ea43 5e9da426aa7d4a58 5d3f98dd7b29c363 54314dff825e2b22
   aceb5d06101e514e d22cccad2e391cd4 95d49494f5a0d14a b81a51e0c96ccf77
28 fd258ff809b2253d 3b62dd973298ea43 5e9da426aa7d4a58 5d3f98dd7b29c363
```

```
  26c991e85352da6f aceb5d06101e514e d22cccad2e391cd4 95d49494f5a0d14a
29 b462a20846af417d fd258ff809b2253d 3b62dd973298ea43 5e9da426aa7d4a58
  291eee54c034c326 26c991e85352da6f aceb5d06101e514e d22cccad2e391cd4
30 d5471e3dc7171224 b462a20846af417d fd258ff809b2253d 3b62dd973298ea43
  0aaf99c59e7fadbd 291eee54c034c326 26c991e85352da6f aceb5d06101e514e
31 9ace856ba1290e6e d5471e3dc7171224 b462a20846af417d fd258ff809b2253d
  658f0bea63804d05 0aaf99c59e7fadbd 291eee54c034c326 26c991e85352da6f
32 80a0d154506b37c4 9ace856ba1290e6e d5471e3dc7171224 b462a20846af417d
  bbe6e3b3bb7fefab 658f0bea63804d05 0aaf99c59e7fadbd 291eee54c034c326
33 fb90a8a76dea1bfe 80a0d154506b37c4 9ace856ba1290e6e d5471e3dc7171224
  65234d5b5049e665 bbe6e3b3bb7fefab 658f0bea63804d05 0aaf99c59e7fadbd
34 f517b690d940a294 fb90a8a76dea1bfe 80a0d154506b37c4 9ace856ba1290e6e
  e4dd663f44d313bc 65234d5b5049e665 bbe6e3b3bb7fefab 658f0bea63804d05
35 b70883992932880d f517b690d940a294 fb90a8a76dea1bfe 80a0d154506b37c4
  dc5dd7c12b1cb6e3 e4dd663f44d313bc 65234d5b5049e665 bbe6e3b3bb7fefab
36 b2a2be77b0fcf3bf b70883992932880d f517b690d940a294 fb90a8a76dea1bfe
  50fca57291e19874 dc5dd7c12b1cb6e3 e4dd663f44d313bc 65234d5b5049e665
37 8575839b0f08472b b2a2be77b0fcf3bf b70883992932880d f517b690d940a294
  bd7176bd099bb2f2 50fca57291e19874 dc5dd7c12b1cb6e3 e4dd663f44d313bc
38 4405d2765de0adfc 8575839b0f08472b b2a2be77b0fcf3bf b70883992932880d
  7ca4916f2cd8db10 bd7176bd099bb2f2 50fca57291e19874 dc5dd7c12b1cb6e3
39 eec6fca5aa657661 4405d2765de0adfc 8575839b0f08472b b2a2be77b0fcf3bf
  7be0b7e70bdabe53 7ca4916f2cd8db10 bd7176bd099bb2f2 50fca57291e19874
40 bb3fcd7585b59e32 eec6fca5aa657661 4405d2765de0adfc 8575839b0f08472b
  2201c7cbd34e31fe 7be0b7e70bdabe53 7ca4916f2cd8db10 bd7176bd099bb2f2
41 0e109efc47927341 bb3fcd7585b59e32 eec6fca5aa657661 4405d2765de0adfc
  d43e5686506fa05d 2201c7cbd34e31fe 7be0b7e70bdabe53 7ca4916f2cd8db10
42 55c0dba83bcdc6e0 0e109efc47927341 bb3fcd7585b59e32 eec6fca5aa657661
  5b634502f1671535 d43e5686506fa05d 2201c7cbd34e31fe 7be0b7e70bdabe53
43 f5756f847bfaef67 55c0dba83bcdc6e0 0e109efc47927341 bb3fcd7585b59e32
  e2d307fd94f4818a 5b634502f1671535 d43e5686506fa05d 2201c7cbd34e31fe
44 f1438c9cf271c06e f5756f847bfaef67 55c0dba83bcdc6e0 0e109efc47927341
  ad8ac1ed966b2dc6 e2d307fd94f4818a 5b634502f1671535 d43e5686506fa05d
45 a7dcaffdbefb9d4a f1438c9cf271c06e f5756f847bfaef67 55c0dba83bcdc6e0
  9e46e9f915099c34 ad8ac1ed966b2dc6 e2d307fd94f4818a 5b634502f1671535
46 985ba373680b8e94 a7dcaffdbefb9d4a f1438c9cf271c06e f5756f847bfaef67
  7d4c0abc676b1a8b 9e46e9f915099c34 ad8ac1ed966b2dc6 e2d307fd94f4818a
47 807f45784852303f 985ba373680b8e94 a7dcaffdbefb9d4a f1438c9cf271c06e
  082ee70d3f352aac 7d4c0abc676b1a8b 9e46e9f915099c34 ad8ac1ed966b2dc6
48 d9c523173b1a1e05 807f45784852303f 985ba373680b8e94 a7dcaffdbefb9d4a
  e301dca32c44ca05 082ee70d3f352aac 7d4c0abc676b1a8b 9e46e9f915099c34
49 b6df019ca515cafb d9c523173b1a1e05 807f45784852303f 985ba373680b8e94
  754b3a461a665640 e301dca32c44ca05 082ee70d3f352aac 7d4c0abc676b1a8b
50 427a642921b2e645 b6df019ca515cafb d9c523173b1a1e05 807f45784852303f
  08a30fefe981f2ec 754b3a461a665640 e301dca32c44ca05 082ee70d3f352aac
51 7aab58dbe1b9df7b 427a642921b2e645 b6df019ca515cafb d9c523173b1a1e05
  2749c52d0b3d1225 08a30fefe981f2ec 754b3a461a665640 e301dca32c44ca05
52 974ddd552aec16ce 7aab58dbe1b9df7b 427a642921b2e645 b6df019ca515cafb
  a9e6cbfb416a591f 2749c52d0b3d1225 08a30fefe981f2ec 754b3a461a665640
53 55e0b99d4404f6ca 974ddd552aec16ce 7aab58dbe1b9df7b 427a642921b2e645
  6c24ad697b41b1b9 a9e6cbfb416a591f 2749c52d0b3d1225 08a30fefe981f2ec
54 901f632579ee1eee 55e0b99d4404f6ca 974ddd552aec16ce 7aab58dbe1b9df7b
  4ee99476db1bb7a9 6c24ad697b41b1b9 a9e6cbfb416a591f 2749c52d0b3d1225
55 f90db9f292a60463 901f632579ee1eee 55e0b99d4404f6ca 974ddd552aec16ce
  5401644992a1f8b8 4ee99476db1bb7a9 6c24ad697b41b1b9 a9e6cbfb416a591f
56 9b906a7df1007357 f90db9f292a60463 901f632579ee1eee 55e0b99d4404f6ca
  f5e402ee21db8915 5401644992a1f8b8 4ee99476db1bb7a9 6c24ad697b41b1b9
57 71a0a998fb48c0fc 9b906a7df1007357 f90db9f292a60463 901f632579ee1eee
  96bece755cd203cb f5e402ee21db8915 5401644992a1f8b8 4ee99476db1bb7a9
58 c25e798e50752535 71a0a998fb48c0fc 9b906a7df1007357 f90db9f292a60463
  9d548440d8e110f2 96bece755cd203cb f5e402ee21db8915 5401644992a1f8b8
59 1ce4f2591812e6ae c25e798e50752535 71a0a998fb48c0fc 9b906a7df1007357
  b27252537a83cf27 9d548440d8e110f2 96bece755cd203cb f5e402ee21db8915
```

```
60 c1700e250dc6ffed 1ce4f2591812e6ae c25e798e50752535 71a0a998fb48c0fc
  970088839126bda5 b27252537a83cf27 9d548440d8e110f2 96bece755cd203cb
61 f8e6924412fd0c64 c1700e250dc6ffed 1ce4f2591812e6ae c25e798e50752535
  d50cf4f73910e3ee 970088839126bda5 b27252537a83cf27 9d548440d8e110f2
62 d53e0a39eee47528 f8e6924412fd0c64 c1700e250dc6ffed 1ce4f2591812e6ae
  1b6d7234ace15d7d d50cf4f73910e3ee 970088839126bda5 b27252537a83cf27
63 3960545ab926c0d5 d53e0a39eee47528 f8e6924412fd0c64 c1700e250dc6ffed
  9eabb5618b4fcd13 1b6d7234ace15d7d d50cf4f73910e3ee 970088839126bda5
64 b2c164d71abb92fe 3960545ab926c0d5 d53e0a39eee47528 f8e6924412fd0c64
  f1736fbbfb6ebe72 9eabb5618b4fcd13 1b6d7234ace15d7d d50cf4f73910e3ee
65 4d979e985b067e75 b2c164d71abb92fe 3960545ab926c0d5 d53e0a39eee47528
  d1fb300f35992350 f1736fbbfb6ebe72 9eabb5618b4fcd13 1b6d7234ace15d7d
66 59d0238ce137abd7 4d979e985b067e75 b2c164d71abb92fe 3960545ab926c0d5
  5f3c64b7546e2cec d1fb300f35992350 f1736fbbfb6ebe72 9eabb5618b4fcd13
67 bf8d9453b9876b0a 59d0238ce137abd7 4d979e985b067e75 b2c164d71abb92fe
  6c27893a31b0e07e 5f3c64b7546e2cec d1fb300f35992350 f1736fbbfb6ebe72
68 c45dd4a2d2fea059 bf8d9453b9876b0a 59d0238ce137abd7 4d979e985b067e75
  48253e21b26d8cf9 6c27893a31b0e07e 5f3c64b7546e2cec d1fb300f35992350
69 e08471946c17b0b6 c45dd4a2d2fea059 bf8d9453b9876b0a 59d0238ce137abd7
  714e2adf4e23ff24 48253e21b26d8cf9 6c27893a31b0e07e 5f3c64b7546e2cec
70 b4838c1c28fee7bc e08471946c17b0b6 c45dd4a2d2fea059 bf8d9453b9876b0a
  371f12f333f7e5b9 714e2adf4e23ff24 48253e21b26d8cf9 6c27893a31b0e07e
71 851cf60a77f6e6d1 b4838c1c28fee7bc e08471946c17b0b6 c45dd4a2d2fea059
  a2a475deac0e8b42 371f12f333f7e5b9 714e2adf4e23ff24 48253e21b26d8cf9
72 f53d23c50249af2d 851cf60a77f6e6d1 b4838c1c28fee7bc e08471946c17b0b6
  1e99cae9d4cf0409 a2a475deac0e8b42 371f12f333f7e5b9 714e2adf4e23ff24
73 b81e85d427045550 f53d23c50249af2d 851cf60a77f6e6d1 b4838c1c28fee7bc
  f5794711faa60f63 1e99cae9d4cf0409 a2a475deac0e8b42 371f12f333f7e5b9
74 ae70c7d11ea84a83 b81e85d427045550 f53d23c50249af2d 851cf60a77f6e6d1
  dc0d633411c289b2 f5794711faa60f63 1e99cae9d4cf0409 a2a475deac0e8b42
75 5c54592e13c76135 ae70c7d11ea84a83 b81e85d427045550 f53d23c50249af2d
  1620dd5479e94b9b dc0d633411c289b2 f5794711faa60f63 1e99cae9d4cf0409
76 03a0f79087078a93 5c54592e13c76135 ae70c7d11ea84a83 b81e85d427045550
  57e90fa678e4cc97 1620dd5479e94b9b dc0d633411c289b2 f5794711faa60f63
77 8df0baad4c6ed50c 03a0f79087078a93 5c54592e13c76135 ae70c7d11ea84a83
  c6e7246f7f0bdac6 57e90fa678e4cc97 1620dd5479e94b9b dc0d633411c289b2
78 bfa9f194894db5b6 8df0baad4c6ed50c 03a0f79087078a93 5c54592e13c76135
  90bb8597bb41da1a c6e7246f7f0bdac6 57e90fa678e4cc97 1620dd5479e94b9b
79 4b7c99fbaf72a571 bfa9f194894db5b6 8df0baad4c6ed50c 03a0f79087078a93
  78955227fde03a42 90bb8597bb41da1a c6e7246f7f0bdac6 57e90fa678e4cc97
```

The following eight words, Y_0, Y_1, Y_2, Y_3, Y_4, Y_5, Y_6 and Y_7, represent the output of the final iteration of the round-function.

Y_0 = 4319017a2b706e69 ⊎ 4b7c99fbaf72a571 = 8e959b75dae313da
Y_1 = cd4b05938bae5e89 ⊎ bfa9f194894db5b6 = 8cf4f72814fc143f
Y_2 = 0186bf199f30aa95 ⊎ 8df0baad4c6ed50c = 8f7779c6eb9f7fa1
Y_3 = 6ef8b71d2f810585 ⊎ 03a0f79087078a93 = 7299aeadb6889018
Y_4 = d787d6764b20bda2 ⊎ 78955227fde03a42 = 501d289e4900f7e4
Y_5 = a260144709736920 ⊎ 90bb8597bb41da1a = 331b99dec4b5433a
Y_6 = 00ec057f37d14b8e ⊎ c6e7246f7f0bdac6 = c7d329eeb6dd2654
Y_7 = 06add5b50e671c72 ⊎ 57e90fa678e4cc97 = 5e96e55b874be909

The following is the hash value for this message.

```
8e959b75dae313da 8cf4f72814fc143f 8f7779c6eb9f7fa1 7299aeadb6889018
501d289e4900f7e4 331b99dec4b5433a c7d329eeb6dd2654 5e96e55b874be909
```

B.6.11 Example 11

In this example, the data string is the 32-byte string consisting of the ASCII-coded version of

"abcdbcdecdefdefgefghfghighijhijk"

The hash-code is the following 512-bit string.

```
c50e7a500d4058bf 530ec603b66b032a 989a3e033a340090 dc51086cfd8cb222
09027932ea830f9b 6bc09dafe882f908 38c2c91018245904 828c1232fc0942eb
```

B.7 Dedicated Hash-Function 6 (SHA-384)

B.7.1 Example 1

In this example, the data string is the empty string, i.e. the string of length zero.

The hash-code is the following 384-bit string.

```
38b060a751ac9638 4cd9327eb1b1e36a 21fdb71114be0743 4c0cc7bf63f6e1da
                 274edebfe76f65fb d51ad2f14898b95b
```

B.7.2 Example 2

In this example, the data string consists of a single byte, namely the ASCII-coded version of the letter “a”.

The hash-code is the following 384-bit string.

```
54a59b9f22b0b808 80d8427e548b7c23 abd873486e1f035d ce9cd697e8517503
                 3caa88e6d57bc35e fae0b5afd3145f31
```

B.7.3 Example 3

In this example, the data string is the 3-byte string consisting of the ASCII-coded version of “abc”. This is equivalent to the bit string “01100001 01100010 01100011”.

After the padding process, the single 16-word block derived from the data string is as follows.

```
61626380 00000000 00000000 00000000 00000000 00000000 00000000 00000000
00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000
00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000
00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000018
```

The following are (hexadecimal representations of) the successive values of the variables X_0, X_1, X_2, X_3, X_4, X_5, X_6 and X_7.

```
init  cbbb9d5dc1059ed8 629a292a367cd507 9159015a3070dd17 152fecd8f70e5939
   67332667ffc00b31 8eb44a8768581511 db0c2e0d64f98fa7 47b5481dbefa4fa4
 0  470994ad30873f88 cbbb9d5dc1059ed8 629a292a367cd507 9159015a3070dd17
   bd03f724be6075f9 67332667ffc00b31 8eb44a8768581511 db0c2e0d64f98fa7
 1  2e91230306a12ae0 470994ad30873f88 cbbb9d5dc1059ed8 629a292a367cd507
   5e1b4e1695372b9e bd03f724be6075f9 67332667ffc00b31 8eb44a8768581511
 2  eebe5d379be707ad 2e91230306a12ae0 470994ad30873f88 cbbb9d5dc1059ed8
   54074a65aef34336 5e1b4e1695372b9e bd03f724be6075f9 67332667ffc00b31
 3  e308483153e15ad6 eebe5d379be707ad 2e91230306a12ae0 470994ad30873f88
   086c5b2d36a89178 54074a65aef34336 5e1b4e1695372b9e bd03f724be6075f9
 4  3a7a023c593d8479 e308483153e15ad6 eebe5d379be707ad 2e91230306a12ae0
   8aa1144850633794 086c5b2d36a89178 54074a65aef34336 5e1b4e1695372b9e
 5  333199a85f92b052 3a7a023c593d8479 e308483153e15ad6 eebe5d379be707ad
   7a6316f0ef047ce7 8aa1144850633794 086c5b2d36a89178 54074a65aef34336
 6  76f0741213dd2ef6 333199a85f92b052 3a7a023c593d8479 e308483153e15ad6
   74063cba385f0675 7a6316f0ef047ce7 8aa1144850633794 086c5b2d36a89178
 7  02f2a04d3aab1629 76f0741213dd2ef6 333199a85f92b052 3a7a023c593d8479
   1688b9bf14980fc0 74063cba385f0675 7a6316f0ef047ce7 8aa1144850633794
 8  73e5b2a1704a0349 02f2a04d3aab1629 76f0741213dd2ef6 333199a85f92b052
   fd00139f705907d0 1688b9bf14980fc0 74063cba385f0675 7a6316f0ef047ce7
 9  bf3f67ba12882648 73e5b2a1704a0349 02f2a04d3aab1629 76f0741213dd2ef6
   652e311d4f0a4257 fd00139f705907d0 1688b9bf14980fc0 74063cba385f0675
```

```
10 33254508bb2ea48d bf3f67ba12882648 73e5b2a1704a0349 02f2a04d3aab1629
  9e18991c4f39f0ba 652e311d4f0a4257 fd00139f705907d0 1688b9bf14980fc0
11 c1fdb2a0205ea0e5 33254508bb2ea48d bf3f67ba12882648 73e5b2a1704a0349
  04732e8bc4044582 9e18991c4f39f0ba 652e311d4f0a4257 fd00139f705907d0
12 185f9ff038a50f39 c1fdb2a0205ea0e5 33254508bb2ea48d bf3f67ba12882648
  8b4acfc4d2b8afe6 04732e8bc4044582 9e18991c4f39f0ba 652e311d4f0a4257
13 e5f06744c0d7563a 185f9ff038a50f39 c1fdb2a0205ea0e5 33254508bb2ea48d
  2fa93d1ce9523015 8b4acfc4d2b8afe6 04732e8bc4044582 9e18991c4f39f0ba
14 7e32dc0e9f414783 e5f06744c0d7563a 185f9ff038a50f39 c1fdb2a0205ea0e5
  3a9950aaa5e75884 2fa93d1ce9523015 8b4acfc4d2b8afe6 04732e8bc4044582
15 1eab6159ae87ef6d 7e32dc0e9f414783 e5f06744c0d7563a 185f9ff038a50f39
  153b895cfbc436c5 3a9950aaa5e75884 2fa93d1ce9523015 8b4acfc4d2b8afe6
16 33ef2cebbf1739aa 1eab6159ae87ef6d 7e32dc0e9f414783 e5f06744c0d7563a
  9d1a64baf1d366aa 153b895cfbc436c5 3a9950aaa5e75884 2fa93d1ce9523015
17 7df1b65f1b87d6ca 33ef2cebbf1739aa 1eab6159ae87ef6d 7e32dc0e9f414783
  5b6e369d36e8e181 9d1a64baf1d366aa 153b895cfbc436c5 3a9950aaa5e75884
18 63a24014a34bb0f6 7df1b65f1b87d6ca 33ef2cebbf1739aa 1eab6159ae87ef6d
  e13e610eae680d85 5b6e369d36e8e181 9d1a64baf1d366aa 153b895cfbc436c5
19 f1aabd313309509b 63a24014a34bb0f6 7df1b65f1b87d6ca 33ef2cebbf1739aa
  674385f0d87db94f e13e610eae680d85 5b6e369d36e8e181 9d1a64baf1d366aa
20 9ba737ae88a72c64 f1aabd313309509b 63a24014a34bb0f6 7df1b65f1b87d6ca
  3fc2614c43906c0f 674385f0d87db94f e13e610eae680d85 5b6e369d36e8e181
21 042c2dc9a5bf558a 9ba737ae88a72c64 f1aabd313309509b 63a24014a34bb0f6
  19316bebc88e01f2 3fc2614c43906c0f 674385f0d87db94f e13e610eae680d85
22 7799c75acc748c0f 042c2dc9a5bf558a 9ba737ae88a72c64 f1aabd313309509b
  a7bbd65bf64f58c8 19316bebc88e01f2 3fc2614c43906c0f 674385f0d87db94f
23 ccf99a80f92bf002 7799c75acc748c0f 042c2dc9a5bf558a 9ba737ae88a72c64
  e52a24fae4e8fc9b a7bbd65bf64f58c8 19316bebc88e01f2 3fc2614c43906c0f
24 ae993474363efe68 ccf99a80f92bf002 7799c75acc748c0f 042c2dc9a5bf558a
  587f308d58681928 e52a24fae4e8fc9b a7bbd65bf64f58c8 19316bebc88e01f2
25 335063d1a2aec92f ae993474363efe68 ccf99a80f92bf002 7799c75acc748c0f
  c2d6d65e38c6ea79 587f308d58681928 e52a24fae4e8fc9b a7bbd65bf64f58c8
26 53a78b0cca01ba37 335063d1a2aec92f ae993474363efe68 ccf99a80f92bf002
  3b65a26c3c92c8f3 c2d6d65e38c6ea79 587f308d58681928 e52a24fae4e8fc9b
27 ab7ffa529f622930 53a78b0cca01ba37 335063d1a2aec92f ae993474363efe68
  b9d8a2f2762901ea 3b65a26c3c92c8f3 c2d6d65e38c6ea79 587f308d58681928
28 e428bb43afe3d63e ab7ffa529f622930 53a78b0cca01ba37 335063d1a2aec92f
  6a8527525f898726 b9d8a2f2762901ea 3b65a26c3c92c8f3 c2d6d65e38c6ea79
29 bbed541a5128088c e428bb43afe3d63e ab7ffa529f622930 53a78b0cca01ba37
  7973aadbde294be9 6a8527525f898726 b9d8a2f2762901ea 3b65a26c3c92c8f3
30 4c5c38df7ec8baf4 bbed541a5128088c e428bb43afe3d63e ab7ffa529f622930
  422ceea0200e9ee4 7973aadbde294be9 6a8527525f898726 b9d8a2f2762901ea
31 4ba456ec244033ed 4c5c38df7ec8baf4 bbed541a5128088c e428bb43afe3d63e
  7cf40857056d86b0 422ceea0200e9ee4 7973aadbde294be9 6a8527525f898726
32 aa4a6ab2ac5f5dd8 4ba456ec244033ed 4c5c38df7ec8baf4 bbed541a5128088c
  ad2b1ecfb5bfc556 7cf40857056d86b0 422ceea0200e9ee4 7973aadbde294be9
33 9cb941f2ced774b3 aa4a6ab2ac5f5dd8 4ba456ec244033ed 4c5c38df7ec8baf4
  029f66c7b4569bf0 ad2b1ecfb5bfc556 7cf40857056d86b0 422ceea0200e9ee4
34 39265f358594de27 9cb941f2ced774b3 aa4a6ab2ac5f5dd8 4ba456ec244033ed
  3f7b1c260c82e54f 029f66c7b4569bf0 ad2b1ecfb5bfc556 7cf40857056d86b0
35 09cca487d39b02a1 39265f358594de27 9cb941f2ced774b3 aa4a6ab2ac5f5dd8
  4a22b37b58a5b1b0 3f7b1c260c82e54f 029f66c7b4569bf0 ad2b1ecfb5bfc556
36 d48d97ce438cf4f0 09cca487d39b02a1 39265f358594de27 9cb941f2ced774b3
  a239e00b8baa0410 4a22b37b58a5b1b0 3f7b1c260c82e54f 029f66c7b4569bf0
37 d6f41e25a8b634d6 d48d97ce438cf4f0 09cca487d39b02a1 39265f358594de27
  25755cb8179dd0b0 a239e00b8baa0410 4a22b37b58a5b1b0 3f7b1c260c82e54f
38 54078334358573b4 d6f41e25a8b634d6 d48d97ce438cf4f0 09cca487d39b02a1
  0e419fb0802b0efc 25755cb8179dd0b0 a239e00b8baa0410 4a22b37b58a5b1b0
39 db24f9a03f4fff6b 54078334358573b4 d6f41e25a8b634d6 d48d97ce438cf4f0
  d30e99b4b394b090 0e419fb0802b0efc 25755cb8179dd0b0 a239e00b8baa0410
40 3604c53a845efc37 db24f9a03f4fff6b 54078334358573b4 d6f41e25a8b634d6
  791b2b4af7338b99 d30e99b4b394b090 0e419fb0802b0efc 25755cb8179dd0b0
41 f41b1c0eee89bdc6 3604c53a845efc37 db24f9a03f4fff6b 54078334358573b4
```

```
  e319b77d9e4e87f9 791b2b4af7338b99 d30e99b4b394b090 0e419fb0802b0efc
42 36644ae374632e3a f41b1c0eee89bdc6 3604c53a845efc37 db24f9a03f4fff6b
  458250878a3972b2 e319b77d9e4e87f9 791b2b4af7338b99 d30e99b4b394b090
43 88806f6ae9fcd65b 36644ae374632e3a f41b1c0eee89bdc6 3604c53a845efc37
  cfde2e6ea54fa576 458250878a3972b2 e319b77d9e4e87f9 791b2b4af7338b99
44 51dcaa36995c301d 88806f6ae9fcd65b 36644ae374632e3a f41b1c0eee89bdc6
  e37f778353998050 cfde2e6ea54fa576 458250878a3972b2 e319b77d9e4e87f9
45 ef5e3885a2f238df 51dcaa36995c301d 88806f6ae9fcd65b 36644ae374632e3a
  740e347f24e18fda e37f778353998050 cfde2e6ea54fa576 458250878a3972b2
46 eb3753f4283f4818 ef5e3885a2f238df 51dcaa36995c301d 88806f6ae9fcd65b
  0ae48cf840bb8be9 740e347f24e18fda e37f778353998050 cfde2e6ea54fa576
47 a6998d63a5d09e04 eb3753f4283f4818 ef5e3885a2f238df 51dcaa36995c301d
  e21095012ee0b72a 0ae48cf840bb8be9 740e347f24e18fda e37f778353998050
48 d3698fb64df175b0 a6998d63a5d09e04 eb3753f4283f4818 ef5e3885a2f238df
  c2f0b90ffce80739 e21095012ee0b72a 0ae48cf840bb8be9 740e347f24e18fda
49 317a3b295b991914 d3698fb64df175b0 a6998d63a5d09e04 eb3753f4283f4818
  1cadff2e6cb5aa4d c2f0b90ffce80739 e21095012ee0b72a 0ae48cf840bb8be9
50 0941da08148ba463 317a3b295b991914 d3698fb64df175b0 a6998d63a5d09e04
  833eb9a4bb5a073e 1cadff2e6cb5aa4d c2f0b90ffce80739 e21095012ee0b72a
51 494ac238d68c3d0b 0941da08148ba463 317a3b295b991914 d3698fb64df175b0
  80c8fc138e645028 833eb9a4bb5a073e 1cadff2e6cb5aa4d c2f0b90ffce80739
52 c87e9168db9e97de 494ac238d68c3d0b 0941da08148ba463 317a3b295b991914
  65cf7f6a829aca04 80c8fc138e645028 833eb9a4bb5a073e 1cadff2e6cb5aa4d
53 edb4448879391dbb c87e9168db9e97de 494ac238d68c3d0b 0941da08148ba463
  7729c85475dd318f 65cf7f6a829aca04 80c8fc138e645028 833eb9a4bb5a073e
54 073775c2456dc7db edb4448879391dbb c87e9168db9e97de 494ac238d68c3d0b
  a9cca0b6266b1d77 7729c85475dd318f 65cf7f6a829aca04 80c8fc138e645028
55 54de8857b24afaf7 073775c2456dc7db edb4448879391dbb c87e9168db9e97de
  8de51cff2ae4b068 a9cca0b6266b1d77 7729c85475dd318f 65cf7f6a829aca04
56 8a9cdd80f7f09c05 54de8857b24afaf7 073775c2456dc7db edb4448879391dbb
  a60ba5e9ebaeb96a 8de51cff2ae4b068 a9cca0b6266b1d77 7729c85475dd318f
57 3eeb22a7524d8d7f 8a9cdd80f7f09c05 54de8857b24afaf7 073775c2456dc7db
  e2e6830b139df58f a60ba5e9ebaeb96a 8de51cff2ae4b068 a9cca0b6266b1d77
58 0ed77c9cde8883d3 3eeb22a7524d8d7f 8a9cdd80f7f09c05 54de8857b24afaf7
  38413a2052387a9e e2e6830b139df58f a60ba5e9ebaeb96a 8de51cff2ae4b068
59 e64e4135f9d30dbc 0ed77c9cde8883d3 3eeb22a7524d8d7f 8a9cdd80f7f09c05
  45b640454c75c349 38413a2052387a9e e2e6830b139df58f a60ba5e9ebaeb96a
60 1ca93a293d544328 e64e4135f9d30dbc 0ed77c9cde8883d3 3eeb22a7524d8d7f
  efbef83a35c0319e 45b640454c75c349 38413a2052387a9e e2e6830b139df58f
61 3dc764f89e54043a 1ca93a293d544328 e64e4135f9d30dbc 0ed77c9cde8883d3
  a57784945550cf94 efbef83a35c0319e 45b640454c75c349 38413a2052387a9e
62 56fb5883f1c87a05 3dc764f89e54043a 1ca93a293d544328 e64e4135f9d30dbc
  f5198a41eb80e022 a57784945550cf94 efbef83a35c0319e 45b640454c75c349
63 24a1124262a331c7 56fb5883f1c87a05 3dc764f89e54043a 1ca93a293d544328
  06edacae6e7b54ad f5198a41eb80e022 a57784945550cf94 efbef83a35c0319e
64 eb85d19201c89694 24a1124262a331c7 56fb5883f1c87a05 3dc764f89e54043a
  9ced24983eec8723 06edacae6e7b54ad f5198a41eb80e022 a57784945550cf94
65 cc981ab3a59c1db4 eb85d19201c89694 24a1124262a331c7 56fb5883f1c87a05
  eac5516336bc8882 9ced24983eec8723 06edacae6e7b54ad f5198a41eb80e022
66 ceef5d997e148b44 cc981ab3a59c1db4 eb85d19201c89694 24a1124262a331c7
  617bbf70bb165212 eac5516336bc8882 9ced24983eec8723 06edacae6e7b54ad
67 689edf608a8e3f14 ceef5d997e148b44 cc981ab3a59c1db4 eb85d19201c89694
  3280d88472c100fd 617bbf70bb165212 eac5516336bc8882 9ced24983eec8723
68 1e6e0255ab88079f 689edf608a8e3f14 ceef5d997e148b44 cc981ab3a59c1db4
  f2001138439902b1 3280d88472c100fd 617bbf70bb165212 eac5516336bc8882
69 8c5d3b7fdad66e70 1e6e0255ab88079f 689edf608a8e3f14 ceef5d997e148b44
  90d18ec8b69f0345 f2001138439902b1 3280d88472c100fd 617bbf70bb165212
70 32e5ed8655871e9b 8c5d3b7fdad66e70 1e6e0255ab88079f 689edf608a8e3f14
  51105f6241313777 90d18ec8b69f0345 f2001138439902b1 3280d88472c100fd
71 bcd5061679be7336 32e5ed8655871e9b 8c5d3b7fdad66e70 1e6e0255ab88079f
  454b99f654443ad0 51105f6241313777 90d18ec8b69f0345 f2001138439902b1
72 e7d913b6678e78ef bcd5061679be7336 32e5ed8655871e9b 8c5d3b7fdad66e70
  1ff613b5aa63776e 454b99f654443ad0 51105f6241313777 90d18ec8b69f0345
```

```
73 e6b8cb8dfa3475ab e7d913b6678e78ef bcd5061679be7336 32e5ed8655871e9b
  2e75f34303d39bb0 1ff613b5aa63776e 454b99f654443ad0 51105f6241313777
74 fdd4a30e168c4ae5 e6b8cb8dfa3475ab e7d913b6678e78ef bcd5061679be7336
  83a35dbe2a64fc26 2e75f34303d39bb0 1ff613b5aa63776e 454b99f654443ad0
75 12aeb6268dfa3e14 fdd4a30e168c4ae5 e6b8cb8dfa3475ab e7d913b6678e78ef
  f660943b276786f7 83a35dbe2a64fc26 2e75f34303d39bb0 1ff613b5aa63776e
76 055b73814cf102b4 12aeb6268dfa3e14 fdd4a30e168c4ae5 e6b8cb8dfa3475ab
  c4b149710f5d6a71 f660943b276786f7 83a35dbe2a64fc26 2e75f34303d39bb0
77 95d33150de6df44c 055b73814cf102b4 12aeb6268dfa3e14 fdd4a30e168c4ae5
  c7f7bff08ebf0d30 c4b149710f5d6a71 f660943b276786f7 83a35dbe2a64fc26
78 5306143f64497b00 95d33150de6df44c 055b73814cf102b4 12aeb6268dfa3e14
  ca06a219cc701096 c7f7bff08ebf0d30 c4b149710f5d6a71 f660943b276786f7
79 ff44d7e1849dbfb3 5306143f64497b00 95d33150de6df44c 055b73814cf102b4
  1952e0c3a227c0f2 ca06a219cc701096 c7f7bff08ebf0d30 c4b149710f5d6a71
```

The following eight words, Y_0, Y_1, Y_2, Y_3, Y_4, Y_5, Y_6 and Y_7, represent the output of the final iteration of the round-function.

Y_0 = cbbb9d5dc1059ed8 ⊎ ff44d7e1849dbfb3 = cb00753f45a35e8b
Y_1 = 629a292a367cd507 ⊎ 5306143f64497b00 = b5a03d699ac65007
Y_2 = 9159015a3070dd17 ⊎ 95d33150de6df44c = 272c32ab0eded163
Y_3 = 152fecd8f70e5939 ⊎ 055b73814cf102b4 = 1a8b605a43ff5bed
Y_4 = 67332667ffc00b31 ⊎ 1952e0c3a227c0f2 = 8086072ba1e7cc23
Y_5 = 8eb44a8768581511 ⊎ ca06a219cc701096 = 58baeca134c825a7
Y_6 = db0c2e0d64f98fa7 ⊎ c7f7bff08ebf0d30 = a303edfdf3b89cd7
Y_7 = 47b5481dbefa4fa4 ⊎ c4b149710f5d6a71 = 0c66918ece57ba15

The hash value is the following 384-bit string.

```
cb00753f45a35e8b b5a03d699ac65007 272c32ab0eded163 1a8b605a43ff5bed
                 8086072ba1e7cc23 58baeca134c825a7
```

B.7.4 Example 4

In this example, the data string is the 14-byte string consisting of the ASCII-coded version of

"message digest"

The hash-code is the following 384-bit string.

```
473ed35167ec1f5d 8e550368a3db39be 54639f828868e945 4c239fc8b52e3c61
                 dbd0d8b4de1390c2 56dcbb5d5fd99cd5
```

B.7.5 Example 5

In this example, the data string is the 26-byte string consisting of the ASCII-coded version of

"abcdefghijklmnopqrstuvwxyz"

The hash-code is the following 384-bit string.

```
feb67349df3db6f5 924815d6c3dc133f 091809213731fe5c 7b5f4999e463479f
                 f2877f5f2936fa63 bb43784b12f3ebb4
```

B.7.6 Example 6

In this example, the data string is the 62-byte string consisting of the ASCII-coded version of

"ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz0123456789"

The hash-code is the following 384-bit string.

```
1761336e3f7cbfe5 1deb137f026f89e0 1a448e3b1fafa640 39c1464ee8732f11
                 a5341a6f41e0c202 294736ed64db1a84
```

B.7.7 Example 7

In this example, the data string is the 80-byte string consisting of the ASCII-coded version of eight repetitions of

"1234567890"

The hash-code is the following 384-bit string.

```
b12932b0627d1c06 0942f54477641556 55bd4da0c9afa6dd 9b9ef53129af1b8f
                 b0195996d2de9ca0 df9d821ffee67026
```

B.7.8 Example 8

In this example, the data string is the 56-byte string consisting of the ASCII-coded version of

"abcdbcdecdefdefgefghfghighijhijkijkljklmklmnlmnomnopnopq"

The hash-code is the following 384-bit string.

```
3391fdddfc8dc739 3707a65b1b470939 7cf8b1d162af05ab fe8f450de5f36bc6
                 b0455a8520bc4e6f 5fe95b1fe3c8452b
```

B.7.9 Example 9

In this example, the data string is the 1 000 000-byte string consisting of the ASCII-coded version of "a" repeated 10^6 times.

The hash-code is the following 384-bit string.

```
9d0e1809716474cb 086e834e310a4a1c ed149e9c00f24852 7972cec5704c2a5b
                 07b8b3dc38ecc4eb ae97ddd87f3d8985
```

B.7.10 Example 10

In this example, the data string is the 112-byte string consisting of the ASCII-coded version of

"abcdefghbcdefghicdefghijdefghijkefghijklfghijklmghijklmn
hijklmnoijklmnopjklmnopqklmnopqrlmnopqrsmnopqrstnopqrstu"

(with no line break after the first n).

After the padding process, the following two 16-word blocks are derived from the data string.

```
61626364 65666768 62636465 66676869 63646566 6768696a 64656667 68696a6b
65666768 696a6b6c 66676869 6a6b6c6d 6768696a 6b6c6d6e 68696a6b 6c6d6e6f
696a6b6c 6d6e6f70 6a6b6c6d 6e6f7071 6b6c6d6e 6f707172 6c6d6e6f 70717273
6d6e6f70 71727374 6e6f7071 72737475 80000000 00000000 00000000 00000000

00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000
00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000
00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000
00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000380
```

The following are (hexadecimal representations of) the successive values of the variables X_0, X_1, X_2, X_3, X_4, X_5, X_6 and X_7 in the first block process.

```
init  cbbb9d5dc1059ed8 629a292a367cd507 9159015a3070dd17 152fecd8f70e5939
   67332667ffc00b31 8eb44a8768581511 db0c2e0d64f98fa7 47b5481dbefa4fa4
 0  4709949195eda6f0 cbbb9d5dc1059ed8 629a292a367cd507 9159015a3070dd17
   bd03f70923c6dd61 67332667ffc00b31 8eb44a8768581511 db0c2e0d64f98fa7
 1  78d3f8bc03a38303 4709949195eda6f0 cbbb9d5dc1059ed8 629a292a367cd507
   ae067f071cd18a36 bd03f70923c6dd61 67332667ffc00b31 8eb44a8768581511
 2  ed59d30beff95306 78d3f8bc03a38303 4709949195eda6f0 cbbb9d5dc1059ed8
   c180c7a74ed5cf1f ae067f071cd18a36 bd03f70923c6dd61 67332667ffc00b31
```

```
3  8e7fe2aba3168f2b ed59d30beff95306 78d3f8bc03a38303 4709949195eda6f0
  d92d19667920b327 c180c7a74ed5cf1f ae067f071cd18a36 bd03f70923c6dd61
4  1174f9b374a9263a 8e7fe2aba3168f2b ed59d30beff95306 78d3f8bc03a38303
  dd371f2d13661c52 d92d19667920b327 c180c7a74ed5cf1f ae067f071cd18a36
5  27aaafb7fbef806b 1174f9b374a9263a 8e7fe2aba3168f2b ed59d30beff95306
  21af3c6430a9af9c dd371f2d13661c52 d92d19667920b327 c180c7a74ed5cf1f
6  b352d03a0bd34d65 27aaafb7fbef806b 1174f9b374a9263a 8e7fe2aba3168f2b
  69397de9a30e1473 21af3c6430a9af9c dd371f2d13661c52 d92d19667920b327
7  412db7f990563d7c b352d03a0bd34d65 27aaafb7fbef806b 1174f9b374a9263a
  5062fd5924e2b62e 69397de9a30e1473 21af3c6430a9af9c dd371f2d13661c52
8  0f79040546e6edf7 412db7f990563d7c b352d03a0bd34d65 27aaafb7fbef806b
  6b6c511b25a6bdbc 5062fd5924e2b62e 69397de9a30e1473 21af3c6430a9af9c
9  ebf02410f67b8ee7 0f79040546e6edf7 412db7f990563d7c b352d03a0bd34d65
  dac695b91543ae80 6b6c511b25a6bdbc 5062fd5924e2b62e 69397de9a30e1473
10 97aa05d89b8dbe6d ebf02410f67b8ee7 0f79040546e6edf7 412db7f990563d7c
  83b8b72646c0b598 dac695b91543ae80 6b6c511b25a6bdbc 5062fd5924e2b62e
11 23d0a36b692118eb 97aa05d89b8dbe6d ebf02410f67b8ee7 0f79040546e6edf7
  a5f6c5155e221e8c 83b8b72646c0b598 dac695b91543ae80 6b6c511b25a6bdbc
12 e1041368d2fca1a2 23d0a36b692118eb 97aa05d89b8dbe6d ebf02410f67b8ee7
  ae01675bfb003180 a5f6c5155e221e8c 83b8b72646c0b598 dac695b91543ae80
13 45bd6f69efec540d e1041368d2fca1a2 23d0a36b692118eb 97aa05d89b8dbe6d
  c35cc50c1cf7ef98 ae01675bfb003180 a5f6c5155e221e8c 83b8b72646c0b598
14 c237fa23abb9bc16 45bd6f69efec540d e1041368d2fca1a2 23d0a36b692118eb
  a16c4f134b28923e c35cc50c1cf7ef98 ae01675bfb003180 a5f6c5155e221e8c
15 b4092df1c0f81853 c237fa23abb9bc16 45bd6f69efec540d e1041368d2fca1a2
  008178e17fa649f2 a16c4f134b28923e c35cc50c1cf7ef98 ae01675bfb003180
16 21e5c91d11809c13 b4092df1c0f81853 c237fa23abb9bc16 45bd6f69efec540d
  a26dfa04ed8c9b63 008178e17fa649f2 a16c4f134b28923e c35cc50c1cf7ef98
17 2c957137cd4304a5 21e5c91d11809c13 b4092df1c0f81853 c237fa23abb9bc16
  6be210614b10949b a26dfa04ed8c9b63 008178e17fa649f2 a16c4f134b28923e
18 2180e61afe322bc7 2c957137cd4304a5 21e5c91d11809c13 b4092df1c0f81853
  76396996200065f7 6be210614b10949b a26dfa04ed8c9b63 008178e17fa649f2
19 f2911c11c96e5ff5 2180e61afe322bc7 2c957137cd4304a5 21e5c91d11809c13
  1bc2160f4f3711dc 76396996200065f7 6be210614b10949b a26dfa04ed8c9b63
20 5eab10b19a5143a8 f2911c11c96e5ff5 2180e61afe322bc7 2c957137cd4304a5
  98d2b19d201f2bb6 1bc2160f4f3711dc 76396996200065f7 6be210614b10949b
21 29c5348d87cd5590 5eab10b19a5143a8 f2911c11c96e5ff5 2180e61afe322bc7
  4324c8caccf7753c 98d2b19d201f2bb6 1bc2160f4f3711dc 76396996200065f7
22 33c6b4a0166b7c9c 29c5348d87cd5590 5eab10b19a5143a8 f2911c11c96e5ff5
  d49cef5bd2dec121 4324c8caccf7753c 98d2b19d201f2bb6 1bc2160f4f3711dc
23 1db4ee606d2a7a96 33c6b4a0166b7c9c 29c5348d87cd5590 5eab10b19a5143a8
  b17d15b397521ab3 d49cef5bd2dec121 4324c8caccf7753c 98d2b19d201f2bb6
24 5cef5b2f00142660 1db4ee606d2a7a96 33c6b4a0166b7c9c 29c5348d87cd5590
  789e540f22e13932 b17d15b397521ab3 d49cef5bd2dec121 4324c8caccf7753c
25 ff74f4a162435903 5cef5b2f00142660 1db4ee606d2a7a96 33c6b4a0166b7c9c
  6c0be33dcc6e7572 789e540f22e13932 b17d15b397521ab3 d49cef5bd2dec121
26 41740b736e9676a9 ff74f4a162435903 5cef5b2f00142660 1db4ee606d2a7a96
  d8e401251592da6c 6c0be33dcc6e7572 789e540f22e13932 b17d15b397521ab3
27 931059fe9279ff1d 41740b736e9676a9 ff74f4a162435903 5cef5b2f00142660
  7f31116887eea596 d8e401251592da6c 6c0be33dcc6e7572 789e540f22e13932
28 356d08d982e2ead4 931059fe9279ff1d 41740b736e9676a9 ff74f4a162435903
  40c28c34b1bbe906 7f31116887eea596 d8e401251592da6c 6c0be33dcc6e7572
29 89dc825e7235c74b 356d08d982e2ead4 931059fe9279ff1d 41740b736e9676a9
  7a499ae05da50bf2 40c28c34b1bbe906 7f31116887eea596 d8e401251592da6c
30 97901f333e662fdc 89dc825e7235c74b 356d08d982e2ead4 931059fe9279ff1d
  4472b2e331ddfab4 7a499ae05da50bf2 40c28c34b1bbe906 7f31116887eea596
31 69c8f40eb38b6022 97901f333e662fdc 89dc825e7235c74b 356d08d982e2ead4
  177589502dd39aa2 4472b2e331ddfab4 7a499ae05da50bf2 40c28c34b1bbe906
32 4920943ffe52b207 69c8f40eb38b6022 97901f333e662fdc 89dc825e7235c74b
  6b813a0d0cdf4991 177589502dd39aa2 4472b2e331ddfab4 7a499ae05da50bf2
33 b4cb0df332d108ab 4920943ffe52b207 69c8f40eb38b6022 97901f333e662fdc
  8fe3d28097f18618 6b813a0d0cdf4991 177589502dd39aa2 4472b2e331ddfab4
34 e7748fbf744a5240 b4cb0df332d108ab 4920943ffe52b207 69c8f40eb38b6022
```

```
  0d7ab03208f1d7a5 8fe3d28097f18618 6b813a0d0cdf4991 177589502dd39aa2
35 7416ca18d9e265e0 e7748fbf744a5240 b4cb0df332d108ab 4920943ffe52b207
  11200c2d47c082f8 0d7ab03208f1d7a5 8fe3d28097f18618 6b813a0d0cdf4991
36 75476f5456e82f9c 7416ca18d9e265e0 e7748fbf744a5240 b4cb0df332d108ab
  3024702447f76224 11200c2d47c082f8 0d7ab03208f1d7a5 8fe3d28097f18618
37 f638a568b53a2f8f 75476f5456e82f9c 7416ca18d9e265e0 e7748fbf744a5240
  6217c1c02153302c 3024702447f76224 11200c2d47c082f8 0d7ab03208f1d7a5
38 c418f6f90602c79a f638a568b53a2f8f 75476f5456e82f9c 7416ca18d9e265e0
  87f0901c227adbb3 6217c1c02153302c 3024702447f76224 11200c2d47c082f8
39 4f1f4f21df3dcf43 c418f6f90602c79a f638a568b53a2f8f 75476f5456e82f9c
  fb7c63fcddf4a1c2 87f0901c227adbb3 6217c1c02153302c 3024702447f76224
40 13eb82e4b98d0e67 4f1f4f21df3dcf43 c418f6f90602c79a f638a568b53a2f8f
  fb6c0e54d48d4f2d fb7c63fcddf4a1c2 87f0901c227adbb3 6217c1c02153302c
41 820e75046567bace 13eb82e4b98d0e67 4f1f4f21df3dcf43 c418f6f90602c79a
  b16a9397472f0123 fb6c0e54d48d4f2d fb7c63fcddf4a1c2 87f0901c227adbb3
42 741fa5dc290dd02c 820e75046567bace 13eb82e4b98d0e67 4f1f4f21df3dcf43
  ed40c88214823792 b16a9397472f0123 fb6c0e54d48d4f2d fb7c63fcddf4a1c2
43 a4809bf6da6aa8bd 741fa5dc290dd02c 820e75046567bace 13eb82e4b98d0e67
  bec3d7e88c855194 ed40c88214823792 b16a9397472f0123 fb6c0e54d48d4f2d
44 d70b1aa4c800979c a4809bf6da6aa8bd 741fa5dc290dd02c 820e75046567bace
  4962f310bdbd54b0 bec3d7e88c855194 ed40c88214823792 b16a9397472f0123
45 9a195492cfdb4745 d70b1aa4c800979c a4809bf6da6aa8bd 741fa5dc290dd02c
  2c82d09cf05cf687 4962f310bdbd54b0 bec3d7e88c855194 ed40c88214823792
46 b7e68364f07f017e 9a195492cfdb4745 d70b1aa4c800979c a4809bf6da6aa8bd
  2a1ffb84031b1b6c 2c82d09cf05cf687 4962f310bdbd54b0 bec3d7e88c855194
47 0e574b8e0b35e452 b7e68364f07f017e 9a195492cfdb4745 d70b1aa4c800979c
  29bdab29ee472a23 2a1ffb84031b1b6c 2c82d09cf05cf687 4962f310bdbd54b0
48 c176009cf82fa842 0e574b8e0b35e452 b7e68364f07f017e 9a195492cfdb4745
  cca47fbe31b335f4 29bdab29ee472a23 2a1ffb84031b1b6c 2c82d09cf05cf687
49 5d4f78c7a9bdbed2 c176009cf82fa842 0e574b8e0b35e452 b7e68364f07f017e
  eaf198615e99ffdc cca47fbe31b335f4 29bdab29ee472a23 2a1ffb84031b1b6c
50 51ab3be828d8d13c 5d4f78c7a9bdbed2 c176009cf82fa842 0e574b8e0b35e452
  bd527cd188fb59ae eaf198615e99ffdc cca47fbe31b335f4 29bdab29ee472a23
51 4d639ef80d0f6d3e 51ab3be828d8d13c 5d4f78c7a9bdbed2 c176009cf82fa842
  b2611b90f90d732f bd527cd188fb59ae eaf198615e99ffdc cca47fbe31b335f4
52 bba9c9efe0fbc6c8 4d639ef80d0f6d3e 51ab3be828d8d13c 5d4f78c7a9bdbed2
  fc0579337591a2c9 b2611b90f90d732f bd527cd188fb59ae eaf198615e99ffdc
53 3405d7cad2e8a689 bba9c9efe0fbc6c8 4d639ef80d0f6d3e 51ab3be828d8d13c
  0f6649f64ec8e109 fc0579337591a2c9 b2611b90f90d732f bd527cd188fb59ae
54 ea54d908505798b3 3405d7cad2e8a689 bba9c9efe0fbc6c8 4d639ef80d0f6d3e
  ef48a48999108077 0f6649f64ec8e109 fc0579337591a2c9 b2611b90f90d732f
55 be31d1c0ccc143bc ea54d908505798b3 3405d7cad2e8a689 bba9c9efe0fbc6c8
  4fc2d4cad0c91afc ef48a48999108077 0f6649f64ec8e109 fc0579337591a2c9
56 285a76d23f6a0073 be31d1c0ccc143bc ea54d908505798b3 3405d7cad2e8a689
  a730855599b738a3 4fc2d4cad0c91afc ef48a48999108077 0f6649f64ec8e109
57 a714ceff14bebc24 285a76d23f6a0073 be31d1c0ccc143bc ea54d908505798b3
  53c581dae1831d80 a730855599b738a3 4fc2d4cad0c91afc ef48a48999108077
58 697ca14913a50a26 a714ceff14bebc24 285a76d23f6a0073 be31d1c0ccc143bc
  34d39344354aacd2 53c581dae1831d80 a730855599b738a3 4fc2d4cad0c91afc
59 3a38fa3775d7007c 697ca14913a50a26 a714ceff14bebc24 285a76d23f6a0073
  e26f3a21e9a27691 34d39344354aacd2 53c581dae1831d80 a730855599b738a3
60 44ea14d8e450c844 3a38fa3775d7007c 697ca14913a50a26 a714ceff14bebc24
  5319374fb88dd485 e26f3a21e9a27691 34d39344354aacd2 53c581dae1831d80
61 0928b75c925f91e2 44ea14d8e450c844 3a38fa3775d7007c 697ca14913a50a26
  79f4be3c5a372911 5319374fb88dd485 e26f3a21e9a27691 34d39344354aacd2
62 6db5469fa19c0e27 0928b75c925f91e2 44ea14d8e450c844 3a38fa3775d7007c
  16beec0fec168e79 79f4be3c5a372911 5319374fb88dd485 e26f3a21e9a27691
63 384e3159898a7362 6db5469fa19c0e27 0928b75c925f91e2 44ea14d8e450c844
  55fa3ad1102298a8 16beec0fec168e79 79f4be3c5a372911 5319374fb88dd485
64 483c64d3fdebf828 384e3159898a7362 6db5469fa19c0e27 0928b75c925f91e2
  1a238431921ea75e 55fa3ad1102298a8 16beec0fec168e79 79f4be3c5a372911
65 c9464988a1939bcf 483c64d3fdebf828 384e3159898a7362 6db5469fa19c0e27
  e3f3f08ac90f86cd 1a238431921ea75e 55fa3ad1102298a8 16beec0fec168e79
```

```
 66 98bc93bca795059c c9464988a1939bcf 483c64d3fdebf828 384e3159898a7362
  9e04fb49a5fd91de e3f3f08ac90f86cd 1a238431921ea75e 55fa3ad1102298a8
 67 b6fc101ad1d74e20 98bc93bca795059c c9464988a1939bcf 483c64d3fdebf828
  fd13cd3620f6c1f4 9e04fb49a5fd91de e3f3f08ac90f86cd 1a238431921ea75e
 68 fac26e6e4da4705d b6fc101ad1d74e20 98bc93bca795059c c9464988a1939bcf
  0d60228aa6e55b6e fd13cd3620f6c1f4 9e04fb49a5fd91de e3f3f08ac90f86cd
 69 2a630c58cc27fcaa fac26e6e4da4705d b6fc101ad1d74e20 98bc93bca795059c
  a2f7f27a3ec25aba 0d60228aa6e55b6e fd13cd3620f6c1f4 9e04fb49a5fd91de
 70 159a02d4faee11b4 2a630c58cc27fcaa fac26e6e4da4705d b6fc101ad1d74e20
  b2860fc55bdedaa6 a2f7f27a3ec25aba 0d60228aa6e55b6e fd13cd3620f6c1f4
 71 9d38bdb9df22b557 159a02d4faee11b4 2a630c58cc27fcaa fac26e6e4da4705d
  dfc37c68af65f8bc b2860fc55bdedaa6 a2f7f27a3ec25aba 0d60228aa6e55b6e
 72 d42c3a57cfa78513 9d38bdb9df22b557 159a02d4faee11b4 2a630c58cc27fcaa
  bb56dea6a325ba32 dfc37c68af65f8bc b2860fc55bdedaa6 a2f7f27a3ec25aba
 73 abab4b0ca75a17c7 d42c3a57cfa78513 9d38bdb9df22b557 159a02d4faee11b4
  9ac71d1c037a8bbd bb56dea6a325ba32 dfc37c68af65f8bc b2860fc55bdedaa6
 74 500f7b61186f6c2e abab4b0ca75a17c7 d42c3a57cfa78513 9d38bdb9df22b557
  8347f5736531b3ec 9ac71d1c037a8bbd bb56dea6a325ba32 dfc37c68af65f8bc
 75 4abe0af6a67db2fe 500f7b61186f6c2e abab4b0ca75a17c7 d42c3a57cfa78513
  14e986342ddced0f 8347f5736531b3ec 9ac71d1c037a8bbd bb56dea6a325ba32
 76 e1053fc85f9e56be 4abe0af6a67db2fe 500f7b61186f6c2e abab4b0ca75a17c7
  4779767cc2ec5321 14e986342ddced0f 8347f5736531b3ec 9ac71d1c037a8bbd
 77 7001201948fb3d71 e1053fc85f9e56be 4abe0af6a67db2fe 500f7b61186f6c2e
  5cdf6c58fc052572 4779767cc2ec5321 14e986342ddced0f 8347f5736531b3ec
 78 88146da76ff6f23a 7001201948fb3d71 e1053fc85f9e56be 4abe0af6a67db2fe
  8901cffe7a74db98 5cdf6c58fc052572 4779767cc2ec5321 14e986342ddced0f
 79 5ec3802b9ecfef33 88146da76ff6f23a 7001201948fb3d71 e1053fc85f9e56be
  5f2eead69efb4233 8901cffe7a74db98 5cdf6c58fc052572 4779767cc2ec5321
```

The following eight words, Y_0, Y_1, Y_2, Y_3, Y_4, Y_5, Y_6 and Y_7, represent the output of the round-function in the first block process.

Y_0 = cbbb9d5dc1059ed8 ⊎ 5ec3802b9ecfef33 = 2a7f1d895fd58e0b
Y_1 = 629a292a367cd507 ⊎ 88146da76ff6f23a = eaae96d1a673c741
Y_2 = 9159015a3070dd17 ⊎ 7001201948fb3d71 = 015a2173796c1a88
Y_3 = 152fecd8f70e5939 ⊎ e1053fc85f9e56be = f6352ca156acaff7
Y_4 = 67332667ffc00b31 ⊎ 5f2eead69efb4233 = c662113e9ebb4d64
Y_5 = 8eb44a8768581511 ⊎ 8901cffe7a74db98 = 17b61a85e2ccf0a9
Y_6 = db0c2e0d64f98fa7 ⊎ 5cdf6c58fc052572 = 37eb9a6660feb519
Y_7 = 47b5481dbefa4fa4 ⊎ 4779767cc2ec5321 = 8f2ebe9a81e6a2c5

The following are (hexadecimal representations of) the successive values of the variables Y_0, Y_1, Y_2, Y_3, Y_4, Y_5, Y_6 and Y_7 in the second block process.

```
init  2a7f1d895fd58e0b eaae96d1a673c741 015a2173796c1a88 f6352ca156acaff7
   c662113e9ebb4d64 17b61a85e2ccf0a9 37eb9a6660feb519 8f2ebe9a81e6a2c5
  0  657a3c2ca9639d40 2a7f1d895fd58e0b eaae96d1a673c741 015a2173796c1a88
   791f2ad0055fdd62 c662113e9ebb4d64 17b61a85e2ccf0a9 37eb9a6660feb519
  1  2a4ad5d9b9fd6d86 657a3c2ca9639d40 2a7f1d895fd58e0b eaae96d1a673c741
   dbf2e656b5be3f14 791f2ad0055fdd62 c662113e9ebb4d64 17b61a85e2ccf0a9
  2  f0aa6758653d1664 2a4ad5d9b9fd6d86 657a3c2ca9639d40 2a7f1d895fd58e0b
   6e0466c82f4fd35d dbf2e656b5be3f14 791f2ad0055fdd62 c662113e9ebb4d64
  3  43a76f011a73d317 f0aa6758653d1664 2a4ad5d9b9fd6d86 657a3c2ca9639d40
   1367bd36d15e8b40 6e0466c82f4fd35d dbf2e656b5be3f14 791f2ad0055fdd62
  4  d802c2dfd7cc48f6 43a76f011a73d317 f0aa6758653d1664 2a4ad5d9b9fd6d86
   f73d759b839a2a21 1367bd36d15e8b40 6e0466c82f4fd35d dbf2e656b5be3f14
  5  481208e5e8314602 d802c2dfd7cc48f6 43a76f011a73d317 f0aa6758653d1664
   6b2271a46f14c843 f73d759b839a2a21 1367bd36d15e8b40 6e0466c82f4fd35d
  6  af9f8112df35cf33 481208e5e8314602 d802c2dfd7cc48f6 43a76f011a73d317
   257f4a7d524d7b0b 6b2271a46f14c843 f73d759b839a2a21 1367bd36d15e8b40
  7  6730781342d1131b af9f8112df35cf33 481208e5e8314602 d802c2dfd7cc48f6
   81957ad408cec995 257f4a7d524d7b0b 6b2271a46f14c843 f73d759b839a2a21
  8  82e64c677356a82e 6730781342d1131b af9f8112df35cf33 481208e5e8314602
```

```
  10b62fdce4ebaa51 81957ad408cec995 257f4a7d524d7b0b 6b2271a46f14c843
9  203578820a8f27d0 82e64c677356a82e 6730781342d1131b af9f8112df35cf33
  9937b3a0cb9248a1 10b62fdce4ebaa51 81957ad408cec995 257f4a7d524d7b0b
10 0bac2a84c29a1e2b 203578820a8f27d0 82e64c677356a82e 6730781342d1131b
  6ad288dab3de0d53 9937b3a0cb9248a1 10b62fdce4ebaa51 81957ad408cec995
11 dd3ff8a140485c25 0bac2a84c29a1e2b 203578820a8f27d0 82e64c677356a82e
  3149b728123c465e 6ad288dab3de0d53 9937b3a0cb9248a1 10b62fdce4ebaa51
12 e826239f830c5346 dd3ff8a140485c25 0bac2a84c29a1e2b 203578820a8f27d0
  4bb7b199c4ced186 3149b728123c465e 6ad288dab3de0d53 9937b3a0cb9248a1
13 32215ce49aae40f8 e826239f830c5346 dd3ff8a140485c25 0bac2a84c29a1e2b
  9a2872c72d790d49 4bb7b199c4ced186 3149b728123c465e 6ad288dab3de0d53
14 859533bac457f94e 32215ce49aae40f8 e826239f830c5346 dd3ff8a140485c25
  539f225d25ebeb4c 9a2872c72d790d49 4bb7b199c4ced186 3149b728123c465e
15 a88704d9962849f3 859533bac457f94e 32215ce49aae40f8 e826239f830c5346
  63bf0472ef24f7a5 539f225d25ebeb4c 9a2872c72d790d49 4bb7b199c4ced186
16 3aa5c566a6cfad1c a88704d9962849f3 859533bac457f94e 32215ce49aae40f8
  ce23f6380ead33c2 63bf0472ef24f7a5 539f225d25ebeb4c 9a2872c72d790d49
17 2e9c483a7c08c9c1 3aa5c566a6cfad1c a88704d9962849f3 859533bac457f94e
  b033f945f3e6b4a2 ce23f6380ead33c2 63bf0472ef24f7a5 539f225d25ebeb4c
18 5a68585ae0835231 2e9c483a7c08c9c1 3aa5c566a6cfad1c a88704d9962849f3
  8a0187a9ce93d875 b033f945f3e6b4a2 ce23f6380ead33c2 63bf0472ef24f7a5
19 cf9cd481e6407ced 5a68585ae0835231 2e9c483a7c08c9c1 3aa5c566a6cfad1c
  37a29fa30531bac7 8a0187a9ce93d875 b033f945f3e6b4a2 ce23f6380ead33c2
20 3f463f864f6474d9 cf9cd481e6407ced 5a68585ae0835231 2e9c483a7c08c9c1
  0cf45bb3c07e847d 37a29fa30531bac7 8a0187a9ce93d875 b033f945f3e6b4a2
21 cea26288dff931a5 3f463f864f6474d9 cf9cd481e6407ced 5a68585ae0835231
  34f1b5f46bf48a73 0cf45bb3c07e847d 37a29fa30531bac7 8a0187a9ce93d875
22 89634cd0f4f6c08a cea26288dff931a5 3f463f864f6474d9 cf9cd481e6407ced
  3a728a543405a8e4 34f1b5f46bf48a73 0cf45bb3c07e847d 37a29fa30531bac7
23 625fa38464e5c880 89634cd0f4f6c08a cea26288dff931a5 3f463f864f6474d9
  cee1b47a49b2fc42 3a728a543405a8e4 34f1b5f46bf48a73 0cf45bb3c07e847d
24 7dd21453a15a3b92 625fa38464e5c880 89634cd0f4f6c08a cea26288dff931a5
  9308bfa1be1f800b cee1b47a49b2fc42 3a728a543405a8e4 34f1b5f46bf48a73
25 3d76277bc8cb0601 7dd21453a15a3b92 625fa38464e5c880 89634cd0f4f6c08a
  480e017f5d1f0b1e 9308bfa1be1f800b cee1b47a49b2fc42 3a728a543405a8e4
26 c8d904196f5a1f54 3d76277bc8cb0601 7dd21453a15a3b92 625fa38464e5c880
  4bd2f1f6e940c332 480e017f5d1f0b1e 9308bfa1be1f800b cee1b47a49b2fc42
27 b033139b58b6e423 c8d904196f5a1f54 3d76277bc8cb0601 7dd21453a15a3b92
  f816ec1cbe0adafb 4bd2f1f6e940c332 480e017f5d1f0b1e 9308bfa1be1f800b
28 097768182cb65f57 b033139b58b6e423 c8d904196f5a1f54 3d76277bc8cb0601
  62e3de54dcd8f974 f816ec1cbe0adafb 4bd2f1f6e940c332 480e017f5d1f0b1e
29 3196649ab5f5cc39 097768182cb65f57 b033139b58b6e423 c8d904196f5a1f54
  f6887de116d0bd8f 62e3de54dcd8f974 f816ec1cbe0adafb 4bd2f1f6e940c332
30 f78d3d221d16965f 3196649ab5f5cc39 097768182cb65f57 b033139b58b6e423
  c7e4859c2858ed3c f6887de116d0bd8f 62e3de54dcd8f974 f816ec1cbe0adafb
31 f58e9876b4984b51 f78d3d221d16965f 3196649ab5f5cc39 097768182cb65f57
  621352b394b8ca02 c7e4859c2858ed3c f6887de116d0bd8f 62e3de54dcd8f974
32 38fbf0e726e04f78 f58e9876b4984b51 f78d3d221d16965f 3196649ab5f5cc39
  4319856f17a0a430 621352b394b8ca02 c7e4859c2858ed3c f6887de116d0bd8f
33 f4be0b32a57597a2 38fbf0e726e04f78 f58e9876b4984b51 f78d3d221d16965f
  c6d392a3b4eb0ed8 4319856f17a0a430 621352b394b8ca02 c7e4859c2858ed3c
34 f8a6b3fe2e4f0634 f4be0b32a57597a2 38fbf0e726e04f78 f58e9876b4984b51
  602663c0f34eff33 c6d392a3b4eb0ed8 4319856f17a0a430 621352b394b8ca02
35 9bc3871be8046113 f8a6b3fe2e4f0634 f4be0b32a57597a2 38fbf0e726e04f78
  05542ecd9883c6ba 602663c0f34eff33 c6d392a3b4eb0ed8 4319856f17a0a430
36 f1bd2d46be619585 9bc3871be8046113 f8a6b3fe2e4f0634 f4be0b32a57597a2
  e47b9933bafdc655 05542ecd9883c6ba 602663c0f34eff33 c6d392a3b4eb0ed8
37 24c84b58d119affe f1bd2d46be619585 9bc3871be8046113 f8a6b3fe2e4f0634
  5ae0b1175beb5d2b e47b9933bafdc655 05542ecd9883c6ba 602663c0f34eff33
38 ec6d3abc2b291fd3 24c84b58d119affe f1bd2d46be619585 9bc3871be8046113
  9ecc381d277748a3 5ae0b1175beb5d2b e47b9933bafdc655 05542ecd9883c6ba
39 e266c1f77d5ee90e ec6d3abc2b291fd3 24c84b58d119affe f1bd2d46be619585
  d92f34c110296b32 9ecc381d277748a3 5ae0b1175beb5d2b e47b9933bafdc655
```

```
40 5adbaa463642b570 e266c1f77d5ee90e ec6d3abc2b291fd3 24c84b58d119affe
  83e8f410f859388e d92f34c110296b32 9ecc381d277748a3 5ae0b1175beb5d2b
41 50fdb7bb2e499a34 5adbaa463642b570 e266c1f77d5ee90e ec6d3abc2b291fd3
  257ed8ea645e933a 83e8f410f859388e d92f34c110296b32 9ecc381d277748a3
42 06514212bb7fa152 50fdb7bb2e499a34 5adbaa463642b570 e266c1f77d5ee90e
  466781db35181abe 257ed8ea645e933a 83e8f410f859388e d92f34c110296b32
43 673ed5a55ff2b07d 06514212bb7fa152 50fdb7bb2e499a34 5adbaa463642b570
  ba78f3545e7914f0 466781db35181abe 257ed8ea645e933a 83e8f410f859388e
44 125e2e5118393e2b 673ed5a55ff2b07d 06514212bb7fa152 50fdb7bb2e499a34
  4453b23a3e13b090 ba78f3545e7914f0 466781db35181abe 257ed8ea645e933a
45 07ee813df5910cec 125e2e5118393e2b 673ed5a55ff2b07d 06514212bb7fa152
  eae013a0510d23cc 4453b23a3e13b090 ba78f3545e7914f0 466781db35181abe
46 0a0508f0a1d719c3 07ee813df5910cec 125e2e5118393e2b 673ed5a55ff2b07d
  a93815eb58891016 eae013a0510d23cc 4453b23a3e13b090 ba78f3545e7914f0
47 0fc8f3b3efcb1b96 0a0508f0a1d719c3 07ee813df5910cec 125e2e5118393e2b
  a071cc73b966e801 a93815eb58891016 eae013a0510d23cc 4453b23a3e13b090
48 02aa5b28199f304a 0fc8f3b3efcb1b96 0a0508f0a1d719c3 07ee813df5910cec
  a49f1e14f8a2be7a a071cc73b966e801 a93815eb58891016 eae013a0510d23cc
49 9223e1b34382f104 02aa5b28199f304a 0fc8f3b3efcb1b96 0a0508f0a1d719c3
  bfe2106e512a7331 a49f1e14f8a2be7a a071cc73b966e801 a93815eb58891016
50 e01a1e47ee8d5656 9223e1b34382f104 02aa5b28199f304a 0fc8f3b3efcb1b96
  592b899b35469a78 bfe2106e512a7331 a49f1e14f8a2be7a a071cc73b966e801
51 fa7b17aad857c2f4 e01a1e47ee8d5656 9223e1b34382f104 02aa5b28199f304a
  eb6e85e4682c1671 592b899b35469a78 bfe2106e512a7331 a49f1e14f8a2be7a
52 0c523b7a3c84ab77 fa7b17aad857c2f4 e01a1e47ee8d5656 9223e1b34382f104
  b5e80e871ac0c005 eb6e85e4682c1671 592b899b35469a78 bfe2106e512a7331
53 c773d8b69da1fde2 0c523b7a3c84ab77 fa7b17aad857c2f4 e01a1e47ee8d5656
  be2b0602fc6f8f65 b5e80e871ac0c005 eb6e85e4682c1671 592b899b35469a78
54 c6b1bc79a4f23679 c773d8b69da1fde2 0c523b7a3c84ab77 fa7b17aad857c2f4
  c80bdc57f38a05e4 be2b0602fc6f8f65 b5e80e871ac0c005 eb6e85e4682c1671
55 bef9bb0fe467fd60 c6b1bc79a4f23679 c773d8b69da1fde2 0c523b7a3c84ab77
  1dab0bd116e434e5 c80bdc57f38a05e4 be2b0602fc6f8f65 b5e80e871ac0c005
56 8e3db3e380ec7f22 bef9bb0fe467fd60 c6b1bc79a4f23679 c773d8b69da1fde2
  32ef50751734ffee 1dab0bd116e434e5 c80bdc57f38a05e4 be2b0602fc6f8f65
57 1003ec42412c7b7d 8e3db3e380ec7f22 bef9bb0fe467fd60 c6b1bc79a4f23679
  1ec0d46f349fd058 32ef50751734ffee 1dab0bd116e434e5 c80bdc57f38a05e4
58 375facc76291f85e 1003ec42412c7b7d 8e3db3e380ec7f22 bef9bb0fe467fd60
  59c8bc0488f9768b 1ec0d46f349fd058 32ef50751734ffee 1dab0bd116e434e5
59 bd113d92e0354fb9 375facc76291f85e 1003ec42412c7b7d 8e3db3e380ec7f22
  e66c73db3fad397d 59c8bc0488f9768b 1ec0d46f349fd058 32ef50751734ffee
60 2f61d4fd8e36d9d4 bd113d92e0354fb9 375facc76291f85e 1003ec42412c7b7d
  e9f21933e1c02948 e66c73db3fad397d 59c8bc0488f9768b 1ec0d46f349fd058
61 1b1ad88b92701ae2 2f61d4fd8e36d9d4 bd113d92e0354fb9 375facc76291f85e
  6fd0c1719bcac335 e9f21933e1c02948 e66c73db3fad397d 59c8bc0488f9768b
62 93d09fc06a19c5da 1b1ad88b92701ae2 2f61d4fd8e36d9d4 bd113d92e0354fb9
  b765273f571a571e 6fd0c1719bcac335 e9f21933e1c02948 e66c73db3fad397d
63 04bea2ce99cc3bf6 93d09fc06a19c5da 1b1ad88b92701ae2 2f61d4fd8e36d9d4
  6ab0e443c2f63714 b765273f571a571e 6fd0c1719bcac335 e9f21933e1c02948
64 02ebfc0a13492f52 04bea2ce99cc3bf6 93d09fc06a19c5da 1b1ad88b92701ae2
  77300c52e05af415 6ab0e443c2f63714 b765273f571a571e 6fd0c1719bcac335
65 1bf525abce8d6f04 02ebfc0a13492f52 04bea2ce99cc3bf6 93d09fc06a19c5da
  8faf12c33bb371b9 77300c52e05af415 6ab0e443c2f63714 b765273f571a571e
66 b6a36a3431547328 1bf525abce8d6f04 02ebfc0a13492f52 04bea2ce99cc3bf6
  fa8bb40b4e08100f 8faf12c33bb371b9 77300c52e05af415 6ab0e443c2f63714
67 ffdaf83202af0d72 b6a36a3431547328 1bf525abce8d6f04 02ebfc0a13492f52
  8045a82f723a9b4e fa8bb40b4e08100f 8faf12c33bb371b9 77300c52e05af415
68 12737373d2985232 ffdaf83202af0d72 b6a36a3431547328 1bf525abce8d6f04
  870dbce23bad8988 8045a82f723a9b4e fa8bb40b4e08100f 8faf12c33bb371b9
69 6189f68162b256b5 12737373d2985232 ffdaf83202af0d72 b6a36a3431547328
  8c059af157146580 870dbce23bad8988 8045a82f723a9b4e fa8bb40b4e08100f
70 20b0a9a1d21c482d 6189f68162b256b5 12737373d2985232 ffdaf83202af0d72
  f22b874c96785ec8 8c059af157146580 870dbce23bad8988 8045a82f723a9b4e
71 ef6d863c2127b394 20b0a9a1d21c482d 6189f68162b256b5 12737373d2985232
```

```
 b7aee28337d69dab f22b874c96785ec8 8c059af157146580 870dbce23bad8988
72 d3efe8b442689074 ef6d863c2127b394 20b0a9a1d21c482d 6189f68162b256b5
 22491ab9cdecb6b0 b7aee28337d69dab f22b874c96785ec8 8c059af157146580
73 4694354944a9f487 d3efe8b442689074 ef6d863c2127b394 20b0a9a1d21c482d
 659890a5818d0c50 22491ab9cdecb6b0 b7aee28337d69dab f22b874c96785ec8
74 b93c2403773dd08c 4694354944a9f487 d3efe8b442689074 ef6d863c2127b394
 88c2c2ac52c4f679 659890a5818d0c50 22491ab9cdecb6b0 b7aee28337d69dab
75 025848e3ab6b69d3 b93c2403773dd08c 4694354944a9f487 d3efe8b442689074
 750da3d4e16a1b64 88c2c2ac52c4f679 659890a5818d0c50 22491ab9cdecb6b0
76 396b53e58d04471b 025848e3ab6b69d3 b93c2403773dd08c 4694354944a9f487
 700486bf252cba75 750da3d4e16a1b64 88c2c2ac52c4f679 659890a5818d0c50
77 51b6f9a3c1ceeb4a 396b53e58d04471b 025848e3ab6b69d3 b93c2403773dd08c
 e6b3850de8ae6230 700486bf252cba75 750da3d4e16a1b64 88c2c2ac52c4f679
78 526a98f5dc595406 51b6f9a3c1ceeb4a 396b53e58d04471b 025848e3ab6b69d3
 4f0dcf74aea76f90 e6b3850de8ae6230 700486bf252cba75 750da3d4e16a1b64
79 deb3eeaa973bb9dd 526a98f5dc595406 51b6f9a3c1ceeb4a 396b53e58d04471b
 3665b5dbb6c2e055 4f0dcf74aea76f90 e6b3850de8ae6230 700486bf252cba75
```

The following eight words, Y_0, Y_1, Y_2, Y_3, Y_4, Y_5, Y_6 and Y_7, represent the output of the final iteration of the round-function.

Y_0 = 2a7f1d895fd58e0b ⊎ deb3eeaa973bb9dd = 09330c33f71147e8
Y_1 = eaae96d1a673c741 ⊎ 526a98f5dc595406 = 3d192fc782cd1b47
Y_2 = 015a2173796c1a88 ⊎ 51b6f9a3c1ceeb4a = 53111b173b3b05d2
Y_3 = f6352ca156acaff7 ⊎ 396b53e58d04471b = 2fa08086e3b0f712
Y_4 = c662113e9ebb4d64 ⊎ 3665b5dbb6c2e055 = fcc7c71a557e2db9
Y_5 = 17b61a85e2ccf0a9 ⊎ 4f0dcf74aea76f90 = 66c3e9fa91746039
Y_6 = 37eb9a6660feb519 ⊎ e6b3850de8ae6230 = 1e9f1f7449ad1749
Y_7 = 8f2ebe9a81e6a2c5 ⊎ 700486bf252cba75 = ff334559a7135d3a

The following is the hash value for this message.

```
09330c33f71147e8 3d192fc782cd1b47 53111b173b3b05d2 2fa08086e3b0f712
                 fcc7c71a557e2db9 66c3e9fa91746039
```

B.7.11Example 11

In this example, the data string is the 32-byte string consisting of the ASCII-coded version of

"abcdbcdecdefdefgefghfghighijhijk"

The hash-code is the following 384-bit string.

```
d4cc646a83a55044 df94814db93b6062 e656623db0b9e2da b8819174589bf0c9
                 d7192b9799e30169 8b97adaa3d82e20c
```

B.8 Dedicated Hash-Function 7 (WHIRLPOOL)

B.8.1 Example 1

In this example, the data string is the empty string, i.e. the string of length zero.

The hash-code is the following 512-bit string.

```
19FA61D75522A466 9B44E39C1D2E1726 C530232130D407F8 9AFEE0964997F7A7
3E83BE698B288FEB CF88E3E03C4F0757 EA8964E59B63D937 08B138CC42A66EB3
```

B.8.2 Example 2

In this example, the data string consists of a single byte, namely the ASCII-coded version of the letter “a”.

The hash-code is the following 512-bit string.

```
8ACA2602792AEC6F 11A67206531FB7D7 F0DFF59413145E69 73C45001D0087B42
D11BC645413AEFF6 3A42391A39145A59 1A92200D560195E5 3B478584FDAE231A
```

B.8.3 Example 3

In this example, the data string is the 3-byte string consisting of the ASCII-coded version of “abc”.

After the padding process, the 8 × 8 matrix Z' derived from the data string is as follows.

```
61 62 63 80 00 00 00 00
00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 18
```

The K_0 matrix (from the initialization value, IV) and X'' matrix are as follows.

```
00 00 00 00 00 00 00 00        61 62 63 80 00 00 00 00
00 00 00 00 00 00 00 00        00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00        00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00        00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00        00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00        00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00        00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00        00 00 00 00 00 00 00 18
```

The following are (hexadecimal representations of) the successive values of the variables K_i for i = 1 to 10 and W'.

```
                          i = 1:
30 0B EE C0 AF 90 29 67        0F 34 9A FF 3F F3 2F E0
28 28 28 28 28 28 28 28        EB CD CD 13 CD 26 DE 87
28 28 28 28 28 28 28 28        2D 2C 98 98 5A 98 B4 C2
28 28 28 28 28 28 28 28        89 03 83 8F 8F 06 8F 0C
28 28 28 28 28 28 28 28        00 00 00 00 00 00 00 00
28 28 28 28 28 28 28 28        00 00 00 00 00 00 00 00
28 28 28 28 28 28 28 28        05 14 05 28 11 0A 2D 05
28 28 28 28 28 28 28 28        00 00 00 00 00 00 00 00

                          i = 2:
3B AB 89 F8 EA D1 AE 24        1D 0D 4C DA 43 F6 B0 98
44 45 45 66 45 E9 CB AF        E4 5E 3F B8 7B C7 AA 10
70 FE A4 A4 C5 A4 B2 89        C3 31 D1 56 FD E7 7B 8F
C5 FA A9 E1 E1 CC E1 A0        68 2F 47 A1 BE 4A 53 39
48 AC C0 5C FC FC B8 FC        B2 A2 B8 2F 20 72 F0 6C
8F F7 0E 26 90 8F 8F 69        03 D9 F4 6C 67 B1 79 72
96 79 14 07 D7 85 79 79        2C 67 87 6E FD 5C 25 F8
F8 A8 F8 68 B8 C8 78 F8        44 E6 4C 70 50 7C D8 26

                          i = 3:
D3 19 BF DB 30 46 70 58        EF ED 35 67 80 8E 8D 63
29 5B 23 D1 AF CF 37 DB        2F 03 49 91 5B 18 5C 24
01 2C 8A C2 8B 95 AC 98        77 96 F6 03 BF AA F8 E3
81 63 9E B1 C0 B2 06 A7        0A DC 04 7B 58 5A A5 A1
44 5E 60 7A B0 B2 09 DB        47 96 DA 7F 56 E4 CC 29
```

```
73 5B 2C CF BC 8C BC 71        20 70 D5 D8 50 01 C8 98
DC 67 09 24 EF ED DD D3        A7 4C 23 FA F6 81 49 A1
7B 8D 3B F0 D7 3B 7D 19        4A CE 46 7D 7D B0 73 A9

                          i = 4:
38 BE AA C1 DE 11 65 86        95 BD DE 1E CA 0F CA 19
68 7C F3 D0 4A 87 33 7F        D3 C1 CF 6C A0 2E 41 E8
F3 37 FA DB 98 AD F0 57        74 C3 5C 63 15 C5 B9 8A
C5 E2 42 58 EE 35 8D BC        36 F0 4E 42 FE 2D D0 5E
11 09 F0 E8 99 6E 24 7E        0A 3C 50 76 A1 91 F8 EC
01 C5 D6 ED 10 B0 34 01        48 6B C7 3E 61 D2 A4 DC
FB C9 52 F1 7B 28 EC D3        ED B8 F0 C5 2C F0 5C 72
32 56 DC 0C C7 F1 27 40        FA 3D 00 D4 FB 9A 66 FF

                          i = 5:
AF 25 A5 20 94 9B CF 14        06 A6 BA 18 05 54 8D 33
C1 36 26 A9 E3 C4 53 4D        84 55 FE C4 1F B2 0B 1C
E6 0F 7D 86 77 40 F9 E1        6E A2 93 49 3F 17 89 B7
91 5D E6 BB E2 6A 06 29        7D 02 C9 A0 52 85 BB EF
96 5A 54 CC 4C FE 5E 8D        AC 55 D7 A9 44 48 89 A9
BE E9 31 CB 62 32 3A A6        CB DE BE 43 AA 4D B5 A0
B1 7B 59 18 96 84 6A 47        60 A6 BA C0 25 D9 4F 8C
D4 F0 C9 36 27 59 AF 31        D7 E4 62 E5 D4 A8 CC C0

                          i = 6:
E2 F9 B5 C0 25 37 0B B0        DB 1D A8 4A 33 38 4D B3
39 2B CB A2 16 84 94 A5        97 4C 8E 1A 3E 51 F3 48
60 8A F8 CE FA 34 8C 14        47 66 64 C2 33 F5 F2 A9
7A A5 37 64 41 8C 92 19        85 FD AA B1 D5 CB C3 6E
B3 F3 46 A1 FA 83 3F 89        5D 89 59 F2 E1 F8 71 D4
97 49 3F 48 78 02 CF 7C        8C 1F B9 78 8C 16 DD 05
DC AD E8 BA 1E 00 8F 23        62 AF 63 5F 6D EE D5 F4
92 77 4F 49 ED B0 32 3D        D8 5B 74 35 5F 8A 98 47

                          i = 7:
75 41 63 82 77 4D FF 2F        59 3D 86 BD A8 CE 25 E5
FF FA 38 D0 55 03 46 00        BB 33 95 78 26 63 7D 82
BF 7D 02 49 3E 98 F3 61        EF 46 1D AE DC AD 0C 3C
F4 A8 60 C2 9A E5 CE 0B        AF A0 E2 86 5E 8B A3 F9
C8 DF 5A 44 EE 5D 9D 27        C8 8C 0B 43 27 84 31 F4
23 F4 5A 55 04 75 00 A4        41 5F 51 64 4E 55 78 C2
B0 16 10 12 02 F9 E2 8C        F4 C7 C3 B5 EE A4 C5 86
AC 30 CD 29 68 33 33 1D        49 F8 AB 68 4A 4C 96 B7

                          i = 8:
03 6B F1 82 68 84 AD 89        9C 0D 38 97 73 B2 E4 35
99 40 C6 62 D8 46 71 63        4D 44 89 58 D4 59 27 E8
4C 43 3E 17 4B 19 C2 10        AD 59 2E B0 4C A3 63 32
E2 9C CF D3 4C FF 86 C5        E0 D4 70 F3 83 5A 15 59
21 FF 11 A0 42 DF 26 53        9A 92 69 8C 76 40 A1 51
1B 8E 00 CB 6C E4 4B 13        57 2E 81 EA CB A4 3C 36
A6 12 3B F7 A3 47 B7 CE        5D 63 2F A7 36 BE 4B 61
D9 18 90 0E 3B 28 33 CA        40 0F DA CB 8B 9D E3 8A

                          i = 9:
D0 1C 67 7A 0A 9A 2C F9        4B F0 5E 9B 46 14 16 D0
2A 94 2F 53 4A 63 B6 B2        72 A8 C1 34 47 13 17 2D
88 42 22 46 FE AC A8 B4        17 33 2A 69 FB 34 98 98
47 4A 5C C7 3D 58 35 59        83 B1 EE 37 93 47 EC A0
74 A6 92 5D A5 5C 6F A1        3B 39 67 11 23 35 B5 78
77 17 E6 8C C4 73 5C 39        FC 78 3D 1F 9D 2F B6 AE
08 2A 3B 0B 53 EC 1A C6        3C F9 38 64 96 9B DE 6C
2A F6 58 EB 81 4D E7 62        42 5A D1 47 6C 0C 49 AE
```

```
                          i = 10:
48 95 48 B6 01 EE BC 3A        2F 46 2B 24 C6 F4 86 BB
A5 0D 6B C6 6B ED 8E 81        16 B6 56 2C 73 B4 02 0B
E0 CE 3D CF 88 26 5A 75        F3 04 3E 3A 73 1B CE 72
C2 8C 4A DB C0 F6 9C E9        1A E1 B3 03 D9 7E 6D 4C
54 B7 9C D5 7F 71 85 13        71 81 EE BD B6 C5 7E 27
43 41 4B 8A 97 7D 0B 7B        7D 0E 34 95 71 14 CB D6
63 19 35 BB DB F6 15 7A        C7 97 FC 9D 95 D8 B5 82
6A 7A 4E F6 37 01 82 27        D2 25 29 20 76 D4 EE ED
```

The value of Y' output from the round-function is as follows.

```
4E 24 48 A4 C6 F4 86 BB
16 B6 56 2C 73 B4 02 0B
F3 04 3E 3A 73 1B CE 72
1A E1 B3 03 D9 7E 6D 4C
71 81 EE BD B6 C5 7E 27
7D 0E 34 95 71 14 CB D6
C7 97 FC 9D 95 D8 B5 82
D2 25 29 20 76 D4 EE F5
```

The hash-code is the following 512-bit string.

```
4E2448A4C6F486BB 16B6562C73B4020B F3043E3A731BCE72 1AE1B303D97E6D4C
7181EEBDB6C57E27 7D0E34957114CBD6 C797FC9D95D8B582 D225292076D4EEF5
```

B.8.4 Example 4

In this example, the data string is the 14-byte string consisting of the ASCII-coded version of

```
"message digest"
```

The hash-code is the following 512-bit string.

```
378C84A4126E2DC6 E56DCC7458377AAC 838D00032230F53C E1F5700C0FFB4D3B
8421557659EF55C1 06B4B52AC5A4AAA6 92ED920052838F33 62E86DBD37A8903E
```

B.8.5 Example 5

In this example, the data string is the 26-byte string consisting of the ASCII-coded version of

```
"abcdefghijklmnopqrstuvwxyz"
```

The hash-code is the following 512-bit string.

```
F1D754662636FFE9 2C82EBB9212A484A 8D38631EAD4238F5 442EE13B8054E41B
08BF2A9251C30B6A 0B8AAE86177AB4A6 F68F673E7207865D 5D9819A3DBA4EB3B
```

B.8.6 Example 6

In this example, the data string is the 62-byte string consisting of the ASCII-coded version of

```
"ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz0123456789"
```

The hash-code is the following 512-bit string.

```
DC37E008CF9EE69B F11F00ED9ABA2690 1DD7C28CDEC066CC 6AF42E40F82F3A1E
08EBA26629129D8F B7CB57211B9281A6 5517CC879D7B9621 42C65F5A7AF01467
```

B.8.7 Example 7

In this example, the data string is the 80-byte string consisting of the ASCII-coded version of eight repetitions of

"1234567890"

The hash-code is the following 512-bit string.

```
466EF18BABB0154D 25B9D38A6414F5C0 8784372BCCB204D6 549C4AFADB601429
4D5BD8DF2A6C44E5 38CD047B2681A51A 2C60481E88C5A20B 2C2A80CF3A9A083B
```

B.8.8 Example 8

In this example, the data string is the 32-byte string consisting of the ASCII-coded version of

"abcdbcdecdefdefgefghfghighijhijk"

After the padding process, the two 8 × 8 matrices derived from the data string are as follows.

```
61 62 63 64 62 63 64 65        00 00 00 00 00 00 00 00
63 64 65 66 64 65 66 67        00 00 00 00 00 00 00 00
65 66 67 68 66 67 68 69        00 00 00 00 00 00 00 00
67 68 69 6A 68 69 6A 6B        00 00 00 00 00 00 00 00
80 00 00 00 00 00 00 00        00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00        00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00        00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00        00 00 00 00 00 00 01 00
```

The first Z' matrix is as follows.

```
61 62 63 64 62 63 64 65
63 64 65 66 64 65 66 67
65 66 67 68 66 67 68 69
67 68 69 6A 68 69 6A 6B
80 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00
```

For the first Z' matrix, the K_0 matrix (from the initialization value, IV) and the X'' matrix are as follows.

```
00 00 00 00 00 00 00 00        61 62 63 64 62 63 64 65
00 00 00 00 00 00 00 00        63 64 65 66 64 65 66 67
00 00 00 00 00 00 00 00        65 66 67 68 66 67 68 69
00 00 00 00 00 00 00 00        67 68 69 6A 68 69 6A 6B
00 00 00 00 00 00 00 00        80 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00        00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00        00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00        00 00 00 00 00 00 00 00
```

The following are (hexadecimal representations of) the successive values of the variables K_i for i = 1 to 10 and W'.

```
                               i = 1:
30 0B EE C0 AF 90 29 67        86 B9 56 DD B4 BD 40 C2
28 28 28 28 28 28 28 28        0B 48 C1 2E 83 9C 2E 41
28 28 28 28 28 28 28 28        40 5E 0A ED 5C E9 42 E7
28 28 28 28 28 28 28 28        B2 1E 5B 93 43 07 7C 4D
28 28 28 28 28 28 28 28        19 04 67 A3 57 CF DA ED
28 28 28 28 28 28 28 28        59 36 7D 57 F8 E7 EA 60
28 28 28 28 28 28 28 28        98 D1 1B 6A C6 1C 4B CD
28 28 28 28 28 28 28 28        5E B9 76 56 F3 51 F4 43
```

```
                        i = 2:
3B AB 89 F8 EA D1 AE 24         10 54 A2 C2 9E 00 80 4F
44 45 45 66 45 E9 CB AF         6B C6 9F 0A 98 41 BA 45
70 FE A4 A4 C5 A4 B2 89         6B 0B DE 38 1B F6 5A 3F
C5 FA A9 E1 E1 CC E1 A0         34 F5 52 E4 38 30 DA 32
48 AC C0 5C FC FC B8 FC         A7 4E 3B C9 F2 58 65 5B
8F F7 0E 26 90 8F 8F 69         2C 84 5C F8 DE BA 57 52
96 79 14 07 D7 85 79 79         0B 0B CB 4F 5F 5F 13 10
F8 A8 F8 68 B8 C8 78 F8         B4 43 90 D6 92 4F 65 12

                        i = 3:
D3 19 BF DB 30 46 70 58         8F 55 E3 10 51 E9 E7 43
29 5B 23 D1 AF CF 37 DB         F3 AE 56 A1 2E 86 11 01
01 2C 8A C2 8B 95 AC 98         01 78 57 78 4C 25 EE 95
81 63 9E B1 C0 B2 06 A7         8B 13 D5 66 9A EA A5 53
44 5E 60 7A B0 B2 09 DB         55 E0 9A 46 78 79 57 56
73 5B 2C CF BC 8C BC 71         E2 3E F3 AF D4 5F 66 62
DC 67 09 24 EF ED DD D3         05 E9 CA 43 59 FC 08 53
7B 8D 3B F0 D7 3B 7D 19         6A 11 68 9A 3D 24 86 2C

                        i = 4:
38 BE AA C1 DE 11 65 86         BD A3 5F AC C8 4B 7B 24
68 7C F3 D0 4A 87 33 7F         D4 D5 53 36 8A FA 90 C8
F3 37 FA DB 98 AD F0 57         7D 9A 3C 52 B5 B9 28 0B
C5 E2 42 58 EE 35 8D BC         FE CD D7 48 5D 98 AC 21
11 09 F0 E8 99 6E 24 7E         F6 D3 E3 F5 A1 C0 68 F0
01 C5 D6 ED 10 B0 34 01         D9 77 56 2D F1 C4 3C B6
FB C9 52 F1 7B 28 EC D3         C2 85 71 D3 B2 94 91 69
32 56 DC 0C C7 F1 27 40         E2 B9 81 C5 7C 60 42 23

                        i = 5:
AF 25 A5 20 94 9B CF 14         15 03 B3 53 CF 70 04 4D
C1 36 26 A9 E3 C4 53 4D         D0 74 26 9B 60 EC 9B 92
E6 0F 7D 86 77 40 F9 E1         BE 22 90 B3 34 54 C2 84
91 5D E6 BB E2 6A 06 29         20 F3 7D 53 7D D1 C1 BA
96 5A 54 CC 4C FE 5E 8D         87 0E 9B F5 41 7C 2D 29
BE E9 31 CB 62 32 3A A6         A8 52 51 52 21 71 D5 9D
B1 7B 59 18 96 84 6A 47         96 9C 26 6D 4A B9 C6 AB
D4 F0 C9 36 27 59 AF 31         5A 2B DD 3C D9 8A D1 04

                        i = 6:
E2 F9 B5 C0 25 37 0B B0         B1 44 C5 6B 09 97 59 91
39 2B CB A2 16 84 94 A5         CF 0D 2C 26 C0 C7 93 54
60 8A F8 CE FA 34 8C 14         18 D0 BE 9C 7A 35 09 8A
7A A5 37 64 41 8C 92 19         32 8B E8 B4 2C B0 10 2A
B3 F3 46 A1 FA 83 3F 89         02 01 B5 CC 2C 68 E9 9C
97 49 3F 48 78 02 CF 7C         12 BF E0 28 EB 7D 3F F1
DC AD E8 BA 1E 00 8F 23         49 BD 0B 4E 55 81 21 AA
92 77 4F 49 ED B0 32 3D         35 F4 59 17 F1 5C 49 DF

                        i = 7:
75 41 63 82 77 4D FF 2F         DD D3 6C 6C F0 7A C1 16
FF FA 38 D0 55 03 46 00         03 42 87 2D A6 3A 4C F4
BF 7D 02 49 3E 98 F3 61         5D C0 C5 7D 6B BC 49 81
F4 A8 60 C2 9A E5 CE 0B         7C 12 58 40 F0 CD DA 1E
C8 DF 5A 44 EE 5D 9D 27         46 AD D5 C4 F9 77 40 C7
23 F4 5A 55 04 75 00 A4         FF 2E 7D 33 E9 7D 27 BA
B0 16 10 12 02 F9 E2 8C         2C CC DF EF 3A 86 58 08
AC 30 CD 29 68 33 33 1D         FB AC B4 52 D2 63 9C 25
```

```
                          i = 8:
03 6B F1 82 68 84 AD 89         7B 3B 3C 7B 2D 73 FF 3C
99 40 C6 62 D8 46 71 63         32 7A 01 65 DD 7C 8C 7A
4C 43 3E 17 4B 19 C2 10         0F 70 81 E9 7B A3 B6 80
E2 9C CF D3 4C FF 86 C5         25 DF D5 33 66 08 A2 55
21 FF 11 A0 42 DF 26 53         AB 95 54 FC ED D2 51 92
1B 8E 00 CB 6C E4 4B 13         10 3A 15 9C FE CA CF 6E
A6 12 3B F7 A3 47 B7 CE         38 DA 67 14 8A 69 EB B3
D9 18 90 0E 3B 28 33 CA         92 2A 69 0B 03 4B 46 69

                          i = 9:
D0 1C 67 7A 0A 9A 2C F9         56 21 86 2A 9C 0B D3 95
2A 94 2F 53 4A 63 B6 B2         D4 5A B8 28 42 F2 59 DC
88 42 22 46 FE AC A8 B4         B2 55 11 33 27 2D E8 43
47 4A 5C C7 3D 58 35 59         B7 2C 18 04 84 19 B2 C7
74 A6 92 5D A5 5C 6F A1         0A DD FF 03 52 91 16 83
77 17 E6 8C C4 73 5C 39         3E A7 8D 11 02 CF E8 C8
08 2A 3B 0B 53 EC 1A C6         A1 22 69 ED AD B3 2A B4
2A F6 58 EB 81 4D E7 62         BE 53 E9 F0 7C B0 79 E7

                         i = 10:
48 95 48 B6 01 EE BC 3A         16 5A 82 D1 23 C3 52 8F
A5 0D 6B C6 6B ED 8E 81         26 E9 35 9E 6B C5 7A 23
E0 CE 3D CF 88 26 5A 75         17 EE A9 FF B7 C7 B4 99
C2 8C 4A DB C0 F6 9C E9         71 FD 96 BC 8F 74 63 4E
54 B7 9C D5 7F 71 85 13         B3 BE 30 9F 01 2A 59 09
43 41 4B 8A 97 7D 0B 7B         72 91 14 59 5F 08 6E 76
63 19 35 BB DB F6 15 7A         07 18 AF E3 65 BC 09 DE
6A 7A 4E F6 37 01 82 27         B6 AF A1 80 BC EC 2A 98
```

The value of Y' output from the round-function for the first Z' matrix is as follows.

```
77 38 E1 B5 41 A0 36 EA
45 8D 50 F8 0F A0 1C 44
72 88 CE 97 D1 A0 DC F0
16 95 FF D6 E7 1D 09 25
33 BE 30 9F 01 2A 59 09
72 91 14 59 5F 08 6E 76
07 18 AF E3 65 BC 09 DE
B6 AF A1 80 BC EC 2A 98
```

The second Z' matrix is as follows.

```
00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00
00 00 00 00 00 00 01 00
```

For the second Z' matrix, the K_0 matrix and the X'' matrix are as follows.

```
77 38 E1 B5 41 A0 36 EA         77 38 E1 B5 41 A0 36 EA
45 8D 50 F8 0F A0 1C 44         45 8D 50 F8 0F A0 1C 44
72 88 CE 97 D1 A0 DC F0         72 88 CE 97 D1 A0 DC F0
16 95 FF D6 E7 1D 09 25         16 95 FF D6 E7 1D 09 25
33 BE 30 9F 01 2A 59 09         33 BE 30 9F 01 2A 59 09
72 91 14 59 5F 08 6E 76         72 91 14 59 5F 08 6E 76
07 18 AF E3 65 BC 09 DE         07 18 AF E3 65 BC 09 DE
B6 AF A1 80 BC EC 2A 98         B6 AF A1 80 BC EC 2B 98
```

The following are (hexadecimal representations of) the successive values of the variables K_i for i = 1 to 10 and W'.

```
                          i = 1:
1A 78 4D 7D BD 4C 17 E6         18 23 C6 E8 87 B8 01 4F
27 31 10 AA 63 C5 9E 25         00 00 00 00 00 00 00 00
7A 2E B7 48 C4 5D E0 23         00 00 00 00 00 00 00 00
6D 0D 61 9F 6C 1D 80 AE         00 00 00 00 00 00 00 00
01 A2 D5 6E DB 41 D9 A0         00 00 00 00 00 00 00 00
E9 06 4C D1 27 95 FA 86         8C 23 05 AF 46 26 23 23
77 62 31 BC B4 4E C6 01         00 00 00 00 00 00 00 00
6F CD BC 98 10 78 6F EC         00 00 00 00 00 00 00 00

                          i = 2:
EB 0F 86 07 40 38 54 4F         DF 8A 74 7E 14 4C 22 D0
87 EF DC C8 FE 45 3D 83         2B 04 B7 AE 74 89 5A 13
99 0E F5 4E 73 1F C0 EA         2F FD BC A4 26 03 AD 74
EF E0 05 7F D2 C2 41 39         99 67 EA 50 34 08 BD B9
65 8F 5D 92 3E 9A AF 47         A8 7B 8E 1A 3B 56 CD 91
A9 1D 1C 13 BD 15 73 41         77 59 60 2D DD A2 4A 70
81 AD 80 BD 88 B3 B3 C3         03 43 90 91 2B DE 8E 37
16 26 63 99 AC 18 5D D0         48 6B C0 54 B9 C6 72 C9

                          i = 3:
7A A3 A3 3A 99 FD F6 5E         6B 92 48 05 C3 F4 1A 6D
E0 78 67 CD 3E 60 BF A7         45 20 59 41 0D 59 73 6D
BC 06 8D 5D 98 70 34 84         AF 72 CF 6A 4B B6 11 F4
80 E8 69 7D 44 CF 6B E6         A2 6D AD C1 12 CC 43 6C
7E 35 09 07 AF 76 70 C3         95 8F C4 AE 60 94 74 74
3B 7E 15 0D CA 5E A9 0A         4B AB 72 C2 3E 2C BC 6D
8D 10 98 19 22 3B FC 57         ED BF 23 B0 D6 82 B0 E8
AB DE A9 DD D3 B6 68 14         C0 4B 32 6B B5 14 B7 BB

                          i = 4:
3D 21 15 88 E4 48 75 78         78 5A 13 A3 25 81 79 C9
47 BF 56 CC 8E D4 63 CA         DC 69 90 E0 14 F2 39 AC
AE F0 D0 31 74 25 3C 4E         89 5A 8F 66 7F F9 FC E3
08 F7 59 13 4F 6D DD 37         3B 5C C5 02 8C 4D 96 0A
C9 70 32 87 D8 F2 C1 E8         00 28 03 E7 DA 63 5E F5
90 E9 2D 7C AB A0 8E A7         DA 35 A5 BF B6 AB C7 EA
BF 22 A6 93 C1 6E 34 74         0D 5B 90 B8 88 56 C7 9F
58 40 F3 10 BF 03 3C 14         65 09 D2 D8 ED DA C6 B1

                          i = 5:
AE 58 59 43 80 F4 F6 14         6B 77 9A 58 6E 21 06 C1
14 5C 2E E0 5F B0 8E FD         A7 2D B3 6D 1D AD 9E 3C
CF B7 1F C1 9A AC 6B 6A         32 CF E9 10 D3 AD CD EB
92 5C 25 E7 6C 28 7B 6B         EE 4B 44 77 56 BC BC 63
57 B5 8E 30 FB E4 61 9B         41 05 39 5E 0B A3 8A 46
38 5D B4 49 F9 44 F8 C9         07 B9 8B 76 67 41 AC BD
A5 EE 29 38 0C 2D A8 70         E9 86 74 54 82 35 6F D9
45 8B FE 5E 05 C3 A6 89         27 FB C9 68 EE 1E C7 57

                          i = 6:
B1 F3 E2 33 93 63 14 AC         53 41 C7 63 02 40 D8 3F
DD 80 87 12 BF E5 70 0E         7F D8 0D FB 5D 97 CF 7A
A5 F5 16 A8 2A 82 CC 76         52 47 5A 93 4A BC D9 84
8A F5 DD F3 5F B1 11 57         95 47 26 76 78 E9 10 42
62 34 D3 BC 57 72 C7 DC         E5 BA FB 23 2C 32 7B 6D
8D E2 8A 61 DC 88 CB 1A         62 CA FA 6D 35 F6 AA 13
53 35 F7 4C 99 ED 19 26         43 BF 3B F2 1B 0D B4 46
95 01 75 82 F7 A6 F7 2D         BC 1C 9F 38 97 77 17 5B
```

```
                          i = 7:
7E 42 E3 38 39 72 B7 82         61 E7 C2 37 B0 E6 F6 2B
79 B2 EA 12 B3 68 75 B0         46 FE 01 CA 0E 34 5A 26
D8 8D 5F 05 2F AA 73 D2         80 2E F8 49 0D 5F 17 60
90 FC 91 61 30 BB 7B 5C         89 D5 48 F0 59 6D 73 E8
5A 1B F6 C2 20 10 61 23         72 D8 71 5E 44 80 9B E3
E5 31 C5 68 BC 4F 85 F8         8C 90 07 54 63 6B 77 0D
60 72 0A BA A7 90 27 03         63 1B 4E CF D7 C6 5D B5
A7 FD 03 BB E3 E9 CA 19         91 92 11 87 0F FE EA AB

                          i = 8:
12 EF 8A A7 F3 B5 7E F6         42 C9 DC 71 10 DA FA 7C
E9 59 60 9F 18 84 D3 ED         02 5B 59 54 A2 45 83 20
93 3E 12 E9 EA 51 D7 C1         53 B6 C4 85 4D C3 52 A5
EF DA 8A 82 CB 14 13 93         3B 65 C0 24 87 E8 20 BD
4C F0 7B 81 0D 03 9C F3         C5 3C E3 C4 9C DE 93 9F
2F 40 9C A8 76 D4 7D A3         CD 47 4A B3 CB C3 69 1B
32 72 85 CE 7A BD 39 58         24 5E FB 0E 45 E6 7A 96
06 1A CE 00 E7 5F EC B5         2B 36 CC A8 8A 64 C1 40

                          i = 9:
7C D9 89 12 FC AB 39 B2         AC C3 BD D6 26 A6 41 F0
20 E1 E9 E6 79 8D 5E 4F         E7 D8 5F 60 03 D2 7B F8
99 70 2C 2A CA E1 07 48         3F 48 9A 48 16 88 0E 1D
A4 85 C1 1F 74 6C 23 DC         D9 C7 62 1D 42 6F 86 A4
CF C8 1D F4 64 41 C6 1B         AD A6 9F 9A 29 CC 8C 6D
7B 0D 6B 84 2A 58 16 40         14 63 22 F6 04 B0 94 F4
4F 0A 55 C3 38 6A 0C 2D         E9 1D 7D 05 0C A8 44 F4
E6 31 16 BA AE C9 AC EC         A7 B1 5B F5 48 C5 2E F7

                         i = 10:
B4 74 E1 56 96 31 B9 6C         5D A0 9F 11 4E 31 46 8B
21 A1 B6 33 CC 89 68 1A         B0 5B A0 58 EB C4 53 0C
B1 97 25 86 7B 2B 3F 09         F8 F2 94 C5 0F 4E B9 92
4C 73 C7 62 93 A8 15 CF         11 50 9D 2F 6F F4 55 4C
55 15 C0 C0 9A 05 05 16         25 03 F8 9C 1A EF E7 12
23 44 8D 8D D3 5F B3 6E         09 05 62 60 A1 0D 65 20
7E 6C 2D 37 12 D0 F3 3E         94 83 05 43 C8 43 93 38
CE B8 04 F2 8D 9F C9 99         C2 F4 DA 98 A0 D7 C8 65
```

The value of Y' output from the round-function for the second Z' matrix is as follows.

```
2A 98 7E A4 0F 91 70 61
F5 D6 F0 A0 E4 64 4F 48
8A 7A 5A 52 DE EE 65 62
07 C5 62 F9 88 E9 5C 69
16 BD C8 03 1B C5 BE 1B
7B 94 76 39 FE 05 0B 56
93 9B AA A0 AD FF 9A E6
74 5B 7B 18 1C 3B E3 FD
```

The hash-code is the following 512-bit string.

```
2A987EA40F917061 F5D6F0A0E4644F48 8A7A5A52DEEE6562 07C562F988E95C69
16BDC8031BC5BE1B 7B947639FE050B56 939BAAA0ADFF9AE6 745B7B181C3BE3FD
```

B.8.9 Example 9

In this example, the data string is the 1 000 000-byte string consisting of the ASCII-coded version of "a" repeated 10^6 times.

The hash-code is the following 512-bit string.

```
0C99005BEB57EFF5 0A7CF005560DDF5D 29057FD86B20BFD6 2DECA0F1CCEA4AF5
1FC15490EDDC47AF 32BB2B66C34FF9AD 8C6008AD677F7712 6953B226E4ED8B01
```

B.9 Dedicated Hash-Function 8 (SHA-224)

B.9.1 Example 1

In this example, the data string is the empty string, i.e. the string of length zero.

The hash-code is the following 224-bit string.

```
d14a028c 2a3a2bc9 476102bb 288234c4 15a2b01f 828ea62a c5b3e42f
```

B.9.2 Example 2

In this example, the data string consists of a single byte, namely the ASCII-coded version of the letter "a".

The hash-code is the following 224-bit string.

```
abd37534 c7d9a2ef b9465de9 31cd7055 ffdb8879 563ae980 78d6d6d5
```

B.9.3 Example 3

In this example, the data string is the 3-byte string consisting of the ASCII-coded version of "abc". This is equivalent to the bit string "01100001 01100010 01100011".

After the padding process, the single 16-word block derived from the data string is as follows.

```
61626380 00000000 00000000 00000000 00000000 00000000 00000000 00000000
00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000018
```

The following are (hexadecimal representations of) the successive values of the variables X_0, X_1, X_2, X_3, X_4, X_5, X_6 and X_7.

```
init: c1059ed8 367cd507 3070dd17 f70e5939 ffc00b31 68581511 64f98fa7 befa4fa4
  0 0e96b2da c1059ed8 367cd507 3070dd17 0434225e ffc00b31 68581511 64f98fa7
  1 c20dab6b 0e96b2da c1059ed8 367cd507 9cab416f 0434225e ffc00b31 68581511
  2 ab113b7a c20dab6b 0e96b2da c1059ed8 82177fe8 9cab416f 0434225e ffc00b31
  3 8253cc1a ab113b7a c20dab6b 0e96b2da 8346b27d 82177fe8 9cab416f 0434225e
  4 08a0dc0c 8253cc1a ab113b7a c20dab6b 05b557db 8346b27d 82177fe8 9cab416f
  5 b2ca3a91 08a0dc0c 8253cc1a ab113b7a 898dc7bb 05b557db 8346b27d 82177fe8
  6 0b6b9023 b2ca3a91 08a0dc0c 8253cc1a a2e49147 898dc7bb 05b557db 8346b27d
  7 f09d116d 0b6b9023 b2ca3a91 08a0dc0c 7a84120d a2e49147 898dc7bb 05b557db
  8 ed6fa633 f09d116d 0b6b9023 b2ca3a91 c037faad 7a84120d a2e49147 898dc7bb
  9 55e6a367 ed6fa633 f09d116d 0b6b9023 aae50091 c037faad 7a84120d a2e49147
 10 0817e82b 55e6a367 ed6fa633 f09d116d c8c53a2c aae50091 c037faad 7a84120d
 11 17142334 0817e82b 55e6a367 ed6fa633 dd4c7be9 c8c53a2c aae50091 c037faad
 12 fc4f023e 17142334 0817e82b 55e6a367 87bea51a dd4c7be9 c8c53a2c aae50091
 13 be316902 fc4f023e 17142334 0817e82b 65141125 87bea51a dd4c7be9 c8c53a2c
 14 1d80d178 be316902 fc4f023e 17142334 4545f53a 65141125 87bea51a dd4c7be9
 15 9f341a45 1d80d178 be316902 fc4f023e 6a61c411 4545f53a 65141125 87bea51a
 16 0f324db9 9f341a45 1d80d178 be316902 06c80d6a 6a61c411 4545f53a 65141125
 17 ffe7012b 0f324db9 9f341a45 1d80d178 b7b601f4 06c80d6a 6a61c411 4545f53a
 18 62932ab8 ffe7012b 0f324db9 9f341a45 763b627a b7b601f4 06c80d6a 6a61c411
 19 5207d867 62932ab8 ffe7012b 0f324db9 7fbba936 763b627a b7b601f4 06c80d6a
 20 07d55ccb 5207d867 62932ab8 ffe7012b 9ba5a6ea 7fbba936 763b627a b7b601f4
```

```
21 dece98a4 07d55ccb 5207d867 62932ab8 293ffb5d 9ba5a6ea 7fbba936 763b627a
22 e62a812e dece98a4 07d55ccb 5207d867 28fe0fd9 293ffb5d 9ba5a6ea 7fbba936
23 57206fb8 e62a812e dece98a4 07d55ccb c76084ea 28fe0fd9 293ffb5d 9ba5a6ea
24 6a6abcf0 57206fb8 e62a812e dece98a4 b2614c5e c76084ea 28fe0fd9 293ffb5d
25 937514f0 6a6abcf0 57206fb8 e62a812e b42ec21c b2614c5e c76084ea 28fe0fd9
26 82af3ffb 937514f0 6a6abcf0 57206fb8 be6f6760 b42ec21c b2614c5e c76084ea
27 eca3bcd5 82af3ffb 937514f0 6a6abcf0 1dccbb10 be6f6760 b42ec21c b2614c5e
28 2d1576c4 eca3bcd5 82af3ffb 937514f0 01641929 1dccbb10 be6f6760 b42ec21c
29 fe3c8658 2d1576c4 eca3bcd5 82af3ffb fc4b36c5 01641929 1dccbb10 be6f6760
30 0d7cce07 fe3c8658 2d1576c4 eca3bcd5 a4a4a3a4 fc4b36c5 01641929 1dccbb10
31 cce1951d 0d7cce07 fe3c8658 2d1576c4 4be9475c a4a4a3a4 fc4b36c5 01641929
32 09b76257 cce1951d 0d7cce07 fe3c8658 0ccddd86 4be9475c a4a4a3a4 fc4b36c5
33 f827767e 09b76257 cce1951d 0d7cce07 db116db7 0ccddd86 4be9475c a4a4a3a4
34 e4a0bb48 f827767e 09b76257 cce1951d 994e2bac db116db7 0ccddd86 4be9475c
35 d8bb1041 e4a0bb48 f827767e 09b76257 5b730abb 994e2bac db116db7 0ccddd86
36 2a2e32f4 d8bb1041 e4a0bb48 f827767e 22e15c59 5b730abb 994e2bac db116db7
37 0d275ca8 2a2e32f4 d8bb1041 e4a0bb48 f6c39382 22e15c59 5b730abb 994e2bac
38 7902369c 0d275ca8 2a2e32f4 d8bb1041 d9f8c2e0 f6c39382 22e15c59 5b730abb
39 f3c80288 7902369c 0d275ca8 2a2e32f4 00e3a7bb d9f8c2e0 f6c39382 22e15c59
40 483bba4d f3c80288 7902369c 0d275ca8 f0a8198c 00e3a7bb d9f8c2e0 f6c39382
41 d75d4d26 483bba4d f3c80288 7902369c fcecdcd4 f0a8198c 00e3a7bb d9f8c2e0
42 0744b618 d75d4d26 483bba4d f3c80288 03186faa fcecdcd4 f0a8198c 00e3a7bb
43 9cce9f01 0744b618 d75d4d26 483bba4d a56f6bbf 03186faa fcecdcd4 f0a8198c
44 a3701bd9 9cce9f01 0744b618 d75d4d26 af1bef5f a56f6bbf 03186faa fcecdcd4
45 131d4c09 a3701bd9 9cce9f01 0744b618 ecb77e1b af1bef5f a56f6bbf 03186faa
46 fb3777d9 131d4c09 a3701bd9 9cce9f01 1d601f44 ecb77e1b af1bef5f a56f6bbf
47 847ea00e fb3777d9 131d4c09 a3701bd9 503a7b95 1d601f44 ecb77e1b af1bef5f
48 aaa69347 847ea00e fb3777d9 131d4c09 5eeb9930 503a7b95 1d601f44 ecb77e1b
49 505caf28 aaa69347 847ea00e fb3777d9 ce695893 5eeb9930 503a7b95 1d601f44
50 675e0b02 505caf28 aaa69347 847ea00e c22dd75f ce695893 5eeb9930 503a7b95
51 abd26099 675e0b02 505caf28 aaa69347 1409c3f8 c22dd75f ce695893 5eeb9930
52 0df9857a abd26099 675e0b02 505caf28 2d864d9f 1409c3f8 c22dd75f ce695893
53 308b8799 0df9857a abd26099 675e0b02 02524f02 2d864d9f 1409c3f8 c22dd75f
54 909cc059 308b8799 0df9857a abd26099 6f2a444a 02524f02 2d864d9f 1409c3f8
55 8d25bd94 909cc059 308b8799 0df9857a 1273c622 6f2a444a 02524f02 2d864d9f
56 f32141da 8d25bd94 909cc059 308b8799 1771ed3f 1273c622 6f2a444a 02524f02
57 8ce24395 f32141da 8d25bd94 909cc059 f52f66a6 1771ed3f 1273c622 6f2a444a
58 07bcd846 8ce24395 f32141da 8d25bd94 149db547 f52f66a6 1771ed3f 1273c622
59 622d5e5b 07bcd846 8ce24395 f32141da b6f4c630 149db547 f52f66a6 1771ed3f
60 c693fc7a 622d5e5b 07bcd846 8ce24395 13dfb889 b6f4c630 149db547 f52f66a6
61 55d1c760 c693fc7a 622d5e5b 07bcd846 7e730e00 13dfb889 b6f4c630 149db547
62 fd89031b 55d1c760 c693fc7a 622d5e5b 55489ee6 7e730e00 13dfb889 b6f4c630
63 6203de4a fd89031b 55d1c760 c693fc7a 2aedb1b3 55489ee6 7e730e00 13dfb889
```

The following eight words, Y_0, Y_1, Y_2, Y_3, Y_4, Y_5, Y_6 and Y_7, represent the output of the final iteration of the round-function.

$$Y_0 = \text{c1059ed8} \boxplus \text{6203de4a} = \text{23097d22}$$
$$Y_1 = \text{367cd507} \boxplus \text{fd89031b} = \text{3405d822}$$
$$Y_2 = \text{3070dd17} \boxplus \text{55d1c760} = \text{8642a477}$$
$$Y_3 = \text{f70e5939} \boxplus \text{c693fc7a} = \text{bda255b3}$$
$$Y_4 = \text{ffc00b31} \boxplus \text{2aedb1b3} = \text{2aadbce4}$$
$$Y_5 = \text{68581511} \boxplus \text{55489ee6} = \text{bda0b3f7}$$
$$Y_6 = \text{64f98fa7} \boxplus \text{7e730e00} = \text{e36c9da7}$$
$$Y_7 = \text{befa4fa4} \boxplus \text{13dfb889} = \text{ad25f72d}$$

The hash value is the following 224-bit string.

```
23097d22 3405d822 8642a477 bda255b3 2aadbce4 bda0b3f7 e36c9da7
```

B.9.4 Example 4

In this example, the data string is the 14-byte string consisting of the ASCII-coded version of

"message digest"

The hash-code is the following 224-bit string.

2cb21c83 ae2f004d e7e81c3c 7019cbcb 65b71ab6 56b22d6d 0c39b8eb

B.9.5 Example 5

In this example, the data string is the 62-byte string consisting of the ASCII-coded version of

"ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz0123456789"

The hash-code is the following 224-bit string.

bff72b4f cb7d75e5 632900ac 5f90d219 e05e97a7 bde72e74 0db393d9

B.9.6 Example 6

In this example, the data string is the 80-byte string consisting of the ASCII-coded version of eight repetitions of

"1234567890"

The hash-code is the following 224-bit string.

b50aecbe 4e9bb0b5 7bc5f3ae 760a8e01 db24f203 fb3cdcd1 3148046e

B.9.7 Example 7

In this example, the data string is the 56-byte string consisting of the ASCII-coded version of

"abcdbcdecdefdefgefghfghighijhijkijkljklmklmnlmnomnopnopq"

After the padding process, the following two 16-word blocks are derived from the data string.

```
61626364 62636465 63646566 64656667 65666768 66676869 6768696a 68696a6b
696a6b6c 6a6b6c6d 6b6c6d6e 6c6d6e6f 6d6e6f70 6e6f7071 80000000 00000000
00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000
00000000 00000000 00000000 00000000 00000000 00000000 00000000 000001c0
```

The following are (hexadecimal representations of) the successive values of the variables X_0, X_1, X_2, X_3, X_4, X_5, X_6 and X_7 in the first block process.

```
init:  c1059ed8 367cd507 3070dd17 f70e5939 ffc00b31 68581511 64f98fa7 befa4fa4
  0  0e96b2be c1059ed8 367cd507 3070dd17 04342242 ffc00b31 68581511 64f98fa7
  1  51d17d7b 0e96b2be c1059ed8 367cd507 2f8ea3d4 04342242 ffc00b31 68581511
  2  ff1cbd7f 51d17d7b 0e96b2be c1059ed8 79a896fa 2f8ea3d4 04342242 ffc00b31
  3  24bcc047 ff1cbd7f 51d17d7b 0e96b2be 1f60795a 79a896fa 2f8ea3d4 04342242
  4  7d56a6ac 24bcc047 ff1cbd7f 51d17d7b de395286 1f60795a 79a896fa 2f8ea3d4
  5  745beb11 7d56a6ac 24bcc047 ff1cbd7f d863d132 de395286 1f60795a 79a896fa
  6  0dd41573 745beb11 7d56a6ac 24bcc047 2e60d323 d863d132 de395286 1f60795a
  7  9a2541fd 0dd41573 745beb11 7d56a6ac 08d2b348 2e60d323 d863d132 de395286
  8  3140e909 9a2541fd 0dd41573 745beb11 95dfd707 08d2b348 2e60d323 d863d132
  9  b2954925 3140e909 9a2541fd 0dd41573 05ef5e3d 95dfd707 08d2b348 2e60d323
 10  b2a874fb b2954925 3140e909 9a2541fd 9dcaf118 05ef5e3d 95dfd707 08d2b348
 11  116ce44d b2a874fb b2954925 3140e909 0e6d566a 9dcaf118 05ef5e3d 95dfd707
 12  5ff9349a 116ce44d b2a874fb b2954925 08eb3305 0e6d566a 9dcaf118 05ef5e3d
 13  7fa9d65d 5ff9349a 116ce44d b2a874fb 4657cf17 08eb3305 0e6d566a 9dcaf118
 14  006b1b16 7fa9d65d 5ff9349a 116ce44d 08d09e8d 4657cf17 08eb3305 0e6d566a
 15  b301c98a 006b1b16 7fa9d65d 5ff9349a 6fbefa1d 08d09e8d 4657cf17 08eb3305
```

```
16  e623ecc0 b301c98a 006b1b16 7fa9d65d 2b3f859c 6fbefa1d 08d09e8d 4657cf17
17  d9244a78 e623ecc0 b301c98a 006b1b16 e66d8d9c 2b3f859c 6fbefa1d 08d09e8d
18  99c72726 d9244a78 e623ecc0 b301c98a b26a409c e66d8d9c 2b3f859c 6fbefa1d
19  ab0cbed2 99c72726 d9244a78 e623ecc0 010d7c65 b26a409c e66d8d9c 2b3f859c
20  78062878 ab0cbed2 99c72726 d9244a78 5678a949 010d7c65 b26a409c e66d8d9c
21  d7c5c5d5 78062878 ab0cbed2 99c72726 b280360c 5678a949 010d7c65 b26a409c
22  bad2ee72 d7c5c5d5 78062878 ab0cbed2 0d4cd0c4 b280360c 5678a949 010d7c65
23  bcf47346 bad2ee72 d7c5c5d5 78062878 d6a19dc8 0d4cd0c4 b280360c 5678a949
24  5ecc417b bcf47346 bad2ee72 d7c5c5d5 3337a11c d6a19dc8 0d4cd0c4 b280360c
25  e15bfa57 5ecc417b bcf47346 bad2ee72 0ce15173 3337a11c d6a19dc8 0d4cd0c4
26  fae6167b e15bfa57 5ecc417b bcf47346 73dbe5c7 0ce15173 3337a11c d6a19dc8
27  991c3f99 fae6167b e15bfa57 5ecc417b 8602a31f 73dbe5c7 0ce15173 3337a11c
28  7055843b 991c3f99 fae6167b e15bfa57 eb4de5f8 8602a31f 73dbe5c7 0ce15173
29  08dcfb6d 7055843b 991c3f99 fae6167b 4606d126 eb4de5f8 8602a31f 73dbe5c7
30  2964b340 08dcfb6d 7055843b 991c3f99 213b3e63 4606d126 eb4de5f8 8602a31f
31  5b3677d0 2964b340 08dcfb6d 7055843b c9689cb0 213b3e63 4606d126 eb4de5f8
32  1ee0fe7d 5b3677d0 2964b340 08dcfb6d 14318a4d c9689cb0 213b3e63 4606d126
33  6b918d6e 1ee0fe7d 5b3677d0 2964b340 216054a8 14318a4d c9689cb0 213b3e63
34  a6710d0d 6b918d6e 1ee0fe7d 5b3677d0 bc823a58 216054a8 14318a4d c9689cb0
35  5e198fed a6710d0d 6b918d6e 1ee0fe7d c49933fe bc823a58 216054a8 14318a4d
36  136c320a 5e198fed a6710d0d 6b918d6e 75687ccb c49933fe bc823a58 216054a8
37  40ee0c43 136c320a 5e198fed a6710d0d f1c2caf6 75687ccb c49933fe bc823a58
38  aa96d78c 40ee0c43 136c320a 5e198fed f48b4ceb f1c2caf6 75687ccb c49933fe
39  27c97b86 aa96d78c 40ee0c43 136c320a b556216a f48b4ceb f1c2caf6 75687ccb
40  b07bd327 27c97b86 aa96d78c 40ee0c43 30ec2d76 b556216a f48b4ceb f1c2caf6
41  d88d56bd b07bd327 27c97b86 aa96d78c dc2fa5a4 30ec2d76 b556216a f48b4ceb
42  5c775077 d88d56bd b07bd327 27c97b86 5fad6db5 dc2fa5a4 30ec2d76 b556216a
43  1526cca3 5c775077 d88d56bd b07bd327 da8a0b1c 5fad6db5 dc2fa5a4 30ec2d76
44  c09dda14 1526cca3 5c775077 d88d56bd d98ec23a da8a0b1c 5fad6db5 dc2fa5a4
45  f885e124 c09dda14 1526cca3 5c775077 e4f23e41 d98ec23a da8a0b1c 5fad6db5
46  5447f0ad f885e124 c09dda14 1526cca3 bfb7497c e4f23e41 d98ec23a da8a0b1c
47  e6227061 5447f0ad f885e124 c09dda14 5b09619b bfb7497c e4f23e41 d98ec23a
48  009cebea e6227061 5447f0ad f885e124 59ecab46 5b09619b bfb7497c e4f23e41
49  92b0d169 009cebea e6227061 5447f0ad 9a572b85 59ecab46 5b09619b bfb7497c
50  8d224e54 92b0d169 009cebea e6227061 32144602 9a572b85 59ecab46 5b09619b
51  c1fcac71 8d224e54 92b0d169 009cebea 4e98a8b7 32144602 9a572b85 59ecab46
52  8e6ce843 c1fcac71 8d224e54 92b0d169 2c1823be 4e98a8b7 32144602 9a572b85
53  000f54de 8e6ce843 c1fcac71 8d224e54 f32cf2a8 2c1823be 4e98a8b7 32144602
54  2fe2af3a 000f54de 8e6ce843 c1fcac71 20f763ee f32cf2a8 2c1823be 4e98a8b7
55  1fd539af 2fe2af3a 000f54de 8e6ce843 5acdbd62 20f763ee f32cf2a8 2c1823be
56  7f86644e 1fd539af 2fe2af3a 000f54de 9fc10216 5acdbd62 20f763ee f32cf2a8
57  0e08dc77 7f86644e 1fd539af 2fe2af3a 2a4ea749 9fc10216 5acdbd62 20f763ee
58  0b9f4851 0e08dc77 7f86644e 1fd539af 18b1dfb9 2a4ea749 9fc10216 5acdbd62
59  dbce97c3 0b9f4851 0e08dc77 7f86644e 6ec6ba5b 18b1dfb9 2a4ea749 9fc10216
60  3cd78fe1 dbce97c3 0b9f4851 0e08dc77 3e1ca2f1 6ec6ba5b 18b1dfb9 2a4ea749
61  35f4bf1c 3cd78fe1 dbce97c3 0b9f4851 ba1a8a1b 3e1ca2f1 6ec6ba5b 18b1dfb9
62  86795a7d 35f4bf1c 3cd78fe1 dbce97c3 2ce11258 ba1a8a1b 3e1ca2f1 6ec6ba5b
63  c14b4785 86795a7d 35f4bf1c 3cd78fe1 1108ac7f 2ce11258 ba1a8a1b 3e1ca2f1
```

The following eight words, Y_0, Y_1, Y_2, Y_3, Y_4, Y_5, Y_6 and Y_7, represent the output of the round-function in the first block process.

$$Y_0 = \text{c1059ed8} \boxplus \text{c14b4785} = \text{8250e65d}$$
$$Y_1 = \text{367cd507} \boxplus \text{86795a7d} = \text{bcf62f84}$$
$$Y_2 = \text{3070dd17} \boxplus \text{35f4bf1c} = \text{66659c33}$$
$$Y_3 = \text{f70e5939} \boxplus \text{3cd78fe1} = \text{33e5e91a}$$
$$Y_4 = \text{ffc00b31} \boxplus \text{1108ac7f} = \text{10c8b7b0}$$
$$Y_5 = \text{68581511} \boxplus \text{2ce11258} = \text{95392769}$$
$$Y_6 = \text{64f98fa7} \boxplus \text{ba1a8a1b} = \text{1f1419c2}$$
$$Y_7 = \text{befa4fa4} \boxplus \text{3e1ca2f1} = \text{fd16f295}$$

The following are (hexadecimal representations of) the successive values of the variables Y_0, Y_1, Y_2, Y_3, Y_4, Y_5, Y_6 and Y_7 in the second block process.

```
init: 8250e65d bcf62f84 66659c33 33e5e91a 10c8b7b0 95392769 1f1419c2 fd16f295
  0 692e407d 8250e65d bcf62f84 66659c33 e4be1e69 10c8b7b0 95392769 1f1419c2
  1 608d83e1 692e407d 8250e65d bcf62f84 3ddb8cee e4be1e69 10c8b7b0 95392769
  2 09bfa89f 608d83e1 692e407d 8250e65d f5813490 3ddb8cee e4be1e69 10c8b7b0
  3 2375fbc5 09bfa89f 608d83e1 692e407d c3e18529 f5813490 3ddb8cee e4be1e69
  4 717e79e7 2375fbc5 09bfa89f 608d83e1 77d39ccc c3e18529 f5813490 3ddb8cee
  5 a9319748 717e79e7 2375fbc5 09bfa89f fdbb9913 77d39ccc c3e18529 f5813490
  6 27a42f04 a9319748 717e79e7 2375fbc5 b999cce4 fdbb9913 77d39ccc c3e18529
  7 3419081e 27a42f04 a9319748 717e79e7 54e69e21 b999cce4 fdbb9913 77d39ccc
  8 0ab393c2 3419081e 27a42f04 a9319748 ad29647e 54e69e21 b999cce4 fdbb9913
  9 006784eb 0ab393c2 3419081e 27a42f04 aff457e7 ad29647e 54e69e21 b999cce4
 10 ecd5c9db 006784eb 0ab393c2 3419081e 9af42a0e aff457e7 ad29647e 54e69e21
 11 4762e8f0 ecd5c9db 006784eb 0ab393c2 8fb6f3d8 9af42a0e aff457e7 ad29647e
 12 af93b2a8 4762e8f0 ecd5c9db 006784eb 97e63d39 8fb6f3d8 9af42a0e aff457e7
 13 533c517c af93b2a8 4762e8f0 ecd5c9db 7364bae6 97e63d39 8fb6f3d8 9af42a0e
 14 03c0a51b 533c517c af93b2a8 4762e8f0 3afb010d 7364bae6 97e63d39 8fb6f3d8
 15 5fd065bd 03c0a51b 533c517c af93b2a8 b8e64229 3afb010d 7364bae6 97e63d39
 16 18b268b5 5fd065bd 03c0a51b 533c517c 38eda38d b8e64229 3afb010d 7364bae6
 17 b87d63b4 18b268b5 5fd065bd 03c0a51b 25c2c397 38eda38d b8e64229 3afb010d
 18 b1d846e0 b87d63b4 18b268b5 5fd065bd d674405f 25c2c397 38eda38d b8e64229
 19 8ba0aed6 b1d846e0 b87d63b4 18b268b5 b8109422 d674405f 25c2c397 38eda38d
 20 1485f843 8ba0aed6 b1d846e0 b87d63b4 1c58cd66 b8109422 d674405f 25c2c397
 21 238f4cda 1485f843 8ba0aed6 b1d846e0 39b2eb5f 1c58cd66 b8109422 d674405f
 22 7031b061 238f4cda 1485f843 8ba0aed6 4b8262ad 39b2eb5f 1c58cd66 b8109422
 23 d4e7ec62 7031b061 238f4cda 1485f843 163c3aa0 4b8262ad 39b2eb5f 1c58cd66
 24 66582df3 d4e7ec62 7031b061 238f4cda c0976260 163c3aa0 4b8262ad 39b2eb5f
 25 dedb8199 66582df3 d4e7ec62 7031b061 b73e2dec c0976260 163c3aa0 4b8262ad
 26 f8536917 dedb8199 66582df3 d4e7ec62 7c2af9c4 b73e2dec c0976260 163c3aa0
 27 d7333b8a f8536917 dedb8199 66582df3 b2b0b71a 7c2af9c4 b73e2dec c0976260
 28 760847c1 d7333b8a f8536917 dedb8199 5898eff2 b2b0b71a 7c2af9c4 b73e2dec
 29 7eabc6d7 760847c1 d7333b8a f8536917 24dd3883 5898eff2 b2b0b71a 7c2af9c4
 30 90c49624 7eabc6d7 760847c1 d7333b8a cce25e67 24dd3883 5898eff2 b2b0b71a
 31 0b876264 90c49624 7eabc6d7 760847c1 e4e4a53b cce25e67 24dd3883 5898eff2
 32 04cb36c0 0b876264 90c49624 7eabc6d7 5403a391 e4e4a53b cce25e67 24dd3883
 33 d58cc34a 04cb36c0 0b876264 90c49624 b78767c3 5403a391 e4e4a53b cce25e67
 34 0ed14dd7 d58cc34a 04cb36c0 0b876264 fdcdc9d9 b78767c3 5403a391 e4e4a53b
 35 5a89a942 0ed14dd7 d58cc34a 04cb36c0 790c4a20 fdcdc9d9 b78767c3 5403a391
 36 4d30424c 5a89a942 0ed14dd7 d58cc34a f95bf853 790c4a20 fdcdc9d9 b78767c3
 37 47f58c5c 4d30424c 5a89a942 0ed14dd7 0ec9be3b f95bf853 790c4a20 fdcdc9d9
 38 b5ad85d7 47f58c5c 4d30424c 5a89a942 cf9f1dbe 0ec9be3b f95bf853 790c4a20
 39 762fecbc b5ad85d7 47f58c5c 4d30424c 15427ed3 cf9f1dbe 0ec9be3b f95bf853
 40 32abe746 762fecbc b5ad85d7 47f58c5c 4053e12e 15427ed3 cf9f1dbe 0ec9be3b
 41 84adb2a0 32abe746 762fecbc b5ad85d7 7cece4e2 4053e12e 15427ed3 cf9f1dbe
 42 c6e1c5af 84adb2a0 32abe746 762fecbc 42f9990b 7cece4e2 4053e12e 15427ed3
 43 35e14bfa c6e1c5af 84adb2a0 32abe746 c9965792 42f9990b 7cece4e2 4053e12e
 44 7410bfd8 35e14bfa c6e1c5af 84adb2a0 ca54ce51 c9965792 42f9990b 7cece4e2
 45 3fe9e763 7410bfd8 35e14bfa c6e1c5af ae7cdb66 ca54ce51 c9965792 42f9990b
 46 853c3a00 3fe9e763 7410bfd8 35e14bfa c2be054d ae7cdb66 ca54ce51 c9965792
 47 f7d035e7 853c3a00 3fe9e763 7410bfd8 f6d59d2c c2be054d ae7cdb66 ca54ce51
 48 20bae2b8 f7d035e7 853c3a00 3fe9e763 cab73f06 f6d59d2c c2be054d ae7cdb66
 49 ae6bf667 20bae2b8 f7d035e7 853c3a00 52384d2f cab73f06 f6d59d2c c2be054d
 50 12e504e5 ae6bf667 20bae2b8 f7d035e7 f9a8377f 52384d2f cab73f06 f6d59d2c
 51 f3497054 12e504e5 ae6bf667 20bae2b8 d0ab7cfc f9a8377f 52384d2f cab73f06
 52 9f166cdb f3497054 12e504e5 ae6bf667 71b3459b d0ab7cfc f9a8377f 52384d2f
 53 ccd8fa44 9f166cdb f3497054 12e504e5 0f557ddd 71b3459b d0ab7cfc f9a8377f
 54 f5e664bd ccd8fa44 9f166cdb f3497054 a679a5e9 0f557ddd 71b3459b d0ab7cfc
 55 d4ea8c7e f5e664bd ccd8fa44 9f166cdb 2958ce2a a679a5e9 0f557ddd 71b3459b
 56 e8c8fec7 d4ea8c7e f5e664bd ccd8fa44 35f6800e 2958ce2a a679a5e9 0f557ddd
 57 882ed69e e8c8fec7 d4ea8c7e f5e664bd 30267d8e 35f6800e 2958ce2a a679a5e9
 58 4ec725f6 882ed69e e8c8fec7 d4ea8c7e ce1d1ce4 30267d8e 35f6800e 2958ce2a
```

```
59 5c9cfc69 4ec725f6 882ed69e e8c8fec7 c8242b92 ce1d1ce4 30267d8e 35f6800e
60 c9a31836 5c9cfc69 4ec725f6 882ed69e 9e40a370 c8242b92 ce1d1ce4 30267d8e
61 f754c16e c9a31836 5c9cfc69 4ec725f6 333e0b63 9e40a370 c8242b92 ce1d1ce4
62 94314748 f754c16e c9a31836 5c9cfc69 1fbc63b0 333e0b63 9e40a370 c8242b92
63 f2e7a4b9 94314748 f754c16e c9a31836 9ffd8dac 1fbc63b0 333e0b63 9e40a370
```

The following eight words, Y_0, Y_1, Y_2, Y_3, Y_4, Y_5, Y_6 and Y_7, represent the output of the final iteration of the round-function.

$$Y_0 = 8250e65d \boxplus f2e7a4b9 = 75388b16$$
$$Y_1 = bcf62f84 \boxplus 94314748 = 512776cc$$
$$Y_2 = 66659c33 \boxplus f754c16e = 5dba5da1$$
$$Y_3 = 33e5e91a \boxplus c9a31836 = fd890150$$
$$Y_4 = 10c8b7b0 \boxplus 9ffd8dac = b0c6455c$$
$$Y_5 = 95392769 \boxplus 1fbc63b0 = b4f58b19$$
$$Y_6 = 1f1419c2 \boxplus 333e0b63 = 52522525$$
$$Y_7 = fd16f295 \boxplus 9e40a370 = 635651e5$$

The hash value is the following 224-bit string.

```
75388b16 512776cc 5dba5da1 fd890150 b0c6455c b4f58b19 52522525
```

B.9.8 Example 8

In this example, the data string is the 1 000 000-byte string consisting of the ASCII-coded version of “a” repeated 10^6 times.

The hash-code is the following 224-bit string.

```
20794655 980c91d8 bbb4c1ea 97618a4b f03f4258 1948b2ee 4ee7ad67
```

B.9.9 Example 9

In this example, the data string consists of a single bit, namely 0.

The hash-code is the following 224-bit string.

```
d3fe57cb 76cdd24e 9eb23e7e 15684e03 9c75459b eaae100f 89712e9d
```

B.9.10 Example 10

In this example, the data string consists of a single bit, namely 1.

The hash-code is the following 224-bit string.

```
0d05096b ca2a4a77 a2b47a05 a59618d0 1174b378 92376135 c1b6e957
```

B.9.11 Example 11

In this example, the data string consists of 101 bits, namely 1010101…01.

The hash-code is the following 224-bit string.

```
2b1d4a34 155c04d7 a51065d6 a4476203 9a38dffd 73e76b17 b043555c
```

B.9.12 Example 12

In this example, the data string consists of 256 octets, namely 00 01 02 03 … FE FF.

The hash-code is the following 224-bit string.

```
88702e63 237824c4 eb0d0fcf e41469a4 62493e8b eb2a75bb e5981734
```

B.9.13 Example 13

In this example, the data string is the H_0 consists of 224 0 bits. For i = 1 to 100 let H_i be the hash-code of H_{i-1}.

The hash-code H_{100} is the following 224-bit string.

```
a0884cc1 a335042b fe452bf4 6777ed20 217a3472 81dc389e 7b1fbfee
```

B.10 Complete numerical examples for Dedicated Hash-Functions 4, 5, 6 and 7

The dedicated hash-functions SHA-256, SHA-384, SHA-512 and SHA-224 are described in B.4, B.5, B.6 and B.8, respectively. Numerical examples for these four hash-functions are also provided. An important limitation of these examples is that all of the input values are composed solely of ASCII-encoded alphanumeric characters. This annex contains a more complete set of numerical examples for these hash-functions.

The choice of numerical examples is based on the following considerations.

a) Inputs of length 1 up to 512 (for SHA-224 and SHA-256) or 1 024 (for SHA-384 and SHA-512) have been defined in order to test the padding scheme. (The examples in B.4 to B.6 and B.8 contain only messages with lengths that are a multiple of 8.) A small number of numerical examples with greater length have been included.

b) It has been ensured that all 32-bit words (SHA-224 and SHA-256) or all 64-bit words (SHA-384 and SHA-512) with Hamming weight 1 occur at least once as part of the input. This has been done in order to test the message expansion functions.

c) The treatment of carry overflow from one byte to another is tested by ensuring that the following additions occur at least once:

   1) For SHA-224 and SHA-256

      i) `0xFFFFFFFF + 0x00000001`

      ii) `0xFFFF0000 + 0x00010000`

      iii) `0x0000FFFF + 0x00000001`

      iv) `0xFF00FF00 + 0x01000100`

      v) `0x00FF00FF + 0x00010001`

   b) For SHA-384 and SHA-512

      i) `0xFFFFFFFFFFFFFFFF + 0x0000000000000001`

      ii) `0xFFFFFFFF00000000 + 0x0000000100000000`

      iii) `0x00000000FFFFFFFF + 0x0000000000000001`

      iv) `0xFFFF0000FFFF0000 + 0x0001000000010000`

      v) `0x0000FFFF0000FFFF + 0x0000000100000001`

vi) 0xFF00FF00FF00FF00 + 0x0100010001000100

vii) 0x00FF00FF00FF00FF + 0x0001000100010001

The complete list of numerical examples can be found at the following URL: http://www.iaik.tu-graz.ac.at/research/sha2_testvectors.zip.

NOTE Complete numerical examples for the remaining hash-functions contained in this document are not available at the above referenced URL. Analysis is currently ongoing to determine whether additional numerical examples will be required for the remaining hash-functions, and if so, what the required considerations will be. If additional numerical examples are necessary, a second amendment to this document may be considered.

B.11 Dedicated Hash-Function 9 (SHA-512/224)

B.11.1 Example 1

In this example, the input message is “abc”. The padded one block input (1 024 bits) is

```
Z[ 0] = 6162638000000000
Z[ 1] = 0000000000000000
Z[ 2] = 0000000000000000
Z[ 3] = 0000000000000000
Z[ 4] = 0000000000000000
Z[ 5] = 0000000000000000
Z[ 6] = 0000000000000000
Z[ 7] = 0000000000000000
Z[ 8] = 0000000000000000
Z[ 9] = 0000000000000000
Z[10] = 0000000000000000
Z[11] = 0000000000000000
Z[12] = 0000000000000000
Z[13] = 0000000000000000
Z[14] = 0000000000000000
Z[15] = 0000000000000018
```

The following are (hexadecimal representations of) the successive values of the variables X_0, X_1, X_2, X_3, X_4, X_5, X_6 and X_7 in each round.

```
t= 0: 9F8617B9DCE5AAD2  8C3D37C819544DA2  73E1996689DCD4D6  1DFAB7AE32FF9C82
   E606D304F5742303  0F6D2B697BD44DA8  77E36F7304C48942  3F9D85A86A1D36C8
t= 1: 39EEF9EA0D97D0E7  9F8617B9DCE5AAD2  8C3D37C819544DA2  73E1996689DCD4D6
   ED6A8CE6AC02AE3B  E606D304F5742303  0F6D2B697BD44DA8  77E36F7304C48942
t= 2: 9F956BCC32F99C4B  39EEF9EA0D97D0E7  9F8617B9DCE5AAD2  8C3D37C819544DA2
   E7C4F75F0018AB16  ED6A8CE6AC02AE3B  E606D304F5742303  0F6D2B697BD44DA8
t= 3: 624C8289051D5B40  9F956BCC32F99C4B  39EEF9EA0D97D0E7  9F8617B9DCE5AAD2
   93C0EDD577EF4338  E7C4F75F0018AB16  ED6A8CE6AC02AE3B  E606D304F5742303
t= 4: 8445DB53436C52F8  624C8289051D5B40  9F956BCC32F99C4B  39EEF9EA0D97D0E7
   E5662EE45E149450  93C0EDD577EF4338  E7C4F75F0018AB16  ED6A8CE6AC02AE3B
t= 5: 9873F29F683128C8  8445DB53436C52F8  624C8289051D5B40  9F956BCC32F99C4B
   0B843D2CDE075711  E5662EE45E149450  93C0EDD577EF4338  E7C4F75F0018AB16
t= 6: 134D4DD913EC29E7  9873F29F683128C8  8445DB53436C52F8  624C8289051D5B40
   CACE421FD59538B6  0B843D2CDE075711  E5662EE45E149450  93C0EDD577EF4338
t= 7: 6A01F4E5758D5A14  134D4DD913EC29E7  9873F29F683128C8  8445DB53436C52F8
   73EA4F37F91D77F0  CACE421FD59538B6  0B843D2CDE075711  E5662EE45E149450
t= 8: 0B9D8BDA33530FA3  6A01F4E5758D5A14  134D4DD913EC29E7  9873F29F683128C8
   A64384D872C70950  73EA4F37F91D77F0  CACE421FD59538B6  0B843D2CDE075711
t= 9: 2C961F00E387DF1D  0B9D8BDA33530FA3  6A01F4E5758D5A14  134D4DD913EC29E7
   AC79A3FFDAC317FC  A64384D872C70950  73EA4F37F91D77F0  CACE421FD59538B6
t=10: 78953995DD54A904  2C961F00E387DF1D  0B9D8BDA33530FA3  6A01F4E5758D5A14
   5FF1DE02C59C17E6  AC79A3FFDAC317FC  A64384D872C70950  73EA4F37F91D77F0
t=11: 82A6A4ED5164390E  78953995DD54A904  2C961F00E387DF1D  0B9D8BDA33530FA3
```

```
   3A6E6AED341206D2  5FF1DE02C59C17E6  AC79A3FFDAC317FC  A64384D872C70950
t=12: 6528AFE0F531B8D9  82A6A4ED5164390E  78953995DD54A904  2C961F00E387DF1D
   AF77A75BBF7964C9  3A6E6AED341206D2  5FF1DE02C59C17E6  AC79A3FFDAC317FC
t=13: 206C69B0295CAE2F  6528AFE0F531B8D9  82A6A4ED5164390E  78953995DD54A904
   3CA059F97E654F98  AF77A75BBF7964C9  3A6E6AED341206D2  5FF1DE02C59C17E6
t=14: DB71F51BE96E76D1  206C69B0295CAE2F  6528AFE0F531B8D9  82A6A4ED5164390E
   340B10ABC4B10E09  3CA059F97E654F98  AF77A75BBF7964C9  3A6E6AED341206D2
t=15: A69AF3FA50F71091  DB71F51BE96E76D1  206C69B0295CAE2F  6528AFE0F531B8D9
   6C6A7EF25668BBB4  340B10ABC4B10E09  3CA059F97E654F98  AF77A75BBF7964C9
t=16: F57D3A111596E3F7  A69AF3FA50F71091  DB71F51BE96E76D1  206C69B0295CAE2F
   483FD5187E05AF83  6C6A7EF25668BBB4  340B10ABC4B10E09  3CA059F97E654F98
t=17: 37F983BB8545A2F2  F57D3A111596E3F7  A69AF3FA50F71091  DB71F51BE96E76D1
   22CB500B1745C86F  483FD5187E05AF83  6C6A7EF25668BBB4  340B10ABC4B10E09
t=18: 6AB7291DC27CE806  37F983BB8545A2F2  F57D3A111596E3F7  A69AF3FA50F71091
   CC2D9DA4800A1393  22CB500B1745C86F  483FD5187E05AF83  6C6A7EF25668BBB4
t=19: 8E50B25D469759C2  6AB7291DC27CE806  37F983BB8545A2F2  F57D3A111596E3F7
   50193786D52F5194  CC2D9DA4800A1393  22CB500B1745C86F  483FD5187E05AF83
t=20: 3041190F76AD53DF  8E50B25D469759C2  6AB7291DC27CE806  37F983BB8545A2F2
   746F4B17026AA6ED  50193786D52F5194  CC2D9DA4800A1393  22CB500B1745C86F
t=21: D37D93454B59A769  3041190F76AD53DF  8E50B25D469759C2  6AB7291DC27CE806
   3792AA4013809C0F  746F4B17026AA6ED  50193786D52F5194  CC2D9DA4800A1393
t=22: 28E37AB968D3F5E5  D37D93454B59A769  3041190F76AD53DF  8E50B25D469759C2
   936E64805412DE7D  3792AA4013809C0F  746F4B17026AA6ED  50193786D52F5194
t=23: 05799053E5D280FD  28E37AB968D3F5E5  D37D93454B59A769  3041190F76AD53DF
   BD8F22E3B3312F05  936E64805412DE7D  3792AA4013809C0F  746F4B17026AA6ED
t=24: A24BC13A743FCBCE  05799053E5D280FD  28E37AB968D3F5E5  D37D93454B59A769
   CD7C3D09944BE7B6  BD8F22E3B3312F05  936E64805412DE7D  3792AA4013809C0F
t=25: 1EABC1C5C3A2CDEA  A24BC13A743FCBCE  05799053E5D280FD  28E37AB968D3F5E5
   27A2534198BE3EFB  CD7C3D09944BE7B6  BD8F22E3B3312F05  936E64805412DE7D
t=26: 471543A4179B22FE  1EABC1C5C3A2CDEA  A24BC13A743FCBCE  05799053E5D280FD
   A849D4C8E1909347  27A2534198BE3EFB  CD7C3D09944BE7B6  BD8F22E3B3312F05
t=27: 887298E1C82038F7  471543A4179B22FE  1EABC1C5C3A2CDEA  A24BC13A743FCBCE
   536496733A17ADD7  A849D4C8E1909347  27A2534198BE3EFB  CD7C3D09944BE7B6
t=28: 42FE965258B7E0EC  887298E1C82038F7  471543A4179B22FE  1EABC1C5C3A2CDEA
   A37AD4727F2FB6A7  536496733A17ADD7  A849D4C8E1909347  27A2534198BE3EFB
t=29: B251E1018FD0C473  42FE965258B7E0EC  887298E1C82038F7  471543A4179B22FE
   D4A476A812ED33C2  A37AD4727F2FB6A7  536496733A17ADD7  A849D4C8E1909347
t=30: DDDD91CB1FDBFD41  B251E1018FD0C473  42FE965258B7E0EC  887298E1C82038F7
   04986D7E3FD773AE  D4A476A812ED33C2  A37AD4727F2FB6A7  536496733A17ADD7
t=31: 4AA9D15BECE3FB9F  DDDD91CB1FDBFD41  B251E1018FD0C473  42FE965258B7E0EC
   53C83C436C1A8C55  04986D7E3FD773AE  D4A476A812ED33C2  A37AD4727F2FB6A7
t=32: 063BE3A3BA1F925C  4AA9D15BECE3FB9F  DDDD91CB1FDBFD41  B251E1018FD0C473
   EB8227C63C6143AB  53C83C436C1A8C55  04986D7E3FD773AE  D4A476A812ED33C2
t=33: 0BA0D71206B4CE72  063BE3A3BA1F925C  4AA9D15BECE3FB9F  DDDD91CB1FDBFD41
   672DE7D3FD6CE274  EB8227C63C6143AB  53C83C436C1A8C55  04986D7E3FD773AE
t=34: 344234B9E239CFBD  0BA0D71206B4CE72  063BE3A3BA1F925C  4AA9D15BECE3FB9F
   38893650766BED56  672DE7D3FD6CE274  EB8227C63C6143AB  53C83C436C1A8C55
t=35: 8C098B89A7906A73  344234B9E239CFBD  0BA0D71206B4CE72  063BE3A3BA1F925C
   A7B9698E7EDB54BD  38893650766BED56  672DE7D3FD6CE274  EB8227C63C6143AB
t=36: C5A836CC05300A0C  8C098B89A7906A73  344234B9E239CFBD  0BA0D71206B4CE72
   BC35E565541C0486  A7B9698E7EDB54BD  38893650766BED56  672DE7D3FD6CE274
t=37: CDFE2808D45E7924  C5A836CC05300A0C  8C098B89A7906A73  344234B9E239CFBD
   8B500635C180CC3B  BC35E565541C0486  A7B9698E7EDB54BD  38893650766BED56
t=38: EDC87E1B480C8A77  CDFE2808D45E7924  C5A836CC05300A0C  8C098B89A7906A73
   F309D755002EF931  8B500635C180CC3B  BC35E565541C0486  A7B9698E7EDB54BD
t=39: 13D3A842A45159E7  EDC87E1B480C8A77  CDFE2808D45E7924  C5A836CC05300A0C
   6D9958CC3F974B68  F309D755002EF931  8B500635C180CC3B  BC35E565541C0486
t=40: 17AA585EACBB1D8C  13D3A842A45159E7  EDC87E1B480C8A77  CDFE2808D45E7924
   A62EFC64B5A504C7  6D9958CC3F974B68  F309D755002EF931  8B500635C180CC3B
t=41: 7BCD6230B77F244A  17AA585EACBB1D8C  13D3A842A45159E7  EDC87E1B480C8A77
   543AA84578643C3A  A62EFC64B5A504C7  6D9958CC3F974B68  F309D755002EF931
t=42: BE63D26279808C58  7BCD6230B77F244A  17AA585EACBB1D8C  13D3A842A45159E7
   5D1D742D663F17BE  543AA84578643C3A  A62EFC64B5A504C7  6D9958CC3F974B68
```

```
t=43: C6F1FBBEDEA32F8E  BE63D26279808C58  7BCD6230B77F244A  17AA585EACBB1D8C
   D83E6A094C606812  5D1D742D663F17BE  543AA84578643C3A  A62EFC64B5A504C7
t=44: 6346F580DD1CEC37  C6F1FBBEDEA32F8E  BE63D26279808C58  7BCD6230B77F244A
   5BE7E65BC706B684  D83E6A094C606812  5D1D742D663F17BE  543AA84578643C3A
t=45: 0C618B0042ADC22E  6346F580DD1CEC37  C6F1FBBEDEA32F8E  BE63D26279808C58
   BA9737EA9A33D1D4  5BE7E65BC706B684  D83E6A094C606812  5D1D742D663F17BE
t=46: BF9E3A882B0B4301  0C618B0042ADC22E  6346F580DD1CEC37  C6F1FBBEDEA32F8E
   FCAE077AACC5CF59  BA9737EA9A33D1D4  5BE7E65BC706B684  D83E6A094C606812
t=47: 586A3D84D04FD482  BF9E3A882B0B4301  0C618B0042ADC22E  6346F580DD1CEC37
   45F48765CE6A2794  FCAE077AACC5CF59  BA9737EA9A33D1D4  5BE7E65BC706B684
t=48: 5B2A6269DAF95602  586A3D84D04FD482  BF9E3A882B0B4301  0C618B0042ADC22E
   68B8F9BE61FCFCE0  45F48765CE6A2794  FCAE077AACC5CF59  BA9737EA9A33D1D4
t=49: 5CF5F4502BB65B08  5B2A6269DAF95602  586A3D84D04FD482  BF9E3A882B0B4301
   038E7DBE733DDC71  68B8F9BE61FCFCE0  45F48765CE6A2794  FCAE077AACC5CF59
t=50: DBB34340CCBA2D51  5CF5F4502BB65B08  5B2A6269DAF95602  586A3D84D04FD482
   3107BE9653EA4652  038E7DBE733DDC71  68B8F9BE61FCFCE0  45F48765CE6A2794
t=51: 903B6E3D2CFDFA75  DBB34340CCBA2D51  5CF5F4502BB65B08  5B2A6269DAF95602
   13DD1F6DC423ED9D  3107BE9653EA4652  038E7DBE733DDC71  68B8F9BE61FCFCE0
t=52: 22F68588F55C8E62  903B6E3D2CFDFA75  DBB34340CCBA2D51  5CF5F4502BB65B08
   A6B45F7216FF1A92  13DD1F6DC423ED9D  3107BE9653EA4652  038E7DBE733DDC71
t=53: AF6B1C8DFE414C86  22F68588F55C8E62  903B6E3D2CFDFA75  DBB34340CCBA2D51
   00384D2ED96AE437  A6B45F7216FF1A92  13DD1F6DC423ED9D  3107BE9653EA4652
t=54: BDCB5AC728279AB9  AF6B1C8DFE414C86  22F68588F55C8E62  903B6E3D2CFDFA75
   768B77A7A84E1FDF  00384D2ED96AE437  A6B45F7216FF1A92  13DD1F6DC423ED9D
t=55: AAB7B27B1CE5D524  BDCB5AC728279AB9  AF6B1C8DFE414C86  22F68588F55C8E62
   C4E802298CE15481  768B77A7A84E1FDF  00384D2ED96AE437  A6B45F7216FF1A92
t=56: 983A35EE537826F0  AAB7B27B1CE5D524  BDCB5AC728279AB9  AF6B1C8DFE414C86
   0BE7B3FE43EB3463  C4E802298CE15481  768B77A7A84E1FDF  00384D2ED96AE437
t=57: C2C9007B1BE9CF4D  983A35EE537826F0  AAB7B27B1CE5D524  BDCB5AC728279AB9
   397E5321BD27DD2E  0BE7B3FE43EB3463  C4E802298CE15481  768B77A7A84E1FDF
t=58: 1A0FCFF62C67E0A5  C2C9007B1BE9CF4D  983A35EE537826F0  AAB7B27B1CE5D524
   BECEA5B070FDDE4B  397E5321BD27DD2E  0BE7B3FE43EB3463  C4E802298CE15481
t=59: E7D763B06CC2AC34  1A0FCFF62C67E0A5  C2C9007B1BE9CF4D  983A35EE537826F0
   5744D273C1F38773  BECEA5B070FDDE4B  397E5321BD27DD2E  0BE7B3FE43EB3463
t=60: 486F4BADA8CB4D96  E7D763B06CC2AC34  1A0FCFF62C67E0A5  C2C9007B1BE9CF4D
   6616508EA2133B34  5744D273C1F38773  BECEA5B070FDDE4B  397E5321BD27DD2E
t=61: DC6770B956F0F055  486F4BADA8CB4D96  E7D763B06CC2AC34  1A0FCFF62C67E0A5
   970988E60D971C48  6616508EA2133B34  5744D273C1F38773  BECEA5B070FDDE4B
t=62: 5F7CE563832894E8  DC6770B956F0F055  486F4BADA8CB4D96  E7D763B06CC2AC34
   650678F827F7701F  970988E60D971C48  6616508EA2133B34  5744D273C1F38773
t=63: C32DC022E5937D1B  5F7CE563832894E8  DC6770B956F0F055  486F4BADA8CB4D96
   395087939EBDBDD1  650678F827F7701F  970988E60D971C48  6616508EA2133B34
t=64: FEE659ED0008B0EE  C32DC022E5937D1B  5F7CE563832894E8  DC6770B956F0F055
   C24F9D75EB91E085  395087939EBDBDD1  650678F827F7701F  970988E60D971C48
t=65: A732EB36834C074A  FEE659ED0008B0EE  C32DC022E5937D1B  5F7CE563832894E8
   09A466D6CD127E9D  C24F9D75EB91E085  395087939EBDBDD1  650678F827F7701F
t=66: 5B1682F0AF0FF6A6  A732EB36834C074A  FEE659ED0008B0EE  C32DC022E5937D1B
   DA56B1B76183E9D1  09A466D6CD127E9D  C24F9D75EB91E085  395087939EBDBDD1
t=67: A71757CE29CD6B61  5B1682F0AF0FF6A6  A732EB36834C074A  FEE659ED0008B0EE
   30ABC3DB21388EDB  DA56B1B76183E9D1  09A466D6CD127E9D  C24F9D75EB91E085
t=68: 8202AB6393E0A6D7  A71757CE29CD6B61  5B1682F0AF0FF6A6  A732EB36834C074A
   4EDBCB450C9D68A5  30ABC3DB21388EDB  DA56B1B76183E9D1  09A466D6CD127E9D
t=69: 6508770A9E741395  8202AB6393E0A6D7  A71757CE29CD6B61  5B1682F0AF0FF6A6
   6B4F58DE06441A41  4EDBCB450C9D68A5  30ABC3DB21388EDB  DA56B1B76183E9D1
t=70: F7C52916A6830F3F  6508770A9E741395  8202AB6393E0A6D7  A71757CE29CD6B61
   55F85F28969F648B  6B4F58DE06441A41  4EDBCB450C9D68A5  30ABC3DB21388EDB
t=71: 061595A1758E4E5C  F7C52916A6830F3F  6508770A9E741395  8202AB6393E0A6D7
   D94F8C3E0A2F60A9  55F85F28969F648B  6B4F58DE06441A41  4EDBCB450C9D68A5
t=72: D5368734187EECCB  061595A1758E4E5C  F7C52916A6830F3F  6508770A9E741395
   A8C792C91D097031  D94F8C3E0A2F60A9  55F85F28969F648B  6B4F58DE06441A41
t=73: F338848E621D9D09  D5368734187EECCB  061595A1758E4E5C  F7C52916A6830F3F
   9769EC0E9A73A2BD  A8C792C91D097031  D94F8C3E0A2F60A9  55F85F28969F648B
t=74: 86A48D31E4F7A2E6  F338848E621D9D09  D5368734187EECCB  061595A1758E4E5C
```

```
   019AA3BCBEBBCD10  9769EC0E9A73A2BD  A8C792C91D097031  D94F8C3E0A2F60A9
t=75: 8DFF4C4DDF36D9E2  86A48D31E4F7A2E6  F338848E621D9D09  D5368734187EECCB
   67523326ED58C22B  019AA3BCBEBBCD10  9769EC0E9A73A2BD  A8C792C91D097031
t=76: D6EB4F969D4CF40A  8DFF4C4DDF36D9E2  86A48D31E4F7A2E6  F338848E621D9D09
   054704D916035D9D  67523326ED58C22B  019AA3BCBEBBCD10  9769EC0E9A73A2BD
t=77: F03D357829EF4D22  D6EB4F969D4CF40A  8DFF4C4DDF36D9E2  86A48D31E4F7A2E6
   FDDF88A8DFF1FD36  054704D916035D9D  67523326ED58C22B  019AA3BCBEBBCD10
t=78: 66CCDBC9BC2B6E0C  F03D357829EF4D22  D6EB4F969D4CF40A  8DFF4C4DDF36D9E2
   B3953BA10977D31A  FDDF88A8DFF1FD36  054704D916035D9D  67523326ED58C22B
t=79: B9F6EF4757271CB2  66CCDBC9BC2B6E0C  F03D357829EF4D22  D6EB4F969D4CF40A
   12446E230B3B76AC  B3953BA10977D31A  FDDF88A8DFF1FD36  054704D916035D9D
```

The output is

Y_0 = 8C3D37C819544DA2 ⊎ B9F6EF4757271CB2 = 4634270F707B6A54
Y_1 = 73E1996689DCD4D6 ⊎ 66CCDBC9BC2B6E0C = DAAE7530460842E2
Y_2 = 1DFAB7AE32FF9C82 ⊎ F03D357829EF4D22 = 0E37ED265CEEE9A4
Y_3 = 679DD514582F9FCF ⊎ D6EB4F969D4CF40A = 3E8924AAF57C93D9
Y_4 = 0F6D2B697BD44DA8 ⊎ 12446E230B3B76AC = 21B1998C870FC454
Y_5 = 77E36F7304C48942 ⊎ B3953BA10977D31A = 2B78AB140E3C5C5C
Y_6 = 3F9D85A86A1D36C8 ⊎ FDDF88A8DFF1FD36 = 3D7D0E514A0F33FE
Y_7 = 1112E6AD91D692A1 ⊎ 054704D916035D9D = 1659EB86A7D9F03E

The message digest is

```
4634270F 707B6A54 DAAE7530 460842E2 0E37ED26 5CEEE9A4 3E8924AA
```

B.11.2 Example 2

In this example, the input message is

```
"abcdefghbcdefghicdefghijdefghijkefghijklfghijklmghijklmnhijklmnoijklmnopjklmnopqklmnopqrl
                              mnopqrsmnopqrstnopqrstu"
```

The padded message consists of two blocks.

The first block input (1 024 bits) is

```
Z[ 0] = 6162636465666768
Z[ 1] = 6263646566676869
Z[ 2] = 636465666768696A
Z[ 3] = 6465666768696A6B
Z[ 4] = 65666768696A6B6C
Z[ 5] = 666768696A6B6C6D
Z[ 6] = 6768696A6B6C6D6E
Z[ 7] = 68696A6B6C6D6E6F
Z[ 8] = 696A6B6C6D6E6F70
Z[ 9] = 6A6B6C6D6E6F7071
Z[10] = 6B6C6D6E6F707172
Z[11] = 6C6D6E6F70717273
Z[12] = 6D6E6F7071727374
Z[13] = 6E6F707172737475
Z[14] = 8000000000000000
Z[15] = 0000000000000000
```

The following are (hexadecimal representations of) the successive values of the variables X_0, X_1, X_2, X_3, X_4, X_5, X_6 and X_7 in each round when the first block is processed.

```
t= 0: 9F86179E424C123A  8C3D37C819544DA2  73E1996689DCD4D6  1DFAB7AE32FF9C82
   E606D2E95ADA8A6B  0F6D2B697BD44DA8  77E36F7304C48942  3F9D85A86A1D36C8
t= 1: 533141CB525091B9  9F86179E424C123A  8C3D37C819544DA2  73E1996689DCD4D6
   48B022A85133E95D  E606D2E95ADA8A6B  0F6D2B697BD44DA8  77E36F7304C48942
t= 2: E9CF7C4D67D20354  533141CB525091B9  9F86179E424C123A  8C3D37C819544DA2
   57425F1189DC982C  48B022A85133E95D  E606D2E95ADA8A6B  0F6D2B697BD44DA8
```

```
t= 3: A5ADFE61082B9ABD  E9CF7C4D67D20354  533141CB525091B9  9F86179E424C123A
   9848CEBCCFD84FEA  57425F1189DC982C  48B022A85133E95D  E606D2E95ADA8A6B
t= 4: 2C3C2C5ED8EBD26D  A5ADFE61082B9ABD  E9CF7C4D67D20354  533141CB525091B9
   E771AD738FE58E76  9848CEBCCFD84FEA  57425F1189DC982C  48B022A85133E95D
t= 5: AFB0D44C82DFF225  2C3C2C5ED8EBD26D  A5ADFE61082B9ABD  E9CF7C4D67D20354
   CFFE93DD39AF3ABF  E771AD738FE58E76  9848CEBCCFD84FEA  57425F1189DC982C
t= 6: 353191AF8D65DEE9  AFB0D44C82DFF225  2C3C2C5ED8EBD26D  A5ADFE61082B9ABD
   DCF6B078908DFF9D  CFFE93DD39AF3ABF  E771AD738FE58E76  9848CEBCCFD84FEA
t= 7: F0ED5E552EE187D9  353191AF8D65DEE9  AFB0D44C82DFF225  2C3C2C5ED8EBD26D
   FF4C75D2E1DE3279  DCF6B078908DFF9D  CFFE93DD39AF3ABF  E771AD738FE58E76
t= 8: 779397867FBA1360  F0ED5E552EE187D9  353191AF8D65DEE9  AFB0D44C82DFF225
   DE20103108B0A669  FF4C75D2E1DE3279  DCF6B078908DFF9D  CFFE93DD39AF3ABF
t= 9: B2DFC180C2685A63  779397867FBA1360  F0ED5E552EE187D9  353191AF8D65DEE9
   842E374C7133F9F6  DE20103108B0A669  FF4C75D2E1DE3279  DCF6B078908DFF9D
t=10: 360F5422F09700EC  B2DFC180C2685A63  779397867FBA1360  F0ED5E552EE187D9
   60C5AE3708E67485  842E374C7133F9F6  DE20103108B0A669  FF4C75D2E1DE3279
t=11: DAEFF6A462386C20  360F5422F09700EC  B2DFC180C2685A63  779397867FBA1360
   A4889E7CE945580A  60C5AE3708E67485  842E374C7133F9F6  DE20103108B0A669
t=12: 0DECA4759C7E00AD  DAEFF6A462386C20  360F5422F09700EC  B2DFC180C2685A63
   5EE3BD7D600E83AB  A4889E7CE945580A  60C5AE3708E67485  842E374C7133F9F6
t=13: 13B00ED20E90DAC9  0DECA4759C7E00AD  DAEFF6A462386C20  360F5422F09700EC
   5BD8653319107D74  5EE3BD7D600E83AB  A4889E7CE945580A  60C5AE3708E67485
t=14: D904C89042A3AD4D  13B00ED20E90DAC9  0DECA4759C7E00AD  DAEFF6A462386C20
   2472BA283736D707  5BD8653319107D74  5EE3BD7D600E83AB  A4889E7CE945580A
t=15: F2787EC95BF1F813  D904C89042A3AD4D  13B00ED20E90DAC9  0DECA4759C7E00AD
   99AC6FC931B828B5  2472BA283736D707  5BD8653319107D74  5EE3BD7D600E83AB
t=16: C73C91546E687207  F2787EC95BF1F813  D904C89042A3AD4D  13B00ED20E90DAC9
   86A4CA2DC3377691  99AC6FC931B828B5  2472BA283736D707  5BD8653319107D74
t=17: 4F773C1E20EF1984  C73C91546E687207  F2787EC95BF1F813  D904C89042A3AD4D
   3A2886065715B415  86A4CA2DC3377691  99AC6FC931B828B5  2472BA283736D707
t=18: 90DE39FF4862F8DE  4F773C1E20EF1984  C73C91546E687207  F2787EC95BF1F813
   E7DB461C33EC4D87  3A2886065715B415  86A4CA2DC3377691  99AC6FC931B828B5
t=19: 9889961BC5B9B080  90DE39FF4862F8DE  4F773C1E20EF1984  C73C91546E687207
   18DBE557A44B8215  E7DB461C33EC4D87  3A2886065715B415  86A4CA2DC3377691
t=20: 00BE5FE77AEEF04D  9889961BC5B9B080  90DE39FF4862F8DE  4F773C1E20EF1984
   919D9DD3F8E192BA  18DBE557A44B8215  E7DB461C33EC4D87  3A2886065715B415
t=21: 4916899865BA519B  00BE5FE77AEEF04D  9889961BC5B9B080  90DE39FF4862F8DE
   494E40936BF36522  919D9DD3F8E192BA  18DBE557A44B8215  E7DB461C33EC4D87
t=22: 2FD4751621FAA436  4916899865BA519B  00BE5FE77AEEF04D  9889961BC5B9B080
   461316088EE39598  494E40936BF36522  919D9DD3F8E192BA  18DBE557A44B8215
t=23: A895267A751BBB51  2FD4751621FAA436  4916899865BA519B  00BE5FE77AEEF04D
   7BF13FD8BDEC96E5  461316088EE39598  494E40936BF36522  919D9DD3F8E192BA
t=24: 413510E472DEBCAB  A895267A751BBB51  2FD4751621FAA436  4916899865BA519B
   E047DEF947ECF770  7BF13FD8BDEC96E5  461316088EE39598  494E40936BF36522
t=25: 0D9BD60E7ECF0CA0  413510E472DEBCAB  A895267A751BBB51  2FD4751621FAA436
   33635248DD1081A9  E047DEF947ECF770  7BF13FD8BDEC96E5  461316088EE39598
t=26: 2B6939189B6398BD  0D9BD60E7ECF0CA0  413510E472DEBCAB  A895267A751BBB51
   E1EA008EABBDDD8A  33635248DD1081A9  E047DEF947ECF770  7BF13FD8BDEC96E5
t=27: 88C8D5C8FDF31407  2B6939189B6398BD  0D9BD60E7ECF0CA0  413510E472DEBCAB
   864D416A722024F2  E1EA008EABBDDD8A  33635248DD1081A9  E047DEF947ECF770
t=28: C48C3778FBDC16E5  88C8D5C8FDF31407  2B6939189B6398BD  0D9BD60E7ECF0CA0
   8A4110030D28BE95  864D416A722024F2  E1EA008EABBDDD8A  33635248DD1081A9
t=29: D9F2AED6553533CF  C48C3778FBDC16E5  88C8D5C8FDF31407  2B6939189B6398BD
   EC047BC2E5A7C98B  8A4110030D28BE95  864D416A722024F2  E1EA008EABBDDD8A
t=30: 9C7DF3E0118B2A03  D9F2AED6553533CF  C48C3778FBDC16E5  88C8D5C8FDF31407
   946A5AB5B814086C  EC047BC2E5A7C98B  8A4110030D28BE95  864D416A722024F2
t=31: 2642E04B9FC242CC  9C7DF3E0118B2A03  D9F2AED6553533CF  C48C3778FBDC16E5
   F51B8137241F6AEE  946A5AB5B814086C  EC047BC2E5A7C98B  8A4110030D28BE95
t=32: 9EE2EDA5DE6A4BBF  2642E04B9FC242CC  9C7DF3E0118B2A03  D9F2AED6553533CF
   3A110967CED1066A  F51B8137241F6AEE  946A5AB5B814086C  EC047BC2E5A7C98B
t=33: 96DD4E3F9F4ECB4B  9EE2EDA5DE6A4BBF  2642E04B9FC242CC  9C7DF3E0118B2A03
   F7EA1DB2DE0E0F9C  3A110967CED1066A  F51B8137241F6AEE  946A5AB5B814086C
t=34: 0A6F2F765D8F08D4  96DD4E3F9F4ECB4B  9EE2EDA5DE6A4BBF  2642E04B9FC242CC
```

```
   A4289B29B081DC1E  F7EA1DB2DE0E0F9C  3A110967CED1066A  F51B8137241F6AEE
t=35: 7696BAE1D69A401A  0A6F2F765D8F08D4  96DD4E3F9F4ECB4B  9EE2EDA5DE6A4BBF
   5AC1DA918A905421  A4289B29B081DC1E  F7EA1DB2DE0E0F9C  3A110967CED1066A
t=36: 90B4206FAB7D0530  7696BAE1D69A401A  0A6F2F765D8F08D4  96DD4E3F9F4ECB4B
   39083A7BEA35DAC5  5AC1DA918A905421  A4289B29B081DC1E  F7EA1DB2DE0E0F9C
t=37: 071FA5F764C98E5F  90B4206FAB7D0530  7696BAE1D69A401A  0A6F2F765D8F08D4
   08ECE17FD62AF2F9  39083A7BEA35DAC5  5AC1DA918A905421  A4289B29B081DC1E
t=38: CE0FCC34AD8DA36C  071FA5F764C98E5F  90B4206FAB7D0530  7696BAE1D69A401A
   4685454816101EE6  08ECE17FD62AF2F9  39083A7BEA35DAC5  5AC1DA918A905421
t=39: FB78ADD4117E0D4C  CE0FCC34AD8DA36C  071FA5F764C98E5F  90B4206FAB7D0530
   510D7EED2F67960B  4685454816101EE6  08ECE17FD62AF2F9  39083A7BEA35DAC5
t=40: 595A8250371D868B  FB78ADD4117E0D4C  CE0FCC34AD8DA36C  071FA5F764C98E5F
   5F514945AC2AF500  510D7EED2F67960B  4685454816101EE6  08ECE17FD62AF2F9
t=41: F1DC306C639EFB88  595A8250371D868B  FB78ADD4117E0D4C  CE0FCC34AD8DA36C
   413017F53DFED208  5F514945AC2AF500  510D7EED2F67960B  4685454816101EE6
t=42: 275D96E89981CFE3  F1DC306C639EFB88  595A8250371D868B  FB78ADD4117E0D4C
   0245872EE399310A  413017F53DFED208  5F514945AC2AF500  510D7EED2F67960B
t=43: 5BFB82DA35571E11  275D96E89981CFE3  F1DC306C639EFB88  595A8250371D868B
   76C80FF098F6ABB4  0245872EE399310A  413017F53DFED208  5F514945AC2AF500
t=44: E58F44F1BD431603  5BFB82DA35571E11  275D96E89981CFE3  F1DC306C639EFB88
   5EBDABABF6D782FD  76C80FF098F6ABB4  0245872EE399310A  413017F53DFED208
t=45: 53B71BC37D03FACE  E58F44F1BD431603  5BFB82DA35571E11  275D96E89981CFE3
   8598A1A47D0357A5  5EBDABABF6D782FD  76C80FF098F6ABB4  0245872EE399310A
t=46: 345AE4AA187437E1  53B71BC37D03FACE  E58F44F1BD431603  5BFB82DA35571E11
   7E74231C4177D4D1  8598A1A47D0357A5  5EBDABABF6D782FD  76C80FF098F6ABB4
t=47: 626CEEE8A84D84E0  345AE4AA187437E1  53B71BC37D03FACE  E58F44F1BD431603
   F35A915AD59125EC  7E74231C4177D4D1  8598A1A47D0357A5  5EBDABABF6D782FD
t=48: C46DD1206FE63A9F  626CEEE8A84D84E0  345AE4AA187437E1  53B71BC37D03FACE
   B7E272EFF6528CD5  F35A915AD59125EC  7E74231C4177D4D1  8598A1A47D0357A5
t=49: A6190DF4A1B0F666  C46DD1206FE63A9F  626CEEE8A84D84E0  345AE4AA187437E1
   F01D59E16E01FC67  B7E272EFF6528CD5  F35A915AD59125EC  7E74231C4177D4D1
t=50: D1EA1DDDE4EF669B  A6190DF4A1B0F666  C46DD1206FE63A9F  626CEEE8A84D84E0
   45B6FA884E24396A  F01D59E16E01FC67  B7E272EFF6528CD5  F35A915AD59125EC
t=51: 9F33EE7183AED669  D1EA1DDDE4EF669B  A6190DF4A1B0F666  C46DD1206FE63A9F
   B133508E689D5618  45B6FA884E24396A  F01D59E16E01FC67  B7E272EFF6528CD5
t=52: B13ECBE9C5AB549B  9F33EE7183AED669  D1EA1DDDE4EF669B  A6190DF4A1B0F666
   257000654C161D77  B133508E689D5618  45B6FA884E24396A  F01D59E16E01FC67
t=53: 372E19656F4C71F6  B13ECBE9C5AB549B  9F33EE7183AED669  D1EA1DDDE4EF669B
   53B78D2B828C9FD0  257000654C161D77  B133508E689D5618  45B6FA884E24396A
t=54: AE694575918CF0FA  372E19656F4C71F6  B13ECBE9C5AB549B  9F33EE7183AED669
   6349FBF49B89B65D  53B78D2B828C9FD0  257000654C161D77  B133508E689D5618
t=55: 617B509949F118FD  AE694575918CF0FA  372E19656F4C71F6  B13ECBE9C5AB549B
   B1F1CB2F4FC0A9DE  6349FBF49B89B65D  53B78D2B828C9FD0  257000654C161D77
t=56: 22C244C694B15B1C  617B509949F118FD  AE694575918CF0FA  372E19656F4C71F6
   AC9793625B6713A6  B1F1CB2F4FC0A9DE  6349FBF49B89B65D  53B78D2B828C9FD0
t=57: 3311FB1C405F0D0F  22C244C694B15B1C  617B509949F118FD  AE694575918CF0FA
   E4C449F90128CC38  AC9793625B6713A6  B1F1CB2F4FC0A9DE  6349FBF49B89B65D
t=58: 594961E04CE3A122  3311FB1C405F0D0F  22C244C694B15B1C  617B509949F118FD
   B6F7A90EB9C18C0A  E4C449F90128CC38  AC9793625B6713A6  B1F1CB2F4FC0A9DE
t=59: 0A392F484AF8A380  594961E04CE3A122  3311FB1C405F0D0F  22C244C694B15B1C
   1AD7E0EE097FDEB0  B6F7A90EB9C18C0A  E4C449F90128CC38  AC9793625B6713A6
t=60: E146E2A7C1A65C6B  0A392F484AF8A380  594961E04CE3A122  3311FB1C405F0D0F
   BB4DDA7E6C53497D  1AD7E0EE097FDEB0  B6F7A90EB9C18C0A  E4C449F90128CC38
t=61: 529AB3BCA586375B  E146E2A7C1A65C6B  0A392F484AF8A380  594961E04CE3A122
   96D42DDC61058438  BB4DDA7E6C53497D  1AD7E0EE097FDEB0  B6F7A90EB9C18C0A
t=62: 70A7E4A859B8B382  529AB3BCA586375B  E146E2A7C1A65C6B  0A392F484AF8A380
   7F8CAECE994D7B17  96D42DDC61058438  BB4DDA7E6C53497D  1AD7E0EE097FDEB0
t=63: 1F5F60BBFE7CCCE7  70A7E4A859B8B382  529AB3BCA586375B  E146E2A7C1A65C6B
   DBBB47B6F5183CB6  7F8CAECE994D7B17  96D42DDC61058438  BB4DDA7E6C53497D
t=64: 9D537AF704E642F0  1F5F60BBFE7CCCE7  70A7E4A859B8B382  529AB3BCA586375B
   BC4B7813CCB07A48  DBBB47B6F5183CB6  7F8CAECE994D7B17  96D42DDC61058438
t=65: 0F178025C27E422C  9D537AF704E642F0  1F5F60BBFE7CCCE7  70A7E4A859B8B382
   E3065FF6F7ADDF6D  BC4B7813CCB07A48  DBBB47B6F5183CB6  7F8CAECE994D7B17
```

```
t=66: A93AA5F85D1BCDEA  0F178025C27E422C  9D537AF704E642F0  1F5F60BBFE7CCCE7
   DD8BDB1945B27133  E3065FF6F7ADDF6D  BC4B7813CCB07A48  DBBB47B6F5183CB6
t=67: B93B21F8AEB8F329  A93AA5F85D1BCDEA  0F178025C27E422C  9D537AF704E642F0
   1546C7737C00F978  DD8BDB1945B27133  E3065FF6F7ADDF6D  BC4B7813CCB07A48
t=68: CF675521103494C7  B93B21F8AEB8F329  A93AA5F85D1BCDEA  0F178025C27E422C
   9202AE67985172D8  1546C7737C00F978  DD8BDB1945B27133  E3065FF6F7ADDF6D
t=69: 6BD1BCB0F69DEAB9  CF675521103494C7  B93B21F8AEB8F329  A93AA5F85D1BCDEA
   CC4A167A12B10D07  9202AE67985172D8  1546C7737C00F978  DD8BDB1945B27133
t=70: 36FB6D38EC7A9F8F  6BD1BCB0F69DEAB9  CF675521103494C7  B93B21F8AEB8F329
   BF2DF292FDA17376  A167CC4A12B10D07  9202AE67985172D8  1546C7737C00F978
t=71: B45C8408593C88F6  36FB6D38EC7A9F8F  6BD1BCB0F69DEAB9  CF675521103494C7
   70347EA05752DF76  BF2DF292FDA17376  A167CC4A12B10D07  9202AE67985172D8
t=72: 0CA25CCF6FF6180E  B45C8408593C88F6  36FB6D38EC7A9F8F  6BD1BCB0F69DEAB9
   0FFA31707E364987  70347EA05752DF76  BF2DF292FDA17376  A167CC4A12B10D07
t=73: D49316BE5F130748  0CA25CCF6FF6180E  B45C8408593C88F6  36FB6D38EC7A9F8F
   51269C93931E39F7  0FFA31707E364987  70347EA05752DF76  BF2DF292FDA17376
t=74: 896EE1FEC0F16E4B  D49316BE5F130748  0CA25CCF6FF6180E  B45C8408593C88F6
   118DA75760797D25  51269C93931E39F7  0FFA31707E364987  70347EA05752DF76
t=75: 22007C194C5B05AD  896EE1FEC0F16E4B  D49316BE5F130748  0CA25CCF6FF6180E
   070F4D2C71FD0609  118DA75760797D25  51269C93931E39F7  0FFA31707E364987
t=76: ED4C5451ED5670B7  22007C194C5B05AD  896EE1FEC0F16E4B  D49316BE5F130748
   D5AE0EB0DE35A312  070F4D2C71FD0609  118DA75760797D25  51269C93931E39F7
t=77: F61D35F056C47639  ED4C5451ED5670B7  22007C194C5B05AD  896EE1FEC0F16E4B
   137B9CA2A9375030  D5AE0EB0DE35A312  070F4D2C71FD0609  118DA75760797D25
t=78: EC01C4BFEACC2519  F61D35F056C47639  ED4C5451ED5670B7  22007C194C5B05AD
   F6083B6FEFAEF695  137B9CA2A9375030  D5AE0EB0DE35A312  070F4D2C71FD0609
t=79: 09C993659E2DEF45  EC01C4BFEACC2519  F61D35F056C47639  ED4C5451ED5670B7
   1617F9FA73004761  F6083B6FEFAEF695  137B9CA2A9375030  D5AE0EB0DE35A312
```

The output after processing the first block is

$$Y_0 = 8C3D37C819544DA2 \boxplus 09C993659E2DEF45 = 9606CB2DB7823CE7$$
$$Y_1 = 73E1996689DCD4D6 \boxplus EC01C4BFEACC2519 = 5FE35E2674A8F9EF$$
$$Y_2 = 1DFAB7AE32FF9C82 \boxplus F61D35F056C47639 = 1417ED9E89C412BB$$
$$Y_3 = 679DD514582F9FCF \boxplus ED4C5451ED5670B7 = 54EA296645861086$$
$$Y_4 = 0F6D2B697BD44DA8 \boxplus 1617F9FA73004761 = 25852563EED49509$$
$$Y_5 = 77E36F7304C48942 \boxplus F6083B6FEFAEF695 = 6DEBAAE2F4737FD7$$
$$Y_6 = 3F9D85A86A1D36C8 \boxplus 137B9CA2A9375030 = 5319224B135486F8$$
$$Y_7 = 1112E6AD91D692A1 \boxplus D5AE0EB0DE35A312 = E6C0F55E700C35B3$$

The second block input (1 024 bits) is

```
Z[ 0] = 0000000000000000
Z[ 1] = 0000000000000000
Z[ 2] = 0000000000000000
Z[ 3] = 0000000000000000
Z[ 4] = 0000000000000000
Z[ 5] = 0000000000000000
Z[ 6] = 0000000000000000
Z[ 7] = 0000000000000000
Z[ 8] = 0000000000000000
Z[ 9] = 0000000000000000
Z[10] = 0000000000000000
Z[11] = 0000000000000000
Z[12] = 0000000000000000
Z[13] = 0000000000000000
Z[14] = 0000000000000000
Z[15] = 0000000000000380
```

The following are (hexadecimal representations of) the successive values of the variables X_0, X_1, X_2, X_3, X_4, X_5, X_6 and X_7 in each round when the second block is processed.

```
t= 0: C62A1109950BC4B0  9606CB2DB7823CE7  5FE35E2674A8F9EF  1417ED9E89C412BB
   B6602607DA508EC1  25852563EED49509  6DEBAAE2F4737FD7  5319224B135486F8
t= 1: 4A2EB8F6FF304F81  C62A1109950BC4B0  9606CB2DB7823CE7  5FE35E2674A8F9EF
   614F9DBEA0C1A45C  B6602607DA508EC1  25852563EED49509  6DEBAAE2F4737FD7
t= 2: D708ED5418B1A603  4A2EB8F6FF304F81  C62A1109950BC4B0  9606CB2DB7823CE7
   CF8726E0E363D72E  614F9DBEA0C1A45C  B6602607DA508EC1  25852563EED49509
t= 3: 44D5660E0E213AA5  D708ED5418B1A603  4A2EB8F6FF304F81  C62A1109950BC4B0
   EFAA0CF5A58EB13D  CF8726E0E363D72E  614F9DBEA0C1A45C  B6602607DA508EC1
t= 4: 957D13471214C5F4  44D5660E0E213AA5  D708ED5418B1A603  4A2EB8F6FF304F81
   981291723204C874  EFAA0CF5A58EB13D  CF8726E0E363D72E  614F9DBEA0C1A45C
t= 5: 76E8C9D1C9DD8AB8  957D13471214C5F4  44D5660E0E213AA5  D708ED5418B1A603
   7FCCD3C31337A90E  981291723204C874  EFAA0CF5A58EB13D  CF8726E0E363D72E
t= 6: 4B16F79453BE3727  76E8C9D1C9DD8AB8  957D13471214C5F4  44D5660E0E213AA5
   80E62F655E7ED37B  7FCCD3C31337A90E  981291723204C874  EFAA0CF5A58EB13D
t= 7: 5E63338FBE9889D9  4B16F79453BE3727  76E8C9D1C9DD8AB8  957D13471214C5F4
   441041F54BE0537B  80E62F655E7ED37B  7FCCD3C31337A90E  981291723204C874
t= 8: C7338364B83DF9C6  5E63338FBE9889D9  4B16F79453BE3727  76E8C9D1C9DD8AB8
   E4FA1425EB9F0182  441041F54BE0537B  80E62F655E7ED37B  7FCCD3C31337A90E
t= 9: 5ED78CF2D7AD0133  C7338364B83DF9C6  5E63338FBE9889D9  4B16F79453BE3727
   21EC095197532090  E4FA1425EB9F0182  441041F54BE0537B  80E62F655E7ED37B
t=10: 75C6A9870347B569  5ED78CF2D7AD0133  C7338364B83DF9C6  5E63338FBE9889D9
   37D613B93BD7DFB5  21EC095197532090  E4FA1425EB9F0182  441041F54BE0537B
t=11: 2330FC9F6CEAC437  75C6A9870347B569  5ED78CF2D7AD0133  C7338364B83DF9C6
   2F1071A0C464DD6B  37D613B93BD7DFB5  21EC095197532090  E4FA1425EB9F0182
t=12: B56EA6063E644DAF  2330FC9F6CEAC437  75C6A9870347B569  5ED78CF2D7AD0133
   D97C54DC192D2B1A  2F1071A0C464DD6B  37D613B93BD7DFB5  21EC095197532090
t=13: F60601BFD3CE4BA2  B56EA6063E644DAF  2330FC9F6CEAC437  75C6A9870347B569
   B9D5E11F983972F8  D97C54DC192D2B1A  2F1071A0C464DD6B  37D613B93BD7DFB5
t=14: FA6E99A8556DF258  F60601BFD3CE4BA2  B56EA6063E644DAF  2330FC9F6CEAC437
   015DEA3F41B9C289  B9D5E11F983972F8  D97C54DC192D2B1A  2F1071A0C464DD6B
t=15: 38E5F661C3F1191B  FA6E99A8556DF258  F60601BFD3CE4BA2  B56EA6063E644DAF
   5279EE55AFE8AFCC  015DEA3F41B9C289  B9D5E11F983972F8  D97C54DC192D2B1A
t=16: ACDC1A5C38C85CD5  38E5F661C3F1191B  FA6E99A8556DF258  F60601BFD3CE4BA2
   DB79F8F12D277F02  5279EE55AFE8AFCC  015DEA3F41B9C289  B9D5E11F983972F8
t=17: 4B9240C9BA6F1B53  ACDC1A5C38C85CD5  38E5F661C3F1191B  FA6E99A8556DF258
   4DE55D4B2EA4F33C  DB79F8F12D277F02  5279EE55AFE8AFCC  015DEA3F41B9C289
t=18: 4635F911BF4C6D0D  4B9240C9BA6F1B53  ACDC1A5C38C85CD5  38E5F661C3F1191B
   BCB192998C798DEA  4DE55D4B2EA4F33C  DB79F8F12D277F02  5279EE55AFE8AFCC
t=19: E586156D13060B8C  4635F911BF4C6D0D  4B9240C9BA6F1B53  ACDC1A5C38C85CD5
   176C6027F44C42A5  BCB192998C798DEA  4DE55D4B2EA4F33C  DB79F8F12D277F02
t=20: 65E9087A1372B7EE  E586156D13060B8C  4635F911BF4C6D0D  4B9240C9BA6F1B53
   1CA79B5218212A16  176C6027F44C42A5  BCB192998C798DEA  4DE55D4B2EA4F33C
t=21: 61D617FF18A51FA7  65E9087A1372B7EE  E586156D13060B8C  4635F911BF4C6D0D
   FFF208DDA4ACF3BF  1CA79B5218212A16  176C6027F44C42A5  BCB192998C798DEA
t=22: EAE30855B7D727BF  61D617FF18A51FA7  65E9087A1372B7EE  E586156D13060B8C
   1908F447D8261EFD  FFF208DDA4ACF3BF  1CA79B5218212A16  176C6027F44C42A5
t=23: E17F4AA3CA31951F  EAE30855B7D727BF  61D617FF18A51FA7  65E9087A1372B7EE
   A93A3B339DE2E79E  1908F447D8261EFD  FFF208DDA4ACF3BF  1CA79B5218212A16
t=24: CBDA7FD5D72B0448  E17F4AA3CA31951F  EAE30855B7D727BF  61D617FF18A51FA7
   39CB25C47F7F1E76  A93A3B339DE2E79E  1908F447D8261EFD  FFF208DDA4ACF3BF
t=25: 875B7C8BD1FC6FFF  CBDA7FD5D72B0448  E17F4AA3CA31951F  EAE30855B7D727BF
   5061761EF4A7B430  39CB25C47F7F1E76  A93A3B339DE2E79E  1908F447D8261EFD
t=26: 7493EB03CB083DCB  875B7C8BD1FC6FFF  CBDA7FD5D72B0448  E17F4AA3CA31951F
   A00157FD4436BEC5  5061761EF4A7B430  39CB25C47F7F1E76  A93A3B339DE2E79E
t=27: A2194EB42A179534  7493EB03CB083DCB  875B7C8BD1FC6FFF  CBDA7FD5D72B0448
   75E556161E2D8F5E  A00157FD4436BEC5  5061761EF4A7B430  39CB25C47F7F1E76
t=28: 50120D72503F50A3  A2194EB42A179534  7493EB03CB083DCB  875B7C8BD1FC6FFF
   B2288596FBF78C7A  75E556161E2D8F5E  A00157FD4436BEC5  5061761EF4A7B430
t=29: 9388C45EF9BEDABA  50120D72503F50A3  A2194EB42A179534  7493EB03CB083DCB
   377650FBEE17C4B3  B2288596FBF78C7A  75E556161E2D8F5E  A00157FD4436BEC5
```

```
t=30: FA0D8AF6122631D1  9388C45EF9BEDABA  50120D72503F50A3  A2194EB42A179534
   4417C8D07BA5397A  377650FBEE17C4B3  B2288596FBF78C7A  75E556161E2D8F5E
t=31: 9E234A4F427D2B06  FA0D8AF6122631D1  9388C45EF9BEDABA  50120D72503F50A3
   23652F849EA698BE  4417C8D07BA5397A  377650FBEE17C4B3  B2288596FBF78C7A
t=32: 8D9DC47628B2D452  9E234A4F427D2B06  FA0D8AF6122631D1  9388C45EF9BEDABA
   D9DD068BDE33B870  23652F849EA698BE  4417C8D07BA5397A  377650FBEE17C4B3
t=33: DBC5AB3931DBA353  8D9DC47628B2D452  9E234A4F427D2B06  FA0D8AF6122631D1
   E3F00F8D49C43EC4  D9DD068BDE33B870  23652F849EA698BE  4417C8D07BA5397A
t=34: 90BBFAFE9E70D4DE  DBC5AB3931DBA353  8D9DC47628B2D452  9E234A4F427D2B06
   C79450C5A27F1152  E3F00F8D49C43EC4  D9DD068BDE33B870  23652F849EA698BE
t=35: 0176074A50D737DC  90BBFAFE9E70D4DE  DBC5AB3931DBA353  8D9DC47628B2D452
   484DCDA447B167ED  C79450C5A27F1152  E3F00F8D49C43EC4  D9DD068BDE33B870
t=36: 8A31589736A222D9  0176074A50D737DC  90BBFAFE9E70D4DE  DBC5AB3931DBA353
   77F0533A9F4225D4  484DCDA447B167ED  C79450C5A27F1152  E3F00F8D49C43EC4
t=37: DB9603572C370B39  8A31589736A222D9  0176074A50D737DC  90BBFAFE9E70D4DE
   AD407246D492B9C9  77F0533A9F4225D4  484DCDA447B167ED  C79450C5A27F1152
t=38: A0BC2200492231A3  DB9603572C370B39  8A31589736A222D9  0176074A50D737DC
   001CFA61F6A94907  AD407246D492B9C9  77F0533A9F4225D4  484DCDA447B167ED
t=39: D17150907EDA767B  A0BC2200492231A3  DB9603572C370B39  8A31589736A222D9
   C7398391FEE339DE  001CFA61F6A94907  AD407246D492B9C9  77F0533A9F4225D4
t=40: A3312953448FA7E1  D17150907EDA767B  A0BC2200492231A3  DB9603572C370B39
   88C2310AFA13D7FD  C7398391FEE339DE  001CFA61F6A94907  AD407246D492B9C9
t=41: A1974BE1E531F375  A3312953448FA7E1  D17150907EDA767B  A0BC2200492231A3
   9CABA67B2C460999  88C2310AFA13D7FD  C7398391FEE339DE  001CFA61F6A94907
t=42: 34BFABB3D67367DF  A1974BE1E531F375  A3312953448FA7E1  D17150907EDA767B
   4AB15B8120A75FA0  9CABA67B2C460999  88C2310AFA13D7FD  C7398391FEE339DE
t=43: 47FB83EA0B09CFDF  34BFABB3D67367DF  A1974BE1E531F375  A3312953448FA7E1
   82AF65BB8CF42FDF  4AB15B8120A75FA0  9CABA67B2C460999  88C2310AFA13D7FD
t=44: BE123C3EE4765CED  47FB83EA0B09CFDF  34BFABB3D67367DF  A1974BE1E531F375
   553B3C12510AF392  82AF65BB8CF42FDF  4AB15B8120A75FA0  9CABA67B2C460999
t=45: 1BBD79A592A8BD47  BE123C3EE4765CED  47FB83EA0B09CFDF  34BFABB3D67367DF
   02E864735B8BF844  553B3C12510AF392  82AF65BB8CF42FDF  4AB15B8120A75FA0
t=46: 0A8B7BECB393BFA4  1BBD79A592A8BD47  BE123C3EE4765CED  47FB83EA0B09CFDF
   1A8B439714CE8AF1  02E864735B8BF844  553B3C12510AF392  82AF65BB8CF42FDF
t=47: 9510DFC044C38B79  0A8B7BECB393BFA4  1BBD79A592A8BD47  BE123C3EE4765CED
   F5B8B726BB1A26AC  1A8B439714CE8AF1  02E864735B8BF844  553B3C12510AF392
t=48: 20C6FF36AAF2AFE6  9510DFC044C38B79  0A8B7BECB393BFA4  1BBD79A592A8BD47
   E5BDED3F35816323  F5B8B726BB1A26AC  1A8B439714CE8AF1  02E864735B8BF844
t=49: 7FA16F7BA5EBE14C  20C6FF36AAF2AFE6  9510DFC044C38B79  0A8B7BECB393BFA4
   321838784DA12D56  E5BDED3F35816323  F5B8B726BB1A26AC  1A8B439714CE8AF1
t=50: D2B84B6F18380735  7FA16F7BA5EBE14C  20C6FF36AAF2AFE6  9510DFC044C38B79
   67338C92A9E62CB3  321838784DA12D56  E5BDED3F35816323  F5B8B726BB1A26AC
t=51: 9201269A2C54F51E  D2B84B6F18380735  7FA16F7BA5EBE14C  20C6FF36AAF2AFE6
   18B3943C938E0477  67338C92A9E62CB3  321838784DA12D56  E5BDED3F35816323
t=52: E5AA7485C1241AA4  9201269A2C54F51E  D2B84B6F18380735  7FA16F7BA5EBE14C
   B9CD3EFC85E7C325  18B3943C938E0477  67338C92A9E62CB3  321838784DA12D56
t=53: 5E3B46494F487A51  E5AA7485C1241AA4  9201269A2C54F51E  D2B84B6F18380735
   A1A96A63C2F9C2D5  B9CD3EFC85E7C325  18B3943C938E0477  67338C92A9E62CB3
t=54: 30F07AE985818A3F  5E3B46494F487A51  E5AA7485C1241AA4  9201269A2C54F51E
   F7B2345A39EE53D6  A1A96A63C2F9C2D5  B9CD3EFC85E7C325  18B3943C938E0477
t=55: D5441CF2BBBF4247  30F07AE985818A3F  5E3B46494F487A51  E5AA7485C1241AA4
   08170A5A65B9CC59  F7B2345A39EE53D6  A1A96A63C2F9C2D5  B9CD3EFC85E7C325
t=56: A028FDCCD5B3CD6C  D5441CF2BBBF4247  30F07AE985818A3F  5E3B46494F487A51
   40F68900D8945D8B  08170A5A65B9CC59  F7B2345A39EE53D6  A1A96A63C2F9C2D5
t=57: A7EC8B6433605C8D  A028FDCCD5B3CD6C  D5441CF2BBBF4247  30F07AE985818A3F
   5DCC12B8F92F5A2A  40F68900D8945D8B  08170A5A65B9CC59  F7B2345A39EE53D6
t=58: E7440592C375CD18  A7EC8B6433605C8D  A028FDCCD5B3CD6C  D5441CF2BBBF4247
   800CC35788C7BD7E  5DCC12B8F92F5A2A  40F68900D8945D8B  08170A5A65B9CC59
t=59: 8CFEBA0AA271D1E8  E7440592C375CD18  A7EC8B6433605C8D  A028FDCCD5B3CD6C
   18CEFFE60E5F76E0  800CC35788C7BD7E  5DCC12B8F92F5A2A  40F68900D8945D8B
t=60: 47B9D567B722FB37  8CFEBA0AA271D1E8  E7440592C375CD18  A7EC8B6433605C8D
   A530BEE0AB96F7BF  18CEFFE60E5F76E0  800CC35788C7BD7E  5DCC12B8F92F5A2A
t=61: A3C575002D2A90C4  47B9D567B722FB37  8CFEBA0AA271D1E8  E7440592C375CD18
```

```
   332C2311F81CC391  A530BEE0AB96F7BF  18CEFFE60E5F76E0  800CC35788C7BD7E
t=62: F96FCB96DEB9E494  A3C575002D2A90C4  47B9D567B722FB37  8CFEBA0AA271D1E8
   7EFBDECC5D2B5820  332C2311F81CC391  A530BEE0AB96F7BF  18CEFFE60E5F76E0
t=63: F363C8EC7B1A0888  F96FCB96DEB9E494  A3C575002D2A90C4  47B9D567B722FB37
   2AE76A4CDD0B55BD  7EFBDECC5D2B5820  332C2311F81CC391  A530BEE0AB96F7BF
t=64: B80FA4876347AD57  F363C8EC7B1A0888  F96FCB96DEB9E494  A3C575002D2A90C4
   94D171AE802D6C9D  2AE76A4CDD0B55BD  7EFBDECC5D2B5820  332C2311F81CC391
t=65: 96345101E32B060F  B80FA4876347AD57  F363C8EC7B1A0888  F96FCB96DEB9E494
   5E1C4C06D3B02C21  94D171AE802D6C9D  2AE76A4CDD0B55BD  7EFBDECC5D2B5820
t=66: 35C874D072FDC82C  96345101E32B060F  B80FA4876347AD57  F363C8EC7B1A0888
   3353886B54C833B5  5E1C4C06D3B02C21  94D171AE802D6C9D  2AE76A4CDD0B55BD
t=67: 401E4175643FC458  35C874D072FDC82C  96345101E32B060F  B80FA4876347AD57
   EBEF8A88724B7FF7  3353886B54C833B5  5E1C4C06D3B02C21  94D171AE802D6C9D
t=68: D58E109317C90113  401E4175643FC458  35C874D072FDC82C  96345101E32B060F
   894598AE776D2ED5  EBEF8A88724B7FF7  3353886B54C833B5  5E1C4C06D3B02C21
t=69: 68A4AA1333AEA536  D58E109317C90113  401E4175643FC458  35C874D072FDC82C
   09FCE6C815B259F9  894598AE776D2ED5  EBEF8A88724B7FF7  3353886B54C833B5
t=70: 8A0D8C01F5588CC1  68A4AA1333AEA536  D58E109317C90113  401E4175643FC458
   AEE1595DB3F40CF8  09FCE6C815B259F9  894598AE776D2ED5  EBEF8A88724B7FF7
t=71: 6F485B267B52813E  8A0D8C01F5588CC1  68A4AA1333AEA536  D58E109317C90113
   BBA5B657667A087C  AEE1595DB3F40CF8  09FCE6C815B259F9  894598AE776D2ED5
t=72: CBF0FF8A3EB56D59  6F485B267B52813E  8A0D8C01F5588CC1  68A4AA1333AEA536
   D0686F6ECF9AB51E  BBA5B657667A087C  AEE1595DB3F40CF8  09FCE6C815B259F9
t=73: AD1D1893EE86E3B6  CBF0FF8A3EB56D59  6F485B267B52813E  8A0D8C01F5588CC1
   D9F1FF942480D4D5  D0686F6ECF9AB51E  BBA5B657667A087C  AEE1595DB3F40CF8
t=74: 1443D9D1606FF323  AD1D1893EE86E3B6  CBF0FF8A3EB56D59  6F485B267B52813E
   7AE67C10BF64A97B  D9F1FF942480D4D5  D0686F6ECF9AB51E  BBA5B657667A087C
t=75: 9F07271D479F94DC  1443D9D1606FF323  AD1D1893EE86E3B6  CBF0FF8A3EB56D59
   84D997908D444616  7AE67C10BF64A97B  D9F1FF942480D4D5  D0686F6ECF9AB51E
t=76: 137D219301D78C4D  9F07271D479F94DC  1443D9D1606FF323  AD1D1893EE86E3B6
   2FD56FB46B6F4F93  84D997908D444616  7AE67C10BF64A97B  D9F1FF942480D4D5
t=77: 21BE76D4C61FFBB7  137D219301D78C4D  9F07271D479F94DC  1443D9D1606FF323
   BC85E4FC899BA009  2FD56FB46B6F4F93  84D997908D444616  7AE67C10BF64A97B
t=78: D09E343D96634B44  21BE76D4C61FFBB7  137D219301D78C4D  9F07271D479F94DC
   D7AE6C10F1681576  BC85E4FC899BA009  2FD56FB46B6F4F93  84D997908D444616
t=79: 8DF7FA8DDD53CE3C  D09E343D96634B44  21BE76D4C61FFBB7  137D219301D78C4D
   A2C04D0AEA35A515  D7AE6C10F1681576  BC85E4FC899BA009  2FD56FB46B6F4F93
```

The output after processing the second block is

$$Y_0 = 9606CB2DB7823CE7 \boxplus 8DF7FA8DDD53CE3C = 23FEC5BB94D60B23$$
$$Y_1 = 5FE35E2674A8F9EF \boxplus D09E343D96634B44 = 308192640B0C4533$$
$$Y_2 = 1417ED9E89C412BB \boxplus 21BE76D4C61FFBB7 = 35D664734FE40E72$$
$$Y_3 = 54EA296645861086 \boxplus 137D219301D78C4D = 68674AF9475D9CD3$$
$$Y_4 = 25852563EED49509 \boxplus A2C04D0AEA35A515 = C845726ED90A3A1E$$
$$Y_5 = 6DEBAAE2F4737FD7 \boxplus D7AE6C10F1681576 = 459A16F3E5DB954D$$
$$Y_6 = 5319224B135486F8 \boxplus BC85E4FC899BA009 = 0F9F07479CF02701$$
$$Y_7 = E6C0F55E700C35B3 \boxplus 2FD56FB46B6F4F93 = 16966512DB7B8546$$

The message digest is

```
23FEC5BB 94D60B23 30819264 0B0C4533 35D66473 4FE40E72 68674AF9
```

B.12 Dedicated Hash-Function 10 (SHA-512/256)

B.12.1 Example 1

In this example, the input message is “abc”. The padded one block input (1 024 bits) is

```
Z[ 0] = 6162638000000000
Z[ 1] = 0000000000000000
Z[ 2] = 0000000000000000
Z[ 3] = 0000000000000000
Z[ 4] = 0000000000000000
Z[ 5] = 0000000000000000
Z[ 6] = 0000000000000000
Z[ 7] = 0000000000000000
Z[ 8] = 0000000000000000
Z[ 9] = 0000000000000000
Z[10] = 0000000000000000
Z[11] = 0000000000000000
Z[12] = 0000000000000000
Z[13] = 0000000000000000
Z[14] = 0000000000000000
Z[15] = 0000000000000018
```

The following are (hexadecimal representations of) the successive values of the variables X_0, X_1, X_2, X_3, X_4, X_5, X_6 and X_7 in each round.

```
t= 0: 9A2F6D11C39458FE  22312194FC2BF72C  9F555FA3C84C64C2  2393B86B6F53B151
   3908D19FBCAF1B12  96283EE2A88EFFE3  BE5E1E2553863992  2B0199FC2C85B8AA
t= 1: 9C465A16F85EBD68  9A2F6D11C39458FE  22312194FC2BF72C  9F555FA3C84C64C2
   BB7CF388A65CA549  3908D19FBCAF1B12  96283EE2A88EFFE3  BE5E1E2553863992
t= 2: D983D31C6CEA97C9  9C465A16F85EBD68  9A2F6D11C39458FE  22312194FC2BF72C
   C8A505020ACB43C1  BB7CF388A65CA549  3908D19FBCAF1B12  96283EE2A88EFFE3
t= 3: 1D4E8897FCFF509E  D983D31C6CEA97C9  9C465A16F85EBD68  9A2F6D11C39458FE
   BA2E42D7925DE73B  C8A505020ACB43C1  BB7CF388A65CA549  3908D19FBCAF1B12
t= 4: 47376B4548F81A5F  1D4E8897FCFF509E  D983D31C6CEA97C9  9C465A16F85EBD68
   24ECDAD8A00C274A  BA2E42D7925DE73B  C8A505020ACB43C1  BB7CF388A65CA549
t= 5: AA7B88556927CE7D  47376B4548F81A5F  1D4E8897FCFF509E  D983D31C6CEA97C9
   928BC3FFD85778B3  24ECDAD8A00C274A  BA2E42D7925DE73B  C8A505020ACB43C1
t= 6: B906B3DF822CF7C1  AA7B88556927CE7D  47376B4548F81A5F  1D4E8897FCFF509E
   2023A2CD4FA5A4D8  928BC3FFD85778B3  24ECDAD8A00C274A  BA2E42D7925DE73B
t= 7: 2F839A3929F48358  B906B3DF822CF7C1  AA7B88556927CE7D  47376B4548F81A5F
   245A5F77616E5931  2023A2CD4FA5A4D8  928BC3FFD85778B3  24ECDAD8A00C274A
t= 8: 4B1B0E41FB81C46C  2F839A3929F48358  B906B3DF822CF7C1  AA7B88556927CE7D
   3FE7E2D7D7CED54A  245A5F77616E5931  2023A2CD4FA5A4D8  928BC3FFD85778B3
t= 9: C4F1C71E65B18C15  4B1B0E41FB81C46C  2F839A3929F48358  B906B3DF822CF7C1
   FF5E80C2A75481B7  3FE7E2D7D7CED54A  245A5F77616E5931  2023A2CD4FA5A4D8
t=10: 19D100CB5E1A3438  C4F1C71E65B18C15  4B1B0E41FB81C46C  2F839A3929F48358
   8484655060EBC3EE  FF5E80C2A75481B7  3FE7E2D7D7CED54A  245A5F77616E5931
t=11: 7AAB2807D4F3F022  19D100CB5E1A3438  C4F1C71E65B18C15  4B1B0E41FB81C46C
   BFC3C10D93FF00B8  8484655060EBC3EE  FF5E80C2A75481B7  3FE7E2D7D7CED54A
t=12: C9E2CB6D5D017BA7  7AAB2807D4F3F022  19D100CB5E1A3438  C4F1C71E65B18C15
   0662BFD092E26FB7  BFC3C10D93FF00B8  8484655060EBC3EE  FF5E80C2A75481B7
t=13: 8C4D8B98E0672988  C9E2CB6D5D017BA7  7AAB2807D4F3F022  19D100CB5E1A3438
   996E6405C63D83E3  0662BFD092E26FB7  BFC3C10D93FF00B8  8484655060EBC3EE
t=14: 8D70D5EBDEA6724A  8C4D8B98E0672988  C9E2CB6D5D017BA7  7AAB2807D4F3F022
   CEAAAEEF7189EC61  996E6405C63D83E3  0662BFD092E26FB7  BFC3C10D93FF00B8
t=15: 1EC6365704280063  8D70D5EBDEA6724A  8C4D8B98E0672988  C9E2CB6D5D017BA7
   419C9D961BA8EA8F  CEAAAEEF7189EC61  996E6405C63D83E3  0662BFD092E26FB7
t=16: 3AA569FFD0244EC4  1EC6365704280063  8D70D5EBDEA6724A  8C4D8B98E0672988
   4AC147677B104598  419C9D961BA8EA8F  CEAAAEEF7189EC61  996E6405C63D83E3
t=17: 2B6738209B26B728  3AA569FFD0244EC4  1EC6365704280063  8D70D5EBDEA6724A
```

```
   8EE2964A7ADF0F1D  4AC147677B104598  419C9D961BA8EA8F  CEAAAEEF7189EC61
t=18: 1FE6F882B4543504  2B6738209B26B728  3AA569FFD0244EC4  1EC6365704280063
   9CDC03D015DA1E7D  8EE2964A7ADF0F1D  4AC147677B104598  419C9D961BA8EA8F
t=19: 73F4F92021784BB1  1FE6F882B4543504  2B6738209B26B728  3AA569FFD0244EC4
   6994C169A3D21916  9CDC03D015DA1E7D  8EE2964A7ADF0F1D  4AC147677B104598
t=20: 4E8CA806D9319A74  73F4F92021784BB1  1FE6F882B4543504  2B6738209B26B728
   EDB2C079F68C6C60  6994C169A3D21916  9CDC03D015DA1E7D  8EE2964A7ADF0F1D
t=21: 73214592D44C971F  4E8CA806D9319A74  73F4F92021784BB1  1FE6F882B4543504
   15BBE2C3AA0E7FD7  EDB2C079F68C6C60  6994C169A3D21916  9CDC03D015DA1E7D
t=22: C56EBA713AEEA98F  73214592D44C971F  4E8CA806D9319A74  73F4F92021784BB1
   9D3DFCD24D8FF89C  15BBE2C3AA0E7FD7  EDB2C079F68C6C60  6994C169A3D21916
t=23: 77F4BC54FFD4166B  C56EBA713AEEA98F  73214592D44C971F  4E8CA806D9319A74
   A2981D9590A4F202  9D3DFCD24D8FF89C  15BBE2C3AA0E7FD7  EDB2C079F68C6C60
t=24: B380E5F84D5DD65C  77F4BC54FFD4166B  C56EBA713AEEA98F  73214592D44C971F
   1F5D06ACB369D69F  A2981D9590A4F202  9D3DFCD24D8FF89C  15BBE2C3AA0E7FD7
t=25: D8F368221281F96A  B380E5F84D5DD65C  77F4BC54FFD4166B  C56EBA713AEEA98F
   1E1F4553B9689309  1F5D06ACB369D69F  A2981D9590A4F202  9D3DFCD24D8FF89C
t=26: 73CE37ED59FC4595  D8F368221281F96A  B380E5F84D5DD65C  77F4BC54FFD4166B
   5CB11AE8485959C1  1E1F4553B9689309  1F5D06ACB369D69F  A2981D9590A4F202
t=27: 2B79283E450B25D2  73CE37ED59FC4595  D8F368221281F96A  B380E5F84D5DD65C
   9CA2CDF1A009F7A0  5CB11AE8485959C1  1E1F4553B9689309  1F5D06ACB369D69F
t=28: 7C8479834A5D5E1C  2B79283E450B25D2  73CE37ED59FC4595  D8F368221281F96A
   F68FB52FAD1792EB  9CA2CDF1A009F7A0  5CB11AE8485959C1  1E1F4553B9689309
t=29: 5623A1ED63ACFE9C  7C8479834A5D5E1C  2B79283E450B25D2  73CE37ED59FC4595
   4174C3633D3223CB  F68FB52FAD1792EB  9CA2CDF1A009F7A0  5CB11AE8485959C1
t=30: E0639E0746A1C4B9  5623A1ED63ACFE9C  7C8479834A5D5E1C  2B79283E450B25D2
   1D2D1CA60E71D9C4  4174C3633D3223CB  F68FB52FAD1792EB  9CA2CDF1A009F7A0
t=31: 0ECE8CB912DE792B  E0639E0746A1C4B9  5623A1ED63ACFE9C  7C8479834A5D5E1C
   10EA82370759FF98  1D2D1CA60E71D9C4  4174C3633D3223CB  F68FB52FAD1792EB
t=32: 1011563D5CA6F21D  0ECE8CB912DE792B  E0639E0746A1C4B9  5623A1ED63ACFE9C
   2ABC930AEB105DDA  10EA82370759FF98  1D2D1CA60E71D9C4  4174C3633D3223CB
t=33: 001128D308744A0E  1011563D5CA6F21D  0ECE8CB912DE792B  E0639E0746A1C4B9
   6DF15BD09649437B  2ABC930AEB105DDA  10EA82370759FF98  1D2D1CA60E71D9C4
t=34: 785B23CDC94E4D47  001128D308744A0E  1011563D5CA6F21D  0ECE8CB912DE792B
   75645A2459E2B29C  6DF15BD09649437B  2ABC930AEB105DDA  10EA82370759FF98
t=35: 431A6F9571320866  785B23CDC94E4D47  001128D308744A0E  1011563D5CA6F21D
   C4B1FDB46655F51A  75645A2459E2B29C  6DF15BD09649437B  2ABC930AEB105DDA
t=36: D9E89BCB3B3616FE  431A6F9571320866  785B23CDC94E4D47  001128D308744A0E
   445065C5E0806A68  C4B1FDB46655F51A  75645A2459E2B29C  6DF15BD09649437B
t=37: 4C5C5085AFB86C02  D9E89BCB3B3616FE  431A6F9571320866  785B23CDC94E4D47
   0738C70B69B65E34  445065C5E0806A68  C4B1FDB46655F51A  75645A2459E2B29C
t=38: 49F49406AA9C7915  4C5C5085AFB86C02  D9E89BCB3B3616FE  431A6F9571320866
   DDBFB052E66E151C  0738C70B69B65E34  445065C5E0806A68  C4B1FDB46655F51A
t=39: D53B182812347708  49F49406AA9C7915  4C5C5085AFB86C02  D9E89BCB3B3616FE
   C0233F51F0027715  DDBFB052E66E151C  0738C70B69B65E34  445065C5E0806A68
t=40: 6204009DBFD8D0DB  D53B182812347708  49F49406AA9C7915  4C5C5085AFB86C02
   768286C2D8FD381E  C0233F51F0027715  DDBFB052E66E151C  0738C70B69B65E34
t=41: AF3049C09D76ABCE  6204009DBFD8D0DB  D53B182812347708  49F49406AA9C7915
   11540218448DA4BA  768286C2D8FD381E  C0233F51F0027715  DDBFB052E66E151C
t=42: 6F48A93A6216BDFA  AF3049C09D76ABCE  6204009DBFD8D0DB  D53B182812347708
   60FF3969A7A7545B  11540218448DA4BA  768286C2D8FD381E  C0233F51F0027715
t=43: 163B797CD24C6D2E  6F48A93A6216BDFA  AF3049C09D76ABCE  6204009DBFD8D0DB
   AF4C2A6889A401A2  60FF3969A7A7545B  11540218448DA4BA  768286C2D8FD381E
t=44: 75B6F991523D6EBD  163B797CD24C6D2E  6F48A93A6216BDFA  AF3049C09D76ABCE
   BE913F4585AA524A  AF4C2A6889A401A2  60FF3969A7A7545B  11540218448DA4BA
t=45: 8072323233213D257  75B6F991523D6EBD  163B797CD24C6D2E  6F48A93A6216BDFA
   6269B8150084C5E5  BE913F4585AA524A  AF4C2A6889A401A2  60FF3969A7A7545B
t=46: 5A93EC3C573AB27A  8072323233213D257  75B6F991523D6EBD  163B797CD24C6D2E
   EBCC25FD1EF4B66A  6269B8150084C5E5  BE913F4585AA524A  AF4C2A6889A401A2
t=47: 96F715647C35010B  5A93EC3C573AB27A  8072323233213D257  75B6F991523D6EBD
   3DB3985131165CA8  EBCC25FD1EF4B66A  6269B8150084C5E5  BE913F4585AA524A
t=48: A493F38FA8BD1B7A  96F715647C35010B  5A93EC3C573AB27A  8072323233213D257
   72B27DF2E6E57AA8  3DB3985131165CA8  EBCC25FD1EF4B66A  6269B8150084C5E5
```

```
t=49: D379E2742808F23F  A493F38FA8BD1B7A  96F715647C35010B  5A93EC3C573AB27A
   3EA89437C88CCD1E  72B27DF2E6E57AA8  3DB3985131165CA8  EBCC25FD1EF4B66A
t=50: 8C0C28392DFEEFD0  D379E2742808F23F  A493F38FA8BD1B7A  96F715647C35010B
   ECCF127AA015E2F4  3EA89437C88CCD1E  72B27DF2E6E57AA8  3DB3985131165CA8
t=51: 1D5955ABCFDCADF0  8C0C28392DFEEFD0  D379E2742808F23F  A493F38FA8BD1B7A
   496BCDAFE07B21B5  ECCF127AA015E2F4  3EA89437C88CCD1E  72B27DF2E6E57AA8
t=52: 5799F02F81A7C51F  1D5955ABCFDCADF0  8C0C28392DFEEFD0  D379E2742808F23F
   0532365FC98E332C  496BCDAFE07B21B5  ECCF127AA015E2F4  3EA89437C88CCD1E
t=53: D09E98B45E7412B7  5799F02F81A7C51F  1D5955ABCFDCADF0  8C0C28392DFEEFD0
   E1E81BC465A7CA13  0532365FC98E332C  496BCDAFE07B21B5  ECCF127AA015E2F4
t=54: B404CE9F5B35EB6E  D09E98B45E7412B7  5799F02F81A7C51F  1D5955ABCFDCADF0
   52165E3326D1452E  E1E81BC465A7CA13  0532365FC98E332C  496BCDAFE07B21B5
t=55: 8FE543A7E1C7DE6B  B404CE9F5B35EB6E  D09E98B45E7412B7  5799F02F81A7C51F
   7D7C18AE2648F54D  52165E3326D1452E  E1E81BC465A7CA13  0532365FC98E332C
t=56: BF53B7992F425D82  8FE543A7E1C7DE6B  B404CE9F5B35EB6E  D09E98B45E7412B7
   D6993E728AC1A822  7D7C18AE2648F54D  52165E3326D1452E  E1E81BC465A7CA13
t=57: A7FC20CC2822A712  BF53B7992F425D82  8FE543A7E1C7DE6B  B404CE9F5B35EB6E
   2BA925F0BBBDA744  D6993E728AC1A822  7D7C18AE2648F54D  52165E3326D1452E
t=58: 1F5B9E4E9E470F85  A7FC20CC2822A712  BF53B7992F425D82  8FE543A7E1C7DE6B
   12F8ABBFDCC71F41  2BA925F0BBBDA744  D6993E728AC1A822  7D7C18AE2648F54D
t=59: 1F4AC7E8968E01F9  1F5B9E4E9E470F85  A7FC20CC2822A712  BF53B7992F425D82
   10F69F1491C21C9C  12F8ABBFDCC71F41  2BA925F0BBBDA744  D6993E728AC1A822
t=60: 0B00107983688DDD  1F4AC7E8968E01F9  1F5B9E4E9E470F85  A7FC20CC2822A712
   0E8ABD59D36488D2  10F69F1491C21C9C  12F8ABBFDCC71F41  2BA925F0BBBDA744
t=61: 05774F6D8337D0DF  0B00107983688DDD  1F4AC7E8968E01F9  1F5B9E4E9E470F85
   E8D4AA14CC35666E  0E8ABD59D36488D2  10F69F1491C21C9C  12F8ABBFDCC71F41
t=62: 0E8748C473D5D319  05774F6D8337D0DF  0B00107983688DDD  1F4AC7E8968E01F9
   95EA094366CA9524  E8D4AA14CC35666E  0E8ABD59D36488D2  10F69F1491C21C9C
t=63: 37313BCC31405DD8  0E8748C473D5D319  05774F6D8337D0DF  0B00107983688DDD
   9E24CC56AA903D0D  95EA094366CA9524  E8D4AA14CC35666E  0E8ABD59D36488D2
t=64: 75CAD73882574762  37313BCC31405DD8  0E8748C473D5D319  05774F6D8337D0DF
   F95C519703B8731F  9E24CC56AA903D0D  95EA094366CA9524  E8D4AA14CC35666E
t=65: 7D4BF508527DF4FA  75CAD73882574762  37313BCC31405DD8  0E8748C473D5D319
   D65ADF389D2C1A99  F95C519703B8731F  9E24CC56AA903D0D  95EA094366CA9524
t=66: CEEFB640F1F288C3  7D4BF508527DF4FA  75CAD73882574762  37313BCC31405DD8
   44463E8C945BCBB5  D65ADF389D2C1A99  F95C519703B8731F  9E24CC56AA903D0D
t=67: FC11CC97AE386106  CEEFB640F1F288C3  7D4BF508527DF4FA  75CAD73882574762
   12BF463D7223A309  44463E8C945BCBB5  D65ADF389D2C1A99  F95C519703B8731F
t=68: DAF7189BF71319ED  FC11CC97AE386106  CEEFB640F1F288C3  7D4BF508527DF4FA
   2D2182E71310E6C7  12BF463D7223A309  44463E8C945BCBB5  D65ADF389D2C1A99
t=69: 51A81CBBFD3F7751  DAF7189BF71319ED  FC11CC97AE386106  CEEFB640F1F288C3
   34E0F69B5611C0DC  2D2182E71310E6C7  12BF463D7223A309  44463E8C945BCBB5
t=70: A26F13B306B9736B  51A81CBBFD3F7751  DAF7189BF71319ED  FC11CC97AE386106
   3D6AD7280D27EE41  34E0F69B5611C0DC  2D2182E71310E6C7  12BF463D7223A309
t=71: 93D2426FE4F65643  A26F13B306B9736B  51A81CBBFD3F7751  DAF7189BF71319ED
   F0C0DDC582C521E5  3D6AD7280D27EE41  34E0F69B5611C0DC  2D2182E71310E6C7
t=72: AB4641C14C9D350B  93D2426FE4F65643  A26F13B306B9736B  51A81CBBFD3F7751
   88C22A9BFFF9C4D4  F0C0DDC582C521E5  3D6AD7280D27EE41  34E0F69B5611C0DC
t=73: C7643EF265E0846D  AB4641C14C9D350B  93D2426FE4F65643  A26F13B306B9736B
   5D58F038D47F838C  88C22A9BFFF9C4D4  F0C0DDC582C521E5  3D6AD7280D27EE41
t=74: 0666E64633871262  C7643EF265E0846D  AB4641C14C9D350B  93D2426FE4F65643
   01D41045F938489B  5D58F038D47F838C  88C22A9BFFF9C4D4  F0C0DDC582C521E5
t=75: 126BCBCF100F86E6  0666E64633871262  C7643EF265E0846D  AB4641C14C9D350B
   E5DFBAE06B85B880  01D41045F938489B  5D58F038D47F838C  88C22A9BFFF9C4D4
t=76: 4AAA7A17AEA6C466  126BCBCF100F86E6  0666E64633871262  C7643EF265E0846D
   94AE3C3D5BB9D976  E5DFBAE06B85B880  01D41045F938489B  5D58F038D47F838C
t=77: C12F185AC5A8BBF5  4AAA7A17AEA6C466  126BCBCF100F86E6  0666E64633871262
   578FB21004694EF1  94AE3C3D5BB9D976  E5DFBAE06B85B880  01D41045F938489B
t=78: FBD8CA13A30018E9  C12F185AC5A8BBF5  4AAA7A17AEA6C466  126BCBCF100F86E6
   61A99523C8A086DB  578FB21004694EF1  94AE3C3D5BB9D976  E5DFBAE06B85B880
t=79: 30D36C91856827CD  FBD8CA13A30018E9  C12F185AC5A8BBF5  4AAA7A17AEA6C466
   780D55B8DD49F3A4  61A99523C8A086DB  578FB21004694EF1  94AE3C3D5BB9D976
```

The output is

Y_0 = 22312194FC2BF72C ⊎ 30D36C91856827CD = 53048E2681941EF9
Y_1 = 9F555FA3C84C64C2 ⊎ FBD8CA13A30018E9 = 9B2E29B76B4C7DAB
Y_2 = 2393B86B6F53B151 ⊎ C12F185AC5A8BBF5 = E4C2D0C634FC6D46
Y_3 = 963877195940EABD ⊎ 4AAA7A17AEA6C466 = E0E2F13107E7AF23
Y_4 = 96283EE2A88EFFE3 ⊎ 780D55B8DD49F3A4 = 0E35949B85D8F387
Y_5 = BE5E1E2553863992 ⊎ 61A99523C8A086DB = 2007B3491C26C06D
Y_6 = 2B0199FC2C85B8AA ⊎ 578FB21004694EF1 = 82914C0C30EF079B
Y_7 = 0EB72DDC81C52CA2 ⊎ 94AE3C3D5BB9D976 = A3656A19DD7F0618

The message digest is

53048E26 81941EF9 9B2E29B7 6B4C7DAB E4C2D0C6 34FC6D46 E0E2F131 07E7AF23

B.12.2Example 2

In this example, the input message is

"abcdefghbcdefghicdefghijdefghijkefghijklfghijklmghijklmnhijklmnoijklmnopjklmnopqklmnopqrl
mnopqrsmnopqrstnopqrstu".

The padded message consists of two blocks.

The first block input (1 024 bits) is

Z[0] = 6162636465666768
Z[1] = 6263646566676869
Z[2] = 636465666768696A
Z[3] = 6465666768696A6B
Z[4] = 65666768696A6B6C
Z[5] = 666768696A6B6C6D
Z[6] = 6768696A6B6C6D6E
Z[7] = 68696A6B6C6D6E6F
Z[8] = 696A6B6C6D6E6F70
Z[9] = 6A6B6C6D6E6F7071
Z[10] = 6B6C6D6E6F707172
Z[11] = 6C6D6E6F70717273
Z[12] = 6D6E6F7071727374
Z[13] = 6E6F707172737475
Z[14] = 8000000000000000
Z[15] = 0000000000000000

The following are (hexadecimal representations of) the successive values of the variables X_0, X_1, X_2, X_3, X_4, X_5, X_6 and X_7 in each round when the first block is processed.

t= 0: 9A2F6CF628FAC066 22312194FC2BF72C 9F555FA3C84C64C2 2393B86B6F53B151
3908D1842215827A 96283EE2A88EFFE3 BE5E1E2553863992 2B0199FC2C85B8AA
t= 1: C45A73DC29847669 9A2F6CF628FAC066 22312194FC2BF72C 9F555FA3C84C64C2
63F57A9FE723F8CE 3908D1842215827A 96283EE2A88EFFE3 BE5E1E2553863992
t= 2: 8C3630D3B59711CE C45A73DC29847669 9A2F6CF628FAC066 22312194FC2BF72C
7EDABAB86DFF6A52 63F57A9FE723F8CE 3908D1842215827A 96283EE2A88EFFE3
t= 3: 17BDFF848E242E2F 8C3630D3B59711CE C45A73DC29847669 9A2F6CF628FAC066
9A30B98A6342E77F 7EDABAB86DFF6A52 63F57A9FE723F8CE 3908D1842215827A
t= 4: 81C23A1F69565E3C 17BDFF848E242E2F 8C3630D3B59711CE C45A73DC29847669
CEDB921A04ACEBDD 9A30B98A6342E77F 7EDABAB86DFF6A52 63F57A9FE723F8CE
t= 5: 6E79DFE5A559E037 81C23A1F69565E3C 17BDFF848E242E2F 8C3630D3B59711CE
3B3B402EDC778D6D CEDB921A04ACEBDD 9A30B98A6342E77F 7EDABAB86DFF6A52
t= 6: C39CC278160B5678 6E79DFE5A559E037 81C23A1F69565E3C 17BDFF848E242E2F
50562B0ACB6E7FEB 3B3B402EDC778D6D CEDB921A04ACEBDD 9A30B98A6342E77F
t= 7: 8A78B495684D9DD1 C39CC278160B5678 6E79DFE5A559E037 81C23A1F69565E3C
494234DDD86A4729 50562B0ACB6E7FEB 3B3B402EDC778D6D CEDB921A04ACEBDD
t= 8: 24DF431236CE4D30 8A78B495684D9DD1 C39CC278160B5678 6E79DFE5A559E037
E80E84E515D941E1 494234DDD86A4729 50562B0ACB6E7FEB 3B3B402EDC778D6D

```
t= 9: 7E090CEB07F8BEE9  24DF431236CE4D30  8A78B495684D9DD1  C39CC278160B5678
   A46B4DEC5278E24F  E80E84E515D941E1  494234DDD86A4729  50562B0ACB6E7FEB
t=10: A755CCD779F18FA9  7E090CEB07F8BEE9  24DF431236CE4D30  8A78B495684D9DD1
   D41F5A6BFB41A89D  A46B4DEC5278E24F  E80E84E515D941E1  494234DDD86A4729
t=11: CA6A3AEEEF5311EA  A755CCD779F18FA9  7E090CEB07F8BEE9  24DF431236CE4D30
   3EEE2841CFE10A37  D41F5A6BFB41A89D  A46B4DEC5278E24F  E80E84E515D941E1
t=12: 2885EE23B748F692  CA6A3AEEEF5311EA  A755CCD779F18FA9  7E090CEB07F8BEE9
   CBE0A750BC77AFB9  3EEE2841CFE10A37  D41F5A6BFB41A89D  A46B4DEC5278E24F
t=13: 388A03C85D575053  2885EE23B748F692  CA6A3AEEEF5311EA  A755CCD779F18FA9
   2E195C603FCFE523  CBE0A750BC77AFB9  3EEE2841CFE10A37  D41F5A6BFB41A89D
t=14: E3E1C3D9B4C75FAB  388A03C85D575053  2885EE23B748F692  CA6A3AEEEF5311EA
   1012E63E4E71F612  2E195C603FCFE523  CBE0A750BC77AFB9  3EEE2841CFE10A37
t=15: 4215C380CC7BA71B  E3E1C3D9B4C75FAB  388A03C85D575053  2885EE23B748F692
   51D096BA7563D388  1012E63E4E71F612  2E195C603FCFE523  CBE0A750BC77AFB9
t=16: D4B2ECE1F9EA4139  4215C380CC7BA71B  E3E1C3D9B4C75FAB  388A03C85D575053
   A57AA8000D7E7D45  51D096BA7563D388  1012E63E4E71F612  2E195C603FCFE523
t=17: A83038B321E1282C  D4B2ECE1F9EA4139  4215C380CC7BA71B  E3E1C3D9B4C75FAB
   FADB216834A22046  A57AA8000D7E7D45  51D096BA7563D388  1012E63E4E71F612
t=18: 871C3F72FFF75168  A83038B321E1282C  D4B2ECE1F9EA4139  4215C380CC7BA71B
   FAA41018DA73AA6B  FADB216834A22046  A57AA8000D7E7D45  51D096BA7563D388
t=19: 09CDADF5B09E542C  871C3F72FFF75168  A83038B321E1282C  D4B2ECE1F9EA4139
   223C0812022BF992  FAA41018DA73AA6B  FADB216834A22046  A57AA8000D7E7D45
t=20: A70D03F8958F9BA4  09CDADF5B09E542C  871C3F72FFF75168  A83038B321E1282C
   63FFC78316C85D34  223C0812022BF992  FAA41018DA73AA6B  FADB216834A22046
t=21: EC07BC6D3DE528B1  A70D03F8958F9BA4  09CDADF5B09E542C  871C3F72FFF75168
   8079819B99C99A41  63FFC78316C85D34  223C0812022BF992  FAA41018DA73AA6B
t=22: 8F21796FE4B51BD0  EC07BC6D3DE528B1  A70D03F8958F9BA4  09CDADF5B09E542C
   1DDFFF81567B2DE4  8079819B99C99A41  63FFC78316C85D34  223C0812022BF992
t=23: 9F6F64FCB4C926E7  8F21796FE4B51BD0  EC07BC6D3DE528B1  A70D03F8958F9BA4
   8C8247B93F00D50C  1DDFFF81567B2DE4  8079819B99C99A41  63FFC78316C85D34
t=24: D03596038CD63118  9F6F64FCB4C926E7  8F21796FE4B51BD0  EC07BC6D3DE528B1
   4F5168008F6D598E  8C8247B93F00D50C  1DDFFF81567B2DE4  8079819B99C99A41
t=25: 338B31422B132F48  D03596038CD63118  9F6F64FCB4C926E7  8F21796FE4B51BD0
   571E4796BD2EB595  4F5168008F6D598E  8C8247B93F00D50C  1DDFFF81567B2DE4
t=26: F13D1863C7906343  338B31422B132F48  D03596038CD63118  9F6F64FCB4C926E7
   2D8F44815B3B89BB  571E4796BD2EB595  4F5168008F6D598E  8C8247B93F00D50C
t=27: 92FCCCA21D8FBF2B  F13D1863C7906343  338B31422B132F48  D03596038CD63118
   F1C21531DA4A08B6  2D8F44815B3B89BB  571E4796BD2EB595  4F5168008F6D598E
t=28: 05F58CDABBF55813  92FCCCA21D8FBF2B  F13D1863C7906343  338B31422B132F48
   06CB086E9CE25950  F1C21531DA4A08B6  2D8F44815B3B89BB  571E4796BD2EB595
t=29: 6EC03563D439AE54  05F58CDABBF55813  92FCCCA21D8FBF2B  F13D1863C7906343
   6B6E9C3EA7891D15  06CB086E9CE25950  F1C21531DA4A08B6  2D8F44815B3B89BB
t=30: 2C5C8402B82F7480  6EC03563D439AE54  05F58CDABBF55813  92FCCCA21D8FBF2B
   A56811F482933EA1  6B6E9C3EA7891D15  06CB086E9CE25950  F1C21531DA4A08B6
t=31: 1A0CC3AD581C10FE  2C5C8402B82F7480  6EC03563D439AE54  05F58CDABBF55813
   56A84040EEE67BF6  A56811F482933EA1  6B6E9C3EA7891D15  06CB086E9CE25950
t=32: A5F2FAA00D8A8747  1A0CC3AD581C10FE  2C5C8402B82F7480  6EC03563D439AE54
   F025CE5716C796CD  56A84040EEE67BF6  A56811F482933EA1  6B6E9C3EA7891D15
t=33: AFB7E1D8C7F831C4  A5F2FAA00D8A8747  1A0CC3AD581C10FE  2C5C8402B82F7480
   564993F74B0AD9F5  F025CE5716C796CD  56A84040EEE67BF6  A56811F482933EA1
t=34: ABF4003C5B5F7017  AFB7E1D8C7F831C4  A5F2FAA00D8A8747  1A0CC3AD581C10FE
   28A6C03E6C2A4898  564993F74B0AD9F5  F025CE5716C796CD  56A84040EEE67BF6
t=35: 4F2CB708B47DCE20  ABF4003C5B5F7017  AFB7E1D8C7F831C4  A5F2FAA00D8A8747
   DDAC365E41D4C20D  28A6C03E6C2A4898  564993F74B0AD9F5  F025CE5716C796CD
t=36: EBA175A8080AA725  4F2CB708B47DCE20  ABF4003C5B5F7017  AFB7E1D8C7F831C4
   6634651E9C79BA41  DDAC365E41D4C20D  28A6C03E6C2A4898  564993F74B0AD9F5
t=37: 27DD63A534C4822E  EBA175A8080AA725  4F2CB708B47DCE20  ABF4003C5B5F7017
   1938417C593488CC  6634651E9C79BA41  DDAC365E41D4C20D  28A6C03E6C2A4898
t=38: DC7BFE1851A2E81B  27DD63A534C4822E  EBA175A8080AA725  4F2CB708B47DCE20
   CDB1FB3ED046F991  1938417C593488CC  6634651E9C79BA41  DDAC365E41D4C20D
t=39: 6D07C2C7A947167B  DC7BFE1851A2E81B  27DD63A534C4822E  EBA175A8080AA725
   8D5583BD4628586D  CDB1FB3ED046F991  1938417C593488CC  6634651E9C79BA41
t=40: 8CC57E961CE1F956  6D07C2C7A947167B  DC7BFE1851A2E81B  27DD63A534C4822E
```

```
   1994E5B3F53E4AF2  8D5583BD4628586D  CDB1FB3ED046F991  1938417C593488CC
t=41: 8C6947F81E1FD94A  8CC57E961CE1F956  6D07C2C7A947167B  DC7BFE1851A2E81B
   82E08437768126E4  1994E5B3F53E4AF2  8D5583BD4628586D  CDB1FB3ED046F991
t=42: DDB8B34228A61CD0  8C6947F81E1FD94A  8CC57E961CE1F956  6D07C2C7A947167B
   17A90D3B6D6A2EA1  82E08437768126E4  1994E5B3F53E4AF2  8D5583BD4628586D
t=43: 03BDE346FD50DCCD  DDB8B34228A61CD0  8C6947F81E1FD94A  8CC57E961CE1F956
   5FC3283C3C91B062  17A90D3B6D6A2EA1  82E08437768126E4  1994E5B3F53E4AF2
t=44: 80545AD9644D1756  03BDE346FD50DCCD  DDB8B34228A61CD0  8C6947F81E1FD94A
   97BC9BD263E1FC6C  5FC3283C3C91B062  17A90D3B6D6A2EA1  82E08437768126E4
t=45: EFD4BD2F26343181  80545AD9644D1756  03BDE346FD50DCCD  DDB8B34228A61CD0
   4B766751CFBFDA62  97BC9BD263E1FC6C  5FC3283C3C91B062  17A90D3B6D6A2EA1
t=46: 64624F7253A389BE  EFD4BD2F26343181  80545AD9644D1756  03BDE346FD50DCCD
   C9C38B4792943C06  4B766751CFBFDA62  97BC9BD263E1FC6C  5FC3283C3C91B062
t=47: 3E8CF0C51B035FE0  64624F7253A389BE  EFD4BD2F26343181  80545AD9644D1756
   137F35F60E3A8AB0  C9C38B4792943C06  4B766751CFBFDA62  97BC9BD263E1FC6C
t=48: C91687936637EB79  3E8CF0C51B035FE0  64624F7253A389BE  EFD4BD2F26343181
   5DE2B5C19050BFAE  137F35F60E3A8AB0  C9C38B4792943C06  4B766751CFBFDA62
t=49: 4A994A1444767A2C  C91687936637EB79  3E8CF0C51B035FE0  64624F7253A389BE
   32281CDC06C6E9D8  5DE2B5C19050BFAE  137F35F60E3A8AB0  C9C38B4792943C06
t=50: 7953E11357EBE4CF  4A994A1444767A2C  C91687936637EB79  3E8CF0C51B035FE0
   14269D3481B031D0  32281CDC06C6E9D8  5DE2B5C19050BFAE  137F35F60E3A8AB0
t=51: 4F16072F816AA7A1  7953E11357EBE4CF  4A994A1444767A2C  C91687936637EB79
   B6A3D2D3805DCE61  14269D3481B031D0  32281CDC06C6E9D8  5DE2B5C19050BFAE
t=52: A801F1AAC9415393  4F16072F816AA7A1  7953E11357EBE4CF  4A994A1444767A2C
   7C132F7309D27922  B6A3D2D3805DCE61  14269D3481B031D0  32281CDC06C6E9D8
t=53: A223D983EBA809A8  A801F1AAC9415393  4F16072F816AA7A1  7953E11357EBE4CF
   0FD152F32163372C  7C132F7309D27922  B6A3D2D3805DCE61  14269D3481B031D0
t=54: 080BBDDE727385E5  A223D983EBA809A8  A801F1AAC9415393  4F16072F816AA7A1
   8F9E0452A5063D26  0FD152F32163372C  7C132F7309D27922  B6A3D2D3805DCE61
t=55: 03A460537E8B4F1E  080BBDDE727385E5  A223D983EBA809A8  A801F1AAC9415393
   A37615D60BEBCF33  8F9E0452A5063D26  0FD152F32163372C  7C132F7309D27922
t=56: 1BB7A154850F075F  03A460537E8B4F1E  080BBDDE727385E5  A223D983EBA809A8
   2FAA64724CFCF763  A37615D60BEBCF33  8F9E0452A5063D26  0FD152F32163372C
t=57: AB80BABC87BB7A16  1BB7A154850F075F  03A460537E8B4F1E  080BBDDE727385E5
   694348C139B7EA00  2FAA64724CFCF763  A37615D60BEBCF33  8F9E0452A5063D26
t=58: 8C0E0DB97B2D9C9F  AB80BABC87BB7A16  1BB7A154850F075F  03A460537E8B4F1E
   651F222826594F54  694348C139B7EA00  2FAA64724CFCF763  A37615D60BEBCF33
t=59: 3A4EAE7FE4699540  8C0E0DB97B2D9C9F  AB80BABC87BB7A16  1BB7A154850F075F
   13876F30BECA815D  651F222826594F54  694348C139B7EA00  2FAA64724CFCF763
t=60: BB7C0F789EA3699C  3A4EAE7FE4699540  8C0E0DB97B2D9C9F  AB80BABC87BB7A16
   ECD91F96127B03A8  13876F30BECA815D  651F222826594F54  694348C139B7EA00
t=61: FE629FDEE04ED549  BB7C0F789EA3699C  3A4EAE7FE4699540  8C0E0DB97B2D9C9F
   B2F245A1C977A57A  ECD91F96127B03A8  13876F30BECA815D  651F222826594F54
t=62: A419197F10A2F082  FE629FDEE04ED549  BB7C0F789EA3699C  3A4EAE7FE4699540
   747A1B529D1718B3  B2F245A1C977A57A  ECD91F96127B03A8  13876F30BECA815D
t=63: 12D940B29B43FCAC  A419197F10A2F082  FE629FDEE04ED549  BB7C0F789EA3699C
   5E88DDC8012ABCC8  747A1B529D1718B3  B2F245A1C977A57A  ECD91F96127B03A8
t=64: 60F835EA7AE7A3B1  12D940B29B43FCAC  A419197F10A2F082  FE629FDEE04ED549
   EE41795118402F41  5E88DDC8012ABCC8  747A1B529D1718B3  B2F245A1C977A57A
t=65: 5448E39ABC8584E0  60F835EA7AE7A3B1  12D940B29B43FCAC  A419197F10A2F082
   4D9C54C24C73C5D3  EE41795118402F41  5E88DDC8012ABCC8  747A1B529D1718B3
t=66: 3FF824D6D11EDF6C  5448E39ABC8584E0  60F835EA7AE7A3B1  12D940B29B43FCAC
   4138B86695C59AC4  4D9C54C24C73C5D3  EE41795118402F41  5E88DDC8012ABCC8
t=67: 6E96137693191EDF  3FF824D6D11EDF6C  5448E39ABC8584E0  60F835EA7AE7A3B1
   046EB1A80DD1DF9A  4138B86695C59AC4  4D9C54C24C73C5D3  EE41795118402F41
t=68: EC2D31E61214BDF6  6E96137693191EDF  3FF824D6D11EDF6C  5448E39ABC8584E0
   55DBAB7D6FC52329  046EB1A80DD1DF9A  4138B86695C59AC4  4D9C54C24C73C5D3
t=69: 7E0F0C8461660735  EC2D31E61214BDF6  6E96137693191EDF  3FF824D6D11EDF6C
   F9B0E4BFF6CEE39C  55DBAB7D6FC52329  046EB1A80DD1DF9A  4138B86695C59AC4
t=70: D29A895ED31B66BB  7E0F0C8461660735  EC2D31E61214BDF6  6E96137693191EDF
   9D885DBABB9710B2  F9B0E4BFF6CEE39C  55DBAB7D6FC52329  046EB1A80DD1DF9A
t=71: AE123510491AC45C  D29A895ED31B66BB  7E0F0C8461660735  EC2D31E61214BDF6
   E5C2B9E1DE72B8DC  9D885DBABB9710B2  F9B0E4BFF6CEE39C  55DBAB7D6FC52329
```

```
t=72: AABC342629053FFB  AE123510491AC45C  D29A895ED31B66BB  7E0F0C8461660735
   F55697A28603BF8A  E5C2B9E1DE72B8DC  9D885DBABB9710B2  F9B0E4BFF6CEE39C
t=73: 0573072E1BF3F98C  AABC342629053FFB  AE123510491AC45C  D29A895ED31B66BB
   82A724607E0562C3  F55697A28603BF8A  E5C2B9E1DE72B8DC  9D885DBABB9710B2
t=74: 54404FE2C42230FE  0573072E1BF3F98C  AABC342629053FFB  AE123510491AC45C
   12B422CB3FC344B9  82A724607E0562C3  F55697A28603BF8A  E5C2B9E1DE72B8DC
t=75: 71ADA568EFBA8B62  54404FE2C42230FE  0573072E1BF3F98C  AABC342629053FFB
   E4AC0B9801F5A875  12B422CB3FC344B9  82A724607E0562C3  F55697A28603BF8A
t=76: FF078089585319D0  71ADA568EFBA8B62  54404FE2C42230FE  0573072E1BF3F98C
   42C94B5B6F533B3F  E4AC0B9801F5A875  12B422CB3FC344B9  82A724607E0562C3
t=77: C555881BC0EDEBCD  FF078089585319D0  71ADA568EFBA8B62  54404FE2C42230FE
   942D0C18A267E3B1  42C94B5B6F533B3F  E4AC0B9801F5A875  12B422CB3FC344B9
t=78: 2C666488FF634DC6  C555881BC0EDEBCD  FF078089585319D0  71ADA568EFBA8B62
   C23D16693B02AA5A  942D0C18A267E3B1  42C94B5B6F533B3F  E4AC0B9801F5A875
t=79: 6BA87D1B8505285F  2C666488FF634DC6  C555881BC0EDEBCD  FF078089585319D0
   17FBD871DB354C99  C23D16693B02AA5A  942D0C18A267E3B1  42C94B5B6F533B3F
```

The output after processing the first block is

Y_0 = 22312194FC2BF72C ⊎ 6BA87D1B8505285F = 8DD99EB081311F8B
Y_1 = 9F555FA3C84C64C2 ⊎ 2C666488FF634DC6 = CBBBC42CC7AFB288
Y_2 = 2393B86B6F53B151 ⊎ C555881BC0EDEBCD = E8E9408730419D1E
Y_3 = 963877195940EABD ⊎ FF078089585319D0 = 953FF7A2B194048D
Y_4 = 96283EE2A88EFFE3 ⊎ 17FBD871DB354C99 = AE24175483C44C7C
Y_5 = BE5E1E2553863992 ⊎ C23D16693B02AA5A = 809B348E8E88E3EC
Y_6 = 2B0199FC2C85B8AA ⊎ 942D0C18A267E3B1 = BF2EA614CEED9C5B
Y_7 = 0EB72DDC81C52CA2 ⊎ 42C94B5B6F533B3F = 51807937F11867E1

The second block input (1 024 bits) is

```
Z[ 0] = 0000000000000000
Z[ 1] = 0000000000000000
Z[ 2] = 0000000000000000
Z[ 3] = 0000000000000000
Z[ 4] = 0000000000000000
Z[ 5] = 0000000000000000
Z[ 6] = 0000000000000000
Z[ 7] = 0000000000000000
Z[ 8] = 0000000000000000
Z[ 9] = 0000000000000000
Z[10] = 0000000000000000
Z[11] = 0000000000000000
Z[12] = 0000000000000000
Z[13] = 0000000000000000
Z[14] = 0000000000000000
Z[15] = 0000000000000380
```

The following are (hexadecimal representations of) the successive values of the variables X_0, X_1, X_2, X_3, X_4, X_5, X_6 and X_7 in each round when the second block is processed.

```
t= 0: CA1B701EA8D10380  8DD99EB081311F8B  CBBBC42CC7AFB288  E8E9408730419D1E
   4301C5B7AF4F28EA  AE24175483C44C7C  809B348E8E88E3EC  BF2EA614CEED9C5B
t= 1: 4B560A3D9D8BA236  CA1B701EA8D10380  8DD99EB081311F8B  CBBBC42CC7AFB288
   4E2D9B9CB97640BF  4301C5B7AF4F28EA  AE24175483C44C7C  809B348E8E88E3EC
t= 2: 052AFD3A52839A12  4B560A3D9D8BA236  CA1B701EA8D10380  8DD99EB081311F8B
   40A7CA7D457EBBD6  4E2D9B9CB97640BF  4301C5B7AF4F28EA  AE24175483C44C7C
t= 3: 6D6469537181FB59  052AFD3A52839A12  4B560A3D9D8BA236  CA1B701EA8D10380
   E7E74F3462405FC1  40A7CA7D457EBBD6  4E2D9B9CB97640BF  4301C5B7AF4F28EA
t= 4: 67D25B0D1D465E19  6D6469537181FB59  052AFD3A52839A12  4B560A3D9D8BA236
   81EA993A34CE5FD6  E7E74F3462405FC1  40A7CA7D457EBBD6  4E2D9B9CB97640BF
t= 5: CE2D2DCA6276189B  67D25B0D1D465E19  6D6469537181FB59  052AFD3A52839A12
   2B11C440985F5E14  81EA993A34CE5FD6  E7E74F3462405FC1  40A7CA7D457EBBD6
t= 6: C304AE7968FA6276  CE2D2DCA6276189B  67D25B0D1D465E19  6D6469537181FB59
```

```
   2D925EBD2371D4E0  2B11C440985F5E14  81EA993A34CE5FD6  E7E74F3462405FC1
t= 7: A2F2F352C45E6B92  C304AE7968FA6276  CE2D2DCA6276189B  67D25B0D1D465E19
   2209E227605C477C  2D925EBD2371D4E0  2B11C440985F5E14  81EA993A34CE5FD6
t= 8: B6408732E17EF2BF  A2F2F352C45E6B92  C304AE7968FA6276  CE2D2DCA6276189B
   0A7493CBFB707A28  2209E227605C477C  2D925EBD2371D4E0  2B11C440985F5E14
t= 9: E5A29310956CF4B0  B6408732E17EF2BF  A2F2F352C45E6B92  C304AE7968FA6276
   471CAEB6206FD6A9  0A7493CBFB707A28  2209E227605C477C  2D925EBD2371D4E0
t=10: 619A643B60A72678  E5A29310956CF4B0  B6408732E17EF2BF  A2F2F352C45E6B92
   2AFDCFD70197C551  471CAEB6206FD6A9  0A7493CBFB707A28  2209E227605C477C
t=11: 12E090BCE773988C  619A643B60A72678  E5A29310956CF4B0  B6408732E17EF2BF
   2BB61C87D95F1EF6  2AFDCFD70197C551  471CAEB6206FD6A9  0A7493CBFB707A28
t=12: 844745BEB54BB38D  12E090BCE773988C  619A643B60A72678  E5A29310956CF4B0
   A1B9B2E57ECE02D4  2BB61C87D95F1EF6  2AFDCFD70197C551  471CAEB6206FD6A9
t=13: 728E0FF0A633641C  844745BEB54BB38D  12E090BCE773988C  619A643B60A72678
   D2EB1AE617CFA231  A1B9B2E57ECE02D4  2BB61C87D95F1EF6  2AFDCFD70197C551
t=14: 4294C9F0701FB711  728E0FF0A633641C  844745BEB54BB38D  12E090BCE773988C
   E5722A671CACCC14  D2EB1AE617CFA231  A1B9B2E57ECE02D4  2BB61C87D95F1EF6
t=15: 1EB995845896146C  4294C9F0701FB711  728E0FF0A633641C  844745BEB54BB38D
   F1F73492308170F3  E5722A671CACCC14  D2EB1AE617CFA231  A1B9B2E57ECE02D4
t=16: 2B4D4009404447A0  1EB995845896146C  4294C9F0701FB711  728E0FF0A633641C
   C50207E5516E7902  F1F73492308170F3  E5722A671CACCC14  D2EB1AE617CFA231
t=17: 7EE24648DA164A4F  2B4D4009404447A0  1EB995845896146C  4294C9F0701FB711
   9FFCB15331E1CD35  C50207E5516E7902  F1F73492308170F3  E5722A671CACCC14
t=18: 0D7915D334E98931  7EE24648DA164A4F  2B4D4009404447A0  1EB995845896146C
   0ACF80CA9D91C843  9FFCB15331E1CD35  C50207E5516E7902  F1F73492308170F3
t=19: 7156E5D603D6D2C9  0D7915D334E98931  7EE24648DA164A4F  2B4D4009404447A0
   3ADC14C21552B1A8  0ACF80CA9D91C843  9FFCB15331E1CD35  C50207E5516E7902
t=20: 1DA99E1A512119C7  7156E5D603D6D2C9  0D7915D334E98931  7EE24648DA164A4F
   B9E562D0A2B54D40  3ADC14C21552B1A8  0ACF80CA9D91C843  9FFCB15331E1CD35
t=21: 1FB878880EF4B5E4  1DA99E1A512119C7  7156E5D603D6D2C9  0D7915D334E98931
   CE2590CB43609153  B9E562D0A2B54D40  3ADC14C21552B1A8  0ACF80CA9D91C843
t=22: 3FDC41AC384A3129  1FB878880EF4B5E4  1DA99E1A512119C7  7156E5D603D6D2C9
   32B0C09234E84242  CE2590CB43609153  B9E562D0A2B54D40  3ADC14C21552B1A8
t=23: B836D5F127D2FDB8  3FDC41AC384A3129  1FB878880EF4B5E4  1DA99E1A512119C7
   3714588332FCEC71  32B0C09234E84242  CE2590CB43609153  B9E562D0A2B54D40
t=24: 2EC877975A9F8116  B836D5F127D2FDB8  3FDC41AC384A3129  1FB878880EF4B5E4
   362102EAA0DD5D70  3714588332FCEC71  32B0C09234E84242  CE2590CB43609153
t=25: 565DBE48262353B9  2EC877975A9F8116  B836D5F127D2FDB8  3FDC41AC384A3129
   E54F12F5AED463E6  362102EAA0DD5D70  3714588332FCEC71  32B0C09234E84242
t=26: 40C91B7364704A83  565DBE48262353B9  2EC877975A9F8116  B836D5F127D2FDB8
   4656BB7233467988  E54F12F5AED463E6  362102EAA0DD5D70  3714588332FCEC71
t=27: 53CA178C6B368158  40C91B7364704A83  565DBE48262353B9  2EC877975A9F8116
   4C67542852B3D7A1  4656BB7233467988  E54F12F5AED463E6  362102EAA0DD5D70
t=28: 15D0571DD1178764  53CA178C6B368158  40C91B7364704A83  565DBE48262353B9
   405BD69B2C905BD7  4C67542852B3D7A1  4656BB7233467988  E54F12F5AED463E6
t=29: 264B6149F78D1035  15D0571DD1178764  53CA178C6B368158  40C91B7364704A83
   CC414FDE2C1F1BFA  405BD69B2C905BD7  4C67542852B3D7A1  4656BB7233467988
t=30: 9A33B7A4623C0534  264B6149F78D1035  15D0571DD1178764  53CA178C6B368158
   2C551E8A8C2C7434  CC414FDE2C1F1BFA  405BD69B2C905BD7  4C67542852B3D7A1
t=31: 3CCB61788641971E  9A33B7A4623C0534  264B6149F78D1035  15D0571DD1178764
   06B6D7E811D72282  2C551E8A8C2C7434  CC414FDE2C1F1BFA  405BD69B2C905BD7
t=32: 73152319D664AB4D  3CCB61788641971E  9A33B7A4623C0534  264B6149F78D1035
   961481C44171C469  06B6D7E811D72282  2C551E8A8C2C7434  CC414FDE2C1F1BFA
t=33: A13ED1EBC962EA7E  73152319D664AB4D  3CCB61788641971E  9A33B7A4623C0534
   6CF7B8AA031A207A  961481C44171C469  06B6D7E811D72282  2C551E8A8C2C7434
t=34: 09F847AAB3E15178  A13ED1EBC962EA7E  73152319D664AB4D  3CCB61788641971E
   BF27C53408DBD3E9  6CF7B8AA031A207A  961481C44171C469  06B6D7E811D72282
t=35: 042BD9B3B1A3216D  09F847AAB3E15178  A13ED1EBC962EA7E  73152319D664AB4D
   58307603F69A3141  BF27C53408DBD3E9  6CF7B8AA031A207A  961481C44171C469
t=36: C672CECB0E5C083C  042BD9B3B1A3216D  09F847AAB3E15178  A13ED1EBC962EA7E
   A713876F591E1729  58307603F69A3141  BF27C53408DBD3E9  6CF7B8AA031A207A
t=37: 528D95291F5F694D  C672CECB0E5C083C  042BD9B3B1A3216D  09F847AAB3E15178
   3F065D9605A497B0  A713876F591E1729  58307603F69A3141  BF27C53408DBD3E9
```

```
t=38: D51413BD28942A19  528D95291F5F694D  C672CECB0E5C083C  042BD9B3B1A3216D
   B8C08D67D6372533  3F065D9605A497B0  A713876F591E1729  58307603F69A3141
t=39: D3E65D22ECE41799  D51413BD28942A19  528D95291F5F694D  C672CECB0E5C083C
   48C71BDE787CF9CF  B8C08D67D6372533  3F065D9605A497B0  A713876F591E1729
t=40: 9DC023C14EC9FD06  D3E65D22ECE41799  D51413BD28942A19  528D95291F5F694D
   600D290EB716504D  48C71BDE787CF9CF  B8C08D67D6372533  3F065D9605A497B0
t=41: E201AB4097D56AD9  9DC023C14EC9FD06  D3E65D22ECE41799  D51413BD28942A19
   211AEFF5D426E06A  600D290EB716504D  48C71BDE787CF9CF  B8C08D67D6372533
t=42: D6E25625A771084A  E201AB4097D56AD9  9DC023C14EC9FD06  D3E65D22ECE41799
   FEA9E0A415E0D53B  211AEFF5D426E06A  600D290EB716504D  48C71BDE787CF9CF
t=43: BFEA46AB9859BFA1  D6E25625A771084A  E201AB4097D56AD9  9DC023C14EC9FD06
   678E5BDDAF3C3B71  FEA9E0A415E0D53B  211AEFF5D426E06A  600D290EB716504D
t=44: A16A621A085D68D6  BFEA46AB9859BFA1  D6E25625A771084A  E201AB4097D56AD9
   138B192CEDB50B75  678E5BDDAF3C3B71  FEA9E0A415E0D53B  211AEFF5D426E06A
t=45: 3476332E792C1C4B  A16A621A085D68D6  BFEA46AB9859BFA1  D6E25625A771084A
   2ABC2AB574E9F080  138B192CEDB50B75  678E5BDDAF3C3B71  FEA9E0A415E0D53B
t=46: 24F0545BB7DB3F19  3476332E792C1C4B  A16A621A085D68D6  BFEA46AB9859BFA1
   F5EFACBE2AD8B856  2ABC2AB574E9F080  138B192CEDB50B75  678E5BDDAF3C3B71
t=47: 06959C13A1020AF8  24F0545BB7DB3F19  3476332E792C1C4B  A16A621A085D68D6
   7AE2E87ACB8DDE39  F5EFACBE2AD8B856  2ABC2AB574E9F080  138B192CEDB50B75
t=48: FA114006862CF5D3  06959C13A1020AF8  24F0545BB7DB3F19  3476332E792C1C4B
   976564D9448EB34A  7AE2E87ACB8DDE39  F5EFACBE2AD8B856  2ABC2AB574E9F080
t=49: 67B5638DBE2A3651  FA114006862CF5D3  06959C13A1020AF8  24F0545BB7DB3F19
   A752090797E79FDA  976564D9448EB34A  7AE2E87ACB8DDE39  F5EFACBE2AD8B856
t=50: 884BDAE0CE147578  67B5638DBE2A3651  FA114006862CF5D3  06959C13A1020AF8
   B05132465F5172C1  A752090797E79FDA  976564D9448EB34A  7AE2E87ACB8DDE39
t=51: 4EF7B5C89BCBC776  884BDAE0CE147578  67B5638DBE2A3651  FA114006862CF5D3
   581DAD1B56E18E1C  B05132465F5172C1  A752090797E79FDA  976564D9448EB34A
t=52: 820AD2EC649E6DCC  4EF7B5C89BCBC776  884BDAE0CE147578  67B5638DBE2A3651
   21AB0DF2BC658D9F  581DAD1B56E18E1C  B05132465F5172C1  A752090797E79FDA
t=53: 0563C5F2919ED596  820AD2EC649E6DCC  4EF7B5C89BCBC776  884BDAE0CE147578
   5AC4DB36E7FF1693  21AB0DF2BC658D9F  581DAD1B56E18E1C  B05132465F5172C1
t=54: CEBA54F000A09D5D  0563C5F2919ED596  820AD2EC649E6DCC  4EF7B5C89BCBC776
   F7F8883941A7E321  5AC4DB36E7FF1693  21AB0DF2BC658D9F  581DAD1B56E18E1C
t=55: 40DEC62C74F632D5  CEBA54F000A09D5D  0563C5F2919ED596  820AD2EC649E6DCC
   1F8AF353EC8C6DDA  F7F8883941A7E321  5AC4DB36E7FF1693  21AB0DF2BC658D9F
t=56: 5F961EDFCB27CA82  40DEC62C74F632D5  CEBA54F000A09D5D  0563C5F2919ED596
   91EEDF5727B533B9  1F8AF353EC8C6DDA  F7F8883941A7E321  5AC4DB36E7FF1693
t=57: 0F6AA0004EB91943  5F961EDFCB27CA82  40DEC62C74F632D5  CEBA54F000A09D5D
   C70CF9E635760D8E  91EEDF5727B533B9  1F8AF353EC8C6DDA  F7F8883941A7E321
t=58: 547E34C8E16C8208  0F6AA0004EB91943  5F961EDFCB27CA82  40DEC62C74F632D5
   DAB76359DFE7875E  C70CF9E635760D8E  91EEDF5727B533B9  1F8AF353EC8C6DDA
t=59: 9AFF38B3BC64077D  547E34C8E16C8208  0F6AA0004EB91943  5F961EDFCB27CA82
   BD0DF11423D8727B  DAB76359DFE7875E  C70CF9E635760D8E  91EEDF5727B533B9
t=60: C1BB5920B7C5B67E  9AFF38B3BC64077D  547E34C8E16C8208  0F6AA0004EB91943
   B4B189776407C251  BD0DF11423D8727B  DAB76359DFE7875E  C70CF9E635760D8E
t=61: 035C20D721BA914D  C1BB5920B7C5B67E  9AFF38B3BC64077D  547E34C8E16C8208
   3102071764B6F123  B4B189776407C251  BD0DF11423D8727B  DAB76359DFE7875E
t=62: C32B2ED80EAB3663  035C20D721BA914D  C1BB5920B7C5B67E  9AFF38B3BC64077D
   1625654B4B1F63E8  3102071764B6F123  B4B189776407C251  BD0DF11423D8727B
t=63: 7E2893CE82EE6DDC  C32B2ED80EAB3663  035C20D721BA914D  C1BB5920B7C5B67E
   FCE7A5EA11A84E7F  1625654B4B1F63E8  3102071764B6F123  B4B189776407C251
t=64: C5C6741A461B5C08  7E2893CE82EE6DDC  C32B2ED80EAB3663  035C20D721BA914D
   31010FF1B53793FD  FCE7A5EA11A84E7F  1625654B4B1F63E8  3102071764B6F123
t=65: 250F7D7FC30C144F  C5C6741A461B5C08  7E2893CE82EE6DDC  C32B2ED80EAB3663
   9C824646617DD90A  31010FF1B53793FD  FCE7A5EA11A84E7F  1625654B4B1F63E8
t=66: 2985CBF9ADA94FEF  250F7D7FC30C144F  C5C6741A461B5C08  7E2893CE82EE6DDC
   481E2BA9F24813AD  9C824646617DD90A  31010FF1B53793FD  FCE7A5EA11A84E7F
t=67: 7C3F7808EDDC4373  2985CBF9ADA94FEF  250F7D7FC30C144F  C5C6741A461B5C08
   923A8EC51D528E0D  481E2BA9F24813AD  9C824646617DD90A  31010FF1B53793FD
t=68: FC443DF03A273D02  7C3F7808EDDC4373  2985CBF9ADA94FEF  250F7D7FC30C144F
   9D92992298B6311F  923A8EC51D528E0D  481E2BA9F24813AD  9C824646617DD90A
t=69: C1265539D2F29608  FC443DF03A273D02  7C3F7808EDDC4373  2985CBF9ADA94FEF
```

```
   1DA207AB69A702F0  9D92992298B6311F  923A8EC51D528E0D  481E2BA9F24813AD
t=70: EFC50BC63BDB23A5  C1265539D2F29608  FC443DF03A273D02  7C3F7808EDDC4373
   F4F43A64BADFD219  1DA207AB69A702F0  9D92992298B6311F  923A8EC51D528E0D
t=71: D2BEF501241BE22C  EFC50BC63BDB23A5  C1265539D2F29608  FC443DF03A273D02
   A2870A290A867A1A  F4F43A64BADFD219  1DA207AB69A702F0  9D92992298B6311F
t=72: CA73C49DE77C7AC8  D2BEF501241BE22C  EFC50BC63BDB23A5  C1265539D2F29608
   F820C00AA7E284E6  A2870A290A867A1A  F4F43A64BADFD219  1DA207AB69A702F0
t=73: 558A01B12EC35028  CA73C49DE77C7AC8  D2BEF501241BE22C  EFC50BC63BDB23A5
   15E2469AD6262414  F820C00AA7E284E6  A2870A290A867A1A  F4F43A64BADFD219
t=74: 370DAFCBF2D25DA8  558A01B12EC35028  CA73C49DE77C7AC8  D2BEF501241BE22C
   8E3FA5D1EAE87FA8  15E2469AD6262414  F820C00AA7E284E6  A2870A290A867A1A
t=75: B6FDAC1E04495875  370DAFCBF2D25DA8  558A01B12EC35028  CA73C49DE77C7AC8
   EC3C3233141B55E7  8E3FA5D1EAE87FA8  15E2469AD6262414  F820C00AA7E284E6
t=76: DAAAD0BF300751AD  B6FDAC1E04495875  370DAFCBF2D25DA8  558A01B12EC35028
   7401A3CB07B8228E  EC3C3233141B55E7  8E3FA5D1EAE87FA8  15E2469AD6262414
t=77: 7CE25CB7C7FD48F6  DAAAD0BF300751AD  B6FDAC1E04495875  370DAFCBF2D25DA8
   69A9F1B43ECA54F4  7401A3CB07B8228E  EC3C3233141B55E7  8E3FA5D1EAE87FA8
t=78: 751E755B4A6D7F36  7CE25CB7C7FD48F6  DAAAD0BF300751AD  B6FDAC1E04495875
   CB9D209C7B0DEB01  69A9F1B43ECA54F4  7401A3CB07B8228E  EC3C3233141B55E7
t=79: AB4F42D47A55716D  751E755B4A6D7F36  7CE25CB7C7FD48F6  DAAAD0BF300751AD
   22CA23DE9BE67C24  CB9D209C7B0DEB01  69A9F1B43ECA54F4  7401A3CB07B8228E
```

The output after processing the second block is

Y_0 = 8DD99EB081311F8B ⊎ AB4F42D47A55716D = 3928E184FB8690F8
Y_1 = CBBBC42CC7AFB288 ⊎ 751E755B4A6D7F36 = 40DA3988121D31BE
Y_2 = E8E9408730419D1E ⊎ 7CE25CB7C7FD48F6 = 65CB9D3EF83EE614
Y_3 = 953FF7A2B194048D ⊎ DAAAD0BF300751AD = 6FEAC861E19B563A
Y_4 = AE24175483C44C7C ⊎ 22CA23DE9BE67C24 = D0EE3B331FAAC8A0
Y_5 = 809B348E8E88E3EC ⊎ CB9D209C7B0DEB01 = 4C38552B0996CEED
Y_6 = BF2EA614CEED9C5B ⊎ 69A9F1B43ECA54F4 = 28D897C90DB7F14F
Y_7 = 51807937F11867E1 ⊎ 7401A3CB07B8228E = C5821D02F8D08A6F

The message digest is

3928E184 FB8690F8 40DA3988 121D31BE 65CB9D3E F83EE614 6FEAC861 E19B563A.

B.13 Dedicated Hash-Function 11 (STREEBOG-512)

B.13.1 General

The binary words are expressed in hexadecimal notation. The $4n$-bit word is given in the form a_{n-1}, …, a_0, where $a_i \in Z_{16}$, $i = 0, \ldots, n-1$ is $\mathrm{Vec}_4(a_{n-1}) \| \ldots \| \mathrm{Vec}_4(a_0)$.

It should be noted that in this set of examples, all data strings treated in right-to-left order. Byte ordering convention holds.

B.13.2 Example 1

In this example, the data string is given as a sequence of bytes (in hexadecimal notation):

M_1 = 30 31 32 33 34 35 36 37 38 39 30 31 32 33 34 35 36 37 38 39 30 31 32 33 34 35 36 37 38 39
30 31 32 33 34 35 36 37 38 39 30 31 32 33 34 35 36 37 38 39 30 31 32 33 34 35 36 37 38 39
30 31 32

Assign the following values to the variables:

$h := IV = 0^{512}$;

$N := 0^{512}$;

$\Sigma := 0^{512}$.

The length of the message is $L_{M_1} = 504 < 512$, so the incomplete block is padded:

m := 01323130393837363534333231303938373635343332313039383736353433323130393837363534333231303938373635343332313039383736353433323130.

Calculate $K := LPS(h \oplus N) = LPS(0^{512})$.

After the transformation S:

$S(h \oplus N)$ = fcfcfcfcfcfcfcfcfcfcfcfcfcfcfcfcfcfcfcfcfcfcfcfcfcfcfcfcfcfcfcfc fcfcfcfcfcfcfcfcfcfcfcfcfcfcfcfcfcfcfcfcfcfcfcfcfcfcfcfcfcfcfcfc,

after the transformation P:

$PS(h \oplus N)$ = fcfcfcfcfcfcfcfcfcfcfcfcfcfcfcfcfcfcfcfcfcfcfcfcfcfcfcfcfcfcfcfc fcfcfcfcfcfcfcfcfcfcfcfcfcfcfcfcfcfcfcfcfcfcfcfcfcfcfcfcfcfcfcfc,

after the transformation L:

$K = LPS(h \oplus N)$ = b383fc2eced4a574b383fc2eced4a574b383fc2eced4a574b383fc2eced4a574 b383fc2eced4a574b383fc2eced4a574b383fc2eced4a574b383fc2eced4a574.

Then the transformation $E(K, m)$ is performed:

Iteration 1

K_1 = b383fc2eced4a574b383fc2eced4a574b383fc2eced4a574b383fc2eced4a574 b383fc2eced4a574b383fc2eced4a574b383fc2eced4a574b383fc2eced4a574,

$X[K_1](m)$ = b2b1cd1ef7ec924286b7cf1cffe49c4c84b5c91afde694448abbcb18fbe09646 82b3c516f9e2904080b1cd1ef7ec924286b7cf1cffe49c4c84b5c91afde69444,

$SX[K_1](m)$ = 4645d95fc0beec2c432f8914b62d4efd3e5e37f14b097aead67de417c220b048 2492ac996667e0ebdf45d95fc0beec2c432f8914b62d4efd3e5e37f14b097aea,

$PSX[K_1](m)$ = 46433ed624df433e452f5e7d92452f5ed98937e4acd989375f14f117995f14f1 c0b64bc266c0b64bbe2d092067be2d09ec4e7ab0e0ec4e7a2cfdea48eb2cfdea,

$LPSX[K_1](m)$ = e60059d4d8e0758024c73f6f3183653f56579189602ae4c21e7953ebc0e212a0 ce78a8df475c2fd4fc43fc4b71c01e35be465fb20dad2cf690cdf65028121bb9,

$K_1 \oplus C_1$ = 028ba7f4d01e7f9d5848d3af0eb1d96b9ce98a6de0917562c2cd44a3bb516188 f8ff1cbf5cb3cc7511c1d6266ab47661b6f5881802a0e8576e0399773c72e073,

$S(K_1 \oplus C_1)$ = ddf644e6e15f5733bff249410445536f4e9bd69e200f3596b3d9ea737d70a1d7 d1b6143b9c9288357758f8ef78278aa155f4d717dda7cb12b211e87e7f19203d,

$PS(K_1 \oplus C_1)$ = ddbf4eb3d17755b2f6f29bd9b658f4114449d6ea14f8d7e8e6419e733bef177e e104207d9c78dd7f5f450f709227a719575335a1888acb20336f96d735a1123d,

$LPS(K_1 \oplus C_1)$ = d0b00807642fd78f13f2c3ebc774e80de0e902d23aef2ee9a73d010807dae9c1 88be14f0b2da27973569cd2ba051301036f728bd1d7eec33f4d18af70c46cf1e.

Iteration 2

K_2 = d0b00807642fd78f13f2c3ebc774e80de0e902d23aef2ee9a73d010807dae9c1 88be14f0b2da27973569cd2ba051301036f728bd1d7eec33f4d18af70c46cf1e,

$LPSX[K_2]LPSX[K_1](m)$ = 18e77571e703d19548075c574ce5e50e0480c9c5b9f21d45611ab86cf32 e352a d91854ea7df8f863d46333673f62ff2d3efae1cd966f8e2a74ce49902799aad4.

Iteration 3

K_3 = 9d4475c7899f2d0bb0e8b7dac6ef6e6b44ecf66716d3a0f16681105e2d13712a 1a9387ecc257930e2d61014a1b5c9fc9e24e7d636eb1607e816dbaf927b8fca9,

$LPSX[K_3]...LPSX[K_1](m)$ = 03dc0a9c64d42543ccdb62960d58c17e0b5b805d08a07406ece679d5f 82b70fe a22a7ea56e21814619e8749b308214575489d4d465539852cd4b0cd3829bef39.

Iteration 4

K_4 = 5c283daba5ec1f233b8c833c48e1c670dae2e40cc4c3219c73e58856bd96a72f df9f8055ffe3c004c8cde3b8bf78f95f3370d0a3d6194ac5782487defd83ca0f,

$LPSX[K_4]...LPSX[K_1](m)$ = dbee312ea7301b0d6d13e43855e85db81608c780c43675bc93cfd82c1 b4933b3 898a35b13e1878abe119e4dffb9de4889738ca74d064cd9eb732078c1fb25e04.

Iteration 5

K_5 = 109f33262731f9bd569cbc9317baa551d4d2964fa18d42c41fab4e37225292ec 2fd97d7493784779046388469ae195c436fa7cba93f8239ceb5ffc818826470c,

$LPSX[K_5]...LPSX[K_1](m)$ = 7fb3f15718d90e889f9fb7c38f527bec861c298afb9186934a93c9d96ad e20df 109379bb9c1a1ffd0ad81fce7b45ccd54501e7d127e32874b5d7927b032de7a1.

Iteration 6

K_6 = b32c9b02667911cf8f8a0877be9a170757e25026ccf41e67c6b5da70b1b87474 3e1135cfbefe244237555c676c153d99459bc382573aee2d85d30d99f286c5e7,

$LPSX[K_6]...LPSX[K_1](m)$ = 95efa4e104f235824bae5030fe2d0f170a38de3c9b8fc6d8fa1a9adc2945c4133 89a121501fa71a65067916b0c06f6b87ce18de1a2a98e0a64670985f47d73f1.

Iteration 7

K_7 = 8a13c1b195fd0886ac49989e7d84b08bc7b00e4f3f62765ece6050fcbabdc234 6c8207594714e8e9c9c7aad694edc922d6b01e17285eb7e61502e634559e32f1,

$LPSX[K_7]...LPSX[K_1](m)$ = 7ea4385f7e5e40103bfb25c67e404c7524eec43e33b1d06557469c604985430 4 32b43d941b77ffd476103338e9bd5145d9c1e18b1f262b58a81dcefff6fc6535.

Iteration 8

K_8 = 52cec3b11448bb8617d0ddfbc926f2e88730cb9179d6decea5acbffd323ec376 4c47f7a9e13bb1db56c342034773023d617ff01cc546728e71dff8de5d128cac,

$LPSX[K_8]...LPSX[K_1](m)$ = b2426da0e58d5cfe898c36e797993f902531579d8ecc59f8dd8a60802241a45 6 1f290cf992eb398894424bf681636968c167e870967b1dd9047293331956daba.

Iteration 9

K_9 = f38c5b7947e7736d502007a05ea64a4eb9c243cb82154aa138b963bbb7f28e74 d4d710445389671291d70103f48fd4d4c01fc415e3fb7dc61c6088afa1a1e735,

$LPSX[K_9]...LPSX[K_1](m)$ = 5e0c9978670b25912dd1ede5bdd1cf18ed094d14c6d973b731d50570d0a9bc a2 15415a15031fd20ddefb5bc61b96671d6902f49df4d2fd346ceebda9431cb075.

Iteration 10

K_{10} = 0740b3faa03ed39b257dd6e3db7c1bf56b6e18e40cdaabd30617cecbaddd618e
a5e61bb4654599581dd30c24c1ab877ad0687948286cfefaa7eef99f6068b315,

$LPSX[K_{10}]...LPSX[K_1](m)$ = c1ddd840fe491393a5d460440e03bf451794e792c0c629e49ab0c1001782dd
37 691cb6896f3e00b87f71d37a584c35b9cd8789fad55a46887e5b60e124b51a61.

Iteration 11

K_{11} = 185811cf3c2633aec8cfdfcae9dbb29347011bf92b95910a3ad71e5fca678e45
e374f088f2e5c29496e9695ce8957837107bb3aa56441af11a82164893313116,

$LPSX[K_{11}]...LPSX[K_1](m)$ = 3f75beaf2911c35d575088e30542b689c85b6b1607f8b800405941f5ab7042
84 7b9b08b58b4fbdd6154ed7b366fd3ee778ce647726ddb3c7d48c8ce8866a8435.

Iteration 12

K_{12} = 9d46bf66234a7ed06c3b2120d2a3f15e0fedd87189b75b3cd2f206906b5ee00d
c9a1eab800fb8cc5760b251f4db5cdef427052fa345613fd076451901279ee4c,

$LPSX[K_{12}]...LPSX[K_1](m)$ = f35b0d889eadfcff73b6b17f33413a97417d96f0c4cc9d30cda8ebb7dcd5d1b0
61e620bac75b367370605f474ddc006003bec4c4d7ce59a73fbe6766934c55a2.

Iteration 13

K_{13} = 0f79104026b900d8d768b6e223484c9761e3c585b3a405a6d2d8565ada926c3f
7782ef127cd6b98290bf612558b4b60aa3cbc28fd94f95460d76b621cb45be70,

$LPSX[K_{13}]...LPSX[K_1](m)$ = fc221dc8b814fc27a4de079d10097600209e5375776898961f70bded0647bd
8f 1664cfa8bb8d8ff1e0df3e621568b66aa075064b0e81cce132c8d1475809ebd2.

The result of the transformation $g_N(h, m)$ is

h = fd102cf8812ccb1191ea34af21394f3817a86641445aa9a626488adb33738ebd
2754f6908cbbbac5d3ed0f522c50815c954135793fb1f5d905fee4736b3bdae2.

The variables N and Σ change their values to:

N = 0000000000000000000000000000000000000000000000000000000000000000
00000000000000000000000000000000000000000000000000000000000001f8,

Σ = 013231303938373635343332313039383736353433323130393837363534333231
3130393837363534333231303938373635343332313039383736353433323130.

The result of the transformation $g_0(h, N)$ is

h = 5c881fd924695cf196c2e4fec20d14b642026f2a0b1716ebaabb7067d4d59752
3d2db69d6d3794622147a14f19a66e7f9037e1d662d34501a8901a5de7771d7c.

The result of the transformation $g_0(h, \Sigma)$ is

h = 486f64c1917879417fef082b3381a4e211c324f074654c38823a7b76f830ad00
fa1fbae42b1285c0352f227524bc9ab16254288dd6863dccd5b9f54a1ad0541b.

The hash-code of the message M_1 is the value:

H = 486f64c1917879417fef082b3381a4e211c324f074654c38823a7b76f830ad00
fa1fbae42b1285c0352f227524bc9ab16254288dd6863dccd5b9f54a1ad0541b.

B.13.3 Example 2

In this example, the data string is given as a sequence of bytes (in hexadecimal notation):

M_1 = d1 e5 20 e2 e5 f2 f0 e8 2c 20 d1 f2 f0 e8 e1 ee e6 e8 20 e2 ed f3 f6 e8 2c 20 e2 e5 fe f2 fa 20 f1 20 ec ee f0 ff 20 f1 f2 f0 e5 eb e0 ec e8 20 ed e0 20 f5 f0 e0 e1 f0 fb ff 20 ef eb fa ea fb 20 c8 e3 ee f0 e5 e2 fb.

Assign the following values to the variables:

$h := IV = 0^{512}$;

$N := 0^{512}$;

$\Sigma := 0^{512}$.

The length of the message is $L_{M_1} = 576 < 512$, so a part of this message is initially processed:

m := fbeafaebef20fffbf0e1e0f0f520e0ed20e8ece0ebe5f0f2f120fff0eeec20f1 20faf2fee5e2202ce8f6f3ede220e8e6eee1e8f0f2d1202ce8f0f2e5e220e5d1.

Calculate $K := LPS(h \oplus N) = LPS(0^{512})$.

After the transformation S:

$S(h \oplus N)$ = fcfcfcfcfcfcfcfcfcfcfcfcfcfcfcfcfcfcfcfcfcfcfcfcfcfcfcfcfcfcfcfc fcfcfcfcfcfcfcfcfcfcfcfcfcfcfcfcfcfcfcfcfcfcfcfcfcfcfcfcfcfcfcfc,

after the transformation P:

$PS(h \oplus N)$ = fcfcfcfcfcfcfcfcfcfcfcfcfcfcfcfcfcfcfcfcfcfcfcfcfcfcfcfc fcfcfcfcfcfcfcfcfcfcfcfcfcfcfcfcfcfcfcfcfcfcfcfcfcfcfcfcfcfcfcfc,

after the transformation L:

$K = LPS(h \oplus N)$ = b383fc2eced4a574b383fc2eced4a574b383fc2eced4a574b383fc2eced4a574 b383fc2eced4a574b383fc2eced4a574b383fc2eced4a574b383fc2eced4a574.

Then the transformation $E(K, m)$ is performed:

Iteration 1

K_1 = b383fc2eced4a574b383fc2eced4a574b383fc2eced4a574b383fc2eced4a574 b383fc2eced4a574b383fc2eced4a574b383fc2eced4a574b383fc2eced4a574,

$X[K_1](m)$ = 486906c521f45a8f43621cde3bf44599936b10ce2531558642a303de20388585 93790ed02b3685585b750fc32cf44d925d6214de3c0585585b730ecb2cf440a5,

$SX[K_1](m)$ = f29131ac18e613035196148598e6c8e8de6fe9e75c840c432c731185f906a8a8 de5404e1428fa8bf47354d408be63aecb79693857f6ea8bf473d04e48be6eb00,

$PSX[K_1](m)$ = f251de2cde47b74791966f735435963d3114e911044d9304ac85e785e14085e4 18985cf9428b7f8be6e684068fe66ee613c80ca8a83aa8eb03e843a8bfecbf00,

$LPSX[K_1](m)$ = 909aa733e1f52321a2fe35bfb8f67e92fbc70ef544709d5739d8faaca4acf126 e83e273745c25b7b8f4a83a7436f6353753cbbbe492262cd3a868eace0104af1,

$K_1 \oplus C_1$ = 028ba7f4d01e7f9d5848d3af0eb1d96b9ce98a6de0917562c2cd44a3bb516188 f8ff1cbf5cb3cc7511c1d6266ab47661b6f5881802a0e8576e0399773c72e073,

$S(K_1 \oplus C_1)$ = ddf644e6e15f5733bff249410445536f4e9bd69e200f3596b3d9ea737d70a1d7
d1b6143b9c9288357758f8ef78278aa155f4d717dda7cb12b211e87e7f19203d,

$PS(K_1 \oplus C_1)$ = ddbf4eb3d17755b2f6f29bd9b658f4114449d6ea14f8d7e8e6419e733bef177e
e104207d9c78dd7f5f450f709227a719575335a1888acb20336f96d735a1123d,

$LPS(K_1 \oplus C_1)$ = d0b00807642fd78f13f2c3ebc774e80de0e902d23aef2ee9a73d010807dae9c1
88be14f0b2da27973569cd2ba051301036f728bd1d7eec33f4d18af70c46cf1e.

Iteration 2

K_2 = d0b00807642fd78f13f2c3ebc774e80de0e902d23aef2ee9a73d010807dae9c1
88be14f0b2da27973569cd2ba051301036f728bd1d7eec33f4d18af70c46cf1e,

$LPSX[K_2]LPSX[K_1](m)$ = 301aadd761d13df0b473055b14a2f74a45f408022aecadd4d5f19cab8228883a
021ac0b62600a495950c628354ffce1161c68b7be7e0c58af090ce6b45e49f16.

Iteration 3

K_3 = 9d4475c7899f2d0bb0e8b7dac6ef6e6b44ecf66716d3a0f16681105e2d13712a
1a9387ecc257930e2d61014a1b5c9fc9e24e7d636eb1607e816dbaf927b8fca9,

$LPSX[K_3]...LPSX[K_1](m)$ = 9b83492b9860a93cbca1c0d8e0ce59db04e10500a6ac85d4103304974e78d3
22 59ceff03fbb353147a9c948786582df78a34c9bde3f72b3ca41b9179c2cceef3.

Iteration 4

K_4 = 5c283daba5ec1f233b8c833c48e1c670dae2e40cc4c3219c73e58856bd96a72f
df9f8055ffe3c004c8cde3b8bf78f95f3370d0a3d6194ac5782487defd83ca0f,

$LPSX[K_4]...LPSX[K_1](m)$ = e638e0a1677cdea107ec3402f70698a4038450dab44ac7a447e10155aa33ef1
b daf8f49da7b66f3e05815045fbd39c991cb0dc536e09505fd62d3c2cd00b0f57.

Iteration 5

K_5 = 109f33262731f9bd569cbc9317baa551d4d2964fa18d42c41fab4e37225292ec
2fd97d7493784779046388469ae195c436fa7cba93f8239ceb5ffc818826470c,

$LPSX[K_5]...LPSX[K_1](m)$ = 1c7c8e19b2bf443eb3adc0c787a52a173821a97bc5a8efea58fb8b27861829f6
dd5ff9c97865e08c1ac66f47392b578e21266e323a0aacedeec3ef0314f517c6.

Iteration 6

K_6 = b32c9b02667911cf8f8a0877be9a170757e25026ccf41e67c6b5da70b1b87474
3e1135cfbefe244237555c676c153d99459bc382573aee2d85d30d99f286c5e7,

$LPSX[K_6]...LPSX[K_1](m)$ = 48fecfc5b3eb77998fb39bfcccd128cd42fccb714221be1e675a1c6fdde7e311
98b318622412af7e999a3eff45e6d61609a7f2ae5c2ff1ab7ff3b37be7011ba2.

Iteration 7

K_7 = 8a13c1b195fd0886ac49989e7d84b08bc7b00e4f3f62765ece6050fcbabdc234
6c8207594714e8e9c9c7aad694edc922d6b01e17285eb7e61502e634559e32f1,

$LPSX[K_7]...LPSX[K_1](m)$ = a48f8d781c2c5be417ae644cc2e15a9f01fcead3232e5bd53f18a5ab875cce1b
8a1a400cf48521c7ce27fb1e94452fb54de23118f53b364ee633170a62f5a8a9.

Iteration 8

K_8 = 52cec3b11448bb8617d0ddfbc926f2e88730cb9179d6decea5acbffd323ec376
4c47f7a9e13bb1db56c342034773023d617ff01cc546728e71dff8de5d128cac,

$LPSX[K_8]...LPSX[K_1](m)$ = e8a31b2e34bd2ae21b0ecf29cc4c37c75c4d11d9b82852517515c23e81e906a
4 51b72779c3087141f1a15ab57f96d7da6c7ee38ed25befbdef631216356ff59c.

Iteration 9

K_9 = f38c5b7947e7736d502007a05ea64a4eb9c243cb82154aa138b963bbb7f28e74
d4d710445389671291d70103f48fd4d4c01fc415e3fb7dc61c6088afa1a1e735,

$LPSX[K_9]...LPSX[K_1](m)$ = 34392ed32ea3756e32979cb0a2247c3918e0b38d6455ca88183356bf8e5877
e5 5d542278a696523a8036af0f1c2902e9cbc585de803ee4d26649c9e1f00bda31.

Iteration 10

K_{10} = 0740b3faa03ed39b257dd6e3db7c1bf56b6e18e40cdaabd30617cecbaddd618e
a5e61bb4654599581dd30c24c1ab877ad0687948286cfefaa7eef99f6068b315,

$LPSX[K_{10}]...LPSX[K_1](m)$ = 6a82436950177fea74cce6d507a5a64e54e8a3181458e3bdfbdbc6180c9787
de 7ccb676dd809e7cb1eb2c9ebd016561570801a4e9ce17a438b85212f4409bb5e.

Iteration 11

K_{11} = 185811cf3c2633aec8cfdfcae9dbb29347011bf92b95910a3ad71e5fca678e45
e374f088f2e5c29496e9695ce8957837107bb3aa56441af11a82164893313116,

$LPSX[K_{11}]...LPSX[K_1](m)$ = 7b97603135e2842189b0c9667596e96bd70472ccbc73ae89da7d1599c7286
0c2 85f5771088f1fb0f943d949f22f1413c991eafb51ab8e5ad8644770037765aec.

Iteration 12

K_{12} = 9d46bf66234a7ed06c3b2120d2a3f15e0fedd87189b75b3cd2f206906b5ee00d
c9a1eab800fb8cc5760b251f4db5cdef427052fa345613fd076451901279ee4c,

$LPSX[K_{12}]...LPSX[K_1](m)$ = 39ec8a88db635b46c4321adf41fd9527a39a67f6d7510db5044f05efaf721db
5 cf976a726ef33dc4dfcda94033e741a463770861a5b25fefcb07281eed629c0e.

Iteration 13

K_{13} = 0f79104026b900d8d768b6e223484c9761e3c585b3a405a6d2d8565ada926c3f
7782ef127cd6b98290bf612558b4b60aa3cbc28fd94f95460d76b621cb45be70,

$LPSX[K_{13}]...LPSX[K_1](m)$ = 36959ac8fdda5b9e135aac3d62b5d9b0c279a27364f50813d69753b575e071
8a b8158560122584464f72c8656b53f7aec0bccaee7cfdcaa9c6719e3f2627227e.

The result of the transformation $g_N(h, m)$ is

h = cd7f602312faa465e3bb4ccd9795395de2914e938f10f8e127b7ac459b0c517b
98ef779ef7c7a46aa7843b8889731f482e5d221e8e2cea852e816cdac407c7af.

The variables N and Σ change their values to:

N = 0000000000000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000200,

Σ = fbeafaebef20fffbf0e1e0f0f520e0ed20e8ece0ebe5f0f2f120fff0eeec20f1
20faf2fee5e2202ce8f6f3ede220e8e6eee1e8f0f2d1202ce8f0f2e5e220e5d1.

The length of the rest of the message is less than 512, so the incomplete block is padded.

m := 000000000000000000000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000000001fbe2e5f0eee3c820.

The result of the transformation $g_N(h, m)$ is

h = c544ae6efdf14404f089c72d5faf8dc6aca1db5e28577fc07818095f1df70661
e8b84d0706811cf92dffb8f96e61493dc382795c6ed7a17b64685902cbdc878e.

The variables N and Σ change their values to:

N = 000000000000000000000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000240,

Σ = fbeafaebef20fffbf0e1e0f0f520e0ed20e8ece0ebe5f0f2f120fff0eeec20f1
20faf2fee5e2202ce8f6f3ede220e8e6eee1e8f0f2d1202ee4d3d8d6d104adf1.

The result of the transformation $g_0(h, N)$ is

h = 4deb6649ffa5caf4163d9d3f9967fbbd6eb3da68f916b6a09f41f2518b81292b
703dc5d74e1ace5bcd3458af43bb456e837326088f2b5df14bf83997a0b1ad8d.

The result of the transformation $g_0(h, \Sigma)$ is

h = 28fbc9bada033b1460642bdcddb90c3fb3e56c497ccd0f62b8a2ad4935e85f03
7613966de4ee00531ae60f3b5a47f8dae06915d5f2f194996fcabf2622e6881e.

The hash-code of the message M_2 is the value:

H = 28fbc9bada033b1460642bdcddb90c3fb3e56c497ccd0f62b8a2ad4935e85f03
7613966de4ee00531ae60f3b5a47f8dae06915d5f2f194996fcabf2622e6881e.

B.14 Dedicated Hash-Function 12 (STREEBOG-256)

B.14.1 General

The binary words are expressed in hexadecimal notation. The $4n$-bit word is given in the form $a_{n-1}, \ldots, a_0$, where $a_i \in Z_{16}$, $i = 0, \ldots, n-1$ is $\mathrm{Vec}_4(a_{n-1}) \| \ldots \| \mathrm{Vec}_4(a_0)$.

It should be noted that in this set of examples all data strings treated in right-to-left order. Byte ordering convention holds.

B.14.2 Example 1

In this example, the data string is given as a sequence of bytes (in hexadecimal notation):

M_1 = 30 31 32 33 34 35 36 37 38 39 30 31 32 33 34 35 36 37 38 39 30 31 32 33 34 35 36 37 38 39
30 31 32 33 34 35 36 37 38 39 30 31 32 33 34 35 36 37 38 39 30 31 32 33 34 35 36 37 38 39
30 31 32

Assign the following values to the variables:

$h := IV = (000\ 000\ 01)^{64}$;

$N := 0^{512}$;

$\Sigma := 0^{512}$.

The length of the message is $L_{M_1} = 504 < 512$, so the incomplete block is padded:

$m :=$ 0132313039383736353433323130393837363534333231303938373635343332
3130393837363534333231303938373635343332313039383736353433323130.

Calculate $K := LPS(h \oplus N) = LPS[(000\ 000\ 01)^{64}]$.

After the transformation S:

$S(h \oplus N)$ = eeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeee
eeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeee,

after the transformation P:

$PS(h \oplus N)$ = eeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeee
eeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeee,

after the transformation L:

$K = LPS(h \oplus N)$ = 23c5ee40b07b5f1523c5ee40b07b5f1523c5ee40b07b5f1523c5ee40b07b5f15
23c5ee40b07b5f1523c5ee40b07b5f1523c5ee40b07b5f1523c5ee40b07b5f15.

Then the transformation $E(K, m)$ is performed:

Iteration 1

K_1 = 23c5ee40b07b5f1523c5ee40b07b5f1523c5ee40b07b5f1523c5ee40b07b5f15
23c5ee40b07b5f1523c5ee40b07b5f1523c5ee40b07b5f1523c5ee40b07b5f15,

$X[K_1](m)$ = 22f7df708943682316f1dd72814b662d14f3db7483496e251afdd976854f6c27
12f5d778874d6a2110f7df708943682316f1dd72814b662d14f3db7483496e25,

$SX[K_1](m)$ = 65c061327951f35a99a6d819f5a29a0193d290ffa92ab25cf14b538aa8cc9d21
f0f4fe6dc93a7818e9c061327951f35a99a6d819f5a29a0193d290ffa92ab25c,

$PSX[K_1](m)$ = 659993f1f0e99993c0a6d24bf4c0a6d261d89053fe61d8903219ff8a6d3219ff
79f5a9a8c979f5a951a22acc3a51a22af39ab29d78f39ab25a015c21185a015c,

$LPSX[K_1](m)$ = e549368917a0a2611d5e08c9c2fd5b3c563f18c0f68c410d84ae9d5fbdfb9340
55650121b7aa6d7b3e7d09d46ac4358adaa6ae44fa3b0402c4166d2c3eb2ef02,

$K_1 \oplus C_1$ = 92cdb59aaeb185fcc80ec1c1701e230a0caf98039e3e8f03528b56cdc5fe9be9
68b90ed1221c36148187c448141b8c0026b39a767c0f1236fe458b1942dd1a12,

$S(K_1 \oplus C_1)$ = ecd95e282645a83930045858325f5afa2341dc110ad303110ef676d9ac63509b
f3a3041b65148f93f5c986f293bb7cfcef92288ac34df08f63c8f6362cd8f1f0,

$PS(K_1 \oplus C_1)$ = ec30230ef3f5ef63d90441f6a3c992c85e58dc76048628f6285811d91bf28a36
26320aac6593c32c455fd36314bb4dd8a85a03508f7cf0f139fa119b93fc8ff0,

$LPS(K_1 \oplus C_1)$ = 18ee8f3176b2ebea3bd6cb8233694cea349769df88be26bf451cfab6a904a549
da22de93a66a66b19c7e6b5eea633511e611d68c8401bfcd0c7d0cc39d4a5eb9.

Iteration 2

K_2 = 18ee8f3176b2ebea3bd6cb8233694cea349769df88be26bf451cfab6a904a549
da22de93a66a66b19c7e6b5eea633511e611d68c8401bfcd0c7d0cc39d4a5eb9,

$LPSX[K_2]LPSX[K_1](m)$ = c502dab7e79eb94013fcd1ba64def3b916f18b63855d43d22b77fca1452f9866
c2b45089c62e9d82edf1ef45230db9a23c9e1c521113376628a5f6a5dbc041b2.

Iteration 3

K_3 = aaa4cf31a265959157aec8ce91e7fd46bf27dee21164c5e3940bba1a519e9d1f
ce0913f1253e7757915000cd674be12cc7f68e73ba26fb00fd74af4101805f2d,

$LPSX[K_3]...LPSX[K_1](m)$ = 8e5a4fe41fc790af29944f027aa2f10105d65cf60a66e442832bb9ab5020dc54
772e36b03d4b9aa471037212cde93375226552392ef4d83010a007e1117a07b5.

Iteration 4

K_4 = 61fe0a65cc177af50235e2afadded326a5329a2236747bf8a54228aeca9c4585
cd801ea9dd743a0d98d01ef0602b0e332067fb5ddd6ac156820031192083928 6,

$LPSX[K_4]...LPSX[K_1](m)$ = dee0b40df69997afef726f03bdc13cb6ba9287698201296f2fd8284f06d33ea4
a850a0ff48026dd47c1e88ec813ed2eb1186059d842d8d17f0bfa259e56655b1.

Iteration 5

K_5 = 9983685f4fd3636f1fd5abb75fbf26a8e2934314aa2ecb3ee4693c86c06c7d4e
169bd540af75e1610a546acd63d960bad595394cc199bf6999a5d5309fe73d5a,

$LPSX[K_5]...LPSX[K_1](m)$ = 675ea894d326432e1af7b201bc369f8ab021f6fa58da09678ffc08ef30db43a3
7f1f7347cb77da0f6ba30c85848896c3bac240ab14144283518b89a33d0caf07.

Iteration 6

K_6 = f05772ae2ce7f025156c9a7fbcc6b8fdf1e735d613946e32922994e52820ffea
62615d907eb0551ad170990a86602088af98c83c22cdb0e2be297c13c0f7a156,

$LPSX[K_6]...LPSX[K_1](m)$ = 1bc204bf9506ee9b86bbcf82d254a112aea6910b6db3805e399cb718d1b331
99 64459516967cee4e648e8cfbf81f56dc8da6811c469091be5123e6a1d5e28c73.

Iteration 7

K_7 = 5ad144c362546e4e46b3e7688829fbb77453e9c3211974330b2b8d0e6be2b5ac
c89eb6b35167f159b7b005a43e5959a651a9b18cfc8e4098fcf03d9b81cfbb8d,

$LPSX[K_7]...LPSX[K_1](m)$ = f30d791ed78bdee819022a3d78182242124efcdd54e203f23fb2dc7f94338ff9
55a5afc15ffef03165263c4fdb36933aa982016471fbac9419f892551e9e568b.

Iteration 8

K_8 = 6a6cec9a1ba20a8db64fa840b934352b518c638ed530122a83332fe0b8efdac9
018287e5a9f509c78d6c746adcd5426fb0a0ad5790dfb73fc1f191a539016daa,

$LPSX[K_8]...LPSX[K_1](m)$ = 1fc20f1e91a1801a4293d3f3aa9e91560fcc3810bb15f3ee9741c9b87452519f
67cb9145519884a24de6db736a5cb1430da7458e5e51b80be5204ba5b2600177.

Iteration 9

K_9 = 99217036737aa9b38a8d6643f705bd51f351531f948f0fc5e35fa35fee9dd8bd
bb4c9d580a224e9cd82e0e2069fc49ed367d5f94374435382b8fb6a8f5dd0409,

$LPSX[K_9]...LPSX[K_1](m)$ = 1a52f09d1e81515a36171e0b1a2809c50359bed90f2e78cbd89b7d4afa6d046
6 55c96bdae6ee97055cc7e857267c2ccf28c8f5dd95ed58a9a68c12663bb28967.

Iteration 10

K_{10} = 906763c0fc89fa1ae69288d8ec9e9dda9a7630e8bfd6c3fed703c35d2e62aeaf
f0b35d80a7317a7f76f83022f2526791ca8fdf678fcb337bd74fe5393ccb05d2,

$LPSX[K_{10}]...LPSX[K_1](m)$ = 764043744a0a93687e65aba8cfc25ec8714fb8e1bdc9ae2271e7205eaaa577c
1 b3b83e7325e50a19bd2d56b061b5de39235c9c9fd95e071a1a291a5f24e8c774.

Iteration 11

K_{11} = 88ce996c63618e6404a5c8e03ee433854e2ae3eee68991bbbff3c29d38dadb6e
d6a1dae9a6dc6ddf52ce34af272f96d3159c8c624c3fe6e13d695c0bfc89add5,

$LPSX[K_{11}]...LPSX[K_1](m)$ = 9b1ce8ff26b445cb288c0aeccf84658eea91dbdf14828bf70110a5c9bd146cd9
646350cff4e90e7b63c5cc325e9b441081935f282d4648d9584f71860538f03b.

Iteration 12

K_{12} = 3e0a281ea9bd46063eec550100576f3a506aa168cf82915776b978fccaa32f38
b55f30c79982ca45628e8365d8798477e75a49c68199112a1d7b5a0f7655f2db,

$LPSX[K_{12}]...LPSX[K_1](m)$ = 133aeecede251eb81914b8ba48dcbc0b8a6fc63a292cc49043c3d3346b3f082
9 a9cb71ecff25ed2a91bdcf8f649907c110cb76ff2e43100cdd4ba8a147a572f5.

Iteration 13

K_{13} = f0b273409eb31aebe432fbae1867212262c848422b6a92f93f6cbab54ed18b83
14b21cffc51e3fa319ff433e76ef6adb0ef9f5e03c907fa1fcf9eca06500bf03,

$LPSX[K_{13}]...LPSX[K_1](m)$ = e3889d8e40960453fd26431450bb9d29e8a78e78024656697caf698125ee8
3aa bd796d133a3bd28988428cb112766d1a1e32831f12d36fad21b2440122a5cdf6.

The result of the transformation $g_N(h, m)$ is

h = e3bbadbf78af3264c9137127608aa510de90ba4d3075665844965fb611dbb199
8d48552a0c0ce6bcba71bc802a4f5b2d2a07b12c22e25794178570341096fdc7.

The variables N and Σ change their values to:

N = 0000000000000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000000000000000000000001f8,

Σ = 013231303938373635343332313039383736353433323130393837363534333 2
31303938373635343332313039383736353433323130393837363534333231 30.

The result of the transformation $g_0(h, N)$ is

h = 70f22bada4cfe18a6a56ec4b3f328cd40db8e1bf8a9d5f711d5efab11191279d
715aab7648d07eddbf87dc79c80516e6ffcbcf5678b0ac29ea00fa85c8173cc6.

The result of the transformation $g_0(h, \Sigma)$ is

h = 00557be5e584fd52a449b16b0251d05d27f94ab76cbaa6da890b59d8ef1e159d
2088e482e2acf564e0e9795a51e4dd261f3f667985a2fcc40ac8631faca1709a.

The hash-code of the message M_1 is the value:

H = 00557be5e584fd52a449b16b0251d05d27f94ab76cbaa6da890b59d8ef1e159d.

B.14.3 Example 2

In this example, the data string is given as a sequence of bytes (in hexadecimal notation):

M_2 = d1 e5 20 e2 e5 f2 f0 e8 2c 20 d1 f2 f0 e8 e1 ee e6 e8 20 e2 ed f3 f6 e8 2c 20 e2 e5 fe f2 fa 20 f1 20 ec ee f0 ff 20 f1 f2 f0 e5 eb e0 ec e8 20 ed e0 20 f5 f0 e0 e1 f0 fb ff 20 ef eb fa ea fb 20 c8 e3 ee f0 e5 e2 fb.

Assign the following values to the variables:

$h := IV = (000\ 000\ 01)^{64}$;

$N := 0^{512}$;

$\Sigma := 0^{512}$.

The length of the message is $L_{M_2} = 576 > 512$, so a part of this message is initially processed

m := fbeafaebef20fffbf0e1e0f0f520e0ed20e8ece0ebe5f0f2f120fff0eeec20f1
20faf2fee5e2202ce8f6f3ede220e8e6eee1e8f0f2d1202ce8f0f2e5e220e5d1.

Calculate $K := LPS(h \oplus N) = LPS[(000\ 000\ 01)^{64}]$.

After the transformation S:

$S(h \oplus N)$ = eeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeee
eeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeee,

after the transformation P:

$PS(h \oplus N)$ = eeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeee
eeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeee,

after the transformation L:

$K = LPS(h \oplus N)$ = 23c5ee40b07b5f1523c5ee40b07b5f1523c5ee40b07b5f1523c5ee40b07b5f15
23c5ee40b07b5f1523c5ee40b07b5f1523c5ee40b07b5f1523c5ee40b07b5f15.

Then the transformation $E(K, m)$ is performed:

Iteration 1

K_1 = 23c5ee40b07b5f1523c5ee40b07b5f1523c5ee40b07b5f1523c5ee40b07b5f15
23c5ee40b07b5f1523c5ee40b07b5f1523c5ee40b07b5f1523c5ee40b07b5f15,

$X[K_1](m)$ = d82f14ab5f5ba0eed3240eb0455bbff8032d02a05b9eafe7d2e511b05e977fe4
033f1cbe55997f39cb331dad525bb7f3cd2406b042aa7f39cb351ca5525bbac4,

$SX[K_1](m)$ = 8d4f93828747a76c49e204adc8473bd11101dda7470a415b832b77ad5dbc572d
111f14950ce8570be4aecd9f0e472fd2d9e231ad2c38570be46a14000e47a586,

$PSX[K_1](m)$ = 8d49118311e4d9e44fe2012b1faee26a9304dd7714cd311482ada7ad959fad00
87c8475d0c0e2c0e47470abce8473847a73b4157572f57a56cd15b2d0bd20b86,

$LPSX[K_1](m)$ = a3a72a2e0fb5e6f812681222fec037b0db972086a395a387a6084508cae13093
aa71d352dcbce288e9a39718a727f6fd4c5da5d0bc10fac3707ccd127fe45475,

$K_1 \oplus C_1$ = 92cdb59aaeb185fcc80ec1c1701e230a0caf98039e3e8f03528b56cdc5fe9be9
68b90ed1221c36148187c448141b8c0026b39a767c0f1236fe458b1942dd1a12,

$S(K_1 \oplus C_1)$ = ecd95e282645a83930045858325f5afa2341dc110ad303110ef676d9ac63509b
f3a3041b65148f93f5c986f293bb7cfcef92288ac34df08f63c8f6362cd8f1f0,

$PS(K_1 \oplus C_1)$ = ec30230ef3f5ef63d90441f6a3c992c85e58dc76048628f6285811d91bf28a36
26320aac6593c32c455fd36314bb4dd8a85a03508f7cf0f139fa119b93fc8ff0,

$LPS(K_1 \oplus C_1)$ = 18ee8f3176b2ebea3bd6cb8233694cea349769df88be26bf451cfab6a904a549
da22de93a66a66b19c7e6b5eea633511e611d68c8401bfcd0c7d0cc39d4a5eb9.

Iteration 2

K_2 = 18ee8f3176b2ebea3bd6cb8233694cea349769df88be26bf451cfab6a904a549
da22de93a66a66b19c7e6b5eea633511e611d68c8401bfcd0c7d0cc39d4a5eb9,

$LPSX[K_2]LPSX[K_1](m)$ = 9f50697b1d9ce23680db1f4d35629778864c55780727aa79eb7bb7d648829cba
8674afdac5c62ca352d77556145ca7bc758679fbe1fbd32313ca8268a4a603f1.

Iteration 3

K_3 = aaa4cf31a265959157aec8ce91e7fd46bf27dee21164c5e3940bba1a519e9d1f
ce0913f1253e7757915000cd674be12cc7f68e73ba26fb00fd74af4101805f2d,

$LPSX[K_3]...LPSX[K_1](m)$ = 4183027975b257e9bc239b75c977ecc52ddad82c091e694243c9143a945b4d
85 3116eae14fd81b14bb47f2c06fd283cb6c5e61924edfaf971b78d771858d5310.

Iteration 4

K_4 = 61fe0a65cc177af50235e2afadded326a5329a2236747bf8a54228aeca9c4585
cd801ea9dd743a0d98d01ef0602b0e332067fb5ddd6ac1568200311920839286,

$LPSX[K_4]...LPSX[K_1](m)$ = 0368c884fcee489207b5b97a133ce39a1ebfe5a3ae3cccb3241de1e7ad72857e
76811d324f01fd7a75e0b669e8a22a4d056ce6af3e876453a9c3c47c767e5712.

Iteration 5

K_5 = 9983685f4fd3636f1fd5abb75fbf26a8e2934314aa2ecb3ee4693c86c06c7d4e
169bd540af75e1610a546acd63d960bad595394cc199bf6999a5d5309fe73d5a,

$LPSX[K_5]...LPSX[K_1](m)$ = c31433ceb8061e46440144e65553976512e5a9806ac9a2c771d5932d5f6508
c5 b78e406c4efab98ac5529be0021b4d58fa26f01621eb10b43de4c4c47b63f615.

Iteration 6

K_6 = f05772ae2ce7f025156c9a7fbcc6b8fdf1e735d613946e32922994e52820ffea
62615d907eb0551ad170990a86602088af98c83c22cdb0e2be297c13c0f7a156,

$LPSX[K_6]...LPSX[K_1](m)$ = 5d0ae97f252ad04534503fe5f52e9bd07f483ee3b3d206beadc6e736c6e754bb
713f97ea7339927893eacf2b474a482cadd9ac2e58f09bcb440cf36c2d14a9b6.

Iteration 7

K_7 = 5ad144c362546e4e46b3e7688829fbb77453e9c3211974330b2b8d0e6be2b5ac
c89eb6b35167f159b7b005a43e5959a651a9b18cfc8e4098fcf03d9b81cfbb8d,

$LPSX[K_7]...LPSX[K_1](m)$ = a59aa21e6ad3e330deedb9ab9912205c355b1c479fdfd89a7696d7de66fbf7d3
cec25879f7f1a8cca4c793d5f2888407aecb188bda375eae586a8cfd0245c317.

Iteration 8

K_8 = 6a6cec9a1ba20a8db64fa840b934352b518c638ed530122a83332fe0b8efdac9
018287e5a9f509c78d6c746adcd5426fb0a0ad5790dfb73fc1f191a539016daa,

$LPSX[K_8]...LPSX[K_1](m)$ = 9903145a39d5a8c83d28f70fa1fbd88f31b82dc7cfe17b54b50e276cb2c4ac68
2b4434163f214cf7ce6164a75731bcea5819e6a6a6fea99da9222951d2a28e01.

Iteration 9

K_9 = 99217036737aa9b38a8d6643f705bd51f351531f948f0fc5e35fa35fee9dd8bd
bb4c9d580a224e9cd82e0e2069fc49ed367d5f94374435382b8fb6a8f5dd0409,

$LPSX[K_9]...LPSX[K_1](m)$ = 330e6cb1d04961826aa263f2328f15b4f3370175a6a9fd6505b286efed2d850
5 f71823337ef71513e57a700eb1672a685578e45dad298ee2223d4cb3fda8262f.

Iteration 10

K_{10} = 906763c0fc89fa1ae69288d8ec9e9dda9a7630e8bfd6c3fed703c35d2e62aeaf
f0b35d80a7317a7f76f83022f2526791ca8fdf678fcb337bd74fe5393ccb05d2,

$LPSX[K_{10}]...LPSX[K_1](m)$ = ad347608443ab9c9bbb64f633a5749ab85c45d4174bfd78f6bc79fc4f4ce9ad
1 dd71cb2195b1cfab8dcaaf6f3a65c8bb0079847a0800e4427d3a0a815f40a644.

Iteration 11

K_{11} = 88ce996c63618e6404a5c8e03ee433854e2ae3eee68991bbbff3c29d38dadb6e
d6a1dae9a6dc6ddf52ce34af272f96d3159c8c624c3fe6e13d695c0bfc89add5,

$LPSX[K_{11}]...LPSX[K_1](m)$ = a065c55e2168c31576a756c7ecc1a9129cd3d207f8f43073076c30e111fd5f1
1 9095ca396e9fb78a2bf4781c44e845e447b8fc75b788284aae27582212ec23ee.

Iteration 12

K_{12} = 3e0a281ea9bd46063eec550100576f3a506aa168cf82915776b978fccaa32f38
b55f30c79982ca45628e8365d8798477e75a49c68199112a1d7b5a0f7655f2db,

$LPSX[K_{12}]...LPSX[K_1](m)$ = 2a6549f7a5cd2eb4a271a7c71762c8683e7a3a906985d60f8fc86f64e35908b
2 9f83b1fe3c704f3c116bdfe660704f3b9c8a1d0531baaffaa3940ae9090a33ab.

Iteration 13

K_{13} = f0b273409eb31aebe432fbae1867212262c848422b6a92f93f6cbab54ed18b83
14b21cffc51e3fa319ff433e76ef6adb0ef9f5e03c907fa1fcf9eca06500bf03,

$LPSX[K_{13}]...LPSX[K_1](m)$ = dad73ab73b7e345f46435c690f05e94a5cb272d242ef44f6b0a4d5d1ad88833
1 8b31ad01f96e709f08949cd8169f25e09273e8e50d2ad05b5f6de6496c0a8ca8.

The result of the transformation $g_N(h, m)$ is

h = 203cc15dd55fcaa5b7a3bd98fb2408a67d5b9f33a80bb50540852b204265a2c1
aaca5efe1d8d51b2e1636e34f5becc077d930114fefaf176b69c15ad8f2b6878.

The variables N and Σ changed their values to:

N = 0000000000000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000200,

Σ = fbeafaebef20fffbf0e1e0f0f520e0ed20e8ece0ebe5f0f2f120fff0eeec20f1
20faf2fee5e2202ce8f6f3ede220e8e6eee1e8f0f2d1202ce8f0f2e5e220e5d1.

The length of the rest of the message is less than 512, so the incomplete block is padded:

m := 0000000000000000000000000000000000000000000000000000000000000000
00000000000000000000000000000000000000000001fbe2e5f0eee3c820.

The result of the transformation $g_N(h, m)$ is

h = a69049e7bd076ab775bc2873af26f098c538b17e39a5c027d532f0a2b3b56426
c96b285fa297b9d39ae6afd8b9001d97bb718a65fcc53c41b4ebf4991a617227.

The variables N and Σ change their values to:

N = 0000000000000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000240,

Σ = fbeafaebef20fffbf0e1e0f0f520e0ed20e8ece0ebe5f0f2f120fff0eeec20f1
20faf2fee5e2202ce8f6f3ede220e8e6eee1e8f0f2d1202ee4d3d8d6d104adf1.

The result of the transformation $g_0(h, N)$ is

h = aee3bd55ea6f387bcf28c6dcbdbbfb3ddacc67dcc13dbd8d548c6bf808111d4b
75b8e74d2afae960835ae6a5f03575559c9fd839783ffcd5cf99bd61566b4818.

The result of the transformation $g_0(h, \Sigma)$ is

h = 508f7e553c06501d749a66fc28c6cac0b005746d97537fa85d9e40904efed29d
c345e53d7f84875d5068e4eb743f0793d673f09741f9578471fb2598cb35c230.

The hash-code of the message M_2 is the value:

H = 508f7e553c06501d749a66fc28c6cac0b005746d97537fa85d9e40904efed29d.

B.15 Dedicated Hash-Function 13 (SHA3-224)

NOTE 1 Data is presented in three different ways: bit strings, byte strings and "w" length words (for the lanes).

NOTE 2 Bit strings are the sequence of bits from left to right.

NOTE 3 Byte strings are the bytes are left to right and the bits within the byte are right to left.

NOTE 4 Words are the integer representation of the values in the lanes.

The message as bit string

```
(empty message)
```

XORed state (in bytes)

```
06 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 80
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
            00 00 00 00 00 00 00 00
```


XORed state (as lanes of integers)

```
[0, 0] = 0000000000000006
[1, 0] = 0000000000000000
[2, 0] = 0000000000000000
[3, 0] = 0000000000000000
[4, 0] = 0000000000000000
[0, 1] = 0000000000000000
[1, 1] = 0000000000000000
[2, 1] = 0000000000000000
[3, 1] = 0000000000000000
[4, 1] = 0000000000000000
[0, 2] = 0000000000000000
[1, 2] = 0000000000000000
[2, 2] = 0000000000000000
[3, 2] = 0000000000000000
[4, 2] = 0000000000000000
[0, 3] = 0000000000000000
[1, 3] = 0000000000000000
[2, 3] = 8000000000000000
[3, 3] = 0000000000000000
[4, 3] = 0000000000000000
[0, 4] = 0000000000000000
[1, 4] = 0000000000000000
[2, 4] = 0000000000000000
[3, 4] = 0000000000000000
[4, 4] = 0000000000000000
```

Round #0

After theta

```
06 00 00 00 00 00 00 00 07 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 80
0C 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
07 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 80 0C 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 07 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 80
0C 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
07 00 00 00 00 00 00 00 00 00 00 00 00 00 00 80
00 00 00 00 00 00 00 80 0C 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 07 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 80
            0C 00 00 00 00 00 00 00
```

After rho

```
06 00 00 00 00 00 00 00 0E 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 08 00 00 00 00
00 00 00 60 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 70 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 40 00 00 00 C0 00 00 00 00 00
00 00 00 00 00 00 00 00 00 1C 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 01 00 00 00 00
00 00 00 00 00 06 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 E0 00 00 00 40 00 00 00 00 00 00
00 00 10 00 00 00 00 00 00 0C 00 00 00 00 00 00
00 00 00 00 00 00 00 00 1C 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 80 00
            00 00 03 00 00 00 00 00
```

After pi

```
06 00 00 00 00 00 00 00 00 00 00 00 00 70 00 00
00 00 00 00 00 00 00 00 00 10 00 00 00 00 00 00
00 00 03 00 00 00 00 00 00 00 00 08 00 00 00 00
00 00 C0 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 E0 00 00 00 00 00 00 00 00 00 00
0E 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 01 00 00 00 00 00 0C 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 60 00 00 00 00
00 00 00 00 00 00 00 00 00 1C 00 00 00 00 00 00
00 40 00 00 00 00 00 00 00 00 00 00 00 00 80 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00
00 00 00 00 00 06 00 00 00 00 00 00 00 00 00 00
            1C 00 00 00 00 00 00 00
```

After chi

```
06 00 00 00 00 00 00 00 00 00 10 00 00 70 00 00
00 00 03 00 00 00 00 00 06 00 10 00 00 00 00 00
00 00 03 00 00 70 00 00 00 00 00 08 00 00 00 00
00 00 C0 00 00 E0 00 00 00 00 00 00 00 00 00 00
00 00 00 08 00 E0 00 00 00 00 C0 00 00 00 00 00
0E 00 00 01 00 00 00 00 00 0C 00 00 00 00 00 00
00 00 00 01 00 00 00 00 0E 0C 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 1C 00 60 00 00 00 00
00 40 00 00 00 00 00 00 00 1C 00 00 00 00 80 00
00 40 00 60 00 00 00 00 00 00 00 00 00 00 80 00
00 00 00 00 00 06 00 00 00 00 00 00 00 00 40 00
1C 00 00 00 00 06 00 00 00 00 00 00 00 00 00 00
            1C 00 00 00 00 00 40 00
```

After iota

```
07 00 00 00 00 00 00 00 00 00 10 00 00 70 00 00
00 00 03 00 00 00 00 00 06 00 10 00 00 00 00 00
00 00 03 00 00 70 00 00 00 00 00 08 00 00 00 00
00 00 C0 00 00 E0 00 00 00 00 00 00 00 00 00 00
00 00 00 08 00 E0 00 00 00 00 C0 00 00 00 00 00
0E 00 00 01 00 00 00 00 00 0C 00 00 00 00 00 00
00 00 00 01 00 00 00 00 0E 0C 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 1C 00 60 00 00 00 00
00 40 00 00 00 00 00 00 00 1C 00 00 00 00 80 00
00 40 00 60 00 00 00 00 00 00 00 00 00 00 80 00
00 00 00 00 00 06 00 00 00 00 00 00 00 00 40 00
1C 00 00 00 00 06 00 00 00 00 00 00 00 00 00 00
            1C 00 00 00 00 00 40 00
```

(Skip rounds 1 to 22)

Round #23

After theta

```
23 DE E9 70 36 66 D5 23 91 03 C3 F1 B6 6B 93 28
69 4D 53 70 6B BA E5 B1 E5 9D C2 7E 0A 05 AD B2
50 64 AE 08 3D B0 14 9C FB 89 A8 CE 9E BA 03 4F
0F BB 2E E3 5E 01 F0 E2 4A AC FA E8 B0 11 19 00
D8 15 A2 68 94 D3 D6 73 A3 57 6E 6C B4 F0 14 5C
8B F5 47 AE E7 26 8B 54 6E E4 99 A0 C5 07 C8 83
C1 F7 03 8E 6F 5D 36 A1 B7 B6 AD B9 10 2D E1 37
A8 AD D4 4D DA BD 72 32 08 CF 7B 7F 6E A0 15 01
51 8F EB C7 1E C0 B6 08 CF 77 B8 E7 0C BA 43 70
BB 4E AB 4F 60 CA 82 5E 26 37 0A 73 AA C9 00 D9
57 78 B9 E1 BC E9 EB 13 B9 98 DD 5A FB B1 60 18
E9 0E 7E AC F3 3F F8 6C 5A 92 4F 9E FF FD 74 FF
            FD BB E9 E8 C4 A0 D4 D6
```

After rho

```
23 DE E9 70 36 66 D5 23 22 07 86 E3 6D D7 26 51
5A D3 14 DC 9A 6E 79 6C 50 D0 2A 5B DE 29 EC A7
81 A5 E0 84 22 73 45 E8 EC A9 3B F0 B4 9F 88 EA
32 EE 15 00 2F FE B0 EB 80 12 AB 3E 3A 6C 44 06
0A 51 34 CA 69 EB 39 EC 4F C1 35 7A E5 C6 46 0B
5A AC 3F 72 3D 37 59 A4 0F BA 91 67 82 16 1F 20
70 7C EB B2 09 0D BE 1F 5A C2 6F 6E 6D 5B 73 21
26 ED 5E 39 19 D4 56 EA FE DC 40 2B 02 10 9E F7
FD D8 03 D8 16 21 EA 71 21 B8 E7 3B DC 73 06 DD
59 D0 6B D7 69 F5 09 4C D9 26 37 0A 73 AA C9 00
AF 4F 5C E1 E5 86 F3 A6 E4 62 76 6B ED C7 82 61
DD C1 8F 75 FE 07 9F 2D 92 4F 9E FF FD 74 FF 5A
            B5 75 FF 6E 3A 3A 31 28
```

After pi

```
23 DE E9 70 36 66 D5 23 32 EE 15 00 2F FE B0 EB
70 7C EB B2 09 0D BE 1F 59 D0 6B D7 69 F5 09 4C
B5 75 FF 6E 3A 3A 31 28 50 D0 2A 5B DE 29 EC A7
4F C1 35 7A E5 C6 46 0B 5A AC 3F 72 3D 37 59 A4
FD D8 03 D8 16 21 EA 71 DD C1 8F 75 FE 07 9F 2D
22 07 86 E3 6D D7 26 51 80 12 AB 3E 3A 6C 44 06
5A C2 6F 6E 6D 5B 73 21 D9 26 37 0A 73 AA C9 00
AF 4F 5C E1 E5 86 F3 A6 81 A5 E0 84 22 73 45 E8
EC A9 3B F0 B4 9F 88 EA 0F BA 91 67 82 16 1F 20
21 B8 E7 3B DC 73 06 DD 92 4F 9E FF FD 74 FF 5A
5A D3 14 DC 9A 6E 79 6C 0A 51 34 CA 69 EB 39 EC
26 ED 5E 39 19 D4 56 EA FE DC 40 2B 02 10 9E F7
            E4 62 76 6B ED C7 82 61
```

After chi

```
63 CE 03 C2 36 67 DB 37 3B 6E 15 45 4F 0E B1 AB
D4 59 7F 9A 1B 07 8E 3F 5B 5A 6B C7 6D B1 CD 4F
A5 55 EB 6E 33 A2 11 E0 40 FC 20 5B C6 18 F5 03
EA 91 35 F2 E7 C6 E4 5A 5A AD B3 57 D5 31 4C A8
FD C8 23 D2 16 09 8A F3 D2 C0 9A 55 DF C1 9D 25
78 C7 C2 A3 28 C4 15 70 01 36 BB 3E 28 CC CC 06
7C 8B 27 8F E9 5F 41 87 D9 26 B5 08 7B FB CD 51
2F 5F 75 FD F7 AE B3 A0 82 B7 60 83 20 73 52 E8
CC A9 5D E8 E8 FE 88 37 9D FD 89 A3 A3 12 E6 22
20 18 87 3B DE 70 06 7D FE 47 85 8F 69 F8 77 58
7E 7F 5E ED 8A 7A 3F 6E D2 41 34 C8 6B EB B1 F9
26 CF 68 79 F4 13 56 EA E4 4D 40 BF 10 38 E7 FB
            E4 62 56 69 8C 46 82 E1
```

After iota

```
6B 4E 03 42 36 67 DB B7 3B 6E 15 45 4F 0E B1 AB
D4 59 7F 9A 1B 07 8E 3F 5B 5A 6B C7 6D B1 CD 4F
A5 55 EB 6E 33 A2 11 E0 40 FC 20 5B C6 18 F5 03
EA 91 35 F2 E7 C6 E4 5A 5A AD B3 57 D5 31 4C A8
FD C8 23 D2 16 09 8A F3 D2 C0 9A 55 DF C1 9D 25
78 C7 C2 A3 28 C4 15 70 01 36 BB 3E 28 CC CC 06
7C 8B 27 8F E9 5F 41 87 D9 26 B5 08 7B FB CD 51
2F 5F 75 FD F7 AE B3 A0 82 B7 60 83 20 73 52 E8
CC A9 5D E8 E8 FE 88 37 9D FD 89 A3 A3 12 E6 22
20 18 87 3B DE 70 06 7D FE 47 85 8F 69 F8 77 58
7E 7F 5E ED 8A 7A 3F 6E D2 41 34 C8 6B EB B1 F9
26 CF 68 79 F4 13 56 EA E4 4D 40 BF 10 38 E7 FB
            E4 62 56 69 8C 46 82 E1
```

After permutation

```
6B 4E 03 42 36 67 DB B7 3B 6E 15 45 4F 0E B1 AB
D4 59 7F 9A 1B 07 8E 3F 5B 5A 6B C7 6D B1 CD 4F
A5 55 EB 6E 33 A2 11 E0 40 FC 20 5B C6 18 F5 03
EA 91 35 F2 E7 C6 E4 5A 5A AD B3 57 D5 31 4C A8
FD C8 23 D2 16 09 8A F3 D2 C0 9A 55 DF C1 9D 25
78 C7 C2 A3 28 C4 15 70 01 36 BB 3E 28 CC CC 06
7C 8B 27 8F E9 5F 41 87 D9 26 B5 08 7B FB CD 51
2F 5F 75 FD F7 AE B3 A0 82 B7 60 83 20 73 52 E8
CC A9 5D E8 E8 FE 88 37 9D FD 89 A3 A3 12 E6 22
20 18 87 3B DE 70 06 7D FE 47 85 8F 69 F8 77 58
7E 7F 5E ED 8A 7A 3F 6E D2 41 34 C8 6B EB B1 F9
26 CF 68 79 F4 13 56 EA E4 4D 40 BF 10 38 E7 FB
            E4 62 56 69 8C 46 82 E1
```

State (as lanes of integers)

```
[0, 0] = b7db673642034e6b
[1, 0] = abb10e4f45156e3b
[2, 0] = 3f8e071b9a7f59d4
[3, 0] = 4fcdb16dc76b5a5b
[4, 0] = e011a2336eeb55a5
[0, 1] = 03f518c65b20fc40
[1, 1] = 5ae4c6e7f23591ea
[2, 1] = a84c31d557b3ad5a
[3, 1] = f38a0916d223c8fd
[4, 1] = 259dc1df559ac0d2
[0, 2] = 7015c428a3c2c778
[1, 2] = 06cccc283ebb3601
[2, 2] = 87415fe98f278b7c
[3, 2] = 51cdfb7b08b526d9
[4, 2] = a0b3aef7fd755f2f
[0, 3] = e85273208360b782
[1, 3] = 3788fee8e85da9cc
[2, 3] = 22e612a3a389fd9d
[3, 3] = 7d0670de3b871820
[4, 3] = 5877f8698f8547fe
[0, 4] = 6e3f7a8aed5e7f7e
[1, 4] = f9b1eb6bc83441d2
[2, 4] = ea5613f47968cf26
[3, 4] = fbe73810bf404de4
[4, 4] = e182468c695662e4
```

The hash value is

```
6B 4E 03 42 36 67 DB B7 3B 6E 15 45 4F 0E B1 AB
      D4 59 7F 9A 1B 07 8E 3F 5B 5A 6B C7
```

The message as bit string

```
                  1 1 0 0 1
```

XORed state (in bytes)

```
D3 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 80
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
            00 00 00 00 00 00 00 00
```

XORed state (as lanes of integers)

```
[0, 0] = 00000000000000d3
[1, 0] = 0000000000000000
[2, 0] = 0000000000000000
[3, 0] = 0000000000000000
[4, 0] = 0000000000000000
[0, 1] = 0000000000000000
[1, 1] = 0000000000000000
[2, 1] = 0000000000000000
[3, 1] = 0000000000000000
[4, 1] = 0000000000000000
[0, 2] = 0000000000000000
[1, 2] = 0000000000000000
[2, 2] = 0000000000000000
[3, 2] = 0000000000000000
[4, 2] = 0000000000000000
[0, 3] = 0000000000000000
[1, 3] = 0000000000000000
[2, 3] = 8000000000000000
[3, 3] = 0000000000000000
[4, 3] = 0000000000000000
[0, 4] = 0000000000000000
[1, 4] = 0000000000000000
[2, 4] = 0000000000000000
[3, 4] = 0000000000000000
[4, 4] = 0000000000000000
```

Round #0

After theta

```
D3 00 00 00 00 00 00 00 D2 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 80
A6 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00
D2 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 80 A6 01 00 00 00 00 00 00
00 00 00 00 00 00 00 00 D2 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 80
A6 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00
D2 00 00 00 00 00 00 00 00 00 00 00 00 00 00 80
00 00 00 00 00 00 00 80 A6 01 00 00 00 00 00 00
00 00 00 00 00 00 00 00 D2 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 80
            A6 01 00 00 00 00 00 00
```

After rho

```
D3 00 00 00 00 00 00 00 A4 01 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 08 00 00 00 00
00 00 00 30 0D 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 20 0D 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 40 00 00 00 60 1A 00 00 00 00
00 00 00 00 00 00 00 00 00 48 03 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 01 00 00 00 00
00 00 00 00 00 D3 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 40 1A 00 00 40 00 00 00 00 00 00
00 00 10 00 00 00 00 00 00 A6 01 00 00 00 00 00
00 00 00 00 00 00 00 00 48 03 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 80 00
            00 80 69 00 00 00 00 00
```

After pi

```
D3 00 00 00 00 00 00 00 00 00 00 00 00 20 0D 00
00 00 00 00 00 00 00 00 00 00 10 00 00 00 00 00
00 80 69 00 00 00 00 00 00 00 00 08 00 00 00 00
00 00 60 1A 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 40 1A 00 00 00 00 00 00 00 00 00
A4 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 01 00 00 00 00 00 A6 01 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 30 0D 00 00 00
00 00 00 00 00 00 00 00 00 48 03 00 00 00 00 00
00 40 00 00 00 00 00 00 00 00 00 00 00 00 80 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00
00 00 00 00 00 D3 00 00 00 00 00 00 00 00 00 00
            48 03 00 00 00 00 00 00
```

After chi

```
D3 00 00 00 00 00 00 00 00 00 10 00 00 20 0D 00
00 80 69 00 00 00 00 00 D3 00 10 00 00 00 00 00
00 80 69 00 00 20 0D 00 00 00 00 08 00 00 00 00
00 00 60 1A 00 40 1A 00 00 00 00 00 00 00 00 00
00 00 00 08 00 40 1A 00 00 00 60 12 00 00 00 00
A4 01 00 01 00 00 00 00 00 A6 01 00 00 00 00 00
00 00 00 01 00 00 00 00 A4 A7 01 00 00 00 00 00
00 00 00 00 00 00 00 00 00 48 03 30 0D 00 00 00
00 00 00 00 00 00 00 00 00 48 03 00 00 00 80 00
00 40 00 30 0D 00 00 00 00 00 00 00 00 00 80 00
00 00 00 00 00 D3 00 00 00 00 00 00 00 00 40 00
48 03 00 00 00 D3 00 00 00 00 00 00 00 00 00 00
            48 03 00 00 00 00 40 00
```

After iota

```
D2 00 00 00 00 00 00 00 00 00 10 00 00 20 0D 00
00 80 69 00 00 00 00 00 D3 00 10 00 00 00 00 00
00 80 69 00 00 20 0D 00 00 00 00 08 00 00 00 00
00 00 60 1A 00 40 1A 00 00 00 00 00 00 00 00 00
00 00 00 08 00 40 1A 00 00 00 60 12 00 00 00 00
A4 01 00 01 00 00 00 00 00 A6 01 00 00 00 00 00
00 00 00 01 00 00 00 00 A4 A7 01 00 00 00 00 00
00 00 00 00 00 00 00 00 00 48 03 30 0D 00 00 00
00 00 00 00 00 00 00 00 00 48 03 00 00 00 80 00
00 40 00 30 0D 00 00 00 00 00 00 00 00 00 80 00
00 00 00 00 00 D3 00 00 00 00 00 00 00 00 40 00
48 03 00 00 00 D3 00 00 00 00 00 00 00 00 00 00
            48 03 00 00 00 00 40 00
```

(Skip rounds 1 to 22)

Round #23

After theta

```
F1 B2 6C 63 94 B2 D4 96 0E 77 89 20 45 67 B5 7C
54 76 53 B2 CE 42 7B 45 AE 9C D3 5B 7D 3F CF AE
5B 7D 43 7B 5E D3 9D 8C F4 DB 13 5D 1B 41 E2 B6
46 CE 85 7D 63 60 CC 3C C5 13 00 F1 9C 26 46 A3
68 C9 F4 D7 8F 18 5A 2D 03 51 B3 76 FE 9A 0E 6D
BF 8F A8 FD 7F D7 11 34 54 ED D4 9D 1F 53 45 90
69 AC C0 01 37 37 47 30 30 86 B5 81 65 DB E4 45
E0 E7 D6 4F 28 A3 E0 80 07 AA 7C B5 8D 7A 33 8F
71 1B 55 70 8B 4C 36 EA 61 D3 13 EE B4 F3 C5 41
40 86 6C 78 8D CD 22 A5 C3 9C 81 D4 B3 0A 5F AE
1E 60 28 D1 E3 5A FD A4 F7 A3 3B 46 53 BE 04 26
26 27 89 FB B3 CA 06 B9 A2 E1 6E 85 C6 1E BB 54
            7A 50 60 9F 7C 51 80 37
```

After rho

```
F1 B2 6C 63 94 B2 D4 96 1C EE 12 41 8A CE 6A F9
95 DD 94 AC B3 D0 5E 11 F7 F3 EC EA CA 39 BD D5
9A EE 64 DC EA 1B DA F3 B5 11 24 6E 4B BF 3D D1
D8 37 06 C6 CC 63 E4 5C 68 F1 04 40 3C A7 89 D1
64 FA EB 47 0C AD 16 B4 E9 D0 36 10 35 6B E7 AF
F9 7D 44 ED FF BB 8E A0 41 52 B5 53 77 7E 4C 15
0E B8 B9 39 82 49 63 05 B6 C9 8B 60 0C 6B 03 CB
27 94 51 70 40 F0 73 EB 6A 1B F5 66 1E 0F 54 F9
0A 6E 91 C9 46 3D 6E A3 E2 A0 B0 E9 09 77 DA F9
59 A4 14 C8 90 0D AF B1 AE C3 9C 81 D4 B3 0A 5F
F5 93 7A 80 A1 44 8F 6B DC 8F EE 18 4D F9 12 98
E4 24 71 7F 56 D9 20 D7 E1 6E 85 C6 1E BB 54 A2
            E0 8D 1E 14 D8 27 5F 14
```

After pi

```
F1 B2 6C 63 94 B2 D4 96 D8 37 06 C6 CC 63 E4 5C
0E B8 B9 39 82 49 63 05 59 A4 14 C8 90 0D AF B1
E0 8D 1E 14 D8 27 5F 14 F7 F3 EC EA CA 39 BD D5
E9 D0 36 10 35 6B E7 AF F9 7D 44 ED FF BB 8E A0
0A 6E 91 C9 46 3D 6E A3 E4 24 71 7F 56 D9 20 D7
1C EE 12 41 8A CE 6A F9 68 F1 04 40 3C A7 89 D1
B6 C9 8B 60 0C 6B 03 CB AE C3 9C 81 D4 B3 0A 5F
F5 93 7A 80 A1 44 8F 6B 9A EE 64 DC EA 1B DA F3
B5 11 24 6E 4B BF 3D D1 41 52 B5 53 77 7E 4C 15
E2 A0 B0 E9 09 77 DA F9 E1 6E 85 C6 1E BB 54 A2
95 DD 94 AC B3 D0 5E 11 64 FA EB 47 0C AD 16 B4
27 94 51 70 40 F0 73 EB 6A 1B F5 66 1E 0F 54 F9
            DC 8F EE 18 4D F9 12 98
```

After chi

```
F7 3A D5 5A 96 BA D7 97 89 33 02 06 DC 67 68 EC
AE B1 B3 2D CA 6B 33 01 48 96 74 AB 94 9D 2F 33
E8 88 1C 90 90 66 7F 5C E7 DE AC 07 00 A9 B5 D5
EB D2 A7 10 35 6F 87 AC 1D 7D 24 DB EF 7B 8E F4
19 BD 1D 49 CE 1D F3 A3 EC 24 63 6F 63 9B 62 FD
8A E6 99 61 8A 86 68 F3 60 F3 10 C1 EC 37 81 C5
E7 D9 E9 60 2D 2F 86 EB A6 AF 9C C0 DE 39 6A CF
95 82 7E 80 95 65 0E 6B DA AC F5 CD DE 5B 9A F7
17 B1 24 C6 43 BE AF 39 40 1C B0 55 61 F6 48 17
F8 20 D0 F1 E9 77 50 A8 C4 7F 85 E4 1F 1F 71 A2
96 D9 84 9C F3 80 3F 5A 2C F1 4F 41 12 A2 12 A4
B3 10 5B 68 01 00 71 EB 6B 4B E5 C2 AC 0F 18 F8
            BC AD 85 5B 41 D4 12 3C
```

After iota

```
FF BA D5 DA 96 BA D7 17 89 33 02 06 DC 67 68 EC
AE B1 B3 2D CA 6B 33 01 48 96 74 AB 94 9D 2F 33
E8 88 1C 90 90 66 7F 5C E7 DE AC 07 00 A9 B5 D5
EB D2 A7 10 35 6F 87 AC 1D 7D 24 DB EF 7B 8E F4
19 BD 1D 49 CE 1D F3 A3 EC 24 63 6F 63 9B 62 FD
8A E6 99 61 8A 86 68 F3 60 F3 10 C1 EC 37 81 C5
E7 D9 E9 60 2D 2F 86 EB A6 AF 9C C0 DE 39 6A CF
95 82 7E 80 95 65 0E 6B DA AC F5 CD DE 5B 9A F7
17 B1 24 C6 43 BE AF 39 40 1C B0 55 61 F6 48 17
F8 20 D0 F1 E9 77 50 A8 C4 7F 85 E4 1F 1F 71 A2
96 D9 84 9C F3 80 3F 5A 2C F1 4F 41 12 A2 12 A4
B3 10 5B 68 01 00 71 EB 6B 4B E5 C2 AC 0F 18 F8
            BC AD 85 5B 41 D4 12 3C
```

After permutation

```
FF BA D5 DA 96 BA D7 17 89 33 02 06 DC 67 68 EC
AE B1 B3 2D CA 6B 33 01 48 96 74 AB 94 9D 2F 33
E8 88 1C 90 90 66 7F 5C E7 DE AC 07 00 A9 B5 D5
EB D2 A7 10 35 6F 87 AC 1D 7D 24 DB EF 7B 8E F4
19 BD 1D 49 CE 1D F3 A3 EC 24 63 6F 63 9B 62 FD
8A E6 99 61 8A 86 68 F3 60 F3 10 C1 EC 37 81 C5
E7 D9 E9 60 2D 2F 86 EB A6 AF 9C C0 DE 39 6A CF
95 82 7E 80 95 65 0E 6B DA AC F5 CD DE 5B 9A F7
17 B1 24 C6 43 BE AF 39 40 1C B0 55 61 F6 48 17
F8 20 D0 F1 E9 77 50 A8 C4 7F 85 E4 1F 1F 71 A2
96 D9 84 9C F3 80 3F 5A 2C F1 4F 41 12 A2 12 A4
B3 10 5B 68 01 00 71 EB 6B 4B E5 C2 AC 0F 18 F8
            BC AD 85 5B 41 D4 12 3C
```

State (as lanes of integers)

```
[0, 0] = 17d7ba96dad5baff
[1, 0] = ec6867dc06023389
[2, 0] = 01336bca2db3b1ae
[3, 0] = 332f9d94ab749648
[4, 0] = 5c7f6690901c88e8
[0, 1] = d5b5a90007acdee7
[1, 1] = ac876f3510a7d2eb
[2, 1] = f48e7befdb247d1d
[3, 1] = a3f31dce491dbd19
[4, 1] = fd629b636f6324ec
[0, 2] = f368868a6199e68a
[1, 2] = c58137ecc110f360
[2, 2] = eb862f2d60e9d9e7
[3, 2] = cf6a39dec09cafa6
[4, 2] = 6b0e6595807e8295
[0, 3] = f79a5bdecdf5acda
[1, 3] = 39afbe43c624b117
[2, 3] = 1748f66155b01c40
[3, 3] = a85077e9f1d020f8
[4, 3] = a2711f1fe4857fc4
[0, 4] = 5a3f80f39c84d996
[1, 4] = a412a212414ff12c
[2, 4] = eb710001685b10b3
[3, 4] = f8180facc2e54b6b
[4, 4] = 3c12d4415b85adbc
```

The hash value is

```
FF BA D5 DA 96 BA D7 17 89 33 02 06 DC 67 68 EC
      AE B1 B3 2D CA 6B 33 01 48 96 74 AB
```

SHA3-224 sample

The message as bit string

```
1 1 0 0 1 0 1 0 0 0 0 1 1 0 1 0 1 1 0 1 1 1 1 0 1 0 0 1 1 0
```

XORed state (in bytes)

```
53 58 7B 99 01 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 80
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
```

```
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
               00 00 00 00 00 00 00 00
```

XORed state (as lanes of integers)

```
[0, 0] = 00000001997b5853
[1, 0] = 0000000000000000
[2, 0] = 0000000000000000
[3, 0] = 0000000000000000
[4, 0] = 0000000000000000
[0, 1] = 0000000000000000
[1, 1] = 0000000000000000
[2, 1] = 0000000000000000
[3, 1] = 0000000000000000
[4, 1] = 0000000000000000
[0, 2] = 0000000000000000
[1, 2] = 0000000000000000
[2, 2] = 0000000000000000
[3, 2] = 0000000000000000
[4, 2] = 0000000000000000
[0, 3] = 0000000000000000
[1, 3] = 0000000000000000
[2, 3] = 8000000000000000
[3, 3] = 0000000000000000
[4, 3] = 0000000000000000
[0, 4] = 0000000000000000
[1, 4] = 0000000000000000
[2, 4] = 0000000000000000
[3, 4] = 0000000000000000
[4, 4] = 0000000000000000
```

Round #0

After theta

```
53 58 7B 99 01 00 00 00 52 58 7B 99 01 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 80
A6 B0 F6 32 03 00 00 00 00 00 00 00 00 00 00 00
52 58 7B 99 01 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 80 A6 B0 F6 32 03 00 00 00
00 00 00 00 00 00 00 00 52 58 7B 99 01 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 80
A6 B0 F6 32 03 00 00 00 00 00 00 00 00 00 00 00
52 58 7B 99 01 00 00 00 00 00 00 00 00 00 00 80
00 00 00 00 00 00 00 80 A6 B0 F6 32 03 00 00 00
00 00 00 00 00 00 00 00 52 58 7B 99 01 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 80
               A6 B0 F6 32 03 00 00 00
```

After rho

```
53 58 7B 99 01 00 00 00 A4 B0 F6 32 03 00 00 00
00 00 00 00 00 00 00 00 00 00 00 08 00 00 00 00
00 00 00 30 85 B5 97 19 00 00 00 00 00 00 00 00
97 19 00 00 00 20 85 B5 00 00 00 00 00 00 00 00
00 00 00 00 00 00 40 00 00 00 60 0A 6B 2F 33 00
00 00 00 00 00 00 00 00 00 48 61 ED 65 06 00 00
00 00 00 00 00 00 00 00 00 00 00 01 00 00 00 00
99 01 00 00 00 53 58 7B 00 00 00 00 00 00 00 00
2F 33 00 00 00 40 0A 6B 00 40 00 00 00 00 00 00
00 00 10 00 00 00 00 00 00 A6 B0 F6 32 03 00 00
00 00 00 00 00 00 00 00 48 61 ED 65 06 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 80 00
               00 80 29 AC BD CC 00 00
```

After pi

```
53 58 7B 99 01 00 00 00 97 19 00 00 00 20 85 B5
00 00 00 00 00 00 00 00 00 00 10 00 00 00 00 00
00 80 29 AC BD CC 00 00 00 00 00 08 00 00 00 00
00 00 60 0A 6B 2F 33 00 00 00 00 00 00 00 00 00
2F 33 00 00 00 40 0A 6B 00 00 00 00 00 00 00 00
A4 B0 F6 32 03 00 00 00 00 00 00 00 00 00 00 00
00 00 00 01 00 00 00 00 00 A6 B0 F6 32 03 00 00
00 00 00 00 00 00 00 00 00 00 00 30 85 B5 97 19
00 00 00 00 00 00 00 00 00 48 61 ED 65 06 00 00
00 40 00 00 00 00 00 00 00 00 00 00 00 00 80 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00
99 01 00 00 00 53 58 7B 00 00 00 00 00 00 00 00
            48 61 ED 65 06 00 00 00
```

After chi

```
53 58 7B 99 01 00 00 00 97 19 10 00 00 20 85 B5
00 80 29 AC BD CC 00 00 53 58 42 11 00 00 00 00
84 81 29 AC BD EC 85 B5 00 00 00 08 00 00 00 00
2F 33 60 0A 6B 6F 39 6B 00 00 00 00 00 00 00 00
2F 33 00 08 00 40 0A 6B 00 00 60 02 6B 2F 33 00
A4 B0 F6 33 03 00 00 00 00 A6 B0 F6 32 03 00 00
00 00 00 01 00 00 00 00 A4 16 46 C4 31 03 00 00
00 00 00 00 00 00 00 00 00 48 61 DD E0 B3 97 19
00 00 00 00 00 00 00 00 00 48 61 ED 65 06 80 00
00 40 00 30 85 B5 17 19 00 00 00 00 00 00 80 00
99 01 00 00 00 53 18 7B 00 00 00 00 00 00 40 00
D1 60 ED 65 06 53 58 7B 00 00 00 00 00 00 00 00
            48 61 ED 65 06 00 40 00
```

After iota

```
52 58 7B 99 01 00 00 00 97 19 10 00 00 20 85 B5
00 80 29 AC BD CC 00 00 53 58 42 11 00 00 00 00
84 81 29 AC BD EC 85 B5 00 00 00 08 00 00 00 00
2F 33 60 0A 6B 6F 39 6B 00 00 00 00 00 00 00 00
2F 33 00 08 00 40 0A 6B 00 00 60 02 6B 2F 33 00
A4 B0 F6 33 03 00 00 00 00 A6 B0 F6 32 03 00 00
00 00 00 01 00 00 00 00 A4 16 46 C4 31 03 00 00
00 00 00 00 00 00 00 00 00 48 61 DD E0 B3 97 19
00 00 00 00 00 00 00 00 00 48 61 ED 65 06 80 00
00 40 00 30 85 B5 17 19 00 00 00 00 00 00 80 00
99 01 00 00 00 53 18 7B 00 00 00 00 00 00 40 00
D1 60 ED 65 06 53 58 7B 00 00 00 00 00 00 00 00
            48 61 ED 65 06 00 40 00
```

(Skip rounds 1 to 22)

Round #23

After theta

```
CE E6 EC 95 C4 F1 D8 BE 89 31 6B F4 37 BB C3 10
46 14 61 DF BC 87 EF 0F 7C 55 5A 24 86 54 37 D8
E0 AC 13 D8 C4 E5 DC 0C BC DD EA C7 B1 17 C3 F5
41 48 C6 E8 05 49 7A 33 D1 C3 AD 43 DF 01 5E E4
AF EA B8 23 BA 81 44 F2 56 FF D3 33 B8 A2 FF 0D
66 1F C1 21 27 77 E0 C1 ED D6 CD 84 64 57 02 47
4F 6C 0F 52 20 B9 70 E3 95 51 E1 60 70 06 90 DD
B2 8C 8D 91 20 D9 F9 1D 8A 76 62 3E 60 C1 97 44
37 A2 56 38 9C 16 44 AE FD 9C 49 06 FA 9C 97 F4
F7 3D FF 14 64 81 29 FA 0C 03 CB 10 7C 02 86 C2
E6 06 57 D7 E2 04 71 0E 66 BA 6D 70 70 41 C2 7E
40 7A 6A 65 1B F2 98 0C 22 EB 06 C8 20 08 1E B5
            76 CB 0C 95 A6 57 FB B1
```

After rho

```
CE E6 EC 95 C4 F1 D8 BE 12 63 D6 E8 6F 76 87 21
11 45 D8 37 EF E1 FB 83 48 75 83 CD 57 A5 45 62
2E E7 66 00 67 9D C0 26 1C 7B 31 5C CF DB AD 7E
8C 5E 90 A4 37 13 84 64 79 F4 70 EB D0 77 80 17
75 DC 11 DD 40 22 F9 57 FA DF 60 F5 3F 3D 83 2B
36 FB 08 0E 39 B9 03 0F 1C B5 5B 37 13 92 5D 09
90 02 C9 85 1B 7F 62 7B 0C 20 BB 2B A3 C2 C1 E0
48 90 EC FC 0E 59 C6 C6 7C C0 82 2F 89 14 ED C4
0A 87 D3 82 C8 F5 46 D4 4B FA 7E CE 24 03 7D CE
30 45 FF BE E7 9F 82 2C C2 0C 03 CB 10 7C 02 86
C4 39 98 1B 5C 5D 8B 13 99 E9 B6 C1 C1 05 09 FB
48 4F AD 6C 43 1E 93 01 EB 06 C8 20 08 1E B5 22
            7E AC DD 32 43 A5 E9 D5
```

After pi

```
CE E6 EC 95 C4 F1 D8 BE 8C 5E 90 A4 37 13 84 64
90 02 C9 85 1B 7F 62 7B 30 45 FF BE E7 9F 82 2C
7E AC DD 32 43 A5 E9 D5 48 75 83 CD 57 A5 45 62
FA DF 60 F5 3F 3D 83 2B 36 FB 08 0E 39 B9 03 0F
0A 87 D3 82 C8 F5 46 D4 48 4F AD 6C 43 1E 93 01
12 63 D6 E8 6F 76 87 21 79 F4 70 EB D0 77 80 17
0C 20 BB 2B A3 C2 C1 E0 C2 0C 03 CB 10 7C 02 86
C4 39 98 1B 5C 5D 8B 13 2E E7 66 00 67 9D C0 26
1C 7B 31 5C CF DB AD 7E 1C B5 5B 37 13 92 5D 09
4B FA 7E CE 24 03 7D CE EB 06 C8 20 08 1E B5 22
11 45 D8 37 EF E1 FB 83 75 DC 11 DD 40 22 F9 57
48 90 EC FC 0E 59 C6 C6 7C C0 82 2F 89 14 ED C4
            99 E9 B6 C1 C1 05 09 FB
```

After chi

```
DE E6 A5 94 CC 9D BA A5 AC 1B A6 9E D3 93 04 60
DE AA C9 85 1B 5F 0B AA B0 07 DF 3B 63 CF 92 06
7E B4 CD 12 70 A7 ED 95 4C 55 8B C7 57 25 45 66
F2 DB B3 75 FF 79 C7 FB 76 B3 24 62 3A B3 92 0E
0A B7 D1 03 DC 54 02 B6 FA C5 CD 5C 6B 06 11 08
16 63 5D E8 4C F6 C6 C1 BB F8 70 2B C0 4B 82 11
08 11 23 3B EF C3 48 F1 D0 4E 45 2B 33 5E 06 A6
AD AD B8 18 CC 5C 8B 05 2E 63 2C 23 77 9D 90 27
5F 31 15 94 EB DA 8D B8 BC B1 DB 17 1B 8E DD 29
4F 1B 58 CE 43 82 3D CA FB 1E D9 7C 80 5C 98 7A
19 45 34 17 E1 B8 FD 03 41 9C 13 DE C1 26 D0 57
C9 B9 D8 3C 4E 58 C6 FD 7C C4 CA 19 A7 F4 1F C4
            FD 71 B7 09 C1 07 09 AF
```

After iota

```
D6 66 A5 14 CC 9D BA 25 AC 1B A6 9E D3 93 04 60
DE AA C9 85 1B 5F 0B AA B0 07 DF 3B 63 CF 92 06
7E B4 CD 12 70 A7 ED 95 4C 55 8B C7 57 25 45 66
F2 DB B3 75 FF 79 C7 FB 76 B3 24 62 3A B3 92 0E
0A B7 D1 03 DC 54 02 B6 FA C5 CD 5C 6B 06 11 08
16 63 5D E8 4C F6 C6 C1 BB F8 70 2B C0 4B 82 11
08 11 23 3B EF C3 48 F1 D0 4E 45 2B 33 5E 06 A6
AD AD B8 18 CC 5C 8B 05 2E 63 2C 23 77 9D 90 27
5F 31 15 94 EB DA 8D B8 BC B1 DB 17 1B 8E DD 29
4F 1B 58 CE 43 82 3D CA FB 1E D9 7C 80 5C 98 7A
19 45 34 17 E1 B8 FD 03 41 9C 13 DE C1 26 D0 57
C9 B9 D8 3C 4E 58 C6 FD 7C C4 CA 19 A7 F4 1F C4
            FD 71 B7 09 C1 07 09 AF
```

After permutation

```
D6 66 A5 14 CC 9D BA 25 AC 1B A6 9E D3 93 04 60
DE AA C9 85 1B 5F 0B AA B0 07 DF 3B 63 CF 92 06
7E B4 CD 12 70 A7 ED 95 4C 55 8B C7 57 25 45 66
F2 DB B3 75 FF 79 C7 FB 76 B3 24 62 3A B3 92 0E
0A B7 D1 03 DC 54 02 B6 FA C5 CD 5C 6B 06 11 08
16 63 5D E8 4C F6 C6 C1 BB F8 70 2B C0 4B 82 11
08 11 23 3B EF C3 48 F1 D0 4E 45 2B 33 5E 06 A6
AD AD B8 18 CC 5C 8B 05 2E 63 2C 23 77 9D 90 27
5F 31 15 94 EB DA 8D B8 BC B1 DB 17 1B 8E DD 29
4F 1B 58 CE 43 82 3D CA FB 1E D9 7C 80 5C 98 7A
19 45 34 17 E1 B8 FD 03 41 9C 13 DE C1 26 D0 57
C9 B9 D8 3C 4E 58 C6 FD 7C C4 CA 19 A7 F4 1F C4
           FD 71 B7 09 C1 07 09 AF
```

State (as lanes of integers)

```
[0, 0] = 25ba9dcc14a566d6
[1, 0] = 600493d39ea61bac
[2, 0] = aa0b5f1b85c9aade
[3, 0] = 0692cf633bdf07b0
[4, 0] = 95eda77012cdb47e
[0, 1] = 66452557c78b554c
[1, 1] = fbc779ff75b3dbf2
[2, 1] = 0e92b33a6224b376
[3, 1] = b60254dc03d1b70a
[4, 1] = 0811066b5ccdc5fa
[0, 2] = c1c6f64ce85d6316
[1, 2] = 11824bc02b70f8bb
[2, 2] = f148c3ef3b231108
[3, 2] = a6065e332b454ed0
[4, 2] = 058b5ccc18b8adad
[0, 3] = 27909d77232c632e
[1, 3] = b88ddaeb9415315f
[2, 3] = 29dd8e1b17dbb1bc
[3, 3] = ca3d8243ce581b4f
[4, 3] = 7a985c807cd91efb
[0, 4] = 03fdb8e117344519
[1, 4] = 57d026c1de139c41
[2, 4] = fdc6584e3cd8b9c9
[3, 4] = c41ff4a719cac47c
[4, 4] = af0907c109b771fd
```

The hash value is

```
D6 66 A5 14 CC 9D BA 25 AC 1B A6 9E D3 93 04 60
      DE AA C9 85 1B 5F 0B AA B0 07 DF 3B
```

B.16 Dedicated Hash-Function 14 (SHA3-256)

NOTE 1 Data is presented in three different ways: bit strings, byte strings and *w*-length words (for the lanes).

NOTE 2 Bit strings are the sequence of bits from left to right.

NOTE 3 Byte strings are the bytes from left to right and the bits within the byte are right to left.

NOTE 4 Words are the integer representation of the values in the lanes.

SHA3-256 sample

The message as bit string

```
(empty message)
```

XORed state (in bytes)

```
06 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 80 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
   00 00 00 00 00 00 00 00
```

XORed state (as lanes of integers)

```
[0, 0] = 0000000000000006
[1, 0] = 0000000000000000
[2, 0] = 0000000000000000
[3, 0] = 0000000000000000
[4, 0] = 0000000000000000
[0, 1] = 0000000000000000
[1, 1] = 0000000000000000
[2, 1] = 0000000000000000
[3, 1] = 0000000000000000
[4, 1] = 0000000000000000
[0, 2] = 0000000000000000
[1, 2] = 0000000000000000
[2, 2] = 0000000000000000
[3, 2] = 0000000000000000
[4, 2] = 0000000000000000
[0, 3] = 0000000000000000
[1, 3] = 8000000000000000
[2, 3] = 0000000000000000
[3, 3] = 0000000000000000
[4, 3] = 0000000000000000
[0, 4] = 0000000000000000
[1, 4] = 0000000000000000
[2, 4] = 0000000000000000
[3, 4] = 0000000000000000
[4, 4] = 0000000000000000
```

Round #0

After theta

```
07 00 00 00 00 00 00 00 06 00 00 00 00 00 00 00
00 00 00 00 00 00 00 80 00 00 00 00 00 00 00 00
0C 00 00 00 00 00 00 00 01 00 00 00 00 00 00 00
06 00 00 00 00 00 00 00 00 00 00 00 00 00 00 80
00 00 00 00 00 00 00 00 0C 00 00 00 00 00 00 00
01 00 00 00 00 00 00 00 06 00 00 00 00 00 00 00
00 00 00 00 00 00 00 80 00 00 00 00 00 00 00 00
0C 00 00 00 00 00 00 00 01 00 00 00 00 00 00 00
06 00 00 00 00 00 00 80 00 00 00 00 00 00 00 80
00 00 00 00 00 00 00 00 0C 00 00 00 00 00 00 00
01 00 00 00 00 00 00 00 06 00 00 00 00 00 00 00
00 00 00 00 00 00 00 80 00 00 00 00 00 00 00 00
   0C 00 00 00 00 00 00 00
```

After rho

```
07 00 00 00 00 00 00 00 0C 00 00 00 00 00 00 00
00 00 00 00 00 00 00 20 00 00 00 00 00 00 00 00
00 00 00 60 00 00 00 00 00 00 00 00 10 00 00 00
00 00 00 00 00 60 00 00 20 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 C0 00 00 00 00 00
08 00 00 00 00 00 00 00 00 18 00 00 00 00 00 00
00 00 00 00 00 04 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 06 00 00 00 00 00 00 00 02 00 00
00 00 00 00 00 D0 00 00 00 40 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 0C 00 00 00 00 00 00
00 00 04 00 00 00 00 00 18 00 00 00 00 00 00 00
00 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00
            00 00 03 00 00 00 00 00
```

After pi

```
07 00 00 00 00 00 00 00 00 00 00 00 00 60 00 00
00 00 00 00 00 04 00 00 00 00 00 00 00 00 00 00
00 00 03 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 C0 00 00 00 00 00 08 00 00 00 00 00 00 00
00 00 00 00 00 D0 00 00 00 00 00 00 00 00 00 10
0C 00 00 00 00 00 00 00 20 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 0C 00 00 00 00 00 00
00 00 04 00 00 00 00 00 00 00 00 60 00 00 00 00
00 00 00 00 10 00 00 00 00 18 00 00 00 00 00 00
00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 20 00 00 00 00 00 00 00 00
00 00 00 00 00 06 00 00 00 00 00 00 00 02 00 00
            18 00 00 00 00 00 00 00
```

After chi

```
07 00 00 00 00 04 00 00 00 00 00 00 00 60 00 00
00 00 03 00 00 04 00 00 07 00 00 00 00 00 00 00
00 00 03 00 00 60 00 00 08 00 00 00 00 00 00 00
00 00 C0 00 00 D0 00 00 08 00 00 00 00 00 00 10
00 00 00 00 00 D0 00 00 00 00 C0 00 00 00 00 10
0C 00 00 00 00 00 00 00 20 0C 00 00 00 00 00 00
00 00 04 00 00 00 00 00 0C 0C 00 00 00 00 00 00
20 00 04 00 00 00 00 00 00 18 00 60 00 00 00 00
00 40 00 00 10 00 00 00 00 18 00 00 00 00 00 00
00 40 00 60 00 00 00 00 00 00 00 00 10 00 00 00
00 00 00 00 00 06 00 20 00 00 00 00 00 00 00 00
18 00 00 00 00 06 00 00 00 00 00 00 00 02 00 20
            18 00 00 00 00 00 00 00
```

After iota

```
06 00 00 00 00 04 00 00 00 00 00 00 00 60 00 00
00 00 03 00 00 04 00 00 07 00 00 00 00 00 00 00
00 00 03 00 00 60 00 00 08 00 00 00 00 00 00 00
00 00 C0 00 00 D0 00 00 08 00 00 00 00 00 00 10
00 00 00 00 00 D0 00 00 00 00 C0 00 00 00 00 10
0C 00 00 00 00 00 00 00 20 0C 00 00 00 00 00 00
00 00 04 00 00 00 00 00 0C 0C 00 00 00 00 00 00
20 00 04 00 00 00 00 00 00 18 00 60 00 00 00 00
00 40 00 00 10 00 00 00 00 18 00 00 00 00 00 00
00 40 00 60 00 00 00 00 00 00 00 00 10 00 00 00
00 00 00 00 00 06 00 20 00 00 00 00 00 00 00 00
18 00 00 00 00 06 00 00 00 00 00 00 00 02 00 20
            18 00 00 00 00 00 00 00
```

(Skip rounds 1 to 22)

Round #23

After theta

```
0B 59 CE D1 EF 06 FE FE 38 5F F6 8E 93 9E 40 E5
5C 66 DE 34 99 D3 D8 DF 14 D8 1D F8 4A 47 49 28
15 4F 96 4D 0E 22 B1 D5 B4 62 AC E5 B1 0B AD 03
0A 6D B6 05 78 44 B5 5A 5E 88 06 49 2D E1 CA CF
17 B9 7C 0D 52 BF BE CA 53 F7 B5 93 4F 90 44 7B
23 24 0F FF BE F7 13 6A 20 81 F5 70 53 F7 98 2E
27 5F AB DE 54 A9 1F 3A 59 23 6F 17 94 8D 53 92
B1 16 1C B0 07 E9 00 04 A9 4B 50 26 B1 5C D7 A3
67 21 C4 76 20 9F C7 C0 55 30 C6 37 91 76 45 95
5A 58 E2 7F B2 5A 0C 56 0A C2 D2 F7 03 FC DB 89
6B BB A0 28 1A 30 B3 50 AB D5 DE D6 45 89 84 46
03 A7 B8 A6 97 C5 08 C3 99 28 E1 5B 2E 90 19 BD
            FF CE D2 28 CF 8B 0B 98
```

After rho

```
0B 59 CE D1 EF 06 FE FE 71 BE EC 1D 27 3D 81 CA
97 99 37 4D E6 34 F6 37 74 94 84 42 81 DD 81 AF
10 89 AD AE 78 B2 6C 72 1E BB D0 3A 40 2B C6 5A
5B 80 47 54 AB A5 D0 66 B3 17 A2 41 52 4B B8 F2
5C BE 06 A9 5F 5F E5 8B 49 B4 37 75 5F 3B F9 04
1B 21 79 F8 F7 BD 9F 50 BA 80 04 D6 C3 4D DD 63
F5 A6 4A FD D0 39 F9 5A 1B A7 24 B3 46 DE 2E 28
D8 83 74 00 82 58 0B 0E 4C 62 B9 AE 47 53 97 A0
D8 0E E4 F3 18 F8 2C 84 A2 CA 2A 18 E3 9B 48 BB
8B C1 4A 0B 4B FC 4F 56 89 0A C2 D2 F7 03 FC DB
CC 42 AD ED 82 A2 68 C0 AD 56 7B 5B 17 25 12 1A
E0 14 D7 F4 B2 18 61 78 28 E1 5B 2E 90 19 BD 99
            02 E6 BF B3 34 CA F3 E2
```

After pi

```
0B 59 CE D1 EF 06 FE FE 5B 80 47 54 AB A5 D0 66
F5 A6 4A FD D0 39 F9 5A 8B C1 4A 0B 4B FC 4F 56
02 E6 BF B3 34 CA F3 E2 74 94 84 42 81 DD 81 AF
49 B4 37 75 5F 3B F9 04 1B 21 79 F8 F7 BD 9F 50
D8 0E E4 F3 18 F8 2C 84 E0 14 D7 F4 B2 18 61 78
71 BE EC 1D 27 3D 81 CA B3 17 A2 41 52 4B B8 F2
1B A7 24 B3 46 DE 2E 28 89 0A C2 D2 F7 03 FC DB
CC 42 AD ED 82 A2 68 C0 10 89 AD AE 78 B2 6C 72
1E BB D0 3A 40 2B C6 5A BA 80 04 D6 C3 4D DD 63
A2 CA 2A 18 E3 9B 48 BB 28 E1 5B 2E 90 19 BD 99
97 99 37 4D E6 34 F6 37 5C BE 06 A9 5F 5F E5 8B
D8 83 74 00 82 58 0B 0E 4C 62 B9 AE 47 53 97 A0
            AD 56 7B 5B 17 25 12 1A
```

After chi

```
AF 7F C6 78 BF 1E D7 E6 51 C1 47 56 A0 61 D6 62
F5 80 FF 4D E4 3B 49 FA 82 D8 0A 4B 80 F8 43 4A
52 66 BE B7 34 6B F3 E2 66 95 CC CA 21 59 87 FF
89 BA B3 76 57 7B D9 80 3B 31 6A FC 55 BD DE 28
CC 8E E4 F1 19 3D AC 03 E9 34 E4 C1 EC 3A 19 78
79 1E E8 AF 23 A9 87 C2 33 1F 60 01 E3 4A 68 21
5F E7 09 9E 46 7E 2E 28 B8 B6 82 C2 D2 1E 7D D1
4E 43 AF AD D2 E0 50 F0 B0 89 A9 6A FB F6 75 53
1E F1 FA 32 60 B9 C6 C2 B2 A1 55 F0 D3 4D 68 63
B2 C2 8E 98 8B 39 08 D9 26 D3 0B 3E 90 10 3F 91
17 98 47 4D 66 34 FC 33 58 DE 8F 07 1A 5C 71 2B
79 97 36 51 92 7C 0B 14 5E EB BD AA A7 43 73 85
            E5 70 7B FB 0E 6E 13 92
```

After iota

```
A7 FF C6 F8 BF 1E D7 66 51 C1 47 56 A0 61 D6 62
F5 80 FF 4D E4 3B 49 FA 82 D8 0A 4B 80 F8 43 4A
52 66 BE B7 34 6B F3 E2 66 95 CC CA 21 59 87 FF
89 BA B3 76 57 7B D9 80 3B 31 6A FC 55 BD DE 28
CC 8E E4 F1 19 3D AC 03 E9 34 E4 C1 EC 3A 19 78
79 1E E8 AF 23 A9 87 C2 33 1F 60 01 E3 4A 68 21
5F E7 09 9E 46 7E 2E 28 B8 B6 82 C2 D2 1E 7D D1
4E 43 AF AD D2 E0 50 F0 B0 89 A9 6A FB F6 75 53
1E F1 FA 32 60 B9 C6 C2 B2 A1 55 F0 D3 4D 68 63
B2 C2 8E 98 8B 39 08 D9 26 D3 0B 3E 90 10 3F 91
17 98 47 4D 66 34 FC 33 58 DE 8F 07 1A 5C 71 2B
79 97 36 51 92 7C 0B 14 5E EB BD AA A7 43 73 85
            E5 70 7B FB 0E 6E 13 92
```

After permutation

```
A7 FF C6 F8 BF 1E D7 66 51 C1 47 56 A0 61 D6 62
F5 80 FF 4D E4 3B 49 FA 82 D8 0A 4B 80 F8 43 4A
52 66 BE B7 34 6B F3 E2 66 95 CC CA 21 59 87 FF
89 BA B3 76 57 7B D9 80 3B 31 6A FC 55 BD DE 28
CC 8E E4 F1 19 3D AC 03 E9 34 E4 C1 EC 3A 19 78
79 1E E8 AF 23 A9 87 C2 33 1F 60 01 E3 4A 68 21
5F E7 09 9E 46 7E 2E 28 B8 B6 82 C2 D2 1E 7D D1
4E 43 AF AD D2 E0 50 F0 B0 89 A9 6A FB F6 75 53
1E F1 FA 32 60 B9 C6 C2 B2 A1 55 F0 D3 4D 68 63
B2 C2 8E 98 8B 39 08 D9 26 D3 0B 3E 90 10 3F 91
17 98 47 4D 66 34 FC 33 58 DE 8F 07 1A 5C 71 2B
79 97 36 51 92 7C 0B 14 5E EB BD AA A7 43 73 85
            E5 70 7B FB 0E 6E 13 92
```

State (as lanes of integers)

```
[0, 0] = 66d71ebff8c6ffa7
[1, 0] = 62d661a05647c151
[2, 0] = fa493be44dff80f5
[3, 0] = 4a43f8804b0ad882
[4, 0] = e2f36b34b7be6652
[0, 1] = ff875921cacc9566
[1, 1] = 80d97b5776b3ba89
[2, 1] = 28debd55fc6a313b
[3, 1] = 03ac3d19f1e48ecc
[4, 1] = 78193aecc1e434e9
[0, 2] = c287a923afe81e79
[1, 2] = 21684ae301601f33
[2, 2] = 282e7e469e09e75f
[3, 2] = d17d1ed2c282b6b8
[4, 2] = f050e0d2adaf434e
[0, 3] = 5375f6fb6aa989b0
[1, 3] = c2c6b96032faf11e
[2, 3] = 63684dd3f055a1b2
[3, 3] = d908398b988ec2b2
[4, 3] = 913f10903e0bd326
[0, 4] = 33fc34664d479817
[1, 4] = 2b715c1a078fde58
[2, 4] = 140b7c9251369779
[3, 4] = 857343a7aabdeb5e
[4, 4] = 92136e0efb7b70e5
```

The hash value is

```
A7 FF C6 F8 … 80 F8 43 4A
```

The message as bit string

```
1 1 0 0 1
```

XORed state (in bytes)

```
D3 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 80 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
   00 00 00 00 00 00 00 00
```

XORed state (as lanes of integers)

```
[0, 0] = 00000000000000d3
[1, 0] = 0000000000000000
[2, 0] = 0000000000000000
[3, 0] = 0000000000000000
[4, 0] = 0000000000000000
[0, 1] = 0000000000000000
[1, 1] = 0000000000000000
[2, 1] = 0000000000000000
[3, 1] = 0000000000000000
[4, 1] = 0000000000000000
[0, 2] = 0000000000000000
[1, 2] = 0000000000000000
[2, 2] = 0000000000000000
[3, 2] = 0000000000000000
[4, 2] = 0000000000000000
[0, 3] = 0000000000000000
[1, 3] = 8000000000000000
[2, 3] = 0000000000000000
[3, 3] = 0000000000000000
[4, 3] = 0000000000000000
[0, 4] = 0000000000000000
[1, 4] = 0000000000000000
[2, 4] = 0000000000000000
[3, 4] = 0000000000000000
[4, 4] = 0000000000000000
```

Round #0

After theta

```
D2 00 00 00 00 00 00 00 D3 00 00 00 00 00 00 00
00 00 00 00 00 00 00 80 00 00 00 00 00 00 00 00
A6 01 00 00 00 00 00 00 01 00 00 00 00 00 00 00
D3 00 00 00 00 00 00 00 00 00 00 00 00 00 00 80
00 00 00 00 00 00 00 00 A6 01 00 00 00 00 00 00
01 00 00 00 00 00 00 00 D3 00 00 00 00 00 00 00
00 00 00 00 00 00 00 80 00 00 00 00 00 00 00 00
A6 01 00 00 00 00 00 00 01 00 00 00 00 00 00 00
D3 00 00 00 00 00 00 80 00 00 00 00 00 00 00 80
00 00 00 00 00 00 00 00 A6 01 00 00 00 00 00 00
01 00 00 00 00 00 00 00 D3 00 00 00 00 00 00 00
00 00 00 00 00 00 00 80 00 00 00 00 00 00 00 00
   A6 01 00 00 00 00 00 00
```

After rho

```
D2 00 00 00 00 00 00 00 A6 01 00 00 00 00 00 00
00 00 00 00 00 00 00 20 00 00 00 00 00 00 00 00
00 00 00 30 0D 00 00 00 00 00 00 00 10 00 00 00
00 00 00 00 00 30 0D 00 20 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 60 1A 00 00 00 00
08 00 00 00 00 00 00 00 00 4C 03 00 00 00 00 00
00 00 00 00 00 04 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 D3 00 00 00 00 00 00 00 02 00 00
00 00 00 00 00 70 1A 00 00 40 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 A6 01 00 00 00 00 00
00 00 04 00 00 00 00 00 4C 03 00 00 00 00 00 00
00 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00
            00 80 69 00 00 00 00 00
```

After pi

```
D2 00 00 00 00 00 00 00 00 00 00 00 00 30 0D 00
00 00 00 00 00 04 00 00 00 00 00 00 00 00 00 00
00 80 69 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 60 1A 00 00 00 00 08 00 00 00 00 00 00 00
00 00 00 00 00 70 1A 00 00 00 00 00 00 00 00 10
A6 01 00 00 00 00 00 00 20 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 A6 01 00 00 00 00 00
00 00 04 00 00 00 00 00 00 00 00 30 0D 00 00 00
00 00 00 00 10 00 00 00 00 4C 03 00 00 00 00 00
00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 20 00 00 00 00 00 00 00 00
00 00 00 00 00 D3 00 00 00 00 00 00 00 02 00 00
            4C 03 00 00 00 00 00 00
```

After chi

```
D2 00 00 00 00 04 00 00 00 00 00 00 00 30 0D 00
00 80 69 00 00 04 00 00 D2 00 00 00 00 00 00 00
00 80 69 00 00 30 0D 00 08 00 00 00 00 00 00 00
00 00 60 1A 00 70 1A 00 08 00 00 00 00 00 00 10
00 00 00 00 00 70 1A 00 00 00 60 1A 00 00 00 10
A6 01 00 00 00 00 00 00 20 A6 01 00 00 00 00 00
00 00 04 00 00 00 00 00 A6 A7 01 00 00 00 00 00
00 00 04 00 00 00 00 00 00 4C 03 30 0D 00 00 00
00 00 00 00 10 00 00 00 00 4C 03 00 00 00 00 00
00 40 00 30 0D 00 00 00 00 00 00 00 10 00 00 00
00 00 00 00 00 D3 00 20 00 00 00 00 00 00 00 00
4C 03 00 00 00 D3 00 00 00 00 00 00 00 02 00 20
            4C 03 00 00 00 00 00 00
```

After iota

```
D3 00 00 00 00 04 00 00 00 00 00 00 00 30 0D 00
00 80 69 00 00 04 00 00 D2 00 00 00 00 00 00 00
00 80 69 00 00 30 0D 00 08 00 00 00 00 00 00 00
00 00 60 1A 00 70 1A 00 08 00 00 00 00 00 00 10
00 00 00 00 00 70 1A 00 00 00 60 1A 00 00 00 10
A6 01 00 00 00 00 00 00 20 A6 01 00 00 00 00 00
00 00 04 00 00 00 00 00 A6 A7 01 00 00 00 00 00
00 00 04 00 00 00 00 00 00 4C 03 30 0D 00 00 00
00 00 00 00 10 00 00 00 00 4C 03 00 00 00 00 00
00 40 00 30 0D 00 00 00 00 00 00 00 10 00 00 00
00 00 00 00 00 D3 00 20 00 00 00 00 00 00 00 00
4C 03 00 00 00 D3 00 00 00 00 00 00 00 02 00 20
            4C 03 00 00 00 00 00 00
```

(Skip rounds 1 to 22)

Round #23

After theta

```
7A C0 47 4F 5A 45 7C 12 42 CB B4 2E FF 7C AF 1E
F9 70 2C D1 F8 A9 DE FA D1 44 4E E0 1F 81 9D 0C
81 AA 52 B4 7E BF C1 1B 0D E4 68 B7 A9 C6 EB B5
BC E6 66 DB F3 DF 5A AD 8F B8 18 FD 1A 68 07 B4
D9 A1 B5 E4 D2 ED 8D A5 AF 1A 1A 58 DA C4 F4 03
C7 78 B0 28 86 98 71 6A C8 4B AC EF E9 A2 D9 8C
C8 C6 23 87 6A A6 01 12 06 EF 64 77 5F A0 70 79
3F 1F C3 B3 68 88 AE 9A A3 82 63 1C 8B 11 6F BD
A9 AD 0F A7 D9 91 1D CD B4 C3 93 CA 5F 50 57 A5
3B AD CF FC FB 0D 0D 9A 9A 24 AE D5 6C 72 0C E7
A3 2A 29 68 41 8B 00 C9 71 66 43 5D D7 29 F6 23
60 99 F4 D9 38 70 BB E1 CE E8 1D 04 91 97 41 0D
            5A AE 78 3E 56 2D 77 83
```

After rho

```
7A C0 47 4F 5A 45 7C 12 84 96 69 5D FE F9 5E 3D
3E 1C 4B 34 7E AA B7 7E 11 D8 C9 10 4D E4 04 FE
FB 0D DE 08 54 95 A2 F5 9B 6A BC 5E DB 40 8E 76
B6 3D FF AD D5 CA 6B 6E ED 23 2E 46 BF 06 DA 01
D0 5A 72 E9 F6 C6 D2 EC 4C 3F F0 AA A1 81 A5 4D
3B C6 83 45 31 C4 8C 53 33 22 2F B1 BE A7 8B 66
39 54 33 0D 90 40 36 1E 40 E1 F2 0C DE C9 EE BE
59 34 44 57 CD 9F 8F E1 38 16 23 DE 7A 47 05 C7
E1 34 3B B2 A3 39 B5 F5 AB 52 DA E1 49 E5 2F A8
A1 41 73 A7 F5 99 7F BF E7 9A 24 AE D5 6C 72 0C
02 24 8F AA A4 A0 05 2D C4 99 0D 75 5D A7 D8 8F
2C 93 3E 1B 07 6E 37 1C E8 1D 04 91 97 41 0D CE
            DD A0 96 2B 9E 8F 55 CB
```

After pi

```
7A C0 47 4F 5A 45 7C 12 B6 3D FF AD D5 CA 6B 6E
39 54 33 0D 90 40 36 1E A1 41 73 A7 F5 99 7F BF
DD A0 96 2B 9E 8F 55 CB 11 D8 C9 10 4D E4 04 FE
4C 3F F0 AA A1 81 A5 4D 3B C6 83 45 31 C4 8C 53
E1 34 3B B2 A3 39 B5 F5 2C 93 3E 1B 07 6E 37 1C
84 96 69 5D FE F9 5E 3D ED 23 2E 46 BF 06 DA 01
40 E1 F2 0C DE C9 EE BE E7 9A 24 AE D5 6C 72 0C
02 24 8F AA A4 A0 05 2D FB 0D DE 08 54 95 A2 F5
9B 6A BC 5E DB 40 8E 76 33 22 2F B1 BE A7 8B 66
AB 52 DA E1 49 E5 2F A8 E8 1D 04 91 97 41 0D CE
3E 1C 4B 34 7E AA B7 7E D0 5A 72 E9 F6 C6 D2 EC
59 34 44 57 CD 9F 8F E1 38 16 23 DE 7A 47 05 C7
            C4 99 0D 75 5D A7 D8 8F
```

After chi

```
73 80 47 4F 5A 45 68 02 36 3C BF 0F B0 53 22 CF
65 F4 B7 05 9A 46 36 5E 83 01 32 E3 B5 D9 57 AF
59 9D 2E 8B 1B 05 56 A7 22 18 CA 55 5D A0 0C EC
8C 0F C8 18 23 B8 94 E9 37 45 87 4C 35 82 8E 5B
F0 7C FA B2 EB B9 B5 17 60 B4 0E B1 A7 6F 96 1D
84 56 B9 55 BE 30 7A 83 4A 39 2A E4 BE 22 CA 01
40 C5 79 0C FE 49 EB 9F 63 08 44 FB 8F 35 28 1C
6B 05 89 A8 A5 A6 85 2D DB 0D DD A9 70 32 A3 F5
13 3A 6C 1E 9A 00 AA FE 73 2F 2B A1 28 A7 8B 20
B8 52 00 E9 09 71 8D 99 E8 7F 24 C7 1C 01 01 CC
37 38 4F 22 77 B3 BA 7F F0 58 51 61 C4 86 D2 EA
9D BD 48 76 C8 3F 57 E9 02 12 61 DE 58 4F 22 B7
            04 DB 3D BC DD E3 98 0F
```

After iota

```
7B 00 47 CF 5A 45 68 82 36 3C BF 0F B0 53 22 CF
65 F4 B7 05 9A 46 36 5E 83 01 32 E3 B5 D9 57 AF
59 9D 2E 8B 1B 05 56 A7 22 18 CA 55 5D A0 0C EC
8C 0F C8 18 23 B8 94 E9 37 45 87 4C 35 82 8E 5B
F0 7C FA B2 EB B9 B5 17 60 B4 0E B1 A7 6F 96 1D
84 56 B9 55 BE 30 7A 83 4A 39 2A E4 BE 22 CA 01
40 C5 79 0C FE 49 EB 9F 63 08 44 FB 8F 35 28 1C
6B 05 89 A8 A5 A6 85 2D DB 0D DD A9 70 32 A3 F5
13 3A 6C 1E 9A 00 AA FE 73 2F 2B A1 28 A7 8B 20
B8 52 00 E9 09 71 8D 99 E8 7F 24 C7 1C 01 01 CC
37 38 4F 22 77 B3 BA 7F F0 58 51 61 C4 86 D2 EA
9D BD 48 76 C8 3F 57 E9 02 12 61 DE 58 4F 22 B7
            04 DB 3D BC DD E3 98 0F
```

After permutation

```
7B 00 47 CF 5A 45 68 82 36 3C BF 0F B0 53 22 CF
65 F4 B7 05 9A 46 36 5E 83 01 32 E3 B5 D9 57 AF
59 9D 2E 8B 1B 05 56 A7 22 18 CA 55 5D A0 0C EC
8C 0F C8 18 23 B8 94 E9 37 45 87 4C 35 82 8E 5B
F0 7C FA B2 EB B9 B5 17 60 B4 0E B1 A7 6F 96 1D
84 56 B9 55 BE 30 7A 83 4A 39 2A E4 BE 22 CA 01
40 C5 79 0C FE 49 EB 9F 63 08 44 FB 8F 35 28 1C
6B 05 89 A8 A5 A6 85 2D DB 0D DD A9 70 32 A3 F5
13 3A 6C 1E 9A 00 AA FE 73 2F 2B A1 28 A7 8B 20
B8 52 00 E9 09 71 8D 99 E8 7F 24 C7 1C 01 01 CC
37 38 4F 22 77 B3 BA 7F F0 58 51 61 C4 86 D2 EA
9D BD 48 76 C8 3F 57 E9 02 12 61 DE 58 4F 22 B7
            04 DB 3D BC DD E3 98 0F
```

State (as lanes of integers)

```
[0, 0] = 8268455acf47007b
[1, 0] = cf2253b00fbf3c36
[2, 0] = 5e36469a05b7f465
[3, 0] = af57d9b5e3320183
[4, 0] = a756051b8b2e9d59
[0, 1] = ec0ca05d55ca1822
[1, 1] = e994b82318c80f8c
[2, 1] = 5b8e82354c874537
[3, 1] = 17b5b9ebb2fa7cf0
[4, 1] = 1d966fa7b10eb460
[0, 2] = 837a30be55b95684
[1, 2] = 01ca22bee42a394a
[2, 2] = 9feb49fe0c79c540
[3, 2] = 1c28358ffb440863
[4, 2] = 2d85a6a5a889056b
[0, 3] = f5a33270a9dd0ddb
[1, 3] = feaa009a1e6c3a13
[2, 3] = 208ba728a12b2f73
[3, 3] = 998d7109e90052b8
[4, 3] = cc01011cc7247fe8
[0, 4] = 7fbab377224f3837
[1, 4] = ead286c4615158f0
[2, 4] = e9573fc87648bd9d
[3, 4] = b7224f58de611202
[4, 4] = 0f98e3ddbc3ddb04
```

The hash value is

```
7B 00 47 CF 5A 45 68 82 36 3C BF 0F B0 53 22 CF
65 F4 B7 05 9A 46 36 5E 83 01 32 E3 B5 D9 57 AF
```

The message as bit string

```
1 1 0 0 1 0 1 0 0 0 0 1 1 0 1 0 1 1 0 1 1 1 1 0 1 0 0 1 1 0
```

XORed state (in bytes)

```
53 58 7B 99 01 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 80 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
   00 00 00 00 00 00 00 00
```

XORed state (as lanes of integers)

```
[0, 0] = 00000001997b5853
[1, 0] = 0000000000000000
[2, 0] = 0000000000000000
[3, 0] = 0000000000000000
[4, 0] = 0000000000000000
[0, 1] = 0000000000000000
[1, 1] = 0000000000000000
[2, 1] = 0000000000000000
[3, 1] = 0000000000000000
[4, 1] = 0000000000000000
[0, 2] = 0000000000000000
[1, 2] = 0000000000000000
[2, 2] = 0000000000000000
[3, 2] = 0000000000000000
[4, 2] = 0000000000000000
[0, 3] = 0000000000000000
[1, 3] = 8000000000000000
[2, 3] = 0000000000000000
[3, 3] = 0000000000000000
[4, 3] = 0000000000000000
[0, 4] = 0000000000000000
[1, 4] = 0000000000000000
[2, 4] = 0000000000000000
[3, 4] = 0000000000000000
[4, 4] = 0000000000000000
```

Round #0

After theta

```
52 58 7B 99 01 00 00 00 53 58 7B 99 01 00 00 00
00 00 00 00 00 00 00 80 00 00 00 00 00 00 00 00
A6 B0 F6 32 03 00 00 00 01 00 00 00 00 00 00 00
53 58 7B 99 01 00 00 00 00 00 00 00 00 00 00 80
00 00 00 00 00 00 00 00 A6 B0 F6 32 03 00 00 00
01 00 00 00 00 00 00 00 53 58 7B 99 01 00 00 00
00 00 00 00 00 00 00 80 00 00 00 00 00 00 00 00
A6 B0 F6 32 03 00 00 00 01 00 00 00 00 00 00 00
53 58 7B 99 01 00 00 80 00 00 00 00 00 00 00 80
```

```
00 00 00 00 00 00 00 00 A6 B0 F6 32 03 00 00 00
01 00 00 00 00 00 00 00 53 58 7B 99 01 00 00 00
00 00 00 00 00 00 00 80 00 00 00 00 00 00 00 00
            A6 B0 F6 32 03 00 00 00
```

After rho

```
52 58 7B 99 01 00 00 00 A6 B0 F6 32 03 00 00 00
00 00 00 00 00 00 00 20 00 00 00 00 00 00 00 00
00 00 00 30 85 B5 97 19 00 00 00 00 10 00 00 00
97 19 00 00 00 30 85 B5 20 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 60 0A 6B 2F 33 00
08 00 00 00 00 00 00 00 00 4C 61 ED 65 06 00 00
00 00 00 00 00 04 00 00 00 00 00 00 00 00 00 00
99 01 00 00 00 53 58 7B 00 00 00 00 00 02 00 00
2F 33 00 00 00 70 0A 6B 00 40 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 A6 B0 F6 32 03 00 00
00 00 04 00 00 00 00 00 4C 61 ED 65 06 00 00 00
00 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00
            00 80 29 AC BD CC 00 00
```

After pi

```
52 58 7B 99 01 00 00 00 97 19 00 00 00 30 85 B5
00 00 00 00 00 04 00 00 00 00 00 00 00 00 00 00
00 80 29 AC BD CC 00 00 00 00 00 00 00 00 00 00
00 00 60 0A 6B 2F 33 00 08 00 00 00 00 00 00 00
2F 33 00 00 00 70 0A 6B 00 00 00 00 00 00 00 10
A6 B0 F6 32 03 00 00 00 20 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 A6 B0 F6 32 03 00 00
00 00 04 00 00 00 00 00 00 00 00 30 85 B5 97 19
00 00 00 00 10 00 00 00 00 4C 61 ED 65 06 00 00
00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 20 00 00 00 00 00 00 00 00
99 01 00 00 00 53 58 7B 00 00 00 00 00 02 00 00
            4C 61 ED 65 06 00 00 00
```

After chi

```
52 58 7B 99 01 04 00 00 97 19 00 00 00 30 85 B5
00 80 29 AC BD C8 00 00 52 58 52 11 00 00 00 00
85 81 29 AC BD FC 85 B5 08 00 00 00 00 00 00 00
27 33 60 0A 6B 5F 39 6B 08 00 00 00 00 00 00 10
2F 33 00 00 00 70 0A 6B 00 00 60 0A 6B 2F 33 10
A6 B0 F6 32 03 00 00 00 20 A6 B0 F6 32 03 00 00
00 00 04 00 00 00 00 00 A6 16 42 C4 31 03 00 00
00 00 04 00 00 00 00 00 00 4C 61 DD E0 B3 97 19
00 00 00 00 10 00 00 00 00 4C 61 ED 65 06 00 00
00 40 00 30 85 B5 97 19 00 00 00 00 10 00 00 00
99 01 00 00 00 53 58 5B 00 00 00 00 00 00 00 00
D5 60 ED 65 06 53 58 7B 00 00 00 00 00 02 00 20
            4C 61 ED 65 06 00 00 00
```

After iota

```
53 58 7B 99 01 04 00 00 97 19 00 00 00 30 85 B5
00 80 29 AC BD C8 00 00 52 58 52 11 00 00 00 00
85 81 29 AC BD FC 85 B5 08 00 00 00 00 00 00 00
27 33 60 0A 6B 5F 39 6B 08 00 00 00 00 00 00 10
2F 33 00 00 00 70 0A 6B 00 00 60 0A 6B 2F 33 10
A6 B0 F6 32 03 00 00 00 20 A6 B0 F6 32 03 00 00
00 00 04 00 00 00 00 00 A6 16 42 C4 31 03 00 00
00 00 04 00 00 00 00 00 00 4C 61 DD E0 B3 97 19
00 00 00 00 10 00 00 00 00 4C 61 ED 65 06 00 00
00 40 00 30 85 B5 97 19 00 00 00 00 10 00 00 00
99 01 00 00 00 53 58 5B 00 00 00 00 00 00 00 00
D5 60 ED 65 06 53 58 7B 00 00 00 00 00 02 00 20
            4C 61 ED 65 06 00 00 00
```

(Skip rounds 1 to 22)

Round #23

After theta

```
E0 A8 3E 4F 51 BC 7A EA 31 43 F5 C3 14 A1 71 39
1B 4F 50 1E 76 8B 79 7A F1 34 AF 61 D5 4D 3D 28
6A 52 D5 36 62 0A 0C 4E 07 C1 3D 60 17 F4 CB 82
7D 49 71 1D A3 AE E4 DC 6D E1 43 3A C0 1C D1 8B
55 70 34 6E 5C F3 90 56 39 51 41 B7 2E F6 24 88
EF 8A B3 ED 03 39 1B 7B 11 CD A4 A6 A4 A5 C5 F2
8C 74 30 BE 27 43 64 F3 EB 76 40 BB 3E 2D 84 0D
52 F5 75 CB 70 12 A0 7D DB 7F A6 74 94 69 27 4E
C1 7A 29 C4 5D 0B AD 65 C3 DA 16 FE D6 B7 C2 8E
E9 88 87 8F 87 3D 4D 17 1F 6E 56 FD F7 52 1B CE
D7 77 A3 6C D4 A8 63 74 F3 43 7D FD 59 97 88 63
B2 03 94 5E 27 59 2C 9B 91 64 2E 34 F7 7A 29 5F
            01 98 12 D4 FD 7E 2E 59
```

After rho

```
E0 A8 3E 4F 51 BC 7A EA 62 86 EA 87 29 42 E3 72
C6 13 94 87 DD 62 9E DE DD D4 83 12 4F F3 1A 56
53 60 70 52 93 AA B6 11 76 41 BF 2C 78 10 DC 03
D7 31 EA 4A CE DD 97 14 62 5B F8 90 0E 30 47 F4
38 1A 37 AE 79 48 AB 2A 4F 82 98 13 15 74 EB 62
7B 57 9C 6D 1F C8 D9 D8 CB 47 34 93 9A 92 96 16
F1 3D 19 22 9B 67 A4 83 5A 08 1B D6 ED 80 76 7D
65 38 09 D0 3E A9 FA BA E9 28 D3 4E 9C B6 FF 4C
85 B8 6B A1 B5 2C 58 2F 61 C7 61 6D 0B 7F EB 5B
A7 E9 22 1D F1 F0 F1 B0 CE 1F 6E 56 FD F7 52 1B
8E D1 5D DF 8D B2 51 A3 CD 0F F5 F5 67 5D 22 8E
76 80 D2 EB 24 8B 65 53 64 2E 34 F7 7A 29 5F 91
            4B 56 00 A6 04 75 BF 9F
```

After pi

```
E0 A8 3E 4F 51 BC 7A EA D7 31 EA 4A CE DD 97 14
F1 3D 19 22 9B 67 A4 83 A7 E9 22 1D F1 F0 F1 B0
4B 56 00 A6 04 75 BF 9F DD D4 83 12 4F F3 1A 56
4F 82 98 13 15 74 EB 62 7B 57 9C 6D 1F C8 D9 D8
85 B8 6B A1 B5 2C 58 2F 76 80 D2 EB 24 8B 65 53
62 86 EA 87 29 42 E3 72 62 5B F8 90 0E 30 47 F4
5A 08 1B D6 ED 80 76 7D CE 1F 6E 56 FD F7 52 1B
8E D1 5D DF 8D B2 51 A3 53 60 70 52 93 AA B6 11
76 41 BF 2C 78 10 DC 03 CB 47 34 93 9A 92 96 16
61 C7 61 6D 0B 7F EB 5B 64 2E 34 F7 7A 29 5F 91
C6 13 94 87 DD 62 9E DE 38 1A 37 AE 79 48 AB 2A
65 38 09 D0 3E A9 FA BA E9 28 D3 4E 9C B6 FF 4C
            CD 0F F5 F5 67 5D 22 8E
```

After chi

```
C0 A4 2F 6F 40 9E 5A 69 D1 F1 C8 57 AE 4D C6 24
B9 2B 19 80 9F 62 AA 8C 07 41 1C 54 A0 78 B1 D0
5C 47 C0 A6 8A 34 3A 8B ED 81 87 7E 45 7B 0A CE
CB 2A FB 93 B5 50 EB 45 09 57 0C 27 1F 4B FC 88
0C EC 6A B1 FE 5C 42 2B 74 82 CA EA 34 8F 84 73
7A 86 E9 C1 C8 C2 D3 7B E6 4C 9C 90 1E 47 47 F6
5A C8 0A 5F ED 80 77 DD AE 19 CC 56 DD B7 F0 4B
8E 88 4D CF 8B 82 55 27 DA 66 70 C1 11 28 B4 05
56 C1 FE 40 79 7D B5 4A CF 6F 20 01 EA 92 82 96
72 87 21 6D 8A FD 4B 5B 40 2F BB DB 12 39 17 93
83 33 9C D7 DB C3 CE 4E B0 1A E5 A0 F9 5E AE 6E
61 3F 2D 61 5D E0 FA 38 EB 38 D3 4C 04 94 63 1C
            F5 07 D6 DD 47 55 03 AE
```

After iota

```
C8 24 2F EF 40 9E 5A E9 D1 F1 C8 57 AE 4D C6 24
B9 2B 19 80 9F 62 AA 8C 07 41 1C 54 A0 78 B1 D0
5C 47 C0 A6 8A 34 3A 8B ED 81 87 7E 45 7B 0A CE
CB 2A FB 93 B5 50 EB 45 09 57 0C 27 1F 4B FC 88
0C EC 6A B1 FE 5C 42 2B 74 82 CA EA 34 8F 84 73
7A 86 E9 C1 C8 C2 D3 7B E6 4C 9C 90 1E 47 47 F6
5A C8 0A 5F ED 80 77 DD AE 19 CC 56 DD B7 F0 4B
8E 88 4D CF 8B 82 55 27 DA 66 70 C1 11 28 B4 05
56 C1 FE 40 79 7D B5 4A CF 6F 20 01 EA 92 82 96
72 87 21 6D 8A FD 4B 5B 40 2F BB DB 12 39 17 93
83 33 9C D7 DB C3 CE 4E B0 1A E5 A0 F9 5E AE 6E
61 3F 2D 61 5D E0 FA 38 EB 38 D3 4C 04 94 63 1C
            F5 07 D6 DD 47 55 03 AE
```

After permutation

```
C8 24 2F EF 40 9E 5A E9 D1 F1 C8 57 AE 4D C6 24
B9 2B 19 80 9F 62 AA 8C 07 41 1C 54 A0 78 B1 D0
5C 47 C0 A6 8A 34 3A 8B ED 81 87 7E 45 7B 0A CE
CB 2A FB 93 B5 50 EB 45 09 57 0C 27 1F 4B FC 88
0C EC 6A B1 FE 5C 42 2B 74 82 CA EA 34 8F 84 73
7A 86 E9 C1 C8 C2 D3 7B E6 4C 9C 90 1E 47 47 F6
5A C8 0A 5F ED 80 77 DD AE 19 CC 56 DD B7 F0 4B
8E 88 4D CF 8B 82 55 27 DA 66 70 C1 11 28 B4 05
56 C1 FE 40 79 7D B5 4A CF 6F 20 01 EA 92 82 96
72 87 21 6D 8A FD 4B 5B 40 2F BB DB 12 39 17 93
83 33 9C D7 DB C3 CE 4E B0 1A E5 A0 F9 5E AE 6E
61 3F 2D 61 5D E0 FA 38 EB 38 D3 4C 04 94 63 1C
            F5 07 D6 DD 47 55 03 AE
```

State (as lanes of integers)

```
[0, 0] = e95a9e40ef2f24c8
[1, 0] = 24c64dae57c8f1d1
[2, 0] = 8caa629f80192bb9
[3, 0] = d0b178a0541c4107
[4, 0] = 8b3a348aa6c0475c
[0, 1] = ce0a7b457e8781ed
[1, 1] = 45eb50b593fb2acb
[2, 1] = 88fc4b1f270c5709
[3, 1] = 2b425cfeb16aec0c
[4, 1] = 73848f34eaca8274
[0, 2] = 7bd3c2c8c1e9867a
[1, 2] = f647471e909c4ce6
[2, 2] = dd7780ed5f0ac85a
[3, 2] = 4bf0b7dd56cc19ae
[4, 2] = 2755828bcf4d888e
[0, 3] = 05b42811c17066da
[1, 3] = 4ab57d7940fec156
[2, 3] = 968292ea01206fcf
[3, 3] = 5b4bfd8a6d218772
[4, 3] = 93173912dbbb2f40
[0, 4] = 4ecec3dbd79c3383
[1, 4] = 6eae5ef9a0e51ab0
[2, 4] = 38fae05d612d3f61
[3, 4] = 1c6394044cd338eb
[4, 4] = ae035547ddd607f5
```

The hash value is

```
C8 24 2F EF 40 9E 5A E9 D1 F1 C8 57 AE 4D C6 24
B9 2B 19 80 9F 62 AA 8C 07 41 1C 54 A0 78 B1 D0
```

B.17 Dedicated Hash-Function 15 (SHA3-384)

NOTE 1 Data is presented in three different ways: bit strings, byte strings and *w*-length words (for the lanes).

NOTE 2 Bit strings are the sequence of bits from left to right.

NOTE 3 Byte strings are the bytes from left to right and the bits within the byte are right to left.

NOTE 4 Words are the integer representation of the values in the lanes.

SHA3-384 sample

The message as bit string

```
(empty message)
```

XORed state (in bytes)

```
06 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 80 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
               00 00 00 00 00 00 00 00
```

XORed state (as lanes of integers)

```
[0, 0] = 0000000000000006
[1, 0] = 0000000000000000
[2, 0] = 0000000000000000
[3, 0] = 0000000000000000
[4, 0] = 0000000000000000
[0, 1] = 0000000000000000
[1, 1] = 0000000000000000
[2, 1] = 0000000000000000
[3, 1] = 0000000000000000
[4, 1] = 0000000000000000
[0, 2] = 0000000000000000
[1, 2] = 0000000000000000
[2, 2] = 8000000000000000
[3, 2] = 0000000000000000
[4, 2] = 0000000000000000
[0, 3] = 0000000000000000
[1, 3] = 0000000000000000
[2, 3] = 0000000000000000
[3, 3] = 0000000000000000
[4, 3] = 0000000000000000
[0, 4] = 0000000000000000
[1, 4] = 0000000000000000
[2, 4] = 0000000000000000
[3, 4] = 0000000000000000
[4, 4] = 0000000000000000
```

Round #0

After theta

```
06 00 00 00 00 00 00 00 07 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 80
0C 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
07 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 80 0C 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 07 00 00 00 00 00 00 00
00 00 00 00 00 00 00 80 00 00 00 00 00 00 00 80
0C 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
07 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 80 0C 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 07 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 80
            0C 00 00 00 00 00 00 00
```

After rho

```
06 00 00 00 00 00 00 00 0E 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 08 00 00 00 00
00 00 00 60 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 70 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 40 00 00 00 C0 00 00 00 00 00
00 00 00 00 00 00 00 00 00 1C 00 00 00 00 00 00
00 00 00 00 00 04 00 00 00 00 00 01 00 00 00 00
00 00 00 00 00 06 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 E0 00 00 00 00 00 00 00 00 00 00
00 00 10 00 00 00 00 00 00 0C 00 00 00 00 00 00
00 00 00 00 00 00 00 00 1C 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 80 00
            00 00 03 00 00 00 00 00
```

After pi

```
06 00 00 00 00 00 00 00 00 00 00 00 00 70 00 00
00 00 00 00 00 04 00 00 00 00 10 00 00 00 00 00
00 00 03 00 00 00 00 00 00 00 00 08 00 00 00 00
00 00 C0 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 E0 00 00 00 00 00 00 00 00 00 00
0E 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 01 00 00 00 00 00 0C 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 60 00 00 00 00
00 00 00 00 00 00 00 00 00 1C 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 80 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00
00 00 00 00 00 06 00 00 00 00 00 00 00 00 00 00
            1C 00 00 00 00 00 00 00
```

After chi

```
06 00 00 00 00 04 00 00 00 00 10 00 00 70 00 00
00 00 03 00 00 04 00 00 06 00 10 00 00 00 00 00
00 00 03 00 00 70 00 00 00 00 00 08 00 00 00 00
00 00 C0 00 00 E0 00 00 00 00 00 00 00 00 00 00
00 00 00 08 00 E0 00 00 00 00 C0 00 00 00 00 00
0E 00 00 01 00 00 00 00 00 0C 00 00 00 00 00 00
00 00 00 01 00 00 00 00 0E 0C 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 1C 00 60 00 00 00 00
00 00 00 00 00 00 00 00 00 1C 00 00 00 00 80 00
00 00 00 60 00 00 00 00 00 00 00 00 00 00 80 00
00 00 00 00 00 06 00 00 00 00 00 00 00 00 40 00
1C 00 00 00 00 06 00 00 00 00 00 00 00 00 00 00
            1C 00 00 00 00 00 40 00
```

After iota

```
07 00 00 00 00 04 00 00 00 00 10 00 00 70 00 00
00 00 03 00 00 04 00 00 06 00 10 00 00 00 00 00
00 00 03 00 00 70 00 00 00 00 00 08 00 00 00 00
00 00 C0 00 00 E0 00 00 00 00 00 00 00 00 00 00
00 00 00 08 00 E0 00 00 00 00 C0 00 00 00 00 00
0E 00 00 01 00 00 00 00 00 0C 00 00 00 00 00 00
00 00 00 01 00 00 00 00 0E 0C 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 1C 00 60 00 00 00 00
00 00 00 00 00 00 00 00 00 1C 00 00 00 00 80 00
00 00 00 60 00 00 00 00 00 00 00 00 00 00 80 00
00 00 00 00 00 06 00 00 00 00 00 00 00 00 40 00
1C 00 00 00 00 06 00 00 00 00 00 00 00 00 00 00
            1C 00 00 00 00 00 40 00
```

(Skip rounds 1 to 22)

Round #23

After theta

```
82 C8 A7 F1 04 CC 56 DD 92 34 F3 C3 2B AC A0 86
FD C0 AA 7F 37 23 13 EB 5A FF 0D 29 F9 3E 30 DF
51 C0 BB 57 F0 50 5B 48 55 32 25 4A 13 39 94 30
64 72 91 41 BD 4D AD 46 04 F5 B9 DE 62 D4 EC 57
52 CD 17 96 D3 CC BA 6E 29 23 55 9F 09 26 7E 58
26 CD F6 AD DD 05 DE DA D1 38 07 60 86 FF EA 16
BA 87 E4 70 07 CA 55 D5 35 29 2F D3 CD A8 27 4C
DF 50 FE 4B F8 EF B7 98 C5 2A 0F 3F C8 BB 69 92
78 76 9E 56 EA AC B2 41 8A B0 9E E9 78 C2 9B C9
DF 73 E7 F0 91 CD B4 B6 65 E2 04 F2 F3 CD CE 33
5A B2 23 92 C4 CA 6C AB 5F 32 47 49 35 61 6F E7
4E A1 F3 54 E7 7C F1 81 A0 45 75 8A E7 D5 D6 5A
            81 D5 30 29 ED 17 69 97
```

After rho

```
82 C8 A7 F1 04 CC 56 DD 25 69 E6 87 57 58 41 0D
3F B0 EA DF CD C8 C4 7A EF 03 F3 AD F5 DF 90 92
87 DA 42 8A 02 DE BD 82 34 91 43 09 53 25 53 A2
19 D4 DB D4 6A 44 26 17 15 41 7D AE B7 18 35 FB
E6 0B CB 69 66 5D 37 A9 E2 87 95 32 52 F5 99 60
36 69 B6 6F ED 2E F0 D6 5B 44 E3 1C 80 19 FE AB
87 3B 50 AE AA D6 3D 24 51 4F 98 6A 52 5E A6 9B
25 FC F7 5B CC 6F 28 FF 7E 90 77 D3 24 8B 55 1E
D3 4A 9D 55 36 08 CF CE CD 64 45 58 CF 74 3C E1
99 D6 F6 7B EE 1C 3E B2 33 65 E2 04 F2 F3 CD CE
B3 AD 6A C9 8E 48 12 2B 7F C9 1C 25 D5 84 BD 9D
29 74 9E EA 9C 2F 3E D0 45 75 8A E7 D5 D6 5A A0
            DA 65 60 35 4C 4A FB 45
```

After pi

```
82 C8 A7 F1 04 CC 56 DD 19 D4 DB D4 6A 44 26 17
87 3B 50 AE AA D6 3D 24 99 D6 F6 7B EE 1C 3E B2
DA 65 60 35 4C 4A FB 45 EF 03 F3 AD F5 DF 90 92
E2 87 95 32 52 F5 99 60 36 69 B6 6F ED 2E F0 D6
D3 4A 9D 55 36 08 CF CE 29 74 9E EA 9C 2F 3E D0
25 69 E6 87 57 58 41 0D 15 41 7D AE B7 18 35 FB
51 4F 98 6A 52 5E A6 9B 33 65 E2 04 F2 F3 CD CE
B3 AD 6A C9 8E 48 12 2B 87 DA 42 8A 02 DE BD 82
34 91 43 09 53 25 53 A2 5B 44 E3 1C 80 19 FE AB
CD 64 45 58 CF 74 3C E1 45 75 8A E7 D5 D6 5A A0
3F B0 EA DF CD C8 C4 7A E6 0B CB 69 66 5D 37 A9
25 FC F7 5B CC 6F 28 FF 7E 90 77 D3 24 8B 55 1E
            7F C9 1C 25 D5 84 BD 9D
```

After chi

```
04 E3 A7 DB 84 5E 4F FD 01 10 7D 85 2E 4C 24 85
C5 1A 50 AA AA 94 FC 61 99 5E 71 BB EE 98 3A 2A
C3 71 38 31 26 4A DB 47 FB 6B D1 E0 58 D5 F0 04
23 85 9C 22 40 F5 96 68 1E 5D B4 C5 65 09 C0 C6
15 49 FC 50 57 D8 4F CC 29 F0 9A F8 9E 0F 37 B0
65 67 66 C7 17 1E C3 0D 37 61 1F AA 17 B9 7C BF
D1 C7 90 A3 5E 56 B4 BA 37 25 66 02 A3 E3 8C CA
A3 AD 73 E1 2E 48 26 D9 CC 9E E2 9E 82 C6 11 8B
B0 B1 47 49 1C 41 53 E2 5B 55 69 BB 90 9B BC AB
4F EE 05 50 CD 7C 99 E3 75 74 8B E6 84 F7 18 80
3E 44 DE CD 45 EA CC 2C BC 0B CB E9 46 DD 62 A9
24 B5 FF 7F 1D 6B 80 7E 7E A0 95 09 2C C3 15 7C
            BF C2 1D 05 F7 91 8E 1C
```

After iota

```
0C 63 A7 5B 84 5E 4F 7D 01 10 7D 85 2E 4C 24 85
C5 1A 50 AA AA 94 FC 61 99 5E 71 BB EE 98 3A 2A
C3 71 38 31 26 4A DB 47 FB 6B D1 E0 58 D5 F0 04
23 85 9C 22 40 F5 96 68 1E 5D B4 C5 65 09 C0 C6
15 49 FC 50 57 D8 4F CC 29 F0 9A F8 9E 0F 37 B0
65 67 66 C7 17 1E C3 0D 37 61 1F AA 17 B9 7C BF
D1 C7 90 A3 5E 56 B4 BA 37 25 66 02 A3 E3 8C CA
A3 AD 73 E1 2E 48 26 D9 CC 9E E2 9E 82 C6 11 8B
B0 B1 47 49 1C 41 53 E2 5B 55 69 BB 90 9B BC AB
4F EE 05 50 CD 7C 99 E3 75 74 8B E6 84 F7 18 80
3E 44 DE CD 45 EA CC 2C BC 0B CB E9 46 DD 62 A9
24 B5 FF 7F 1D 6B 80 7E 7E A0 95 09 2C C3 15 7C
            BF C2 1D 05 F7 91 8E 1C
```

After permutation

```
0C 63 A7 5B 84 5E 4F 7D 01 10 7D 85 2E 4C 24 85
C5 1A 50 AA AA 94 FC 61 99 5E 71 BB EE 98 3A 2A
C3 71 38 31 26 4A DB 47 FB 6B D1 E0 58 D5 F0 04
23 85 9C 22 40 F5 96 68 1E 5D B4 C5 65 09 C0 C6
15 49 FC 50 57 D8 4F CC 29 F0 9A F8 9E 0F 37 B0
65 67 66 C7 17 1E C3 0D 37 61 1F AA 17 B9 7C BF
D1 C7 90 A3 5E 56 B4 BA 37 25 66 02 A3 E3 8C CA
A3 AD 73 E1 2E 48 26 D9 CC 9E E2 9E 82 C6 11 8B
B0 B1 47 49 1C 41 53 E2 5B 55 69 BB 90 9B BC AB
4F EE 05 50 CD 7C 99 E3 75 74 8B E6 84 F7 18 80
3E 44 DE CD 45 EA CC 2C BC 0B CB E9 46 DD 62 A9
24 B5 FF 7F 1D 6B 80 7E 7E A0 95 09 2C C3 15 7C
            BF C2 1D 05 F7 91 8E 1C
```

State (as lanes of integers)

```
[0, 0] = 7d4f5e845ba7630c
[1, 0] = 85244c2e857d1001
[2, 0] = 61fc94aaaa501ac5
[3, 0] = 2a3a98eebb715e99
[4, 0] = 47db4a26313871c3
[0, 1] = 04f0d558e0d16bfb
[1, 1] = 6896f540229c8523
[2, 1] = c6c00965c5b45d1e
[3, 1] = cc4fd85750fc4915
[4, 1] = b0370f9ef89af029
[0, 2] = 0dc31e17c7666765
[1, 2] = bf7cb917aa1f6137
[2, 2] = bab4565ea390c7d1
[3, 2] = ca8ce3a302662537
[4, 2] = d926482ee173ada3
[0, 3] = 8b11c6829ee29ecc
```

```
[1, 3] = e253411c4947b1b0
[2, 3] = abbc9b90bb69555b
[3, 3] = e3997ccd5005ee4f
[4, 3] = 8018f784e68b7475
[0, 4] = 2cccea45cdde443e
[1, 4] = a962dd46e9cb0bbc
[2, 4] = 7e806b1d7fffb524
[3, 4] = 7c15c32c0995a07e
[4, 4] = 1c8e91f7051dc2bf
```

The hash value is

```
0C 63 A7 5B 84 5E 4F 7D 01 10 7D 85 2E 4C 24 85
C5 1A 50 AA AA 94 FC 61 99 5E 71 BB EE 98 3A 2A
C3 71 38 31 26 4A DB 47 FB 6B D1 E0 58 D5 F0 04
```

The message as bit string

```
1 1 0 0 1
```

XORed state (in bytes)

```
D3 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 80 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
   00 00 00 00 00 00 00 00
```

XORed state (as lanes of integers)

```
[0, 0] = 00000000000000d3
[1, 0] = 0000000000000000
[2, 0] = 0000000000000000
[3, 0] = 0000000000000000
[4, 0] = 0000000000000000
[0, 1] = 0000000000000000
[1, 1] = 0000000000000000
[2, 1] = 0000000000000000
[3, 1] = 0000000000000000
[4, 1] = 0000000000000000
[0, 2] = 0000000000000000
[1, 2] = 0000000000000000
[2, 2] = 8000000000000000
[3, 2] = 0000000000000000
[4, 2] = 0000000000000000
[0, 3] = 0000000000000000
[1, 3] = 0000000000000000
[2, 3] = 0000000000000000
[3, 3] = 0000000000000000
[4, 3] = 0000000000000000
[0, 4] = 0000000000000000
[1, 4] = 0000000000000000
[2, 4] = 0000000000000000
[3, 4] = 0000000000000000
[4, 4] = 0000000000000000
```

Round #0

After theta

```
D3 00 00 00 00 00 00 00 D2 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 80
A6 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00
D2 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 80 A6 01 00 00 00 00 00 00
00 00 00 00 00 00 00 00 D2 00 00 00 00 00 00 00
00 00 00 00 00 00 00 80 00 00 00 00 00 00 00 80
A6 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00
D2 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 80 A6 01 00 00 00 00 00 00
00 00 00 00 00 00 00 00 D2 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 80
            A6 01 00 00 00 00 00 00
```

After rho

```
D3 00 00 00 00 00 00 00 A4 01 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 08 00 00 00 00
00 00 00 30 0D 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 20 0D 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 40 00 00 00 60 1A 00 00 00 00
00 00 00 00 00 00 00 00 00 48 03 00 00 00 00 00
00 00 00 00 00 04 00 00 00 00 00 01 00 00 00 00
00 00 00 00 00 D3 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 40 1A 00 00 00 00 00 00 00 00 00
00 00 10 00 00 00 00 00 00 A6 01 00 00 00 00 00
00 00 00 00 00 00 00 00 48 03 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 80 00
            00 80 69 00 00 00 00 00
```

After pi

```
D3 00 00 00 00 00 00 00 00 00 00 00 00 20 0D 00
00 00 00 00 00 04 00 00 00 00 10 00 00 00 00 00
00 80 69 00 00 00 00 00 00 00 00 08 00 00 00 00
00 00 60 1A 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 40 1A 00 00 00 00 00 00 00 00 00
A4 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 01 00 00 00 00 00 A6 01 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 30 0D 00 00 00
00 00 00 00 00 00 00 00 00 48 03 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 80 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00
00 00 00 00 00 D3 00 00 00 00 00 00 00 00 00 00
            48 03 00 00 00 00 00 00
```

After chi

```
D3 00 00 00 00 04 00 00 00 00 10 00 00 20 0D 00
00 80 69 00 00 04 00 00 D3 00 10 00 00 00 00 00
00 80 69 00 00 20 0D 00 00 00 00 08 00 00 00 00
00 00 60 1A 00 40 1A 00 00 00 00 00 00 00 00 00
00 00 00 08 00 40 1A 00 00 00 60 12 00 00 00 00
A4 01 00 01 00 00 00 00 00 A6 01 00 00 00 00 00
00 00 00 01 00 00 00 00 A4 A7 01 00 00 00 00 00
00 00 00 00 00 00 00 00 00 48 03 30 0D 00 00 00
00 00 00 00 00 00 00 00 00 48 03 00 00 00 80 00
00 00 00 30 0D 00 00 00 00 00 00 00 00 00 80 00
00 00 00 00 00 D3 00 00 00 00 00 00 00 00 40 00
48 03 00 00 00 D3 00 00 00 00 00 00 00 00 00 00
            48 03 00 00 00 00 40 00
```

After iota

```
D2 00 00 00 00 04 00 00 00 00 10 00 00 20 0D 00
00 80 69 00 00 04 00 00 D3 00 10 00 00 00 00 00
00 80 69 00 00 20 0D 00 00 00 00 08 00 00 00 00
00 00 60 1A 00 40 1A 00 00 00 00 00 00 00 00 00
00 00 00 08 00 40 1A 00 00 00 60 12 00 00 00 00
A4 01 00 01 00 00 00 00 00 A6 01 00 00 00 00 00
00 00 00 01 00 00 00 00 A4 A7 01 00 00 00 00 00
00 00 00 00 00 00 00 00 00 48 03 30 0D 00 00 00
00 00 00 00 00 00 00 00 00 48 03 00 00 00 80 00
00 00 00 30 0D 00 00 00 00 00 00 00 00 00 80 00
00 00 00 00 00 D3 00 00 00 00 00 00 00 00 40 00
48 03 00 00 00 D3 00 00 00 00 00 00 00 00 00 00
            48 03 00 00 00 00 40 00
```

(Skip rounds 1 to 22)

Round #23

After theta

```
F3 BD 8B A1 99 41 E9 3C 51 E0 3A E1 05 12 12 B9
CD FF FD 9E 4D 58 D5 C5 3E D1 C3 D1 E7 7E A2 C7
3D 80 9B EE FA E3 24 6B 49 51 2C 0C BF E2 5B 5E
13 87 5E A5 D2 06 E9 27 ED 7A F5 BA 16 96 92 10
73 95 55 13 68 DA D4 C6 0F 3E 1D 98 6D AA 95 8D
B3 BB 77 B4 DA 14 AA A3 AB 8F A5 0D 74 0C E5 FC
18 6C 98 39 8D 06 3D DC 75 83 32 99 36 C1 40 1F
C6 A3 06 14 D0 38 AE C6 20 F0 90 21 1B 22 F1 AF
FF 44 6D 00 E7 E6 88 FD 1B 5B 81 70 0F 98 F2 4F
15 58 53 53 83 2A 5F 71 5F DB 3B 44 C6 DD 4D 00
27 65 58 D0 56 40 0A 05 7A 42 58 B0 80 31 F5 75
E5 AC 7A ED A8 33 5E 6C 41 D9 A9 82 7F A6 A8 6D
            E7 79 E7 17 2D 2E 46 A5
```

After rho

```
F3 BD 8B A1 99 41 E9 3C A3 C0 75 C2 0B 24 24 72
F3 7F BF 67 13 56 75 71 EE 27 7A EC 13 3D 1C 7D
1F 27 59 EB 01 DC 74 D7 F0 2B BE E5 95 14 C5 C2
55 2A 6D 90 7E 32 71 E8 44 BB 5E BD AE 85 A5 24
CA AA 09 34 6D 6A E3 B9 5A D9 F8 E0 D3 81 D9 A6
9D DD BD A3 D5 A6 50 1D F3 AF 3E 96 36 D0 31 94
CC 69 34 E8 E1 C6 60 C3 82 81 3E EA 06 65 32 6D
0A 68 1C 57 63 E3 51 03 43 36 44 E2 5F 41 E0 21
0D E0 DC 1C B1 FF 9F A8 F9 A7 8D AD 40 B8 07 4C
E5 2B AE 02 6B 6A 6A 50 00 5F DB 3B 44 C6 DD 4D
29 14 9C 94 61 41 5B 01 E9 09 61 C1 02 C6 D4 D7
9C 55 AF 1D 75 C6 8B AD D9 A9 82 7F A6 A8 6D 41
            51 E9 79 DE F9 45 8B 8B
```

After pi

```
F3 BD 8B A1 99 41 E9 3C 55 2A 6D 90 7E 32 71 E8
CC 69 34 E8 E1 C6 60 C3 E5 2B AE 02 6B 6A 6A 50
51 E9 79 DE F9 45 8B 8B EE 27 7A EC 13 3D 1C 7D
5A D9 F8 E0 D3 81 D9 A6 9D DD BD A3 D5 A6 50 1D
0D E0 DC 1C B1 FF 9F A8 9C 55 AF 1D 75 C6 8B AD
A3 C0 75 C2 0B 24 24 72 44 BB 5E BD AE 85 A5 24
82 81 3E EA 06 65 32 6D 00 5F DB 3B 44 C6 DD 4D
29 14 9C 94 61 41 5B 01 1F 27 59 EB 01 DC 74 D7
F0 2B BE E5 95 14 C5 C2 F3 AF 3E 96 36 D0 31 94
F9 A7 8D AD 40 B8 07 4C D9 A9 82 7F A6 A8 6D 41
F3 7F BF 67 13 56 75 71 CA AA 09 34 6D 6A E3 B9
0A 68 1C 57 63 E3 51 03 43 36 44 E2 5F 41 E0 21
            E9 09 61 C1 02 C6 D4 D7
```

After chi

```
7B FC 9B C9 18 85 E9 3F 74 28 E7 92 74 1A 7B F8
DC A9 65 34 71 C3 E1 48 47 3F 2C 23 6B 6A 0A 64
55 EB 1D CE 9F 77 9B 4B 6B 23 7F EF 17 1B 1C 64
5A F9 B8 FC F3 D8 56 06 0D C8 9E A2 91 A6 50 18
6F C2 8C FC B3 C6 8B F8 8C 8D 2F 1D B5 46 4A 2F
21 C0 55 80 0B 44 36 3B 44 E5 9F AC EE 07 68 24
AB 81 3A 6E 27 64 30 6D 82 9F BA 79 4E E2 F9 3F
6D 2F 96 A9 C5 C0 DA 05 1C A3 59 F9 23 1C 44 C3
F8 2B 3F CC D5 3C C3 8A F3 A7 3C C4 90 D0 59 95
FF A1 D4 2D 41 EC 17 DA 39 A1 24 7B 32 A8 EC 41
F3 3F AB 24 11 D7 65 73 8B BC 49 94 71 6A 43 99
A2 61 3D 56 63 65 45 D5 51 40 DA C4 4E 51 C1 01
            E1 89 61 D1 6E EE 56 5F
```

After iota

```
73 7C 9B 49 18 85 E9 BF 74 28 E7 92 74 1A 7B F8
DC A9 65 34 71 C3 E1 48 47 3F 2C 23 6B 6A 0A 64
55 EB 1D CE 9F 77 9B 4B 6B 23 7F EF 17 1B 1C 64
5A F9 B8 FC F3 D8 56 06 0D C8 9E A2 91 A6 50 18
6F C2 8C FC B3 C6 8B F8 8C 8D 2F 1D B5 46 4A 2F
21 C0 55 80 0B 44 36 3B 44 E5 9F AC EE 07 68 24
AB 81 3A 6E 27 64 30 6D 82 9F BA 79 4E E2 F9 3F
6D 2F 96 A9 C5 C0 DA 05 1C A3 59 F9 23 1C 44 C3
F8 2B 3F CC D5 3C C3 8A F3 A7 3C C4 90 D0 59 95
FF A1 D4 2D 41 EC 17 DA 39 A1 24 7B 32 A8 EC 41
F3 3F AB 24 11 D7 65 73 8B BC 49 94 71 6A 43 99
A2 61 3D 56 63 65 45 D5 51 40 DA C4 4E 51 C1 01
            E1 89 61 D1 6E EE 56 5F
```

After permutation

```
73 7C 9B 49 18 85 E9 BF 74 28 E7 92 74 1A 7B F8
DC A9 65 34 71 C3 E1 48 47 3F 2C 23 6B 6A 0A 64
55 EB 1D CE 9F 77 9B 4B 6B 23 7F EF 17 1B 1C 64
5A F9 B8 FC F3 D8 56 06 0D C8 9E A2 91 A6 50 18
6F C2 8C FC B3 C6 8B F8 8C 8D 2F 1D B5 46 4A 2F
21 C0 55 80 0B 44 36 3B 44 E5 9F AC EE 07 68 24
AB 81 3A 6E 27 64 30 6D 82 9F BA 79 4E E2 F9 3F
6D 2F 96 A9 C5 C0 DA 05 1C A3 59 F9 23 1C 44 C3
F8 2B 3F CC D5 3C C3 8A F3 A7 3C C4 90 D0 59 95
FF A1 D4 2D 41 EC 17 DA 39 A1 24 7B 32 A8 EC 41
F3 3F AB 24 11 D7 65 73 8B BC 49 94 71 6A 43 99
A2 61 3D 56 63 65 45 D5 51 40 DA C4 4E 51 C1 01
            E1 89 61 D1 6E EE 56 5F
```

State (as lanes of integers)

```
[0, 0] = bfe98518499b7c73
[1, 0] = f87b1a7492e72874
[2, 0] = 48e1c3713465a9dc
[3, 0] = 640a6a6b232c3f47
[4, 0] = 4b9b779fce1deb55
[0, 1] = 641c1b17ef7f236b
[1, 1] = 0656d8f3fcb8f95a
[2, 1] = 1850a691a29ec80d
[3, 1] = f88bc6b3fc8cc26f
[4, 1] = 2f4a46b51d2f8d8c
[0, 2] = 3b36440b8055c021
[1, 2] = 246807eeac9fe544
[2, 2] = 6d3064276e3a81ab
[3, 2] = 3ff9e24e79ba9f82
[4, 2] = 05dac0c5a9962f6d
```

```
[0, 3] = c3441c23f959a31c
[1, 3] = 8ac33cd5cc3f2bf8
[2, 3] = 9559d090c43ca7f3
[3, 3] = da17ec412dd4a1ff
[4, 3] = 41eca8327b24a139
[0, 4] = 7365d71124ab3ff3
[1, 4] = 99436a719449bc8b
[2, 4] = d5456563563d61a2
[3, 4] = 01c1514ec4da4051
[4, 4] = 5f56ee6ed16189e1
```

The hash value is

```
73 7C 9B 49 18 85 E9 BF 74 28 E7 92 74 1A 7B F8
DC A9 65 34 71 C3 E1 48 47 3F 2C 23 6B 6A 0A 64
55 EB 1D CE 9F 77 9B 4B 6B 23 7F EF 17 1B 1C 64
```

SHA3-384 sample

The message as bit string

```
1 1 0 0 1 0 1 0 0 0 0 1 1 0 1 0 1 1 0 1 1 1 1 0 1 0 0 1 1 0
```

XORed state (in bytes)

```
53 58 7B 99 01 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 80 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
   00 00 00 00 00 00 00 00
```

XORed state (as lanes of integers)

```
[0, 0] = 00000001997b5853
[1, 0] = 0000000000000000
[2, 0] = 0000000000000000
[3, 0] = 0000000000000000
[4, 0] = 0000000000000000
[0, 1] = 0000000000000000
[1, 1] = 0000000000000000
[2, 1] = 0000000000000000
[3, 1] = 0000000000000000
[4, 1] = 0000000000000000
[0, 2] = 0000000000000000
[1, 2] = 0000000000000000
[2, 2] = 8000000000000000
[3, 2] = 0000000000000000
[4, 2] = 0000000000000000
[0, 3] = 0000000000000000
[1, 3] = 0000000000000000
[2, 3] = 0000000000000000
[3, 3] = 0000000000000000
[4, 3] = 0000000000000000
[0, 4] = 0000000000000000
[1, 4] = 0000000000000000
[2, 4] = 0000000000000000
[3, 4] = 0000000000000000
[4, 4] = 0000000000000000
```

Round #0

After theta

```
53 58 7B 99 01 00 00 00 52 58 7B 99 01 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 80
A6 B0 F6 32 03 00 00 00 00 00 00 00 00 00 00 00
52 58 7B 99 01 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 80 A6 B0 F6 32 03 00 00 00
00 00 00 00 00 00 00 00 52 58 7B 99 01 00 00 00
00 00 00 00 00 00 00 80 00 00 00 00 00 00 00 80
A6 B0 F6 32 03 00 00 00 00 00 00 00 00 00 00 00
52 58 7B 99 01 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 80 A6 B0 F6 32 03 00 00 00
00 00 00 00 00 00 00 00 52 58 7B 99 01 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 80
            A6 B0 F6 32 03 00 00 00
```

After rho

```
53 58 7B 99 01 00 00 00 A4 B0 F6 32 03 00 00 00
00 00 00 00 00 00 00 00 00 00 00 08 00 00 00 00
00 00 00 30 85 B5 97 19 00 00 00 00 00 00 00 00
97 19 00 00 00 20 85 B5 00 00 00 00 00 00 00 00
00 00 00 00 00 00 40 00 00 00 60 0A 6B 2F 33 00
00 00 00 00 00 00 00 00 00 48 61 ED 65 06 00 00
00 00 00 00 00 04 00 00 00 00 00 01 00 00 00 00
99 01 00 00 00 53 58 7B 00 00 00 00 00 00 00 00
2F 33 00 00 00 40 0A 6B 00 00 00 00 00 00 00 00
00 00 10 00 00 00 00 00 00 A6 B0 F6 32 03 00 00
00 00 00 00 00 00 00 00 48 61 ED 65 06 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 80 00
            00 80 29 AC BD CC 00 00
```

After pi

```
53 58 7B 99 01 00 00 00 97 19 00 00 00 20 85 B5
00 00 00 00 00 04 00 00 00 00 10 00 00 00 00 00
00 80 29 AC BD CC 00 00 00 00 00 08 00 00 00 00
00 00 60 0A 6B 2F 33 00 00 00 00 00 00 00 00 00
2F 33 00 00 00 40 0A 6B 00 00 00 00 00 00 00 00
A4 B0 F6 32 03 00 00 00 00 00 00 00 00 00 00 00
00 00 00 01 00 00 00 00 00 A6 B0 F6 32 03 00 00
00 00 00 00 00 00 00 00 00 00 00 30 85 B5 97 19
00 00 00 00 00 00 00 00 00 48 61 ED 65 06 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 80 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00
99 01 00 00 00 53 58 7B 00 00 00 00 00 00 00 00
            48 61 ED 65 06 00 00 00
```

After chi

```
53 58 7B 99 01 04 00 00 97 19 10 00 00 20 85 B5
00 80 29 AC BD C8 00 00 53 58 42 11 00 00 00 00
84 81 29 AC BD EC 85 B5 00 00 00 08 00 00 00 00
2F 33 60 0A 6B 6F 39 6B 00 00 00 00 00 00 00 00
2F 33 00 08 00 40 0A 6B 00 00 60 02 6B 2F 33 00
A4 B0 F6 33 03 00 00 00 00 A6 B0 F6 32 03 00 00
00 00 00 01 00 00 00 00 A4 16 46 C4 31 03 00 00
00 00 00 00 00 00 00 00 00 48 61 DD E0 B3 97 19
00 00 00 00 00 00 00 00 00 48 61 ED 65 06 80 00
00 00 00 30 85 B5 17 19 00 00 00 00 00 00 80 00
99 01 00 00 00 53 18 7B 00 00 00 00 00 00 40 00
D1 60 ED 65 06 53 58 7B 00 00 00 00 00 00 00 00
            48 61 ED 65 06 00 40 00
```

After iota

```
52 58 7B 99 01 04 00 00 97 19 10 00 00 20 85 B5
00 80 29 AC BD C8 00 00 53 58 42 11 00 00 00 00
84 81 29 AC BD EC 85 B5 00 00 00 08 00 00 00 00
2F 33 60 0A 6B 6F 39 6B 00 00 00 00 00 00 00 00
2F 33 00 08 00 40 0A 6B 00 00 60 02 6B 2F 33 00
A4 B0 F6 33 03 00 00 00 00 A6 B0 F6 32 03 00 00
00 00 00 01 00 00 00 00 A4 16 46 C4 31 03 00 00
00 00 00 00 00 00 00 00 00 48 61 DD E0 B3 97 19
00 00 00 00 00 00 00 00 00 48 61 ED 65 06 80 00
00 00 00 30 85 B5 17 19 00 00 00 00 00 00 80 00
99 01 00 00 00 53 18 7B 00 00 00 00 00 00 40 00
D1 60 ED 65 06 53 58 7B 00 00 00 00 00 00 00 00
            48 61 ED 65 06 00 40 00
```

(Skip rounds 1 to 22)

Round #23

After theta

```
BD 5B 7B D5 BE 03 9E 1B D9 A6 6A 12 CB 04 FC 5D
D0 76 3F A3 A9 F2 C4 09 73 F7 06 51 68 18 7E FD
7D 8C 28 76 AE 14 D1 94 95 CB 8C F2 5D 99 24 A7
1B E0 72 4D 86 3C F3 72 E0 77 86 C1 EB DE 56 02
53 F2 40 67 99 64 8E 5A 28 C2 52 4C 16 EA 6B E6
44 FC F9 BA AB 82 C3 68 60 00 F5 9D BB 09 26 A1
06 97 90 96 D8 D6 D6 25 8F 47 11 DB 72 4C A5 EA
57 AB F9 4C 32 96 3C C5 31 37 33 94 60 18 D5 F3
28 B3 7D E1 85 AE 9A 77 97 19 4B 51 B3 40 CB 7E
FA CB DB 12 56 A0 79 E2 58 E9 9B B9 02 03 F7 B2
64 6B 36 AE 0D 05 F9 33 A4 B7 F7 90 B3 01 A9 29
24 A7 43 A9 2D C2 F3 DE 9B 7B E1 63 BA 3D F4 70
            B5 F3 BB A0 09 AC 14 1A
```

After rho

```
BD 5B 7B D5 BE 03 9E 1B B2 4D D5 24 96 09 F8 BB
B4 DD CF 68 AA 3C 71 02 86 E1 D7 3F 77 6F 10 85
A5 88 A6 EC 63 44 B1 73 DF 95 49 72 5A B9 CC 28
D7 64 C8 33 2F B7 01 2E 00 F8 9D 61 F0 BA B7 95
79 A0 B3 4C 32 47 AD 29 BE 66 8E 22 2C C5 64 A1
23 E2 CF D7 5D 15 1C 46 84 82 01 D4 77 EE 26 98
B4 C4 B6 B6 2E 31 B8 84 98 4A D5 1F 8F 22 B6 E5
26 19 4B 9E E2 AB D5 7C 28 C1 30 AA E7 63 6E 66
2F BC D0 55 F3 0E 65 B6 65 BF CB 8C A5 A8 59 A0
34 4F 5C 7F 79 5B C2 0A B2 58 E9 9B B9 02 03 F7
E4 CF 90 AD D9 B8 36 14 90 DE DE 43 CE 06 A4 A6
E4 74 28 B5 45 78 DE 9B 7B E1 63 BA 3D F4 70 9B
            85 46 ED FC 2E 68 02 2B
```

After pi

```
BD 5B 7B D5 BE 03 9E 1B D7 64 C8 33 2F B7 01 2E
B4 C4 B6 B6 2E 31 B8 84 34 4F 5C 7F 79 5B C2 0A
85 46 ED FC 2E 68 02 2B 86 E1 D7 3F 77 6F 10 85
BE 66 8E 22 2C C5 64 A1 23 E2 CF D7 5D 15 1C 46
2F BC D0 55 F3 0E 65 B6 E4 74 28 B5 45 78 DE 9B
B2 4D D5 24 96 09 F8 BB 00 F8 9D 61 F0 BA B7 95
98 4A D5 1F 8F 22 B6 E5 B2 58 E9 9B B9 02 03 F7
E4 CF 90 AD D9 B8 36 14 A5 88 A6 EC 63 44 B1 73
DF 95 49 72 5A B9 CC 28 84 82 01 D4 77 EE 26 98
65 BF CB 8C A5 A8 59 A0 7B E1 63 BA 3D F4 70 9B
B4 DD CF 68 AA 3C 71 02 79 A0 B3 4C 32 47 AD 29
26 19 4B 9E E2 AB D5 7C 28 C1 30 AA E7 63 6E 66
            90 DE DE 43 CE 06 A4 A6
```

After chi

```
9D DB 4D 51 BE 03 26 9B D7 6F 80 7A 7E FD 43 24
35 C4 17 36 28 11 B8 A5 0C 56 4E 7E E9 58 5E 1A
C7 62 6D DE 2F DC 03 0F 87 61 96 EA 26 7F 08 C3
B2 7A 9E 22 8E CF 05 11 E3 A2 E7 77 59 65 86 4F
2D 3D 07 5F C1 09 65 B2 DC 72 20 B5 4D F8 BA BB
2A 4F 95 3A 99 09 F8 DB 22 E8 B5 E1 C0 BA B6 87
DC CD C5 3B CF 9A 82 E5 A0 58 AC 9B BF 03 CB 5C
E4 7F 98 EC B9 0A 31 10 A5 8A A6 68 46 02 93 E3
BE A8 83 7A DA B9 95 08 9E C2 21 E6 6F BA 06 83
E1 B7 4F C8 E7 A8 D8 C0 21 F4 2A A8 25 4D 3C 93
B2 C4 87 FA 6A 94 21 56 71 60 83 6C 37 07 87 2B
B6 07 85 DF EA AF 55 FC 0C C0 31 82 C7 5B 3F 66
            D9 FE EE 47 DE 45 28 8F
```

After iota

```
95 5B 4D D1 BE 03 26 1B D7 6F 80 7A 7E FD 43 24
35 C4 17 36 28 11 B8 A5 0C 56 4E 7E E9 58 5E 1A
C7 62 6D DE 2F DC 03 0F 87 61 96 EA 26 7F 08 C3
B2 7A 9E 22 8E CF 05 11 E3 A2 E7 77 59 65 86 4F
2D 3D 07 5F C1 09 65 B2 DC 72 20 B5 4D F8 BA BB
2A 4F 95 3A 99 09 F8 DB 22 E8 B5 E1 C0 BA B6 87
DC CD C5 3B CF 9A 82 E5 A0 58 AC 9B BF 03 CB 5C
E4 7F 98 EC B9 0A 31 10 A5 8A A6 68 46 02 93 E3
BE A8 83 7A DA B9 95 08 9E C2 21 E6 6F BA 06 83
E1 B7 4F C8 E7 A8 D8 C0 21 F4 2A A8 25 4D 3C 93
B2 C4 87 FA 6A 94 21 56 71 60 83 6C 37 07 87 2B
B6 07 85 DF EA AF 55 FC 0C C0 31 82 C7 5B 3F 66
            D9 FE EE 47 DE 45 28 8F
```

After permutation

```
95 5B 4D D1 BE 03 26 1B D7 6F 80 7A 7E FD 43 24
35 C4 17 36 28 11 B8 A5 0C 56 4E 7E E9 58 5E 1A
C7 62 6D DE 2F DC 03 0F 87 61 96 EA 26 7F 08 C3
B2 7A 9E 22 8E CF 05 11 E3 A2 E7 77 59 65 86 4F
2D 3D 07 5F C1 09 65 B2 DC 72 20 B5 4D F8 BA BB
2A 4F 95 3A 99 09 F8 DB 22 E8 B5 E1 C0 BA B6 87
DC CD C5 3B CF 9A 82 E5 A0 58 AC 9B BF 03 CB 5C
E4 7F 98 EC B9 0A 31 10 A5 8A A6 68 46 02 93 E3
BE A8 83 7A DA B9 95 08 9E C2 21 E6 6F BA 06 83
E1 B7 4F C8 E7 A8 D8 C0 21 F4 2A A8 25 4D 3C 93
B2 C4 87 FA 6A 94 21 56 71 60 83 6C 37 07 87 2B
B6 07 85 DF EA AF 55 FC 0C C0 31 82 C7 5B 3F 66
            D9 FE EE 47 DE 45 28 8F
```

State (as lanes of integers)

```
[0, 0] = 1b2603bed14d5b95
[1, 0] = 2443fd7e7a806fd7
[2, 0] = a5b811283617c435
[3, 0] = 1a5e58e97e4e560c
[4, 0] = 0f03dc2fde6d62c7
[0, 1] = c3087f26ea966187
[1, 1] = 1105cf8e229e7ab2
[2, 1] = 4f86655977e7a2e3
[3, 1] = b26509c15f073d2d
[4, 1] = bbbaf84db52072dc
[0, 2] = dbf809993a954f2a
[1, 2] = 87b6bac0e1b5e822
[2, 2] = e5829acf3bc5cddc
[3, 2] = 5ccb03bf9bac58a0
[4, 2] = 10310ab9ec987fe4
```

```
[0, 3] = e393024668a68aa5
[1, 3] = 0895b9da7a83a8be
[2, 3] = 8306ba6fe621c29e
[3, 3] = c0d8a8e7c84fb7e1
[4, 3] = 933c4d25a82af421
[0, 4] = 5621946afa87c4b2
[1, 4] = 2b8707376c836071
[2, 4] = fc55afeadf8507b6
[3, 4] = 663f5bc78231c00c
[4, 4] = 8f2845de47eefed9
```

The hash value is

```
95 5B 4D D1 BE 03 26 1B D7 6F 80 7A 7E FD 43 24
35 C4 17 36 28 11 B8 A5 0C 56 4E 7E E9 58 5E 1A
C7 62 6D DE 2F DC 03 0F 87 61 96 EA 26 7F 08 C3
```

B.18 Dedicated Hash-Function 16 (SHA3-512)

NOTE 1 Data is presented in three different ways: bit strings, byte strings and *w*-length words (for the lanes).

NOTE 2 Bit strings are the sequence of bits from left to right.

NOTE 3 Byte strings are the bytes from left to right and the bits within the byte are right to left.

NOTE 4 Words are the integer representation of the values in the lanes.

SHA3-512 sample

The message as bit string

```
(empty message)
```

XORed state (in bytes)

```
06 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 80 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
   00 00 00 00 00 00 00 00
```

XORed state (as lanes of integers)

```
[0, 0] = 0000000000000006
[1, 0] = 0000000000000000
[2, 0] = 0000000000000000
[3, 0] = 0000000000000000
[4, 0] = 0000000000000000
[0, 1] = 0000000000000000
[1, 1] = 0000000000000000
[2, 1] = 0000000000000000
[3, 1] = 8000000000000000
[4, 1] = 0000000000000000
[0, 2] = 0000000000000000
[1, 2] = 0000000000000000
```

```
[2, 2] = 0000000000000000
[3, 2] = 0000000000000000
[4, 2] = 0000000000000000
[0, 3] = 0000000000000000
[1, 3] = 0000000000000000
[2, 3] = 0000000000000000
[3, 3] = 0000000000000000
[4, 3] = 0000000000000000
[0, 4] = 0000000000000000
[1, 4] = 0000000000000000
[2, 4] = 0000000000000000
[3, 4] = 0000000000000000
[4, 4] = 0000000000000000
```

Round #0

After theta

```
06 00 00 00 00 00 00 00 06 00 00 00 00 00 00 00
01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0C 00 00 00 00 00 00 80 00 00 00 00 00 00 00 00
06 00 00 00 00 00 00 00 01 00 00 00 00 00 00 00
00 00 00 00 00 00 00 80 0C 00 00 00 00 00 00 80
00 00 00 00 00 00 00 00 06 00 00 00 00 00 00 00
01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0C 00 00 00 00 00 00 80 00 00 00 00 00 00 00 00
06 00 00 00 00 00 00 00 01 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 0C 00 00 00 00 00 00 80
00 00 00 00 00 00 00 00 06 00 00 00 00 00 00 00
01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
            0C 00 00 00 00 00 00 80
```

After rho

```
06 00 00 00 00 00 00 00 0C 00 00 00 00 00 00 00
00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00
00 00 00 64 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 60 00 00 40 00 00 00 00 00 00 00
00 00 00 00 00 00 40 00 00 00 C8 00 00 00 00 00
00 00 00 00 00 00 00 00 00 18 00 00 00 00 00 00
00 00 00 00 00 08 00 00 00 00 00 00 00 00 00 00
00 00 00 00 40 06 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 C0 00 00 00 80 00 00 00 00 00 00
00 00 00 00 00 00 00 00 80 0C 00 00 00 00 00 00
00 00 00 00 00 00 00 00 18 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 20 00 00 00 00 00 00 00
            00 20 03 00 00 00 00 00
```

After pi

```
06 00 00 00 00 00 00 00 00 00 00 00 00 60 00 00
00 00 00 00 00 08 00 00 00 00 00 00 00 00 00 00
00 20 03 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 C8 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 C0 00 00 00 00 00 00 00 00 00 20
0C 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 80 0C 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 64 00 00 00 00
00 00 00 00 00 00 00 00 00 18 00 00 00 00 00 00
00 80 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 40 00 00 00 00 00 00 40 00
00 00 00 00 40 06 00 00 00 00 00 00 00 00 00 00
            18 00 00 00 00 00 00 00
```

After chi

```
06 00 00 00 00 08 00 00 00 00 00 00 00 60 00 00
00 20 03 00 00 08 00 00 06 00 00 00 00 00 00 00
00 20 03 00 00 60 00 00 00 00 00 00 00 00 00 00
00 00 C8 00 00 C0 00 00 00 00 00 00 00 00 00 20
00 00 00 00 00 C0 00 00 00 00 C8 00 00 00 00 20
0C 00 00 00 00 00 00 00 C0 0C 00 00 00 00 00 00
00 00 00 00 00 00 00 00 8C 0C 00 00 00 00 00 00
40 00 00 00 00 00 00 00 00 00 18 00 64 00 00 00 00
00 80 00 00 00 00 00 00 00 00 18 00 00 00 00 00 00
00 80 00 64 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 40 06 00 40 00 00 00 00 00 00 40 00
18 00 00 00 40 06 00 00 00 00 00 00 00 00 00 40
            18 00 00 00 00 00 40 00
```

After iota

```
07 00 00 00 00 08 00 00 00 00 00 00 00 60 00 00
00 20 03 00 00 08 00 00 06 00 00 00 00 00 00 00
00 20 03 00 00 60 00 00 00 00 00 00 00 00 00 00
00 00 C8 00 00 C0 00 00 00 00 00 00 00 00 00 20
00 00 00 00 00 C0 00 00 00 00 C8 00 00 00 00 20
0C 00 00 00 00 00 00 00 C0 0C 00 00 00 00 00 00
00 00 00 00 00 00 00 00 8C 0C 00 00 00 00 00 00
40 00 00 00 00 00 00 00 00 00 18 00 64 00 00 00 00
00 80 00 00 00 00 00 00 00 00 18 00 00 00 00 00 00
00 80 00 64 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 40 06 00 40 00 00 00 00 00 00 40 00
18 00 00 00 40 06 00 00 00 00 00 00 00 00 00 40
            18 00 00 00 00 00 40 00
```

(Skip rounds 1 to 22)

Round #23

After theta

```
AC 55 F3 6C 45 3B 9A 54 F3 B6 DB 13 0F 0F 54 16
AA 2B 77 77 09 39 9A 23 C0 30 53 CE 15 21 F0 24
AC 5F 9D 80 59 A4 0D 7B 08 65 07 88 55 78 03 79
74 8F 0C 18 AA D5 85 E1 37 BF CF DB F9 A4 3E E5
44 DE 1C E0 10 D0 A7 6D 51 2A 45 11 3C 32 8D 10
38 FC F6 18 A4 21 AC 04 CD 6E 92 AC 91 33 D1 48
88 28 43 70 19 90 E7 7C FC E9 C2 B5 B0 C0 6C 97
DA A0 65 1D C0 BB 4C EF 48 C4 8C FB EF D1 B2 CD
9D 20 37 49 6A D4 3D 7F A3 38 B2 81 F5 1A 4F FC
29 1C B2 12 B4 45 A2 EC CC 35 72 2D 4D 4F CB 1B
88 D9 B0 40 35 51 83 1E 34 52 E6 C0 03 FD 31 33
09 AF BE 8D 62 DC 6C 1D 9E BC 42 EE 0B AC 4E AD
            68 AC A4 C7 72 12 57 48
```

After rho

```
AC 55 F3 6C 45 3B 9A 54 E6 6D B7 27 1E 1E A8 2C
EA CA DD 5D 42 8E E6 88 11 02 4F 02 0C 33 E5 5C
22 6D D8 63 FD EA 04 CC 58 85 37 90 87 50 76 80
80 A1 5A 5D 18 4E F7 C8 F9 CD EF F3 76 3E A9 4F
6F 0E 70 08 E8 D3 36 22 D3 08 11 A5 52 14 C1 23
C0 E1 B7 C7 20 0D 61 25 23 35 BB 49 B2 46 CE 44
82 CB 80 3C E7 43 44 19 81 D9 2E F9 D3 85 6B 61
0E E0 5D A6 77 6D D0 B2 F7 DF A3 65 9B 91 88 19
26 49 8D BA E7 AF 13 E4 27 FE 51 1C D9 C0 7A 8D
48 94 3D 85 43 56 82 B6 1B CC 35 72 2D 4D 4F CB
0D 7A 20 66 C3 02 D5 44 D0 48 99 03 0F F4 C7 CC
E1 D5 B7 51 8C 9B AD 23 BC 42 EE 0B AC 4E AD 9E
            15 12 1A 2B E9 B1 9C C4
```

After pi

```
AC 55 F3 6C 45 3B 9A 54 80 A1 5A 5D 18 4E F7 C8
82 CB 80 3C E7 43 44 19 48 94 3D 85 43 56 82 B6
15 12 1A 2B E9 B1 9C C4 11 02 4F 02 0C 33 E5 5C
D3 08 11 A5 52 14 C1 23 C0 E1 B7 C7 20 0D 61 25
26 49 8D BA E7 AF 13 E4 E1 D5 B7 51 8C 9B AD 23
E6 6D B7 27 1E 1E A8 2C F9 CD EF F3 76 3E A9 4F
81 D9 2E F9 D3 85 6B 61 1B CC 35 72 2D 4D 4F CB
0D 7A 20 66 C3 02 D5 44 22 6D D8 63 FD EA 04 CC
58 85 37 90 87 50 76 80 23 35 BB 49 B2 46 CE 44
27 FE 51 1C D9 C0 7A 8D BC 42 EE 0B AC 4E AD 9E
EA CA DD 5D 42 8E E6 88 6F 0E 70 08 E8 D3 36 22
0E E0 5D A6 77 6D D0 B2 F7 DF A3 65 9B 91 88 19
            D0 48 99 03 0F F4 C7 CC
```

After chi

```
AE 1F 73 4C A2 3A 9A 45 C8 B5 67 DC 18 5A 75 6E
97 C9 82 16 4F E2 58 59 E0 D1 DC C1 47 5C 80 A6
15 B2 12 3A F1 F5 F9 4C 11 E3 E9 40 2C 3A C5 58
F5 00 19 9D 95 B6 D3 E3 01 75 85 86 28 1D CD 26
36 4B C5 B8 E7 8F 53 B8 23 DD A7 F4 DE 9F AD 00
E6 7D B7 2F 9F 9F EA 0C E3 C9 FE F1 5A 76 AD C5
85 EB 2E FD 11 87 FB 65 F9 C9 A2 73 31 51 67 E3
14 FA 68 B6 A3 22 D4 07 01 5D 50 2A CD EC 8C 88
5C 4F 77 84 CE D0 46 09 BB 35 15 4A 96 48 4B 56
25 D3 41 7C 88 60 7A CD E4 C2 C9 9B AE 5E DF 9E
EA 2A D0 FB 55 A2 26 18 9E 11 D2 49 60 43 3E 2B
0E E0 45 A4 73 09 97 76 DD 5D E7 39 DB 9B A8 19
            D5 4C B9 03 A7 A5 D7 EE
```

After iota

```
A6 9F 73 CC A2 3A 9A C5 C8 B5 67 DC 18 5A 75 6E
97 C9 82 16 4F E2 58 59 E0 D1 DC C1 47 5C 80 A6
15 B2 12 3A F1 F5 F9 4C 11 E3 E9 40 2C 3A C5 58
F5 00 19 9D 95 B6 D3 E3 01 75 85 86 28 1D CD 26
36 4B C5 B8 E7 8F 53 B8 23 DD A7 F4 DE 9F AD 00
E6 7D B7 2F 9F 9F EA 0C E3 C9 FE F1 5A 76 AD C5
85 EB 2E FD 11 87 FB 65 F9 C9 A2 73 31 51 67 E3
14 FA 68 B6 A3 22 D4 07 01 5D 50 2A CD EC 8C 88
5C 4F 77 84 CE D0 46 09 BB 35 15 4A 96 48 4B 56
25 D3 41 7C 88 60 7A CD E4 C2 C9 9B AE 5E DF 9E
EA 2A D0 FB 55 A2 26 18 9E 11 D2 49 60 43 3E 2B
0E E0 45 A4 73 09 97 76 DD 5D E7 39 DB 9B A8 19
            D5 4C B9 03 A7 A5 D7 EE
```

After permutation

```
A6 9F 73 CC A2 3A 9A C5 C8 B5 67 DC 18 5A 75 6E
97 C9 82 16 4F E2 58 59 E0 D1 DC C1 47 5C 80 A6
15 B2 12 3A F1 F5 F9 4C 11 E3 E9 40 2C 3A C5 58
F5 00 19 9D 95 B6 D3 E3 01 75 85 86 28 1D CD 26
36 4B C5 B8 E7 8F 53 B8 23 DD A7 F4 DE 9F AD 00
E6 7D B7 2F 9F 9F EA 0C E3 C9 FE F1 5A 76 AD C5
85 EB 2E FD 11 87 FB 65 F9 C9 A2 73 31 51 67 E3
14 FA 68 B6 A3 22 D4 07 01 5D 50 2A CD EC 8C 88
5C 4F 77 84 CE D0 46 09 BB 35 15 4A 96 48 4B 56
25 D3 41 7C 88 60 7A CD E4 C2 C9 9B AE 5E DF 9E
EA 2A D0 FB 55 A2 26 18 9E 11 D2 49 60 43 3E 2B
0E E0 45 A4 73 09 97 76 DD 5D E7 39 DB 9B A8 19
            D5 4C B9 03 A7 A5 D7 EE
```

State (as lanes of integers)

```
[0, 0] = c59a3aa2cc739fa6
[1, 0] = 6e755a18dc67b5c8
[2, 0] = 5958e24f1682c997
[3, 0] = a6805c47c1dcd1e0
[4, 0] = 4cf9f5f13a12b215
[0, 1] = 58c53a2c40e9e311
[1, 1] = e3d3b6959d1900f5
[2, 1] = 26cd1d2886857501
[3, 1] = b8538fe7b8c54b36
[4, 1] = 00ad9fdef4a7dd23
[0, 2] = 0cea9f9f2fb77de6
[1, 2] = c5ad765af1fec9e3
[2, 2] = 65fb8711fd2eeb85
[3, 2] = e367513173a2c9f9
[4, 2] = 07d422a3b668fa14
[0, 3] = 888ceccd2a505d01
[1, 3] = 0946d0ce84774f5c
[2, 3] = 564b48964a1535bb
[3, 3] = cd7a60887c41d325
[4, 3] = 9edf5eae9bc9c2e4
[0, 4] = 1826a255fbd02aea
[1, 4] = 2b3e436049d2119e
[2, 4] = 76970973a445e00e
[3, 4] = 19a89bdb39e75ddd
[4, 4] = eed7a5a703b94cd5
```

The hash value is

```
A6 9F 73 CC A2 3A 9A C5 C8 B5 67 DC 18 5A 75 6E
97 C9 82 16 4F E2 58 59 E0 D1 DC C1 47 5C 80 A6
15 B2 12 3A F1 F5 F9 4C 11 E3 E9 40 2C 3A C5 58
F5 00 19 9D 95 B6 D3 E3 01 75 85 86 28 1D CD 26
```

The message as bit string

```
1 1 0 0 1
```

XORed state (in bytes)

```
D3 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 80 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
   00 00 00 00 00 00 00 00
```

XORed state (as lanes of integers)

```
[0, 0] = 00000000000000d3
[1, 0] = 0000000000000000
[2, 0] = 0000000000000000
[3, 0] = 0000000000000000
[4, 0] = 0000000000000000
[0, 1] = 0000000000000000
[1, 1] = 0000000000000000
[2, 1] = 0000000000000000
```

```
[3, 1] = 8000000000000000
[4, 1] = 0000000000000000
[0, 2] = 0000000000000000
[1, 2] = 0000000000000000
[2, 2] = 0000000000000000
[3, 2] = 0000000000000000
[4, 2] = 0000000000000000
[0, 3] = 0000000000000000
[1, 3] = 0000000000000000
[2, 3] = 0000000000000000
[3, 3] = 0000000000000000
[4, 3] = 0000000000000000
[0, 4] = 0000000000000000
[1, 4] = 0000000000000000
[2, 4] = 0000000000000000
[3, 4] = 0000000000000000
[4, 4] = 0000000000000000
```

Round #0

After theta

```
D3 00 00 00 00 00 00 00 D3 00 00 00 00 00 00 00
01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
A6 01 00 00 00 00 00 80 00 00 00 00 00 00 00 00
D3 00 00 00 00 00 00 00 01 00 00 00 00 00 00 00
00 00 00 00 00 00 00 80 A6 01 00 00 00 00 00 80
00 00 00 00 00 00 00 00 D3 00 00 00 00 00 00 00
01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
A6 01 00 00 00 00 00 80 00 00 00 00 00 00 00 00
D3 00 00 00 00 00 00 00 01 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 A6 01 00 00 00 00 00 80
00 00 00 00 00 00 00 00 D3 00 00 00 00 00 00 00
01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
            A6 01 00 00 00 00 00 80
```

After rho

```
D3 00 00 00 00 00 00 00 A6 01 00 00 00 00 00 00
00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00
00 00 00 34 0D 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 30 0D 00 40 00 00 00 00 00 00 00
00 00 00 00 00 00 40 00 00 00 68 1A 00 00 00 00
00 00 00 00 00 00 00 00 00 4C 03 00 00 00 00 00
00 00 00 00 00 08 00 00 00 00 00 00 00 00 00 00
00 00 00 00 40 D3 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 60 1A 00 00 80 00 00 00 00 00 00
00 00 00 00 00 00 00 00 80 A6 01 00 00 00 00 00
00 00 00 00 00 00 00 00 4C 03 00 00 00 00 00 00
00 00 00 00 00 00 00 20 00 00 00 00 00 00 00 00
            00 A0 69 00 00 00 00 00
```

After pi

```
D3 00 00 00 00 00 00 00 00 00 00 00 00 30 0D 00
00 00 00 00 00 08 00 00 00 00 00 00 00 00 00 00
00 A0 69 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 68 1A 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 60 1A 00 00 00 00 00 00 00 00 20
A6 01 00 00 00 00 00 00 40 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 80 A6 01 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 34 0D 00 00 00
00 00 00 00 00 00 00 00 00 4C 03 00 00 00 00 00
00 80 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 40 00 00 00 00 00 00 40 00
00 00 00 00 40 D3 00 00 00 00 00 00 00 00 00 00
            4C 03 00 00 00 00 00 00
```

After chi

```
D3 00 00 00 00 08 00 00 00 00 00 00 00 30 0D 00
00 A0 69 00 00 08 00 00 D3 00 00 00 00 00 00 00
00 A0 69 00 00 30 0D 00 00 00 00 00 00 00 00 00
00 00 68 1A 00 60 1A 00 00 00 00 00 00 00 00 20
00 00 00 00 00 60 1A 00 00 00 68 1A 00 00 00 20
A6 01 00 00 00 00 00 00 C0 A6 01 00 00 00 00 00
00 00 00 00 00 00 00 00 26 A7 01 00 00 00 00 00
40 00 00 00 00 00 00 00 00 4C 03 34 0D 00 00 00
00 80 00 00 00 00 00 00 00 4C 03 00 00 00 00 00
00 80 00 34 0D 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 40 D3 00 40 00 00 00 00 00 00 40 00
4C 03 00 00 40 D3 00 00 00 00 00 00 00 00 00 40
            4C 03 00 00 00 00 40 00
```

After iota

```
D2 00 00 00 00 08 00 00 00 00 00 00 00 30 0D 00
00 A0 69 00 00 08 00 00 D3 00 00 00 00 00 00 00
00 A0 69 00 00 30 0D 00 00 00 00 00 00 00 00 00
00 00 68 1A 00 60 1A 00 00 00 00 00 00 00 00 20
00 00 00 00 00 60 1A 00 00 00 68 1A 00 00 00 20
A6 01 00 00 00 00 00 00 C0 A6 01 00 00 00 00 00
00 00 00 00 00 00 00 00 26 A7 01 00 00 00 00 00
40 00 00 00 00 00 00 00 00 4C 03 34 0D 00 00 00
00 80 00 00 00 00 00 00 00 4C 03 00 00 00 00 00
00 80 00 34 0D 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 40 D3 00 40 00 00 00 00 00 00 40 00
4C 03 00 00 40 D3 00 00 00 00 00 00 00 00 00 40
            4C 03 00 00 00 00 40 00
```

(Skip rounds 1 to 22)

Round #23

After theta

```
8C 3E 41 CB D0 65 FC 4C 7D 72 90 CA 3E 31 E5 16
BF 34 08 00 48 62 98 BF F7 11 2F 6C BD 36 ED 59
C3 26 A5 74 61 0B DF 40 80 43 3E 4A 07 80 B7 FD
08 30 A2 25 D7 C2 8D C6 E9 93 68 6B 6B 56 35 C5
7E DE A8 17 F1 8B 42 73 18 0C B8 DD 01 9B 77 E4
D2 90 45 92 85 F5 E6 0F D5 F4 0F 1B A4 3B DA AF
8F A7 AE 44 18 49 22 B3 09 A8 FD C7 C3 40 C0 D1
E3 B2 55 35 3F E5 88 2E 20 8F 13 0A DE F6 23 51
BE B7 81 D8 C4 87 AA C8 33 CA 45 F6 30 F5 40 38
72 4D 2E F8 3B D1 92 3E 95 1E D9 29 82 D7 3B A1
B9 3E B0 E5 2B 29 51 55 90 CA 7E 75 0C 69 34 81
C2 3E 37 EE C2 E0 DB D6 91 C8 5D 11 B2 D4 9F 3B
            E0 54 36 27 2C FD 1B 30
```

After rho

```
8C 3E 41 CB D0 65 FC 4C FA E4 20 95 7D 62 CA 2D
2F 0D 02 00 92 18 E6 EF 6B D3 9E 75 1F F1 C2 D6
5B F8 06 1A 36 29 A5 0B 74 00 78 DB 0F 38 E4 A3
5A 72 2D DC 68 8C 00 23 71 FA 24 DA DA 9A 55 4D
6F D4 8B F8 45 A1 39 3F 79 47 8E C1 80 DB 1D B0
90 86 2C 92 2C AC 37 7F BF 56 D3 3F 6C 90 EE 68
25 C2 48 12 99 7D 3C 75 81 80 A3 13 50 FB 8F 87
9A 9F 72 44 97 71 D9 AA 14 BC ED 47 A2 40 1E 27
10 9B F8 50 15 D9 F7 36 20 9C 19 E5 22 7B 98 7A
5A D2 47 AE C9 05 7F 27 A1 95 1E D9 29 82 D7 3B
44 55 E5 FA C0 96 AF A4 42 2A FB D5 31 A4 D1 04
D8 E7 C6 5D 18 7C DB 5A C8 5D 11 B2 D4 9F 3B 91
            06 0C 38 95 CD 09 4B FF
```

After pi

```
8C 3E 41 CB D0 65 FC 4C 5A 72 2D DC 68 8C 00 23
25 C2 48 12 99 7D 3C 75 5A D2 47 AE C9 05 7F 27
06 0C 38 95 CD 09 4B FF 6B D3 9E 75 1F F1 C2 D6
79 47 8E C1 80 DB 1D B0 90 86 2C 92 2C AC 37 7F
10 9B F8 50 15 D9 F7 36 D8 E7 C6 5D 18 7C DB 5A
FA E4 20 95 7D 62 CA 2D 71 FA 24 DA DA 9A 55 4D
81 80 A3 13 50 FB 8F 87 A1 95 1E D9 29 82 D7 3B
44 55 E5 FA C0 96 AF A4 5B F8 06 1A 36 29 A5 0B
74 00 78 DB 0F 38 E4 A3 BF 56 D3 3F 6C 90 EE 68
20 9C 19 E5 22 7B 98 7A C8 5D 11 B2 D4 9F 3B 91
2F 0D 02 00 92 18 E6 EF 6F D4 8B F8 45 A1 39 3F
9A 9F 72 44 97 71 D9 AA 14 BC ED 47 A2 40 1E 27
            42 2A FB D5 31 A4 D1 04
```

After chi

```
A9 BE 01 C9 41 14 C0 18 00 62 2A 70 28 8C 43 21
21 CE 70 03 9D 75 3C AD D2 E0 06 E4 D9 61 CB 27
54 4C 14 81 E5 81 4B DC EB 53 BE 67 33 D5 E0 99
79 5E 5E 81 91 8A DD B0 58 E2 2A 9F 24 88 3F 37
33 8B E0 70 12 58 F7 B2 C8 E3 C6 DD 98 76 C6 7A
7A E4 A3 94 7D 03 40 AF 51 EF 38 12 F3 9A 05 75
C5 C0 42 31 90 EF A7 03 1B 35 1E DC 14 E2 97 32
45 4F E1 B0 42 0E BA E4 D0 AE 85 3E 56 A9 AF 43
74 88 70 1B 0D 53 F4 B1 77 17 D3 2D B8 14 CD E9
33 3C 1F ED 00 5B 1C 70 EC 5D 69 73 DD 8F 7B 31
BF 06 72 04 00 48 26 6F 6B F4 06 FB 65 A1 3F 3A
D8 9D 60 D4 86 D5 18 AA 39 B9 ED 47 20 58 38 CC
            02 FA 72 2D 74 05 C8 14
```

After iota

```
A1 3E 01 49 41 14 C0 98 00 62 2A 70 28 8C 43 21
21 CE 70 03 9D 75 3C AD D2 E0 06 E4 D9 61 CB 27
54 4C 14 81 E5 81 4B DC EB 53 BE 67 33 D5 E0 99
79 5E 5E 81 91 8A DD B0 58 E2 2A 9F 24 88 3F 37
33 8B E0 70 12 58 F7 B2 C8 E3 C6 DD 98 76 C6 7A
7A E4 A3 94 7D 03 40 AF 51 EF 38 12 F3 9A 05 75
C5 C0 42 31 90 EF A7 03 1B 35 1E DC 14 E2 97 32
45 4F E1 B0 42 0E BA E4 D0 AE 85 3E 56 A9 AF 43
74 88 70 1B 0D 53 F4 B1 77 17 D3 2D B8 14 CD E9
33 3C 1F ED 00 5B 1C 70 EC 5D 69 73 DD 8F 7B 31
BF 06 72 04 00 48 26 6F 6B F4 06 FB 65 A1 3F 3A
D8 9D 60 D4 86 D5 18 AA 39 B9 ED 47 20 58 38 CC
            02 FA 72 2D 74 05 C8 14
```

After permutation

```
A1 3E 01 49 41 14 C0 98 00 62 2A 70 28 8C 43 21
21 CE 70 03 9D 75 3C AD D2 E0 06 E4 D9 61 CB 27
54 4C 14 81 E5 81 4B DC EB 53 BE 67 33 D5 E0 99
79 5E 5E 81 91 8A DD B0 58 E2 2A 9F 24 88 3F 37
33 8B E0 70 12 58 F7 B2 C8 E3 C6 DD 98 76 C6 7A
7A E4 A3 94 7D 03 40 AF 51 EF 38 12 F3 9A 05 75
C5 C0 42 31 90 EF A7 03 1B 35 1E DC 14 E2 97 32
45 4F E1 B0 42 0E BA E4 D0 AE 85 3E 56 A9 AF 43
74 88 70 1B 0D 53 F4 B1 77 17 D3 2D B8 14 CD E9
33 3C 1F ED 00 5B 1C 70 EC 5D 69 73 DD 8F 7B 31
BF 06 72 04 00 48 26 6F 6B F4 06 FB 65 A1 3F 3A
D8 9D 60 D4 86 D5 18 AA 39 B9 ED 47 20 58 38 CC
            02 FA 72 2D 74 05 C8 14
```

State (as lanes of integers)

```
[0, 0] = 98c0144149013ea1
[1, 0] = 21438c28702a6200
[2, 0] = ad3c759d0370ce21
[3, 0] = 27cb61d9e406e0d2
[4, 0] = dc4b81e581144c54
[0, 1] = 99e0d53367be53eb
[1, 1] = b0dd8a91815e5e79
[2, 1] = 373f88249f2ae258
[3, 1] = b2f7581270e08b33
[4, 1] = 7ac67698ddc6e3c8
[0, 2] = af40037d94a3e47a
[1, 2] = 75059af31238ef51
[2, 2] = 03a7ef903142c0c5
[3, 2] = 3297e214dc1e351b
[4, 2] = e4ba0e42b0e14f45
[0, 3] = 43afa9563e85aed0
[1, 3] = b1f4530d1b708874
[2, 3] = e9cd14b82dd31777
[3, 3] = 701c5b00ed1f3c33
[4, 3] = 317b8fdd73695dec
[0, 4] = 6f264800047206bf
[1, 4] = 3a3fa165fb06f46b
[2, 4] = aa18d586d4609dd8
[3, 4] = cc38582047edb939
[4, 4] = 14c805742d72fa02
```

The hash value is

```
A1 3E 01 49 41 14 C0 98 00 62 2A 70 28 8C 43 21
21 CE 70 03 9D 75 3C AD D2 E0 06 E4 D9 61 CB 27
54 4C 14 81 E5 81 4B DC EB 53 BE 67 33 D5 E0 99
79 5E 5E 81 91 8A DD B0 58 E2 2A 9F 24 88 3F 37
```

The message as bit string

```
1 1 0 0 1 0 1 0 0 0 0 1 1 0 1 0 1 1 0 1 1 1 1 0 1 0 0 1 1 0
```

XORed state (in bytes)

```
53 58 7B 99 01 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 80 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
               00 00 00 00 00 00 00 00
```

XORed state (as lanes of integers)

```
[0, 0] = 000000001997b5853
[1, 0] = 0000000000000000
[2, 0] = 0000000000000000
[3, 0] = 0000000000000000
[4, 0] = 0000000000000000
[0, 1] = 0000000000000000
[1, 1] = 0000000000000000
[2, 1] = 0000000000000000
[3, 1] = 8000000000000000
[4, 1] = 0000000000000000
[0, 2] = 0000000000000000
[1, 2] = 0000000000000000
[2, 2] = 0000000000000000
[3, 2] = 0000000000000000
[4, 2] = 0000000000000000
[0, 3] = 0000000000000000
[1, 3] = 0000000000000000
[2, 3] = 0000000000000000
[3, 3] = 0000000000000000
[4, 3] = 0000000000000000
[0, 4] = 0000000000000000
[1, 4] = 0000000000000000
[2, 4] = 0000000000000000
[3, 4] = 0000000000000000
[4, 4] = 0000000000000000
```

Round #0

After theta

```
53 58 7B 99 01 00 00 00 53 58 7B 99 01 00 00 00
01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
A6 B0 F6 32 03 00 00 80 00 00 00 00 00 00 00 00
53 58 7B 99 01 00 00 00 01 00 00 00 00 00 00 00
00 00 00 00 00 00 00 80 A6 B0 F6 32 03 00 00 80
00 00 00 00 00 00 00 00 53 58 7B 99 01 00 00 00
01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
A6 B0 F6 32 03 00 00 80 00 00 00 00 00 00 00 00
53 58 7B 99 01 00 00 00 01 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 A6 B0 F6 32 03 00 00 80
00 00 00 00 00 00 00 00 53 58 7B 99 01 00 00 00
01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
            A6 B0 F6 32 03 00 00 80
```

After rho

```
53 58 7B 99 01 00 00 00 A6 B0 F6 32 03 00 00 00
00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00
00 00 00 34 85 B5 97 19 00 00 00 00 00 00 00 00
97 19 00 00 00 30 85 B5 40 00 00 00 00 00 00 00
00 00 00 00 00 00 40 00 00 00 68 0A 6B 2F 33 00
00 00 00 00 00 00 00 00 00 00 4C 61 ED 65 06 00
00 00 00 00 00 08 00 00 00 00 00 00 00 00 00 00
99 01 00 00 40 53 58 7B 00 00 00 00 00 00 00 00
2F 33 00 00 00 60 0A 6B 00 80 00 00 00 00 00 00
00 00 00 00 00 00 00 00 80 A6 B0 F6 32 03 00 00
00 00 00 00 00 00 00 00 4C 61 ED 65 06 00 00 00
00 00 00 00 00 00 00 00 20 00 00 00 00 00 00 00
            00 A0 29 AC BD CC 00 00
```

After pi

```
53 58 7B 99 01 00 00 00 97 19 00 00 00 30 85 B5
00 00 00 00 00 08 00 00 00 00 00 00 00 00 00 00
00 A0 29 AC BD CC 00 00 00 00 00 00 00 00 00 00
00 00 68 0A 6B 2F 33 00 00 00 00 00 00 00 00 00
2F 33 00 00 00 60 0A 6B 00 00 00 00 00 00 00 20
A6 B0 F6 32 03 00 00 00 40 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 80 A6 B0 F6 32 03 00 00
00 00 00 00 00 00 00 00 00 00 00 34 85 B5 97 19
00 00 00 00 00 00 00 00 00 4C 61 ED 65 06 00 00
00 80 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 40 00 00 00 00 00 00 40 00
99 01 00 00 40 53 58 7B 00 00 00 00 00 00 00 00
            4C 61 ED 65 06 00 00 00
```

After chi

```
53 58 7B 99 01 08 00 00 97 19 00 00 00 30 85 B5
00 A0 29 AC BD C4 00 00 53 58 52 11 00 00 00 00
84 A1 29 AC BD FC 85 B5 00 00 00 00 00 00 00 00
2F 33 68 0A 6B 4F 39 6B 00 00 00 00 00 00 00 00
2F 33 00 00 00 60 0A 6B 00 00 68 0A 6B 2F 33 20
A6 B0 F6 32 03 00 00 00 C0 A6 B0 F6 32 03 00 00
00 00 00 00 00 00 00 00 26 16 46 C4 31 03 00 00
40 00 00 00 00 00 00 00 00 4C 61 D9 E0 B3 97 19
00 80 00 00 00 00 00 00 00 4C 61 ED 65 06 00 00
00 80 00 34 85 B5 97 19 00 00 00 00 00 00 00 00
99 01 00 00 40 53 18 3B 00 00 00 00 00 00 40 00
D5 60 ED 65 46 53 58 7B 00 00 00 00 00 00 00 40
            4C 61 ED 65 06 00 40 00
```

After iota

```
52 58 7B 99 01 08 00 00 97 19 00 00 00 30 85 B5
00 A0 29 AC BD C4 00 00 53 58 52 11 00 00 00 00
84 A1 29 AC BD FC 85 B5 00 00 00 00 00 00 00 00
2F 33 68 0A 6B 4F 39 6B 00 00 00 00 00 00 00 00
2F 33 00 00 00 60 0A 6B 00 00 68 0A 6B 2F 33 20
A6 B0 F6 32 03 00 00 00 C0 A6 B0 F6 32 03 00 00
00 00 00 00 00 00 00 00 26 16 46 C4 31 03 00 00
40 00 00 00 00 00 00 00 00 4C 61 D9 E0 B3 97 19
00 80 00 00 00 00 00 00 00 4C 61 ED 65 06 00 00
00 80 00 34 85 B5 97 19 00 00 00 00 00 00 00 00
99 01 00 00 40 53 18 3B 00 00 00 00 00 00 40 00
D5 60 ED 65 46 53 58 7B 00 00 00 00 00 00 00 40
            4C 61 ED 65 06 00 40 00
```

(Skip rounds 1 to 22)

Round #23

After theta

```
90 F6 4A 2B 92 8C C7 53 FB 93 74 1B F2 C9 3F DA
5C CE AB BF CC 44 7B 46 A9 10 30 E8 9B 33 44 8A
B0 63 1E 7F 5F 54 47 76 4D B7 91 25 DA 72 72 10
D8 F6 AD 87 48 26 80 01 AB FE EA A9 2F 72 74 E0
20 1E DE FE 0D 29 89 54 44 C7 D9 E3 9F C2 B7 55
40 BB FA 09 2A E5 48 75 FA 43 A9 56 2A 7A E9 99
4D CD 11 4B D9 31 7E B3 00 A1 4A 74 91 04 9D BB
9D B6 4F FF F0 43 55 FE B2 69 27 A1 FB D7 83 E0
12 54 52 B5 86 B0 BE 82 10 A5 27 6C CD 62 3A 4D
E0 2A C0 16 4B C6 B7 D0 D6 B1 82 4F 04 ED 4D D1
D9 CA D2 EC 3B 67 4F 5D 2B B1 7F 96 90 64 78 A3
F2 F0 A1 C1 7B FB E3 09 89 72 89 B1 0D D4 0C 7B
            0B AA 42 6A 00 B4 C7 41
```

After rho

```
90 F6 4A 2B 92 8C C7 53 F7 27 E9 36 E4 93 7F B4
97 F3 EA 2F 33 D1 9E 11 39 43 A4 98 0A 01 83 BE
A2 3A B2 83 1D F3 F8 FB A2 2D 27 07 D1 74 1B 59
7A 88 64 02 18 80 6D DF F8 AA BF 7A EA 8B 1C 1D
0F 6F FF 86 94 44 2A 10 7C 5B 45 74 9C 3D FE 29
03 DA D5 4F 50 29 47 AA 67 EA 0F A5 5A A9 E8 A5
58 CA 8E F1 9B 6D 6A 8E 09 3A 77 01 42 95 E8 22
7F F8 A1 2A FF 4E DB A7 42 F7 AF 07 C1 65 D3 4E
AA D6 10 D6 57 50 82 4A 9D 26 88 D2 13 B6 66 31
F8 16 1A 5C 05 D8 62 C9 D1 D6 B1 82 4F 04 ED 4D
3D 75 65 2B 4B B3 EF 9C AE C4 FE 59 42 92 E1 8D
1E 3E 34 78 6F 7F 3C 41 72 89 B1 0D D4 0C 7B 89
            71 D0 82 AA 90 1A 00 ED
```

After pi

```
90 F6 4A 2B 92 8C C7 53 7A 88 64 02 18 80 6D DF
58 CA 8E F1 9B 6D 6A 8E F8 16 1A 5C 05 D8 62 C9
71 D0 82 AA 90 1A 00 ED 39 43 A4 98 0A 01 83 BE
7C 5B 45 74 9C 3D FE 29 03 DA D5 4F 50 29 47 AA
AA D6 10 D6 57 50 82 4A 1E 3E 34 78 6F 7F 3C 41
F7 27 E9 36 E4 93 7F B4 F8 AA BF 7A EA 8B 1C 1D
09 3A 77 01 42 95 E8 22 D1 D6 B1 82 4F 04 ED 4D
3D 75 65 2B 4B B3 EF 9C A2 3A B2 83 1D F3 F8 FB
A2 2D 27 07 D1 74 1B 59 67 EA 0F A5 5A A9 E8 A5
9D 26 88 D2 13 B6 66 31 72 89 B1 0D D4 0C 7B 89
97 F3 EA 2F 33 D1 9E 11 0F 6F FF 86 94 44 2A 10
7F F8 A1 2A FF 4E DB A7 42 F7 AF 07 C1 65 D3 4E
            AE C4 FE 59 42 92 E1 8D
```

After chi

```
90 B4 C0 DA 11 E1 C5 53 DA 9C 74 0E 1C 10 6D 9E
59 0A 0E 53 0B 6F 6A AA 78 30 52 5D 07 5C A5 DB
1B D8 A6 AA 98 1A 28 61 3A C3 34 93 4A 01 82 3C
D4 5F 45 E4 9B 6D 7E 69 17 F2 F1 67 78 06 7B AB
8B 97 90 56 57 50 01 F4 5A 26 75 1C FB 43 40 40
F6 37 A9 37 E4 87 9F 96 28 6E 3F F8 E7 8B 19 50
25 1B 33 28 42 26 EA B2 13 D4 39 96 EB 04 FD 6D
35 FD 73 63 41 BB EF 95 E7 F8 BA 23 17 7A 18 5F
3A 29 A7 55 D0 62 1D 49 05 63 3E A8 9E A1 F1 2D
1D 14 8A 50 1A 45 E6 43 72 8C B4 09 14 08 78 89
E7 63 EA 07 58 DB 4F B6 0F 68 F1 83 94 65 2A 58
D3 F8 F1 72 FD DC FB 26 53 C4 AF 21 F0 24 CD 5E
            A6 C8 EB D9 C6 96 C1 8D
```

After iota

```
98 34 C0 5A 11 E1 C5 D3 DA 9C 74 0E 1C 10 6D 9E
59 0A 0E 53 0B 6F 6A AA 78 30 52 5D 07 5C A5 DB
1B D8 A6 AA 98 1A 28 61 3A C3 34 93 4A 01 82 3C
D4 5F 45 E4 9B 6D 7E 69 17 F2 F1 67 78 06 7B AB
8B 97 90 56 57 50 01 F4 5A 26 75 1C FB 43 40 40
F6 37 A9 37 E4 87 9F 96 28 6E 3F F8 E7 8B 19 50
25 1B 33 28 42 26 EA B2 13 D4 39 96 EB 04 FD 6D
35 FD 73 63 41 BB EF 95 E7 F8 BA 23 17 7A 18 5F
3A 29 A7 55 D0 62 1D 49 05 63 3E A8 9E A1 F1 2D
1D 14 8A 50 1A 45 E6 43 72 8C B4 09 14 08 78 89
E7 63 EA 07 58 DB 4F B6 0F 68 F1 83 94 65 2A 58
D3 F8 F1 72 FD DC FB 26 53 C4 AF 21 F0 24 CD 5E
            A6 C8 EB D9 C6 96 C1 8D
```

After permutation

```
98 34 C0 5A 11 E1 C5 D3 DA 9C 74 0E 1C 10 6D 9E
59 0A 0E 53 0B 6F 6A AA 78 30 52 5D 07 5C A5 DB
1B D8 A6 AA 98 1A 28 61 3A C3 34 93 4A 01 82 3C
D4 5F 45 E4 9B 6D 7E 69 17 F2 F1 67 78 06 7B AB
8B 97 90 56 57 50 01 F4 5A 26 75 1C FB 43 40 40
F6 37 A9 37 E4 87 9F 96 28 6E 3F F8 E7 8B 19 50
25 1B 33 28 42 26 EA B2 13 D4 39 96 EB 04 FD 6D
35 FD 73 63 41 BB EF 95 E7 F8 BA 23 17 7A 18 5F
3A 29 A7 55 D0 62 1D 49 05 63 3E A8 9E A1 F1 2D
1D 14 8A 50 1A 45 E6 43 72 8C B4 09 14 08 78 89
E7 63 EA 07 58 DB 4F B6 0F 68 F1 83 94 65 2A 58
D3 F8 F1 72 FD DC FB 26 53 C4 AF 21 F0 24 CD 5E
            A6 C8 EB D9 C6 96 C1 8D
```

State (as lanes of integers)

```
[0, 0] = d3c5e1115ac03498
[1, 0] = 9e6d101c0e749cda
[2, 0] = aa6a6f0b530e0a59
[3, 0] = dba55c075d523078
[4, 0] = 61281a98aaa6d81b
[0, 1] = 3c82014a9334c33a
[1, 1] = 697e6d9be4455fd4
[2, 1] = ab7b067867f1f217
[3, 1] = f40150575690978b
[4, 1] = 404043fb1c75265a
[0, 2] = 969f87e437a937f6
[1, 2] = 50198be7f83f6e28
[2, 2] = b2ea264228331b25
[3, 2] = 6dfd04eb9639d413
[4, 2] = 95efbb416373fd35
[0, 3] = 5f187a1723baf8e7
[1, 3] = 491d62d055a7293a
[2, 3] = 2df1a19ea83e6305
[3, 3] = 43e6451a508a141d
[4, 3] = 8978081409b48c72
[0, 4] = b64fdb5807ea63e7
[1, 4] = 582a659483f1680f
[2, 4] = 26fbdcfd72f1f8d3
[3, 4] = 5ecd24f021afc453
[4, 4] = 8dc196c6d9ebc8a6
```

The hash value is

```
98 34 C0 5A 11 E1 C5 D3 DA 9C 74 0E 1C 10 6D 9E
59 0A 0E 53 0B 6F 6A AA 78 30 52 5D 07 5C A5 DB
1B D8 A6 AA 98 1A 28 61 3A C3 34 93 4A 01 82 3C
D4 5F 45 E4 9B 6D 7E 69 17 F2 F1 67 78 06 7B AB
```

B.19 Dedicated Hash-Function 17 (SM3)

B.19.1 Example 1

In this example, the data string is the empty string, i.e. the string of length zero.

The hash-code is the following 256-bit string.

```
1ab21d83 55cfa17f 8e611948 31e81a8f 22bec8c7 28fefb74 7ed035eb 5082aa2b
```

B.19.2 Example 2

In this example, the data string consists of a single byte, namely the ASCII-coded version of the letter “a”.

The hash-code is the following 256-bit string.

```
623476ac 18f65a29 09e43c7f ec61b49c 7e764a91 a18ccb82 f1917a29 c86c5e88
```

B.19.3 Example 3

In this example, the data string is the 3-byte string consisting of the ASCII-coded version of “abc”. This is equivalent to the bitstring “01100001 01100010 01100011”.

After the padding process, the single 16-word block derived from the data string is as follows.

```
61626380 00000000 00000000 00000000 00000000 00000000 00000000 00000000
00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000018
```

The following are (hexadecimal representations of) the successive values of the variables X_0, X_1, X_2, X_3, X_4, X_5, X_6 and X_7.

```
init: 7380166f 4914b2b9 172442d7 da8a0600 a96f30bc 163138aa e38dee4d b0fb0e4e
  0 b9edc12b 7380166f 29657292 172442d7 b2ad29f4 a96f30bc c550b189 e38dee4d
  1 ea52428c b9edc12b 002cdee7 29657292 ac353a23 b2ad29f4 85e54b79 c550b189
  2 609f2850 ea52428c db825773 002cdee7 d33ad5fb ac353a23 4fa59569 85e54b79
  3 35037e59 609f2850 a48519d4 db825773 b8204b5f d33ad5fb d11d61a9 4fa59569
  4 1f995766 35037e59 3e50a0c1 a48519d4 8ad212ea b8204b5f afde99d6 d11d61a9
  5 374a0ca7 1f995766 06fcb26a 3e50a0c1 acf0f639 8ad212ea 5afdc102 afde99d6
  6 33130100 374a0ca7 32aecc3f 06fcb26a 3391ec8a acf0f639 97545690 5afdc102
  7 1022ac97 33130100 94194e6e 32aecc3f 367250a1 3391ec8a b1cd6787 97545690
  8 d47caf4c 1022ac97 26020066 94194e6e 6ad473a4 367250a1 64519c8f b1cd6787
  9 59c2744b d47caf4c 45592e20 26020066 c6a3ceae 6ad473a4 8509b392 64519c8f
 10 481ba2a0 59c2744b f95e99a8 45592e20 02afb727 c6a3ceae 9d2356a3 8509b392
 11 694a3d09 481ba2a0 84e896b3 f95e99a8 9dd1b58c 02afb727 7576351e 9d2356a3
 12 89cbcd58 694a3d09 37454090 84e896b3 6370db62 9dd1b58c b938157d 7576351e
 13 24c95abc 89cbcd58 947a12d2 37454090 1a4a2554 6370db62 ac64ee8d b938157d
 14 7c529778 24c95abc 979ab113 947a12d2 3ee95933 1a4a2554 db131b86 ac64ee8d
 15 34d1691e 7c529778 92b57849 979ab113 61f99646 3ee95933 2aa0d251 db131b86
 16 796afab1 34d1691e a52ef0f8 92b57849 067550f5 61f99646 c999f74a 2aa0d251
 17 7d27cc0e 796afab1 a2d23c69 a52ef0f8 b3c8669b 067550f5 b2330fcc c999f74a
 18 d7820ad1 7d27cc0e d5f562f2 a2d23c69 575c37d8 b3c8669b 87a833aa b2330fcc
 19 f84fd372 d7820ad1 4f981cfa d5f562f2 a5dceaf1 575c37d8 34dd9e43 87a833aa
 20 02c57896 f84fd372 0415a3af 4f981cfa 74576681 a5dceaf1 bec2bae1 34dd9e43
 21 4d0c2fcd 02c57896 9fa6e5f0 0415a3af 576f1d09 74576681 578d2ee7 bec2bae1
 22 eeeec41a 4d0c2fcd 8af12c05 9fa6e5f0 b5523911 576f1d09 340ba2bb 578d2ee7
 23 f368da78 eeeec41a 185f9a9a 8af12c05 6a879032 b5523911 e84abb78 340ba2bb
```

```
24 15ce1286 f368da78 dd8835dd 185f9a9a 62063354 6a879032 c88daa91 e84abb78
25 c3fd31c2 15ce1286 d1b4f1e6 dd8835dd 4db58f43 62063354 8193543c c88daa91
26 6243be5e c3fd31c2 9c250c2b d1b4f1e6 131152fe 4db58f43 9aa31031 8193543c
27 a549beaa 6243be5e fa638587 9c250c2b cf65e309 131152fe 7a1a6dac 9aa31031
28 e11eb847 a549beaa 877cbcc4 fa638587 e5b64e96 cf65e309 97f0988a 7a1a6dac
29 ff9bac9d e11eb847 937d554a 877cbcc4 9811b46d e5b64e96 184e7b2f 97f0988a
30 a5a4a2b3 ff9bac9d 3d708fc2 937d554a e92df4ea 9811b46d 74b72db2 184e7b2f
31 89a13e59 a5a4a2b3 37593bff 3d708fc2 0a1ff572 e92df4ea a36cc08d 74b72db2
32 3720bd4e 89a13e59 4945674b 37593bff cf7d1683 0a1ff572 a757496f a36cc08d
33 9ccd089c 3720bd4e 427cb313 4945674b da8c835f cf7d1683 ab9050ff a757496f
34 c7a0744d 9ccd089c 417a9c6e 427cb313 0958ff1b da8c835f b41e7be8 ab9050ff
35 d955c3ed c7a0744d 9a113939 417a9c6e c533f0ff 0958ff1b 1afed464 b41e7be8
36 e142d72b d955c3ed 40e89b8f 9a113939 d4509586 c533f0ff f8d84ac7 1afed464
37 e7250598 e142d72b ab87dbb2 40e89b8f c7f93fd3 d4509586 87fe299f f8d84ac7
38 2f13c4ad e7250598 85ae57c2 ab87dbb2 1a6cabc9 c7f93fd3 ac36a284 87fe299f
39 19f363f9 2f13c4ad 4a0b31ce 85ae57c2 c302badb 1a6cabc9 fe9e3fc9 ac36a284
40 55e1dde2 19f363f9 27895a5e 4a0b31ce 459daccf c302badb 5e48d365 fe9e3fc9
41 d4f4efe3 55e1dde2 e6c7f233 27895a5e 5cfba85a 459daccf d6de1815 5e48d365
42 48dcbc62 d4f4efe3 c3bbc4ab e6c7f233 6f49c7bb 5cfba85a 667a2ced d6de1815
43 8237b8a0 48dcbc62 e9dfc7a9 c3bbc4ab d89d2711 6f49c7bb 42d2e7dd 667a2ced
44 d8685939 8237b8a0 b978c491 e9dfc7a9 8ee87df5 d89d2711 3ddb7a4e 42d2e7dd
45 d2090a86 d8685939 6f714104 b978c491 2e533625 8ee87df5 388ec4e9 3ddb7a4e
46 e51076b3 d2090a86 d0b273b0 6f714104 d9f89e61 2e533625 efac7743 388ec4e9
47 47c5be50 e51076b3 12150da4 d0b273b0 3567734e d9f89e61 b1297299 efac7743
48 abddbdc8 47c5be50 20ed67ca 12150da4 3dfcdd11 3567734e f30ecfc4 b1297299
49 bd708003 abddbdc8 8b7ca08f 20ed67ca 93494bc0 3dfcdd11 9a71ab3b f30ecfc4
50 15e2f5d3 bd708003 bb7b9157 8b7ca08f c3956c3f 93494bc0 e889efe6 9a71ab3b
51 13826486 15e2f5d3 e100077a bb7b9157 cd09a51c c3956c3f 5e049a4a e889efe6
52 4a00ed2f 13826486 c5eba62b e100077a 0741f675 cd09a51c 61fe1cab 5e049a4a
53 f4412e82 4a00ed2f 04c90c27 c5eba62b 7429807c 0741f675 28e6684d 61fe1cab
54 549db4b7 f4412e82 01da5e94 04c90c27 f6bc15ed 7429807c b3a83a0f 28e6684d
55 22a79585 549db4b7 825d05e8 01da5e94 9d4db19a f6bc15ed 03e3a14c b3a83a0f
56 30245b78 22a79585 3b696ea9 825d05e8 f6804c82 9d4db19a af6fb5e0 03e3a14c
57 6598314f 30245b78 4f2b0a45 3b696ea9 f522adb2 f6804c82 8cd4ea6d af6fb5e0
58 c3d629a9 6598314f 48b6f060 4f2b0a45 14fb0764 f522adb2 6417b402 8cd4ea6d
59 ddb0a26a c3d629a9 30629ecb 48b6f060 589f7d5c 14fb0764 6d97a915 6417b402
60 71034d71 ddb0a26a ac535387 30629ecb 14d5c7f6 589f7d5c 3b20a7d8 6d97a915
61 5e636b4b 71034d71 6144d5bb ac535387 09ccd95e 14d5c7f6 eae2c4fb 3b20a7d8
62 2bfa5f60 5e636b4b 069ae2e2 6144d5bb 4ac3cf08 09ccd95e 3fb0a6ae eae2c4fb
63 1547e69b 2bfa5f60 c6d696bc 069ae2e2 e808f43b 4ac3cf08 caf04e66 3fb0a6ae
```

The following eight words, Y_0, Y_1, Y_2, Y_3, Y_4, Y_5, Y_6 and Y_7, represent the output of the final iteration of the round-function.

$$
\begin{aligned}
Y_0 &= \texttt{1547e69b} \oplus \texttt{7380166f} = \texttt{66c7f0f4}\\
Y_1 &= \texttt{2bfa5f60} \oplus \texttt{4914b2b9} = \texttt{62eeedd9}\\
Y_2 &= \texttt{c6d696bc} \oplus \texttt{172442d7} = \texttt{d1f2d46b}\\
Y_3 &= \texttt{069ae2e2} \oplus \texttt{da8a0600} = \texttt{dc10e4e2}\\
Y_4 &= \texttt{e808f43b} \oplus \texttt{a96f30bc} = \texttt{4167c487}\\
Y_5 &= \texttt{4ac3cf08} \oplus \texttt{163138aa} = \texttt{5cf2f7a2}\\
Y_6 &= \texttt{caf04e66} \oplus \texttt{e38dee4d} = \texttt{297da02b}\\
Y_7 &= \texttt{3fb0a6ae} \oplus \texttt{b0fb0e4e} = \texttt{8f4ba8e0}
\end{aligned}
$$

The hash-code is the following 256-bit string.

```
66c7f0f4 62eeedd9 d1f2d46b dc10e4e2 4167c487 5cf2f7a2 297da02b 8f4ba8e0
```

B.19.4 Example 4

In this example, the data string is the 14-byte string consisting of the ASCII-coded version of

```
"message digest"
```

The hash-code is the following 256-bit string.

```
c522a942 e89bd80d 97dd666e 7a5531b3 6188c981 7149e9b2 58dfe51e ce98ed77
```

B.19.5 Example 5

In this example, the data string is the 26-byte string consisting of the ASCII-coded version of

"abcdefghijklmnopqrstuvwxyz"

The hash-code is the following 256-bit string.

```
b80fe97a 4da24afc 277564f6 6a359ef4 40462ad2 8dcc6d63 adb24d5c 20a61595
```

B.19.6 Example 6

In this example, the data string is the 62-byte string consisting of the ASCII-coded version of

"ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz0123456789"

The hash-code is the following 256-bit string.

```
2971d10c 8842b70c 979e5506 3480c50b acffd90e 98e2e60d 2512ab8a bfdfcec5
```

B.19.7 Example 7

In this example, the data string is the 80-byte string consisting of the ASCII-coded version of eight repetitions of

"1234567890"

The hash-code is the following 256-bit string.

```
ad818053 21f3e69d 251235bf 886a5648 44873b56 dd7dde40 0f055b7d de39307a
```

B.19.8 Example 8

In this example, the data string is the 56-byte string consisting of the ASCII-coded version of

"abcdbcdecdefdefgefghfghighijhijkijkljklmklmnlmnomnopnopq"

After the padding process, the following two 16-word blocks are derived from the data string.

```
61626364 62636465 63646566 64656667 65666768 66676869 6768696a 68696a6b
696a6b6c 6a6b6c6d 6b6c6d6e 6c6d6e6f 6d6e6f70 6e6f7071 80000000 00000000

00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000
00000000 00000000 00000000 00000000 00000000 00000000 00000000 000001c0
```

The following are (hexadecimal representations of) the successive values of the variables X_0, X_1, X_2, X_3, X_4, X_5, X_6 and X_7 in the first block process.

init: 7380166f 4914b2b9 172442d7 da8a0600 a96f30bc 163138aa e38dee4d b0fb0e4e

```
 0  5c8f61b7 7380166f 29657292 172442d7 b2e561d0 a96f30bc c550b189 e38dee4d
 1  dc3de4b3 5c8f61b7 002cdee7 29657292 ba8630fd b2e561d0 85e54b79 c550b189
 2  8d1a8984 dc3de4b3 1ec36eb9 002cdee7 c6f3ad94 ba8630fd 0e85972b 85e54b79
 3  bbb4bf50 8d1a8984 7bc967b8 1ec36eb9 68627c7c c6f3ad94 87edd431 0e85972b
 4  3e50b8bc bbb4bf50 3513091a 7bc967b8 55ab956b 68627c7c 6ca6379d 87edd431
 5  8d4276da 3e50b8bc 697ea177 3513091a ac958648 55ab956b e3e34313 6ca6379d
 6  c8da9226 8d4276da a171787c 697ea177 68cee8e5 ac958648 ab5aad5c e3e34313
 7  f33fbdec c8da9226 84edb51a a171787c abf9d51e 68cee8e5 324564ac ab5aad5c
 8  597e4171 f33fbdec b5244d91 84edb51a 970acf5f abf9d51e 472b4677 324564ac
 9  da746360 597e4171 7f7bd9e6 b5244d91 87674d2f 970acf5f a8f55fce 472b4677
10  bbd90a4e da746360 fc82e2b2 7f7bd9e6 04b43d0b 87674d2f 7afcb856 a8f55fce
```

```
11  d97774b7 bbd90a4e e8c6c1b4 fc82e2b2 121d28ac 04b43d0b 697c3b3a 7afcb856
12  78078302 d97774b7 b2149d77 e8c6c1b4 77c1de3d 121d28ac e85825a1 697c3b3a
13  c80f6d38 78078302 eee96fb2 b2149d77 51d1b562 77c1de3d 456090e9 e85825a1
14  eace16f6 c80f6d38 0f0604f0 eee96fb2 6b06c8b2 51d1b562 f1ebbe0e 456090e9
15  2128f407 eace16f6 1eda7190 0f0604f0 5107aff4 6b06c8b2 ab128e8d f1ebbe0e
16  93390d8d 2128f407 9c2dedd5 1eda7190 5ee90335 5107aff4 45935836 ab128e8d
17  b9dcab4b 93390d8d 51e80e42 9c2dedd5 e7081ab8 5ee90335 7fa2883d 45935836
18  95473afd b9dcab4b 721b1b26 51e80e42 c12a2af1 e7081ab8 19aaf748 7fa2883d
19  e100dfda 95473afd b9569773 721b1b26 a2bb4add c12a2af1 d5c73840 19aaf748
20  2f9800cc e100dfda 8e75fb2a b9569773 0838381e a2bb4add 578e0951 d5c73840
21  1a113298 2f9800cc 01bfb5c2 8e75fb2a 41d4677b 0838381e 56ed15da 578e0951
22  7fee2bd4 1a113298 3001985f 01bfb5c2 b77b5fee 41d4677b c0f041c1 56ed15da
23  d615fe59 7fee2bd4 22653034 3001985f c62c3a46 b77b5fee 3bda0ea3 c0f041c1
24  a855127b d615fe59 dc57a8ff 22653034 c47abe3f c62c3a46 ff75bbda 3bda0ea3
25  a8e3132d a855127b 2bfcb3ac dc57a8ff 386d8373 c47abe3f d2363161 ff75bbda
26  1a319d21 a8e3132d aa24f750 2bfcb3ac b4e3cc85 386d8373 f1fe23d5 d2363161
27  b8c7870b 1a319d21 c6265b51 aa24f750 349ab542 b4e3cc85 1b99c36c f1fe23d5
28  ed5910cb b8c7870b 633a4234 c6265b51 826818f2 349ab542 642da71e 1b99c36c
29  b7b7c514 ed5910cb 8f0e1771 633a4234 014d92be 826818f2 aa11a4d5 642da71e
30  332d48cf b7b7c514 b22197da 8f0e1771 67cc5228 014d92be c7941340 aa11a4d5
31  00b8692d 332d48cf 6f8a296f b22197da bd8784c7 67cc5228 95f00a6c c7941340
32  ed95f4e5 00b8692d 5a919e66 6f8a296f a9041b7a bd8784c7 91433e62 95f00a6c
33  d7ec1070 ed95f4e5 70d25a01 5a919e66 ff634bf8 a9041b7a 263dec3c 91433e62
34  6d6df2a0 d7ec1070 2be9cbdb 70d25a01 208c87ac ff634bf8 dbd54820 263dec3c
35  342f3ad6 6d6df2a0 d820e1af 2be9cbdb da74f6be 208c87ac 5fc7fb1a dbd54820
36  822697c1 342f3ad6 dbe540da d820e1af a3c91873 da74f6be 3d610464 5fc7fb1a
37  b75f5102 822697c1 5e75ac68 dbe540da 058dd4eb a3c91873 b5f6d3a7 3d610464
38  ab4d8a3d b75f5102 4d2f8304 5e75ac68 935c9926 058dd4eb c39d1e48 b5f6d3a7
39  586f130a ab4d8a3d bea2056e 4d2f8304 9d26a8a7 935c9926 a7582c6e c39d1e48
40  2dbeec34 586f130a 9b147b56 bea2056e a104c193 9d26a8a7 c9349ae4 a7582c6e
41  2cb7cd53 2dbeec34 de2614b0 9b147b56 bc21d865 a104c193 453ce935 c9349ae4
42  a9ded8fe 2cb7cd53 7dd8685b de2614b0 efcd8176 bc21d865 0c9d0826 453ce935
43  8f6ea284 a9ded8fe 6f9aa659 7dd8685b b0ef6305 efcd8176 c32de10e 0c9d0826
44  4198155f 8f6ea284 bdb1fd53 6f9aa659 d1bf96ef b0ef6305 0bb77e6c c32de10e
45  fe0f20d1 4198155f dd45091e bdb1fd53 6d2b4951 d1bf96ef 182d877b 0bb77e6c
46  939eafe3 fe0f20d1 302abe83 dd45091e f8dd3803 6d2b4951 b77e8dfc 182d877b
47  12a2e11e 939eafe3 1e41a3fc 302abe83 b65b77a8 f8dd3803 4a8b695a b77e8dfc
48  45f88856 12a2e11e 3d5fc727 1e41a3fc 1ead7d75 b65b77a8 c01fc6e9 4a8b695a
49  91d7d82c 45f88856 45c23c25 3d5fc727 c0016d52 1ead7d75 bd45b2db c01fc6e9
50  287ef00e 91d7d82c f110ac8b 45c23c25 b8df8ff0 c0016d52 eba8f56b bd45b2db
51  3d6c1633 287ef00e afb05923 f110ac8b 286928fc b8df8ff0 6a96000b eba8f56b
52  d06316ec 3d6c1633 fde01c50 afb05923 77e4a5f5 286928fc 7f85c6fc 6a96000b
53  5af5093d d06316ec d82c667a fde01c50 e56749bb 77e4a5f5 47e14349 7f85c6fc
54  1658fdf5 5af5093d c62dd9a0 d82c667a 9557584c e56749bb 2fabbf25 47e14349
55  52c7f5ac 1658fdf5 ea127ab5 c62dd9a0 109b96d2 9557584c 4ddf2b3a 2fabbf25
56  be546cf1 52c7f5ac b1fbea2c ea127ab5 e5af8405 109b96d2 c264aaba 4ddf2b3a
57  731577cd be546cf1 8feb58a5 b1fbea2c 2afeba8c e5af8405 b69084dc c264aaba
58  813558cc 731577cd a8d9e37c 8feb58a5 8c01b50c 2afeba8c 202f2d7c b69084dc
59  1986a1c9 813558cc 2aef9ae6 a8d9e37c f217df1c 8c01b50c d46157f5 202f2d7c
60  2d3b8abc 1986a1c9 6ab19902 2aef9ae6 eddf3d93 f217df1c a864600d d46157f5
61  c65c49eb 2d3b8abc 0d439233 6ab19902 e50c2a6d eddf3d93 f8e790be a864600d
62  c3c11ee8 c65c49eb 7715785a 0d439233 ae18f3a1 e50c2a6d ec9f6ef9 f8e790be
63  6abb79fd c3c11ee8 b893d78c 7715785a b9dd7bbb ae18f3a1 536f2861 ec9f6ef9
```

The following eight words, Y_0, Y_1, Y_2, Y_3, Y_4, Y_5, Y_6 and Y_7, represent the output of the round-function in the first block process.

$$Y_0 = 6abb79fd \oplus 7380166f = 193b6f92$$
$$Y_1 = c3c11ee8 \oplus 4914b2b9 = 8ad5ac51$$
$$Y_2 = b893d78c \oplus 172442d7 = afb7955b$$
$$Y_3 = 7715785a \oplus da8a0600 = ad9f7e5a$$
$$Y_4 = b9dd7bbb \oplus a96f30bc = 10b24b07$$
$$Y_5 = ae18f3a1 \oplus 163138aa = b829cb0b$$

Y_6 = 536f2861 ⊕ e38dee4d = b0e2c62c
Y_7 = ec9f6ef9 ⊕ b0fb0e4e = 5c6460b7

The following are (hexadecimal representations of) the successive values of the variables X_0, X_1, X_2, X_3, X_4, X_5, X_6 and X_7 in the second block process.

```
init: 193b6f92 8ad5ac51 afb7955b ad9f7e5a 10b24b07 b829cb0b b0e2c62c 5c6460b7
 0  f71acd25 193b6f92 ab58a315 afb7955b 5d580f7b 10b24b07 585dc14e b0e2c62c
 1  42df670c f71acd25 76df2432 ab58a315 301a33a1 5d580f7b 58388592 585dc14e
 2  96ea0edb 42df670c 359a4bee 76df2432 fece7b76 301a33a1 7bdaeac0 58388592
 3  0851b544 96ea0edb bece1885 359a4bee 094b07b3 fece7b76 9d0980d1 7bdaeac0
 4  00a8966d 0851b544 d41db72d bece1885 6cc097ed 094b07b3 dbb7f673 9d0980d1
 5  ed15efa6 00a8966d a36a8810 d41db72d 519536e5 6cc097ed 3d984a58 dbb7f673
 6  b1820dc8 ed15efa6 512cda01 a36a8810 8c851b7a 519536e5 bf6b6604 3d984a58
 7  93eaecd0 b1820dc8 2bdf4dda 512cda01 422f81a2 8c851b7a b72a8ca9 bf6b6604
 8  6903aca3 93eaecd0 041b9163 2bdf4dda f048bd9b 422f81a2 dbd46428 b72a8ca9
 9  1f2bd8db 6903aca3 d5d9a127 041b9163 e5ae9d27 f048bd9b 0d12117c dbd46428
10  3de4985a 1f2bd8db 075946d2 d5d9a127 77ab882e e5ae9d27 ecdf8245 0d12117c
11  e0edf809 3de4985a 57b1b63e 075946d2 c2715679 77ab882e e93f2d74 ecdf8245
12  9058acfc e0edf809 c930b47b 57b1b63e 72b366db c2715679 4173bd5c e93f2d74
13  ab17dc92 9058acfc dbf013c1 c930b47b 3edbffa9 72b366db b3ce138a 4173bd5c
14  32ddd4f1 ab17dc92 b159f920 dbf013c1 d5f4b6ea 3edbffa9 36db959b b3ce138a
15  3990748b 32ddd4f1 2fb92556 b159f920 94fc9df4 d5f4b6ea fd49f6df 36db959b
16  cda22778 3990748b bba9e265 2fb92556 5edeebf4 94fc9df4 b756afa5 fd49f6df
17  0136ef6f cda22778 20e91673 bba9e265 b55fc7d9 5edeebf4 efa4a7e4 b756afa5
18  ecd46fae 0136ef6f 444ef19b 20e91673 4b390af7 b55fc7d9 5fa2f6f7 efa4a7e4
19  6a5df514 ecd46fae 6ddede02 444ef19b 3bf2e429 4b390af7 3ecdaafe 5fa2f6f7
20  c3b5f0d2 6a5df514 a8df5dd9 6ddede02 bc4ca2bd 3bf2e429 57ba59c8 3ecdaafe
21  645baf5b c3b5f0d2 bbea28d4 a8df5dd9 e1a9773e bc4ca2bd 2149df97 57ba59c8
22  b0ed09e5 645baf5b 6be1a587 bbea28d4 37979efc e1a9773e 15ede265 2149df97
23  85f08fb3 b0ed09e5 b75eb6c8 6be1a587 dc23ce67 37979efc b9f70d4b 15ede265
24  cdec3a25 85f08fb3 da13cb61 b75eb6c8 c79b04e6 dc23ce67 f7e1bcbc b9f70d4b
25  5fe964f7 cdec3a25 e11f670b da13cb61 7233f530 c79b04e6 733ee11e f7e1bcbc
26  7f515284 5fe964f7 d8744b9b e11f670b dce5766b 7233f530 27363cd8 733ee11e
27  07628be9 7f515284 d2c9eebf d8744b9b c4c6eb17 dce5766b a983919f 27363cd8
28  edfb1904 07628be9 a2a508fe d2c9eebf c1284e94 c4c6eb17 b35ee72b a983919f
29  f07795d3 edfb1904 c517d20e a2a508fe f8c23138 c1284e94 58be2637 b35ee72b
30  dad7d8a8 f07795d3 f63209db c517d20e 70d89edf f8c23138 74a60942 58be2637
31  476692e1 dad7d8a8 ef2ba7e0 f63209db 428baca3 70d89edf 89c7c611 74a60942
32  b1745ed9 476692e1 afb151b5 ef2ba7e0 49a04792 428baca3 f6fb86c4 89c7c611
33  985f0eae b1745ed9 cd25c28e afb151b5 1c70f25b 49a04792 651a145d f6fb86c4
34  a4eac3c1 985f0eae e8bdb362 cd25c28e baeafb1d 1c70f25b 3c924d02 651a145d
35  94d3cc2e a4eac3c1 be1d5d30 e8bdb362 f772a4e5 baeafb1d 92d8e387 3c924d02
36  ab64985e 94d3cc2e d5878349 be1d5d30 cfd9abf7 f772a4e5 d8edd757 92d8e387
37  ea650863 ab64985e a7985d29 d5878349 37d676a0 cfd9abf7 272fbb95 d8edd757
38  7e9d76d0 ea650863 c930bd56 a7985d29 0e5b32c2 37d676a0 5fbe7ecd 272fbb95
39  9c804f2f 7e9d76d0 ca10c7d4 c930bd56 b9883a18 0e5b32c2 b501beb3 5fbe7ecd
40  cc8bc84d 9c804f2f 3aeda0fd ca10c7d4 89af8633 b9883a18 961072d9 b501beb3
41  1e44d2cd cc8bc84d 009e5f39 3aeda0fd d3ff5a20 89af8633 d0c5cc41 961072d9
42  9747774e 1e44d2cd 17909b99 009e5f39 94779237 d3ff5a20 319c4d7c d0c5cc41
43  21e48a42 9747774e 89a59a3c 17909b99 319302a0 94779237 d1069ffa 319c4d7c
44  4aa0d479 21e48a42 8eee9d2e 89a59a3c 08a73b8f 319302a0 91bca3bc d1069ffa
45  c9a40b98 4aa0d479 c9148443 8eee9d2e 4d7508ff 08a73b8f 15018c98 91bca3bc
46  050b4233 c9a40b98 41a8f295 c9148443 40c7b509 4d7508ff dc784539 15018c98
47  270a62cb 050b4233 48173193 41a8f295 d06c4a51 40c7b509 47fa6ba8 dc784539
48  7c3fcf98 270a62cb 1684660a 48173193 7ecbfa98 d06c4a51 a84a063d 47fa6ba8
49  0ba56393 7c3fcf98 14c5964e 1684660a 02154736 7ecbfa98 528e8362 a84a063d
50  27548370 0ba56393 7f9f30f8 14c5964e 6d3343b1 02154736 d4c3f65f 528e8362
51  79aaeb0e 27548370 4ac72617 7f9f30f8 f2556152 6d3343b1 39b010aa d4c3f65f
52  bd17409f 79aaeb0e a906e04e 4ac72617 1bdba544 f2556152 1d8b699a 39b010aa
53  5cea4faa bd17409f 55d61cf3 a906e04e 0958fc62 1bdba544 0a9792ab 1d8b699a
54  7fce4d84 5cea4faa 2e813f7a 55d61cf3 b535cb5a 0958fc62 2a20dedd 0a9792ab
55  44232436 7fce4d84 d49f54b9 2e813f7a ea59cc69 b535cb5a e3104ac7 2a20dedd
```

```
56  7fedd3f5 44232436 9c9b08ff d49f54b9 cee4b418 ea59cc69 5ad5a9ae e3104ac7
57  3648449e 7fedd3f5 46486c88 9c9b08ff b1aa5387 cee4b418 634f52ce 5ad5a9ae
58  4a8c2056 3648449e dba7eaff 46486c88 b1892488 b1aa5387 a0c67725 634f52ce
59  c7ff81c0 4a8c2056 90893c6c dba7eaff ae0ada7d b1892488 9c3d8d52 a0c67725
60  d839686f c7ff81c0 1840ac95 90893c6c fd965e23 ae0ada7d 24458c49 9c3d8d52
61  64861392 d839686f ff03818f 1840ac95 d109486d fd965e23 d3ed7056 24458c49
62  6c983266 64861392 72d0dfb0 ff03818f c7df59b2 d109486d f11fecb2 d3ed7056
63  7aa00357 6c983266 0c2724c9 72d0dfb0 1792e073 c7df59b2 436e884a f11fecb2
```

The following eight words, Y_0, Y_1, Y_2, Y_3, Y_4, Y_5, Y_6 and Y_7, represent the output of the final iteration of the round-function.

$$Y_0 = 7aa00357 \oplus 193b6f92 = 639b6cc5$$
$$Y_1 = 6c983266 \oplus 4914b2b9 = e64d9e37$$
$$Y_2 = 0c2724c9 \oplus 172442d7 = a390b192$$
$$Y_3 = 72d0dfb0 \oplus da8a0600 = df4fa1ea$$
$$Y_4 = 1792e073 \oplus a96f30bc = 0720ab74$$
$$Y_5 = c7df59b2 \oplus 163138aa = 7ff692b9$$
$$Y_6 = 436e884a \oplus e38dee4d = f38c4e66$$
$$Y_7 = f11fecb2 \oplus b0fb0e4e = ad7b8c05$$

The hash-code for this message is

639b6cc5 e64d9e37 a390b192 df4fa1ea 0720ab74 7ff692b9 f38c4e66 ad7b8c05.

B.19.9 Example 9

In this example, the data string is the 1 000 000-byte string consisting of the ASCII- coded version of "a" repeated 10^6 times.

The hash-code is the following 256-bit string.

c8aaf894 29554029 e231941a 2acc0ad6 1ff2a5ac d8fadd25 847a3a73 2b3b02c3

B.19.10 Example 10

In this example, the data string is the 112-byte string consisting of the ASCII-coded version of

"abcdefghbcdefghicdefghijdefghijkefghijklfghijklmghijklmn
hijklmnoijklmnopjklmnopqklmnopqrlmnopqrsmnopqrstnopqrstu"

(with no line break after the first n).

The hash-code is the following 256-bit string.

78bcfb58 6acd983d 7fae8e69 30157f15 62019e2c af68f1c9 8a855f1a 95bb89bb

B.19.11 Example 11

In this example, the data string is the 32-byte string consisting of the ASCII-coded version of

"abcdbcdecdefdefgefghfghighijhijk"

The hash-code is the following 256-bit string.

f6556d8d b8bed431 81a678da 7f6affe4 51deba50 115f3150 f19debb8 10b9958a

Annex C
(informative)

SHA-3 Extendable-Output Functions

C.1 SHAKE-128

C.1.1 Parameters, functions and constants

C.1.1.1 Parameters

For SHAKE-128, $L_1 = r = 1\,344$, $L_2 = b = 1\,600$ and $c = b - r = 256$. For SHAKE-128, d is a variable to determine the output length.

C.1.1.2 Byte ordering convention

Each data input D to the round-function ϕ is a block of 1 344 bits that is XORed into the part of the state. The permutation f is then applied to the state. Because the step mappings that comprise the permutation are defined on the array form of the state, it is convenient to regard D as a sequence of 64-bit words that are XORed directly into the state array. For this purpose, when D is represented as a sequence of 168 bytes, B_0, B_1, ..., B_{167}, then D should be interpreted as a sequence of 21 lane words, Z_0, Z_1, ..., Z_{20}, as follows:

$$Z_i = 2^{56}B_{8i+7} + 2^{48}B_{8i+6} + 2^{40}B_{8i+5} + 2^{32}B_{8i+4} + 2^{24}B_{8i+3} + 2^{16}B_{8i+2} + 2^{8}B_{8i+1} + B_{8i},$$

for $0 \le i \le 20$.

Hence, each group of eight consecutive bytes is a word and the bytes of the word are arranged in increasing order of significance, so that the first byte in the group becomes the least significant byte of the word.

Under this interpretation, D is XORed with the state array as follows.

If j and k are the elements of {0, 1, 2, 3, 4}, such that (j, k) is the unique pair for which $i = 5k + j$, then for $0 \le i \le 20$, $Lane'(j, k) = Z_i \oplus Lane(j, k)$, where $Lane'(j, k)$ is the updated value of the lane.

C.1.1.3 Functions

The functions, including the function *Rnd* and step mappings, for the dedicated SHAKE-128 are the same as Dedicated Hash-Function 13 and is specified in Clause 19.

C.1.1.4 Constants

The constants used for the mapping are the offsets defined in 19.2.3.6.2.

C.1.1.5 Initializing value

The initializing value is a 1 600-bit all-zero string.

C.1.2 Padding method

The data M will be padded with "1111" before applying the padding method pad10*1(x, m) specified in 19.2 with $x = 1\,344$.

That is, the padded data is $P = M \,||\, 1111 \,||\, 10^*1$, such that the length of P is a multiple of 1 344.

C.1.3 Description of round-function

The round-function for SHAKE-128 is the permutation KECCAK-*p* specified in Clause 19 Notice that KECCAK-*p* is considered as defined in ISO/IEC 10118-1. However, for each execution of KECCAK-*p*, it iterates the *Rnd* function 24 times. That is, it executes

$$Rnd(\mathbf{A}, i_r) = \iota\,(\chi <\pi\,\{\rho\,[\theta\,(\mathbf{A})]\}>, i_r)$$

for $i_r = 0, 1, ..., 23$.

C.1.4 Output transformation

In step h) of SPONGE[*f*, pad, *r*](*N*, *d*) specified in Clause 19, each execution of *f* in the squeezing stage for SHAKE-128 generates r = 1 344 bits. The output is concatenated until enough bits are generated to obtain d bits. That is, for a given d, after the last data block is inputted, it generates the first r bits of output.

Then, it executes the function f $\lceil d/r \rceil - 1$ times to generate a total of $\lceil d/r \rceil \cdot r$ output bits and then truncates to d bits.

C.1.5 Examples

NOTE 1 Data is presented in three different ways: bit strings, byte strings and "w" length words (for the lanes).

NOTE 2 Bit strings are the sequence of bits from left to right.

NOTE 3 Byte strings are the bytes from left to right and the bits within the byte are right to left.

NOTE 4 Words are the integer representation of the values in the lanes.

SHAKE-128 sample to produce 4096-bits of output

The message as bit string

```
(empty message)
```

about to call last of the absorb phase

XORed state (in bytes)

```
1F 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 80 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
            00 00 00 00 00 00 00 00
```

XORed state (as lanes of integers)

```
[0, 0] = 000000000000001f
[1, 0] = 0000000000000000
[2, 0] = 0000000000000000
[3, 0] = 0000000000000000
[4, 0] = 0000000000000000
[0, 1] = 0000000000000000
[1, 1] = 0000000000000000
[2, 1] = 0000000000000000
[3, 1] = 0000000000000000
[4, 1] = 0000000000000000
[0, 2] = 0000000000000000
[1, 2] = 0000000000000000
[2, 2] = 0000000000000000
[3, 2] = 0000000000000000
[4, 2] = 0000000000000000
[0, 3] = 0000000000000000
[1, 3] = 0000000000000000
[2, 3] = 0000000000000000
[3, 3] = 0000000000000000
[4, 3] = 0000000000000000
[0, 4] = 8000000000000000
[1, 4] = 0000000000000000
[2, 4] = 0000000000000000
[3, 4] = 0000000000000000
[4, 4] = 0000000000000000
```

Round #0

After theta

```
1F 00 00 00 00 00 00 00 1F 00 00 00 00 00 00 80
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
3F 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
1F 00 00 00 00 00 00 80 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 3F 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 1F 00 00 00 00 00 00 80
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
3F 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
1F 00 00 00 00 00 00 80 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 3F 00 00 00 00 00 00 00
00 00 00 00 00 00 00 80 1F 00 00 00 00 00 00 80
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
            3F 00 00 00 00 00 00 00
```

After rho

```
1F 00 00 00 00 00 00 00 3F 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 F8 01 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 F8 01 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 F0 03 00 00 00 00
00 00 00 00 00 00 00 00 00 7E 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 80 1F 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 F0 03 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 3F 00 00 00 00 00 00
00 00 02 00 00 00 00 00 7E 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
            00 C0 0F 00 00 00 00 00
```

After pi

```
1F 00 00 00 00 00 00 00 00 00 00 00 00 F8 01 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 C0 0F 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 F0 03 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 F0 03 00 00 00 00 00 00 00 00 00
3F 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 3F 00 00 00 00 00 00
00 00 02 00 00 00 00 00 00 00 00 F8 01 00 00 00
00 00 00 00 00 00 00 00 00 7E 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 80 1F 00 00 00 00 00 00 00 00 00 00
            7E 00 00 00 00 00 00 00
```

After chi

```
1F 00 00 00 00 00 00 00 00 00 00 00 00 F8 01 00
00 C0 0F 00 00 00 00 00 1F 00 00 00 00 00 00 00
00 C0 0F 00 00 F8 01 00 00 00 00 00 00 00 00 00
00 00 F0 03 00 F0 03 00 00 00 00 00 00 00 00 00
00 00 00 00 00 F0 03 00 00 00 F0 03 00 00 00 00
3F 00 00 00 00 00 00 00 00 3F 00 00 00 00 00 00
00 00 02 00 00 00 00 00 3F 3F 00 00 00 00 00 00
00 00 02 00 00 00 00 00 00 7E 00 F8 01 00 00 00
00 00 00 00 00 00 00 00 00 7E 00 00 00 00 00 00
00 00 00 F8 01 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 80 1F 00 00 00 00 00 00 00 00 00 00
7E 00 00 00 80 1F 00 00 00 00 00 00 00 00 00 00
            7E 00 00 00 00 00 00 00
```

After iota

```
1E 00 00 00 00 00 00 00 00 00 00 00 00 F8 01 00
00 C0 0F 00 00 00 00 00 1F 00 00 00 00 00 00 00
00 C0 0F 00 00 F8 01 00 00 00 00 00 00 00 00 00
00 00 F0 03 00 F0 03 00 00 00 00 00 00 00 00 00
00 00 00 00 00 F0 03 00 00 00 F0 03 00 00 00 00
3F 00 00 00 00 00 00 00 00 3F 00 00 00 00 00 00
00 00 02 00 00 00 00 00 3F 3F 00 00 00 00 00 00
00 00 02 00 00 00 00 00 00 7E 00 F8 01 00 00 00
00 00 00 00 00 00 00 00 00 7E 00 00 00 00 00 00
00 00 00 F8 01 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 80 1F 00 00 00 00 00 00 00 00 00 00
7E 00 00 00 80 1F 00 00 00 00 00 00 00 00 00 00
            7E 00 00 00 00 00 00 00
```

(Skip rounds 1 to 22)

Round #23

After theta

```
F5 86 2B A6 68 65 BA FC 10 4E F5 EE AA FB E0 C4
33 8C FB C6 D3 83 A0 23 DB BC EE C7 0F 60 AD BF
47 27 0B 74 8C A7 51 68 7D B6 65 F4 D1 54 62 D4
60 CC 97 44 A6 82 E7 57 C9 7F A9 4D B1 05 A8 C2
09 99 B6 5D 41 E7 9C 86 6A 84 85 BE B2 F6 54 C1
6B 3D 70 76 CF AE CE DE 5F 9F 5D 03 93 F2 B3 CD
9D 37 63 58 1F 40 58 FE 66 C7 E1 A8 11 DD 4F EB
B1 A9 CB 54 8D A8 4B 33 AC A8 76 D1 29 4A CF 06
61 54 AF E1 B5 72 C9 13 9F 5F E9 3A 08 3F 51 04
53 D5 1C F8 52 52 E1 78 BF 91 01 1A BE D4 39 CF
84 04 0B 06 B2 E7 23 7E FD 0F B0 4B CE 2A 1E 72
BB 9F 26 93 52 D4 77 B1 EB 15 3A 7D 4F D1 8C E6
            BB C7 7B 02 3C 4C D2 44
```

After rho

```
F5 86 2B A6 68 65 BA FC 21 9C EA DD 55 F7 C1 89
0C E3 BE F1 F4 20 E8 C8 00 D6 FA BB CD EB 7E FC
3C 8D 42 3B 3A 59 A0 63 1F 4D 25 46 DD 67 5B 46
49 64 2A 78 7E 05 C6 7C 70 F2 5F 6A 53 6C 01 AA
4C DB AE A0 73 4E C3 84 4F 15 AC 46 58 E8 2B 6B
5E EB 81 B3 7B 76 75 F6 36 7F 7D 76 0D 4C CA CF
C3 FA 00 C2 F2 EF BC 19 BA 9F D6 CD 8E C3 51 23
AA 46 D4 A5 99 D8 D4 65 A2 53 94 9E 0D 58 51 ED
35 BC 56 2E 79 22 8C EA 28 82 CF AF 74 1D 84 9F
2A 1C 6F AA 9A 03 5F 4A CF BF 91 01 1A BE D4 39
8F F8 11 12 2C 18 C8 9E F5 3F C0 2E 39 AB 78 C8
F7 D3 64 52 8A FA 2E 76 15 3A 7D 4F D1 8C E6 EB
            34 D1 EE F1 9E 00 0F 93
```

After pi

```
F5 86 2B A6 68 65 BA FC 49 64 2A 78 7E 05 C6 7C
C3 FA 00 C2 F2 EF BC 19 2A 1C 6F AA 9A 03 5F 4A
34 D1 EE F1 9E 00 0F 93 00 D6 FA BB CD EB 7E FC
4F 15 AC 46 58 E8 2B 6B 5E EB 81 B3 7B 76 75 F6
35 BC 56 2E 79 22 8C EA F7 D3 64 52 8A FA 2E 76
21 9C EA DD 55 F7 C1 89 70 F2 5F 6A 53 6C 01 AA
BA 9F D6 CD 8E C3 51 23 CF BF 91 01 1A BE D4 39
8F F8 11 12 2C 18 C8 9E 3C 8D 42 3B 3A 59 A0 63
1F 4D 25 46 DD 67 5B 46 36 7F 7D 76 0D 4C CA CF
28 82 CF AF 74 1D 84 9F 15 3A 7D 4F D1 8C E6 EB
0C E3 BE F1 F4 20 E8 C8 4C DB AE A0 73 4E C3 84
AA 46 D4 A5 99 D8 D4 65 A2 53 94 9E 0D 58 51 ED
            F5 3F C0 2E 39 AB 78 C8
```

After chi

```
77 1C 2B 24 E8 8F 82 FD 61 60 45 50 76 05 85 3E
D7 3B 80 93 F6 EF BC 88 EB 1A 6E AC FA 66 EF 26
3C B1 EE A9 88 00 4B 93 10 3C FB 0A EE FD 2A 68
6E 01 FA 4A 58 E8 A3 63 9C A8 A1 E3 F9 AE 57 E2
35 B8 CC 87 3C 23 DC 62 B8 D2 60 16 9A FA 2F 75
AB 91 6A 58 D9 74 91 88 35 D2 5E 6A 43 50 85 B2
BA DF D6 DF AA C3 59 A5 EF BB 7B CC 4B 59 D5 38
DF 9A 04 30 2E 10 C8 BC 1C BF 1A 0B 3A 51 20 EA
17 CD A7 CF AD 76 5F 56 23 47 4D 36 8C CC A8 AF
00 07 CD 9F 5E 4C 84 9F 16 7A 58 0B 14 AA BD EF
AE E7 EE F4 7C B0 FC A9 4C CA AE BA 77 4E C2 0C
FF 6A 94 85 A9 7B FC 65 AA 93 AA 4F C9 58 D1 ED
            B5 27 C0 2E 3A E5 7B CC
```

After iota

```
7F 9C 2B A4 E8 8F 82 7D 61 60 45 50 76 05 85 3E
D7 3B 80 93 F6 EF BC 88 EB 1A 6E AC FA 66 EF 26
3C B1 EE A9 88 00 4B 93 10 3C FB 0A EE FD 2A 68
6E 01 FA 4A 58 E8 A3 63 9C A8 A1 E3 F9 AE 57 E2
35 B8 CC 87 3C 23 DC 62 B8 D2 60 16 9A FA 2F 75
AB 91 6A 58 D9 74 91 88 35 D2 5E 6A 43 50 85 B2
BA DF D6 DF AA C3 59 A5 EF BB 7B CC 4B 59 D5 38
DF 9A 04 30 2E 10 C8 BC 1C BF 1A 0B 3A 51 20 EA
17 CD A7 CF AD 76 5F 56 23 47 4D 36 8C CC A8 AF
00 07 CD 9F 5E 4C 84 9F 16 7A 58 0B 14 AA BD EF
AE E7 EE F4 7C B0 FC A9 4C CA AE BA 77 4E C2 0C
FF 6A 94 85 A9 7B FC 65 AA 93 AA 4F C9 58 D1 ED
            B5 27 C0 2E 3A E5 7B CC
```

After permutation

```
7F 9C 2B A4 E8 8F 82 7D 61 60 45 50 76 05 85 3E
D7 3B 80 93 F6 EF BC 88 EB 1A 6E AC FA 66 EF 26
3C B1 EE A9 88 00 4B 93 10 3C FB 0A EE FD 2A 68
6E 01 FA 4A 58 E8 A3 63 9C A8 A1 E3 F9 AE 57 E2
35 B8 CC 87 3C 23 DC 62 B8 D2 60 16 9A FA 2F 75
AB 91 6A 58 D9 74 91 88 35 D2 5E 6A 43 50 85 B2
BA DF D6 DF AA C3 59 A5 EF BB 7B CC 4B 59 D5 38
DF 9A 04 30 2E 10 C8 BC 1C BF 1A 0B 3A 51 20 EA
17 CD A7 CF AD 76 5F 56 23 47 4D 36 8C CC A8 AF
00 07 CD 9F 5E 4C 84 9F 16 7A 58 0B 14 AA BD EF
AE E7 EE F4 7C B0 FC A9 4C CA AE BA 77 4E C2 0C
FF 6A 94 85 A9 7B FC 65 AA 93 AA 4F C9 58 D1 ED
            B5 27 C0 2E 3A E5 7B CC
```

State (as lanes of integers)

```
[0, 0] = 7d828fe8a42b9c7f
[1, 0] = 3e85057650456061
[2, 0] = 88bceff693803bd7
[3, 0] = 26ef66faac6e1aeb
[4, 0] = 934b0088a9eeb13c
[0, 1] = 682afdee0afb3c10
[1, 1] = 63a3e8584afa016e
[2, 1] = e257aef9e3a1a89c
[3, 1] = 62dc233c87ccb835
[4, 1] = 752ffa9a1660d2b8
[0, 2] = 889174d9586a91ab
[1, 2] = b28550436a5ed235
[2, 2] = a559c3aadfd6dfba
[3, 2] = 38d5594bcc7bbbef
[4, 2] = bcc8102e30049adf
[0, 3] = ea20513a0b1abf1c
[1, 3] = 565f76adcfa7cd17
[2, 3] = afa8cc8c364d4723
[3, 3] = 9f844c5e9fcd0700
[4, 3] = efbdaa140b587a16
[0, 4] = a9fcb07cf4eee7ae
[1, 4] = 0cc24e77baaeca4c
[2, 4] = 65fc7ba985946aff
[3, 4] = edd158c94faa93aa
[4, 4] = cc7be53a2ec027b5
```

About to call squeeze (again)

State before permutation

```
7F 9C 2B A4 E8 8F 82 7D 61 60 45 50 76 05 85 3E
D7 3B 80 93 F6 EF BC 88 EB 1A 6E AC FA 66 EF 26
3C B1 EE A9 88 00 4B 93 10 3C FB 0A EE FD 2A 68
6E 01 FA 4A 58 E8 A3 63 9C A8 A1 E3 F9 AE 57 E2
35 B8 CC 87 3C 23 DC 62 B8 D2 60 16 9A FA 2F 75
AB 91 6A 58 D9 74 91 88 35 D2 5E 6A 43 50 85 B2
BA DF D6 DF AA C3 59 A5 EF BB 7B CC 4B 59 D5 38
DF 9A 04 30 2E 10 C8 BC 1C BF 1A 0B 3A 51 20 EA
17 CD A7 CF AD 76 5F 56 23 47 4D 36 8C CC A8 AF
00 07 CD 9F 5E 4C 84 9F 16 7A 58 0B 14 AA BD EF
AE E7 EE F4 7C B0 FC A9 4C CA AE BA 77 4E C2 0C
FF 6A 94 85 A9 7B FC 65 AA 93 AA 4F C9 58 D1 ED
            B5 27 C0 2E 3A E5 7B CC
```

State before permutation (as lanes of integers)

```
[0, 0] = 7d828fe8a42b9c7f
[1, 0] = 3e85057650456061
[2, 0] = 88bceff693803bd7
[3, 0] = 26ef66faac6e1aeb
[4, 0] = 934b0088a9eeb13c
[0, 1] = 682afdee0afb3c10
[1, 1] = 63a3e8584afa016e
[2, 1] = e257aef9e3a1a89c
[3, 1] = 62dc233c87ccb835
[4, 1] = 752ffa9a1660d2b8
[0, 2] = 889174d9586a91ab
[1, 2] = b28550436a5ed235
[2, 2] = a559c3aadfd6dfba
[3, 2] = 38d5594bcc7bbbef
[4, 2] = bcc8102e30049adf
[0, 3] = ea20513a0b1abf1c
[1, 3] = 565f76adcfa7cd17
[2, 3] = afa8cc8c364d4723
[3, 3] = 9f844c5e9fcd0700
[4, 3] = efbdaa140b587a16
[0, 4] = a9fcb07cf4eee7ae
[1, 4] = 0cc24e77baaeca4c
[2, 4] = 65fc7ba985946aff
[3, 4] = edd158c94faa93aa
[4, 4] = cc7be53a2ec027b5
```

Round #0

After theta

```
44 50 E8 05 94 21 95 6E 4D CB 57 61 EF 89 AC EB
80 94 15 F9 75 7A E4 20 36 32 65 E4 5F 19 DC D1
4A EE CC 8C A0 C7 33 20 2B F0 38 AB 92 53 3D 7B
42 AA E8 7B C1 64 8A B6 CB 07 34 89 7A 3B 0F 4A
E8 90 C7 CF 99 5C EF 95 CE 8D 42 33 B2 3D 57 C6
90 5D A9 F9 A5 DA 86 9B 19 79 4C 5B DA DC AC 67
ED 70 43 B5 29 56 01 0D 32 93 70 84 EE 26 E6 CF
A9 C5 26 15 06 D7 B0 0F 27 73 D9 AA 46 FF 37 F9
3B 66 B5 FE 34 FA 76 83 74 E8 D8 5C 0F 59 F0 07
DD 2F C6 D7 FB 33 B7 68 60 25 7A 2E 3C 6D C5 5C
95 2B 2D 55 00 1E EB BA 60 61 BC 8B EE C2 EB D9
A8 C5 01 EF 2A EE A4 CD 77 BB A1 07 6C 27 E2 1A
            C3 78 E2 0B 12 22 03 7F
```

After rho

```
44 50 E8 05 94 21 95 6E 9B 96 AF C2 DE 13 59 D7
20 65 45 7E 9D 1E 39 08 95 C1 1D 6D 23 53 46 FE
3D 9E 01 51 72 67 66 04 2A 39 D5 B3 B7 02 8F B3
BE 17 4C A6 68 2B A4 8A D2 F2 01 4D A2 DE CE 83
C8 E3 E7 4C AE F7 4A 74 73 65 EC DC 28 34 23 DB
84 EC 4A CD 2F D5 36 DC 9E 65 E4 31 6D 69 73 B3
AA 4D B1 0A 68 68 87 1B 4D CC 9F 65 26 E1 08 DD
0A 83 6B D8 87 D4 62 93 55 8D FE 6F F2 4F E6 B2
D6 9F 46 DF 6E 70 C7 AC F8 03 3A 74 6C AE 87 2C
E6 16 AD FB C5 F8 7A 7F 5C 60 25 7A 2E 3C 6D C5
AC EB 56 AE B4 54 01 78 83 85 F1 2E BA 0B AF 67
B5 38 E0 5D C5 9D B4 19 BB A1 07 6C 27 E2 1A 77
            C0 DF 30 9E F8 82 84 C8
```

After pi

```
44 50 E8 05 94 21 95 6E BE 17 4C A6 68 2B A4 8A
AA 4D B1 0A 68 68 87 1B E6 16 AD FB C5 F8 7A 7F
C0 DF 30 9E F8 82 84 C8 95 C1 1D 6D 23 53 46 FE
73 65 EC DC 28 34 23 DB 84 EC 4A CD 2F D5 36 DC
D6 9F 46 DF 6E 70 C7 AC B5 38 E0 5D C5 9D B4 19
9B 96 AF C2 DE 13 59 D7 D2 F2 01 4D A2 DE CE 83
4D CC 9F 65 26 E1 08 DD 5C 60 25 7A 2E 3C 6D C5
AC EB 56 AE B4 54 01 78 3D 9E 01 51 72 67 66 04
2A 39 D5 B3 B7 02 8F B3 9E 65 E4 31 6D 69 73 B3
F8 03 3A 74 6C AE 87 2C BB A1 07 6C 27 E2 1A 77
20 65 45 7E 9D 1E 39 08 C8 E3 E7 4C AE F7 4A 74
0A 83 6B D8 87 D4 62 93 55 8D FE 6F F2 4F E6 B2
            83 85 F1 2E BA 0B AF 67
```

After chi

```
44 18 59 0D 94 61 96 7F FA 05 40 57 ED BB DC EE
AA 84 A1 0E 50 6A 03 9B E2 16 65 FA C1 D9 6B 59
7A D8 34 3C 90 88 A4 48 11 49 1F 6C 24 92 52 FA
21 76 E8 CE 68 14 E2 FB A5 CC EA CD AE 58 06 CD
D6 5E 5B FF 4C 32 85 4A D7 1C 00 CD CD B9 95 18
96 9A 31 E2 DA 32 59 8B C2 D2 21 57 AA C2 AB 83
ED 47 CD E1 B6 A1 08 E5 4F 74 8C 3A 64 3F 35 42
EC 8B 56 A3 94 98 87 78 A9 DA 21 51 3A 0E 16 04
4A 3B CF F7 B7 84 0B BF 9D C5 E1 39 6E 29 6B E0
FC 1D 3A 65 3C AB E3 2C B9 80 D3 CE A2 E2 93 C4
22 65 4D EE 9C 1E 19 8B 9D EF 73 6B DE FC CE 54
88 83 6A D8 8F D4 6B D6 75 ED FA 3F F7 5B F6 BA
            4B 07 53 2E 98 EA ED 13
```

After iota

```
45 18 59 0D 94 61 96 7F FA 05 40 57 ED BB DC EE
AA 84 A1 0E 50 6A 03 9B E2 16 65 FA C1 D9 6B 59
7A D8 34 3C 90 88 A4 48 11 49 1F 6C 24 92 52 FA
21 76 E8 CE 68 14 E2 FB A5 CC EA CD AE 58 06 CD
D6 5E 5B FF 4C 32 85 4A D7 1C 00 CD CD B9 95 18
96 9A 31 E2 DA 32 59 8B C2 D2 21 57 AA C2 AB 83
ED 47 CD E1 B6 A1 08 E5 4F 74 8C 3A 64 3F 35 42
EC 8B 56 A3 94 98 87 78 A9 DA 21 51 3A 0E 16 04
4A 3B CF F7 B7 84 0B BF 9D C5 E1 39 6E 29 6B E0
FC 1D 3A 65 3C AB E3 2C B9 80 D3 CE A2 E2 93 C4
22 65 4D EE 9C 1E 19 8B 9D EF 73 6B DE FC CE 54
88 83 6A D8 8F D4 6B D6 75 ED FA 3F F7 5B F6 BA
            4B 07 53 2E 98 EA ED 13
```

(Skip rounds 1 to 22)

Round #23

After theta

```
38 EB E3 7D 36 5C 29 FB B3 4A 0D 6A BC 96 62 80
A8 AE AB 8A 81 C2 F5 C6 6E A9 B2 90 4D 39 13 24
1C 38 32 7D 93 63 CC EF 72 3E 0E EF 7F C5 39 7C
B0 9C 84 F3 96 FB F9 70 7F 38 FD A8 E4 63 9A 41
74 F7 FA 60 97 0E D4 66 D5 49 8A 48 94 CC F6 C9
8E 33 8C 50 72 E6 8C 7A 75 51 1C 2D 3D 77 42 4C
39 B6 D5 EE 66 D0 F3 92 8C 0D BC ED 0D E3 40 52
A5 7D 92 41 35 0A 21 9D 5C 60 21 27 18 20 67 2C
B2 A7 72 50 8E 9A 47 D5 64 AD 4B 1D 66 DF FE 31
36 CE 9C 89 E7 3B CF 9A 15 E2 E0 AB F2 8C 59 69
3A F0 98 FA 59 9F 6B AA 77 0F B2 DF 43 39 07 F6
DC AA 81 F2 54 DB 92 E7 8F F1 7C 6C 29 40 9A 86
            EF C9 88 30 89 D1 CB B8
```

After rho

```
38 EB E3 7D 36 5C 29 FB 67 95 1A D4 78 2D C5 00
AA EB AA 62 A0 70 BD 31 94 33 41 E2 96 2A 0B D9
1C 63 7E E7 C0 91 E9 9B FE 57 9C C3 27 E7 E3 F0
38 6F B9 9F 0F 07 CB 49 D0 1F 4E 3F 2A F9 98 66
7B 7D B0 4B 07 6A 33 BA 6C 9F 5C 9D A4 88 44 C9
73 9C 61 84 92 33 67 D4 31 D5 45 71 B4 F4 DC 09
76 37 83 9E 97 CC B1 AD C6 81 A4 18 1B 78 DB 1B
A0 1A 85 90 CE D2 3E C9 4E 30 40 CE 58 B8 C0 42
0E CA 51 F3 A8 5A F6 54 FF 18 B2 D6 A5 0E B3 6F
E7 59 D3 C6 99 33 F1 7C 69 15 E2 E0 AB F2 8C 59
AE A9 EA C0 63 EA 67 7D DF 3D C8 7E 0F E5 1C D8
5B 35 50 9E 6A 5B F2 9C F1 7C 6C 29 40 9A 86 8F
            32 EE 7B 32 22 4C 62 F4
```

After pi

```
38 EB E3 7D 36 5C 29 FB 38 6F B9 9F 0F 07 CB 49
76 37 83 9E 97 CC B1 AD E7 59 D3 C6 99 33 F1 7C
32 EE 7B 32 22 4C 62 F4 94 33 41 E2 96 2A 0B D9
6C 9F 5C 9D A4 88 44 C9 73 9C 61 84 92 33 67 D4
0E CA 51 F3 A8 5A F6 54 5B 35 50 9E 6A 5B F2 9C
67 95 1A D4 78 2D C5 00 D0 1F 4E 3F 2A F9 98 66
C6 81 A4 18 1B 78 DB 1B 69 15 E2 E0 AB F2 8C 59
AE A9 EA C0 63 EA 67 7D 1C 63 7E E7 C0 91 E9 9B
FE 57 9C C3 27 E7 E3 F0 31 D5 45 71 B4 F4 DC 09
FF 18 B2 D6 A5 0E B3 6F F1 7C 6C 29 40 9A 86 8F
AA EB AA 62 A0 70 BD 31 7B 7D B0 4B 07 6A 33 BA
A0 1A 85 90 CE D2 3E C9 4E 30 40 CE 58 B8 C0 42
            DF 3D C8 7E 0F E5 1C D8
```

After chi

```
7E FB E1 7D A6 94 19 5F B9 27 E9 DF 07 34 8B 19
66 91 AB AE B5 80 B3 2D EF 58 53 8B 8D 23 F8 77
32 EA 63 B0 2B 4F A0 F4 87 33 60 E2 84 19 28 CD
60 DD 4C EE 8C C0 D4 C9 22 A9 61 88 D0 32 67 5C
8A C8 50 93 3C 7A FF 15 33 B9 4C 83 4A DB B6 9C
61 15 BA D4 69 2D 86 19 F9 0B 0C DF 8A 7B 9C 26
40 29 AC 18 5B 70 B8 3F 28 01 F2 F4 B3 F7 0C 59
3E A3 AE EB 61 3A 7F 1B 1D E3 3F D7 50 81 F5 92
30 5F 2E 45 26 ED C0 96 31 B1 09 58 F4 64 D8 89
F3 1B A0 10 25 0F DA 7F 13 68 EC 29 67 FC 84 EF
2A E9 AF F2 68 E0 B1 70 35 5D F0 05 17 42 F3 B8
31 17 0D A0 C9 97 22 51 6E F2 62 CE F8 A8 61 63
            8E 29 D8 77 08 EF 1E 52
```

After iota

```
76 7B E1 FD A6 94 19 DF B9 27 E9 DF 07 34 8B 19
66 91 AB AE B5 80 B3 2D EF 58 53 8B 8D 23 F8 77
32 EA 63 B0 2B 4F A0 F4 87 33 60 E2 84 19 28 CD
60 DD 4C EE 8C C0 D4 C9 22 A9 61 88 D0 32 67 5C
8A C8 50 93 3C 7A FF 15 33 B9 4C 83 4A DB B6 9C
61 15 BA D4 69 2D 86 19 F9 0B 0C DF 8A 7B 9C 26
40 29 AC 18 5B 70 B8 3F 28 01 F2 F4 B3 F7 0C 59
3E A3 AE EB 61 3A 7F 1B 1D E3 3F D7 50 81 F5 92
30 5F 2E 45 26 ED C0 96 31 B1 09 58 F4 64 D8 89
F3 1B A0 10 25 0F DA 7F 13 68 EC 29 67 FC 84 EF
2A E9 AF F2 68 E0 B1 70 35 5D F0 05 17 42 F3 B8
31 17 0D A0 C9 97 22 51 6E F2 62 CE F8 A8 61 63
            8E 29 D8 77 08 EF 1E 52
```

After permutation

```
76 7B E1 FD A6 94 19 DF B9 27 E9 DF 07 34 8B 19
66 91 AB AE B5 80 B3 2D EF 58 53 8B 8D 23 F8 77
32 EA 63 B0 2B 4F A0 F4 87 33 60 E2 84 19 28 CD
60 DD 4C EE 8C C0 D4 C9 22 A9 61 88 D0 32 67 5C
8A C8 50 93 3C 7A FF 15 33 B9 4C 83 4A DB B6 9C
61 15 BA D4 69 2D 86 19 F9 0B 0C DF 8A 7B 9C 26
40 29 AC 18 5B 70 B8 3F 28 01 F2 F4 B3 F7 0C 59
3E A3 AE EB 61 3A 7F 1B 1D E3 3F D7 50 81 F5 92
30 5F 2E 45 26 ED C0 96 31 B1 09 58 F4 64 D8 89
F3 1B A0 10 25 0F DA 7F 13 68 EC 29 67 FC 84 EF
2A E9 AF F2 68 E0 B1 70 35 5D F0 05 17 42 F3 B8
31 17 0D A0 C9 97 22 51 6E F2 62 CE F8 A8 61 63
            8E 29 D8 77 08 EF 1E 52
```

State (as lanes of integers)

```
[0, 0] = df1994a6fde17b76
[1, 0] = 198b3407dfe927b9
[2, 0] = 2db380b5aeab9166
[3, 0] = 77f8238d8b5358ef
[4, 0] = f4a04f2bb063ea32
[0, 1] = cd281984e2603387
[1, 1] = c9d4c08cee4cdd60
[2, 1] = 5c6732d08861a922
[3, 1] = 15ff7a3c9350c88a
[4, 1] = 9cb6db4a834cb933
[0, 2] = 19862d69d4ba1561
[1, 2] = 269c7b8adf0c0bf9
[2, 2] = 3fb8705b18ac2940
[3, 2] = 590cf7b3f4f20128
[4, 2] = 1b7f3a61ebaea33e
[0, 3] = 92f58150d73fe31d
[1, 3] = 96c0ed26452e5f30
[2, 3] = 89d864f45809b131
[3, 3] = 7fda0f2510a01bf3
[4, 3] = ef84fc6729ec6813
[0, 4] = 70b1e068f2afe92a
[1, 4] = b8f3421705f05d35
[2, 4] = 512297c9a00d1731
[3, 4] = 6361a8f8ce62f26e
[4, 4] = 521eef0877d8298e
```

About to call squeeze (again)

State before permutation (in bytes)

```
76 7B E1 FD A6 94 19 DF B9 27 E9 DF 07 34 8B 19
66 91 AB AE B5 80 B3 2D EF 58 53 8B 8D 23 F8 77
32 EA 63 B0 2B 4F A0 F4 87 33 60 E2 84 19 28 CD
60 DD 4C EE 8C C0 D4 C9 22 A9 61 88 D0 32 67 5C
8A C8 50 93 3C 7A FF 15 33 B9 4C 83 4A DB B6 9C
61 15 BA D4 69 2D 86 19 F9 0B 0C DF 8A 7B 9C 26
40 29 AC 18 5B 70 B8 3F 28 01 F2 F4 B3 F7 0C 59
3E A3 AE EB 61 3A 7F 1B 1D E3 3F D7 50 81 F5 92
30 5F 2E 45 26 ED C0 96 31 B1 09 58 F4 64 D8 89
F3 1B A0 10 25 0F DA 7F 13 68 EC 29 67 FC 84 EF
2A E9 AF F2 68 E0 B1 70 35 5D F0 05 17 42 F3 B8
31 17 0D A0 C9 97 22 51 6E F2 62 CE F8 A8 61 63
            8E 29 D8 77 08 EF 1E 52
```

State before permutation (as lanes of integers)

```
[0, 0] = df1994a6fde17b76
[1, 0] = 198b3407dfe927b9
[2, 0] = 2db380b5aeab9166
[3, 0] = 77f8238d8b5358ef
[4, 0] = f4a04f2bb063ea32
[0, 1] = cd281984e2603387
[1, 1] = c9d4c08cee4cdd60
[2, 1] = 5c6732d08861a922
[3, 1] = 15ff7a3c9350c88a
[4, 1] = 9cb6db4a834cb933
[0, 2] = 19862d69d4ba1561
[1, 2] = 269c7b8adf0c0bf9
[2, 2] = 3fb8705b18ac2940
[3, 2] = 590cf7b3f4f20128
[4, 2] = 1b7f3a61ebaea33e
[0, 3] = 92f58150d73fe31d
[1, 3] = 96c0ed26452e5f30
[2, 3] = 89d864f45809b131
[3, 3] = 7fda0f2510a01bf3
[4, 3] = ef84fc6729ec6813
[0, 4] = 70b1e068f2afe92a
[1, 4] = b8f3421705f05d35
[2, 4] = 512297c9a00d1731
[3, 4] = 6361a8f8ce62f26e
[4, 4] = 521eef0877d8298e
```

Round #0

After theta

```
9F 2C BB 27 A8 69 0A A0 17 1E 87 BD 73 97 54 DD
E3 93 BA 64 3B B3 23 BA AE 8C 5A 40 51 68 89 7C
AD 3D 06 5F 13 C4 F7 00 6E 64 3A 38 8A E4 3B B2
CE E4 22 8C F8 63 0B 0D A7 AB 70 42 5E 01 F7 CB
CB 1C 59 58 E0 31 8E 1E AC 6E 29 6C 72 50 E1 68
88 42 E0 0E 67 D0 95 66 57 32 62 BD FE D8 43 E2
C5 2B BD D2 D5 43 28 A8 69 D5 FB 3F 6F BC 7D 52
A1 74 CB 04 59 B1 28 EF F4 B4 65 0D 5E 7C E6 ED
9E 66 40 27 52 4E 1F 52 B4 B3 18 92 7A 57 48 1E
B2 CF A9 DB F9 44 AB 74 8C BF 89 C6 5F 77 D3 1B
C3 BE F5 28 66 1D A2 0F 9B 64 9E 67 63 E1 2C 7C
B4 15 1C 6A 47 A4 B2 C6 2F 26 6B 05 24 E3 10 68
            11 FE BD 98 30 64 49 A6
```

After rho

```
9F 2C BB 27 A8 69 0A A0 2F 3C 0E 7B E7 2E A9 BA
F8 A4 2E D9 CE EC 88 EE 85 96 C8 E7 CA A8 05 14
20 BE 07 68 ED 31 F8 9A A3 48 BE 23 EB 46 A6 83
C2 88 3F B6 D0 E0 4C 2E F2 E9 2A 9C 90 57 C0 FD
8E 2C 2C F0 18 47 8F 65 15 8E C6 EA 96 C2 26 07
43 14 02 77 38 83 AE 34 89 5F C9 88 F5 FA 63 0F
95 AE 1E 42 41 2D 5E E9 78 FB A4 D2 AA F7 7F DE
82 AC 58 94 F7 50 BA 65 1A BC F8 CC DB E9 69 CB
E8 44 CA E9 43 CA D3 0C 24 0F DA 59 0C 49 BD 2B
68 95 4E F6 39 75 3B 9F 1B 8C BF 89 C6 5F 77 D3
88 3E 0C FB D6 A3 98 75 6D 92 79 9E 8D 85 B3 F0
B6 82 43 ED 88 54 D6 98 26 6B 05 24 E3 10 68 2F
            92 69 84 7F 2F 26 0C 59
```

After pi

```
9F 2C BB 27 A8 69 0A A0 C2 88 3F B6 D0 E0 4C 2E
95 AE 1E 42 41 2D 5E E9 68 95 4E F6 39 75 3B 9F
92 69 84 7F 2F 26 0C 59 85 96 C8 E7 CA A8 05 14
15 8E C6 EA 96 C2 26 07 43 14 02 77 38 83 AE 34
E8 44 CA E9 43 CA D3 0C B6 82 43 ED 88 54 D6 98
2F 3C 0E 7B E7 2E A9 BA F2 E9 2A 9C 90 57 C0 FD
78 FB A4 D2 AA F7 7F DE 1B 8C BF 89 C6 5F 77 D3
88 3E 0C FB D6 A3 98 75 20 BE 07 68 ED 31 F8 9A
A3 48 BE 23 EB 46 A6 83 89 5F C9 88 F5 FA 63 0F
24 0F DA 59 0C 49 BD 2B 26 6B 05 24 E3 10 68 2F
F8 A4 2E D9 CE EC 88 EE 8E 2C 2C F0 18 47 8F 65
82 AC 58 94 F7 50 BA 65 1A BC F8 CC DB E9 69 CB
            6D 92 79 9E 8D 85 B3 F0
```

After chi

```
8A 0A BB 67 A9 64 18 61 AA 99 7F 02 E8 B0 6D 38
07 C6 9E 4B 47 2F 5A A9 65 91 75 F6 B9 3C 39 3F
D2 E9 80 EF 7F A6 48 57 C7 86 C8 F2 E2 A9 8D 24
BD CE 0E 62 D5 8A 77 0F 55 96 03 73 B0 97 AA A4
E9 50 42 EB 01 62 D2 08 A6 8A 45 E5 9C 16 F4 9B
27 2E 8A 39 CD 8E 96 B8 F1 ED 31 95 D4 5F C0 FC
F8 C9 A4 A0 BA 57 F7 FA 3C 8C BD 89 E7 53 56 59
58 FF 2C 7F C6 F2 D8 30 28 A9 46 E0 F9 89 B9 96
87 48 AC 72 E3 47 3A A3 8B 3F CC AC 16 EA 23 0B
24 9B D8 11 00 68 2D BB A5 2B BD 27 E1 56 6E 2E
F8 24 7E DD 29 FC B8 EE 96 3C 8C B8 10 EE CE EF
E7 AE 59 86 F3 54 28 55 8A 98 FE 8D 99 81 61 C5
            6B 9A 79 BE 9D 86 B4 F1
```

After iota

```
8B 0A BB 67 A9 64 18 61 AA 99 7F 02 E8 B0 6D 38
07 C6 9E 4B 47 2F 5A A9 65 91 75 F6 B9 3C 39 3F
D2 E9 80 EF 7F A6 48 57 C7 86 C8 F2 E2 A9 8D 24
BD CE 0E 62 D5 8A 77 0F 55 96 03 73 B0 97 AA A4
E9 50 42 EB 01 62 D2 08 A6 8A 45 E5 9C 16 F4 9B
27 2E 8A 39 CD 8E 96 B8 F1 ED 31 95 D4 5F C0 FC
F8 C9 A4 A0 BA 57 F7 FA 3C 8C BD 89 E7 53 56 59
58 FF 2C 7F C6 F2 D8 30 28 A9 46 E0 F9 89 B9 96
87 48 AC 72 E3 47 3A A3 8B 3F CC AC 16 EA 23 0B
24 9B D8 11 00 68 2D BB A5 2B BD 27 E1 56 6E 2E
F8 24 7E DD 29 FC B8 EE 96 3C 8C B8 10 EE CE EF
E7 AE 59 86 F3 54 28 55 8A 98 FE 8D 99 81 61 C5
            6B 9A 79 BE 9D 86 B4 F1
```

(Skip rounds 1 to 22)

Round #23

After theta

```
24 F3 4C 0B 2B 53 2B E5 01 58 E8 86 76 54 27 BB
E5 CB C8 81 CC B9 AC E4 E7 35 DC 86 4F 5D B1 57
63 96 A9 1E E8 8B 43 5A AC 21 84 1F FE 01 8C A9
CF 3E 10 19 17 03 6B E5 88 F0 B1 AA B6 3C AD 4F
E7 B5 59 BA 83 7E 0B 57 C4 85 48 7C A2 1E E5 C7
02 D1 1B 7B 79 0A 7B 03 47 86 2E 94 35 80 AF E5
AA 5A CB A6 5B 31 93 6C 0B 8D A0 96 16 73 60 82
D0 05 D4 79 71 59 70 81 8A 03 71 AB D6 C1 89 72
A3 5F 4A 54 8E 95 3A EE 93 8B 08 B7 84 CA B1 E0
90 6A E4 9A 38 12 09 72 DD 04 C3 7E 0B 12 60 ED
44 1A CD AE A8 6A D3 2E E3 F4 95 B6 6B 53 43 4C
DE 97 C5 E5 AE E6 E3 05 AA 64 4A 2C 9A 95 46 47
            B5 EA 07 D7 61 5F AD EA
```

After rho

```
24 F3 4C 0B 2B 53 2B E5 03 B0 D0 0D ED A8 4E 76
F9 32 72 20 73 2E 2B 79 D4 15 7B 75 5E C3 6D F8
5F 1C D2 1A B3 4C F5 40 E1 1F C0 98 CA 1A 42 F8
91 71 31 B0 56 FE EC 03 13 22 7C AC AA 2D 4F EB
DA 2C DD 41 BF 85 AB F3 51 7E 4C 5C 88 C4 27 EA
10 88 DE D8 CB 53 D8 1B 96 1F 19 BA 50 D6 00 BE
36 DD 8A 99 64 53 D5 5A E6 C0 04 17 1A 41 2D 2D
BC B8 2C B8 40 E8 02 EA 56 AD 83 13 E5 14 07 E2
89 CA B1 52 C7 7D F4 4B 58 F0 C9 45 84 5B 42 E5
22 41 0E 52 8D 5C 13 47 ED DD 04 C3 7E 0B 12 60
4D BB 10 69 34 BB A2 AA 8D D3 57 DA AE 4D 0D 31
FB B2 B8 DC D5 7C BC C0 64 4A 2C 9A 95 46 47 AA
            AB 7A AD FA C1 75 D8 57
```

After pi

```
24 F3 4C 0B 2B 53 2B E5 91 71 31 B0 56 FE EC 03
36 DD 8A 99 64 53 D5 5A 22 41 0E 52 8D 5C 13 47
AB 7A AD FA C1 75 D8 57 D4 15 7B 75 5E C3 6D F8
51 7E 4C 5C 88 C4 27 EA 10 88 DE D8 CB 53 D8 1B
89 CA B1 52 C7 7D F4 4B FB B2 B8 DC D5 7C BC C0
03 B0 D0 0D ED A8 4E 76 13 22 7C AC AA 2D 4F EB
E6 C0 04 17 1A 41 2D 2D ED DD 04 C3 7E 0B 12 60
4D BB 10 69 34 BB A2 AA 5F 1C D2 1A B3 4C F5 40
E1 1F C0 98 CA 1A 42 F8 96 1F 19 BA 50 D6 00 BE
58 F0 C9 45 84 5B 42 E5 64 4A 2C 9A 95 46 47 AA
F9 32 72 20 73 2E 2B 79 DA 2C DD 41 BF 85 AB F3
BC B8 2C B8 40 E8 02 EA 56 AD 83 13 E5 14 07 E2
            8D D3 57 DA AE 4D 0D 31
```

After chi

```
02 7F C6 02 0B 52 3A BD 91 71 35 F2 DF F2 EE 06
BF E7 2B 31 24 72 1D 4A 26 C0 4E 53 A7 5E 30 E7
3A 7A 9C 4A 95 D9 1C 55 D4 95 E9 F5 1D D0 B5 E9
D8 3C 6D 5E 8C E8 03 AA 62 B8 D6 54 DB 53 D0 9B
8D CF F2 73 CD FE B5 73 FA D8 BC D4 55 78 BE C2
E7 70 D0 1E FD E8 6E 72 1A 3F 7C 6C CE 27 5D AB
E6 E2 14 3F 1A F1 8D A7 EF DD C4 C7 B7 0B 5E 34
5D B9 3C C9 36 BE A3 23 49 1C CB 38 A3 88 F5 46
A9 FF 00 DD 4E 13 00 B9 B2 15 3D 20 41 D2 05 B4
43 E4 1B 45 A6 53 F2 A5 C4 49 2C 1A DD 54 45 12
DD A2 52 98 33 46 2B 71 98 29 5E 42 1A 91 AE F3
35 EA 78 70 4A A1 0A FB 26 8D A3 33 B4 36 25 AA
            8F DF DA 9B 22 CC 8D B3
```

After iota

```
0A FF C6 82 0B 52 3A 3D 91 71 35 F2 DF F2 EE 06
BF E7 2B 31 24 72 1D 4A 26 C0 4E 53 A7 5E 30 E7
3A 7A 9C 4A 95 D9 1C 55 D4 95 E9 F5 1D D0 B5 E9
D8 3C 6D 5E 8C E8 03 AA 62 B8 D6 54 DB 53 D0 9B
8D CF F2 73 CD FE B5 73 FA D8 BC D4 55 78 BE C2
E7 70 D0 1E FD E8 6E 72 1A 3F 7C 6C CE 27 5D AB
E6 E2 14 3F 1A F1 8D A7 EF DD C4 C7 B7 0B 5E 34
5D B9 3C C9 36 BE A3 23 49 1C CB 38 A3 88 F5 46
A9 FF 00 DD 4E 13 00 B9 B2 15 3D 20 41 D2 05 B4
43 E4 1B 45 A6 53 F2 A5 C4 49 2C 1A DD 54 45 12
DD A2 52 98 33 46 2B 71 98 29 5E 42 1A 91 AE F3
35 EA 78 70 4A A1 0A FB 26 8D A3 33 B4 36 25 AA
            8F DF DA 9B 22 CC 8D B3
```

After permutation

```
0A FF C6 82 0B 52 3A 3D 91 71 35 F2 DF F2 EE 06
BF E7 2B 31 24 72 1D 4A 26 C0 4E 53 A7 5E 30 E7
3A 7A 9C 4A 95 D9 1C 55 D4 95 E9 F5 1D D0 B5 E9
D8 3C 6D 5E 8C E8 03 AA 62 B8 D6 54 DB 53 D0 9B
8D CF F2 73 CD FE B5 73 FA D8 BC D4 55 78 BE C2
E7 70 D0 1E FD E8 6E 72 1A 3F 7C 6C CE 27 5D AB
E6 E2 14 3F 1A F1 8D A7 EF DD C4 C7 B7 0B 5E 34
5D B9 3C C9 36 BE A3 23 49 1C CB 38 A3 88 F5 46
A9 FF 00 DD 4E 13 00 B9 B2 15 3D 20 41 D2 05 B4
43 E4 1B 45 A6 53 F2 A5 C4 49 2C 1A DD 54 45 12
DD A2 52 98 33 46 2B 71 98 29 5E 42 1A 91 AE F3
35 EA 78 70 4A A1 0A FB 26 8D A3 33 B4 36 25 AA
           8F DF DA 9B 22 CC 8D B3
```

State (as lanes of integers)

```
[0, 0] = 3d3a520b82c6ff0a
[1, 0] = 06eef2dff2357191
[2, 0] = 4a1d7224312be7bf
[3, 0] = e7305ea7534ec026
[4, 0] = 551cd9954a9c7a3a
[0, 1] = e9b5d01df5e995d4
[1, 1] = aa03e88c5e6d3cd8
[2, 1] = 9bd053db54d6b862
[3, 1] = 73b5fecd73f2cf8d
[4, 1] = c2be7855d4bcd8fa
[0, 2] = 726ee8fd1ed070e7
[1, 2] = ab5d27ce6c7c3f1a
[2, 2] = a78df11a3f14e2e6
[3, 2] = 345e0bb7c7c4ddef
[4, 2] = 23a3be36c93cb95d
[0, 3] = 46f588a338cb1c49
[1, 3] = b900134edd00ffa9
[2, 3] = b405d241203d15b2
[3, 3] = a5f253a6451be443
[4, 3] = 124554dd1a2c49c4
[0, 4] = 712b46339852a2dd
[1, 4] = f3ae911a425e2998
[2, 4] = fb0aa14a7078ea35
[3, 4] = aa2536b433a38d26
[4, 4] = b38dcc229bdadf8f
```

About to call squeeze (again)

State before permutation (in bytes)

```
0A FF C6 82 0B 52 3A 3D 91 71 35 F2 DF F2 EE 06
BF E7 2B 31 24 72 1D 4A 26 C0 4E 53 A7 5E 30 E7
3A 7A 9C 4A 95 D9 1C 55 D4 95 E9 F5 1D D0 B5 E9
D8 3C 6D 5E 8C E8 03 AA 62 B8 D6 54 DB 53 D0 9B
8D CF F2 73 CD FE B5 73 FA D8 BC D4 55 78 BE C2
E7 70 D0 1E FD E8 6E 72 1A 3F 7C 6C CE 27 5D AB
E6 E2 14 3F 1A F1 8D A7 EF DD C4 C7 B7 0B 5E 34
5D B9 3C C9 36 BE A3 23 49 1C CB 38 A3 88 F5 46
A9 FF 00 DD 4E 13 00 B9 B2 15 3D 20 41 D2 05 B4
43 E4 1B 45 A6 53 F2 A5 C4 49 2C 1A DD 54 45 12
DD A2 52 98 33 46 2B 71 98 29 5E 42 1A 91 AE F3
35 EA 78 70 4A A1 0A FB 26 8D A3 33 B4 36 25 AA
           8F DF DA 9B 22 CC 8D B3
```

State before permutation (as lanes of integers)

```
[0, 0] = 3d3a520b82c6ff0a
[1, 0] = 06eef2dff2357191
[2, 0] = 4a1d7224312be7bf
[3, 0] = e7305ea7534ec026
[4, 0] = 551cd9954a9c7a3a
[0, 1] = e9b5d01df5e995d4
[1, 1] = aa03e88c5e6d3cd8
[2, 1] = 9bd053db54d6b862
[3, 1] = 73b5fecd73f2cf8d
[4, 1] = c2be7855d4bcd8fa
[0, 2] = 726ee8fd1ed070e7
[1, 2] = ab5d27ce6c7c3f1a
[2, 2] = a78df11a3f14e2e6
[3, 2] = 345e0bb7c7c4ddef
[4, 2] = 23a3be36c93cb95d
[0, 3] = 46f588a338cb1c49
[1, 3] = b900134edd00ffa9
[2, 3] = b405d241203d15b2
[3, 3] = a5f253a6451be443
[4, 3] = 124554dd1a2c49c4
[0, 4] = 712b46339852a2dd
[1, 4] = f3ae911a425e2998
[2, 4] = fb0aa14a7078ea35
[3, 4] = aa2536b433a38d26
[4, 4] = b38dcc229bdadf8f
```

Round #0

After theta

```
18 3A D9 EA 90 AA CE B2 44 50 0B 2E 78 11 4E E5
9E 35 D0 4D 72 50 1A 59 36 99 37 F4 5A F3 EC F5
40 88 91 49 AD 5F 6F D8 C6 50 F6 9D 86 28 41 66
0D 1D 53 82 2B 0B A3 49 43 6A 2D 28 8D 71 D7 88
9D 96 8B D4 30 53 69 61 80 2A B1 D7 6D FE CD 4F
F5 B5 CF 76 66 10 9A FD CF 1E 42 B0 69 C4 FD 48
C7 30 EF 43 4C D3 8A B4 FF 84 BD 60 4A A6 82 26
27 4B 31 CA 0E 38 D0 AE 5B D9 D4 50 38 70 01 C9
7C DE 3E 01 E9 F0 A0 5A 93 C7 C6 5C 17 F0 02 A7
53 BD 62 E2 5B FE 2E B7 BE BB 21 19 E5 D2 36 9F
CF 67 4D F0 A8 BE DF FE 4D 08 60 9E BD 72 0E 10
14 38 83 0C 1C 83 0D E8 36 D4 DA 94 49 9B F9 B8
            F5 2D D7 98 1A 4A FE 3E
```

After rho

```
18 3A D9 EA 90 AA CE B2 89 A0 16 5C F0 22 9C CA
67 0D 74 93 1C 94 46 96 35 CF 5E 6F 93 79 43 AF
FD 7A C3 06 42 8C 4C 6A 69 88 12 64 66 0C 65 DF
25 B8 B2 30 9A D4 D0 31 E2 90 5A 0B 4A 63 DC 35
CB 45 6A 98 A9 B4 B0 4E DF FC 04 A8 12 7B DD E6
AF AF 7D B6 33 83 D0 EC 23 3D 7B 08 C1 A6 11 F7
1F 62 9A 56 A4 3D 86 79 4C 05 4D FE 09 7B C1 94
65 07 1C 68 D7 93 A5 18 A1 70 E0 02 92 B7 B2 A9
27 20 1D 1E 54 8B CF DB 81 D3 C9 63 63 AE 0B 78
DF E5 76 AA 57 4C 7C CB 9F BE BB 21 19 E5 D2 36
7E FB 3F 9F 35 C1 A3 FA 34 21 80 79 F6 CA 39 40
02 67 90 81 63 B0 01 9D D4 DA 94 49 9B F9 B8 36
            BF 4F 7D CB 35 A6 86 92
```

After pi

```
18 3A D9 EA 90 AA CE B2 25 B8 B2 30 9A D4 D0 31
1F 62 9A 56 A4 3D 86 79 DF E5 76 AA 57 4C 7C CB
BF 4F 7D CB 35 A6 86 92 35 CF 5E 6F 93 79 43 AF
DF FC 04 A8 12 7B DD E6 AF AF 7D B6 33 83 D0 EC
27 20 1D 1E 54 8B CF DB 02 67 90 81 63 B0 01 9D
89 A0 16 5C F0 22 9C CA E2 90 5A 0B 4A 63 DC 35
4C 05 4D FE 09 7B C1 94 9F BE BB 21 19 E5 D2 36
7E FB 3F 9F 35 C1 A3 FA FD 7A C3 06 42 8C 4C 6A
69 88 12 64 66 0C 65 DF 23 3D 7B 08 C1 A6 11 F7
81 D3 C9 63 63 AE 0B 78 D4 DA 94 49 9B F9 B8 36
67 0D 74 93 1C 94 46 96 CB 45 6A 98 A9 B4 B0 4E
65 07 1C 68 D7 93 A5 18 A1 70 E0 02 92 B7 B2 A9
            34 21 80 79 F6 CA 39 40
```

After chi

```
02 78 D1 AC B4 83 C8 FA E5 3D D6 98 C9 94 A8 B3
3F 68 93 17 84 9F 04 69 DF D5 F6 8A D7 44 34 EB
9A CF 5F DB 3F F2 96 93 15 CC 27 79 B2 F9 43 A7
DF FC 04 A0 56 73 D2 F5 AF E8 FD 37 10 B3 D0 E8
12 A8 53 70 C4 C2 8D F9 C8 57 90 01 63 B2 9D DD
85 A5 13 A8 F1 3A 9D 4A 71 2A E8 0A 5A E7 CE 17
2C 44 49 60 2D 7B E0 5C 1E BE BB 61 D9 C7 CE 36
1C EB 77 9C 3F 80 E3 CF FF 4F AA 0E C3 2E 5C 4A
E9 4A 92 07 44 04 6F D7 77 35 6F 00 59 F7 A1 F1
A8 F3 8A 65 23 AA 4F 30 D4 5A 84 29 BF F9 99 A3
43 0F 60 F3 4A 97 43 86 4B 35 8A 9A A9 90 A2 EF
71 06 1C 11 B3 DB AC 58 E2 7C 94 80 9A A3 F4 3F
            BC 61 8A 71 57 EA 89 08
```

After iota

```
03 78 D1 AC B4 83 C8 FA E5 3D D6 98 C9 94 A8 B3
3F 68 93 17 84 9F 04 69 DF D5 F6 8A D7 44 34 EB
9A CF 5F DB 3F F2 96 93 15 CC 27 79 B2 F9 43 A7
DF FC 04 A0 56 73 D2 F5 AF E8 FD 37 10 B3 D0 E8
12 A8 53 70 C4 C2 8D F9 C8 57 90 01 63 B2 9D DD
85 A5 13 A8 F1 3A 9D 4A 71 2A E8 0A 5A E7 CE 17
2C 44 49 60 2D 7B E0 5C 1E BE BB 61 D9 C7 CE 36
1C EB 77 9C 3F 80 E3 CF FF 4F AA 0E C3 2E 5C 4A
E9 4A 92 07 44 04 6F D7 77 35 6F 00 59 F7 A1 F1
A8 F3 8A 65 23 AA 4F 30 D4 5A 84 29 BF F9 99 A3
43 0F 60 F3 4A 97 43 86 4B 35 8A 9A A9 90 A2 EF
71 06 1C 11 B3 DB AC 58 E2 7C 94 80 9A A3 F4 3F
            BC 61 8A 71 57 EA 89 08
```

(Skip rounds 1 to 22)

Round #23

After theta

```
9F 9A 64 FF 91 6E D1 4E E0 09 19 1C 08 53 23 C9
05 F4 79 31 88 3D 47 ED B5 81 93 66 7C C3 CF F6
45 26 41 E5 63 41 BD 53 1A 1A 50 2B 22 D9 A9 34
5B E2 45 6C EF E9 02 8F 1E 94 C0 52 DF 97 85 ED
EC 5B BD DA 1F 0D 85 A9 07 E5 AF C8 B4 A0 65 9E
6D 68 DA 16 B7 76 85 2F FC CA A1 CF 21 76 A4 0A
CA 7B 74 0E 76 37 DD FE 30 67 35 85 78 58 DE 68
EF D6 98 47 0F 55 CB 85 1F 7A 33 E4 23 D9 21 29
8C 6D 66 BE 7D 07 0C 53 7B 76 B5 AC 0B F3 38 C8
1F 59 C5 71 43 C7 4C 2C E9 38 BC C0 33 C9 D2 68
9B 2D 28 8A 7F A4 9E 29 48 33 F4 1B 54 72 A7 68
0C 74 FD 1D E0 08 07 7A E2 F1 31 E9 B6 66 D2 9E
            2E 9B 2C D8 E5 5E 5F 53
```

After rho

```
9F 9A 64 FF 91 6E D1 4E C1 13 32 38 10 A6 46 92
01 7D 5E 0C 62 CF 51 7B 37 FC 6C 5F 1B 38 69 C6
0B EA 9D 2A 32 09 2A 1F 22 92 9D 4A A3 A1 01 B5
C4 F6 9E 2E F0 B8 25 5E BB 07 25 B0 D4 F7 65 61
AD 5E ED 8F 86 C2 54 F6 5A E6 79 50 FE 8A 4C 0B
69 43 D3 B6 B8 B5 2B 7C 2A F0 2B 87 3E 87 D8 91
73 B0 BB E9 F6 57 DE A3 B0 BC D1 60 CE 6A 0A F1
A3 87 AA E5 C2 77 6B CC C8 47 B2 43 52 3E F4 66
CC B7 EF 80 61 8A B1 CD 1C E4 3D BB 5A D6 85 79
98 89 E5 23 AB 38 6E E8 68 E9 38 BC C0 33 C9 D2
7A A6 6C B6 A0 28 FE 91 21 CD D0 6F 50 C9 9D A2
81 AE BF 03 1C E1 40 8F F1 31 E9 B6 66 D2 9E E2
            D7 94 CB 26 0B 76 B9 D7
```

After pi

```
9F 9A 64 FF 91 6E D1 4E C4 F6 9E 2E F0 B8 25 5E
73 B0 BB E9 F6 57 DE A3 98 89 E5 23 AB 38 6E E8
D7 94 CB 26 0B 76 B9 D7 37 FC 6C 5F 1B 38 69 C6
5A E6 79 50 FE 8A 4C 0B 69 43 D3 B6 B8 B5 2B 7C
CC B7 EF 80 61 8A B1 CD 81 AE BF 03 1C E1 40 8F
C1 13 32 38 10 A6 46 92 BB 07 25 B0 D4 F7 65 61
B0 BC D1 60 CE 6A 0A F1 68 E9 38 BC C0 33 C9 D2
7A A6 6C B6 A0 28 FE 91 0B EA 9D 2A 32 09 2A 1F
22 92 9D 4A A3 A1 01 B5 2A F0 2B 87 3E 87 D8 91
1C E4 3D BB 5A D6 85 79 F1 31 E9 B6 66 D2 9E E2
01 7D 5E 0C 62 CF 51 7B AD 5E ED 8F 86 C2 54 F6
A3 87 AA E5 C2 77 6B CC C8 47 B2 43 52 3E F4 66
            21 CD D0 6F 50 C9 9D A2
```

After chi

```
AC 9A 45 3E 97 29 0B EF 4C FF DA 2C F9 90 05 16
34 A4 B1 ED F6 11 4F B4 90 83 C1 FA 3B 30 2E E0
97 F0 51 26 6B E6 9D C7 16 FD EE F9 1B 0D 4A B2
DE 52 55 50 BF 80 DC 8A 68 4B C3 B5 A4 D4 6B 7E
FA E7 AF DC 62 92 98 8D C9 AC AE 03 F8 63 44 86
C1 AB E2 78 1A AE 4C 02 F3 46 0D 2C D4 E6 A4 63
A2 BA 95 62 EE 62 3C F0 E9 F8 2A B4 D0 B5 C9 D0
40 A2 69 36 64 79 DF F0 03 8A BF AF 2E 0F F2 1F
36 96 89 72 E3 F1 04 DD CB E1 EB 83 1A 87 C2 13
16 2E 29 B3 4A DF A5 64 D1 21 E9 F6 E7 72 9F 42
03 FC 5C 6C 22 FA 7A 73 E5 1E FD 8D 96 CA C0 D4
82 0F EA C9 C2 B6 62 4C C8 77 BC 43 70 38 B4 3F
            8D CF 71 EC D4 C9 99 26
```

After iota

```
A4 1A 45 BE 97 29 0B 6F 4C FF DA 2C F9 90 05 16
34 A4 B1 ED F6 11 4F B4 90 83 C1 FA 3B 30 2E E0
97 F0 51 26 6B E6 9D C7 16 FD EE F9 1B 0D 4A B2
DE 52 55 50 BF 80 DC 8A 68 4B C3 B5 A4 D4 6B 7E
FA E7 AF DC 62 92 98 8D C9 AC AE 03 F8 63 44 86
C1 AB E2 78 1A AE 4C 02 F3 46 0D 2C D4 E6 A4 63
A2 BA 95 62 EE 62 3C F0 E9 F8 2A B4 D0 B5 C9 D0
40 A2 69 36 64 79 DF F0 03 8A BF AF 2E 0F F2 1F
36 96 89 72 E3 F1 04 DD CB E1 EB 83 1A 87 C2 13
16 2E 29 B3 4A DF A5 64 D1 21 E9 F6 E7 72 9F 42
03 FC 5C 6C 22 FA 7A 73 E5 1E FD 8D 96 CA C0 D4
82 0F EA C9 C2 B6 62 4C C8 77 BC 43 70 38 B4 3F
            8D CF 71 EC D4 C9 99 26
```

After permutation

```
A4 1A 45 BE 97 29 0B 6F 4C FF DA 2C F9 90 05 16
34 A4 B1 ED F6 11 4F B4 90 83 C1 FA 3B 30 2E E0
97 F0 51 26 6B E6 9D C7 16 FD EE F9 1B 0D 4A B2
DE 52 55 50 BF 80 DC 8A 68 4B C3 B5 A4 D4 6B 7E
FA E7 AF DC 62 92 98 8D C9 AC AE 03 F8 63 44 86
C1 AB E2 78 1A AE 4C 02 F3 46 0D 2C D4 E6 A4 63
A2 BA 95 62 EE 62 3C F0 E9 F8 2A B4 D0 B5 C9 D0
40 A2 69 36 64 79 DF F0 03 8A BF AF 2E 0F F2 1F
36 96 89 72 E3 F1 04 DD CB E1 EB 83 1A 87 C2 13
16 2E 29 B3 4A DF A5 64 D1 21 E9 F6 E7 72 9F 42
03 FC 5C 6C 22 FA 7A 73 E5 1E FD 8D 96 CA C0 D4
82 0F EA C9 C2 B6 62 4C C8 77 BC 43 70 38 B4 3F
           8D CF 71 EC D4 C9 99 26
```

State (as lanes of integers)

```
[0, 0] = 6f0b2997be451aa4
[1, 0] = 160590f92cdaff4c
[2, 0] = b44f11f6edb1a434
[3, 0] = e02e303bfac18390
[4, 0] = c79de66b2651f097
[0, 1] = b24a0d1bf9eefd16
[1, 1] = 8adc80bf505552de
[2, 1] = 7e6bd4a4b5c34b68
[3, 1] = 8d989262dcafe7fa
[4, 1] = 864463f803aeacc9
[0, 2] = 024cae1a78e2abc1
[1, 2] = 63a4e6d42c0d46f3
[2, 2] = f03c62ee6295baa2
[3, 2] = d0c9b5d0b42af8e9
[4, 2] = f0df79643669a240
[0, 3] = 1ff20f2eafbf8a03
[1, 3] = dd04f1e372899636
[2, 3] = 13c2871a83ebe1cb
[3, 3] = 64a5df4ab3292e16
[4, 3] = 429f72e7f6e921d1
[0, 4] = 737afa226c5cfc03
[1, 4] = d4c0ca968dfd1ee5
[2, 4] = 4c62b6c2c9ea0f82
[3, 4] = 3fb4387043bc77c8
[4, 4] = 2699c9d4ec71cf8d
```

The hash value is

```
7F 9C 2B A4 E8 8F 82 7D 61 60 45 50 76 05 85 3E
D7 3B 80 93 F6 EF BC 88 EB 1A 6E AC FA 66 EF 26
3C B1 EE A9 88 00 4B 93 10 3C FB 0A EE FD 2A 68
6E 01 FA 4A 58 E8 A3 63 9C A8 A1 E3 F9 AE 57 E2
35 B8 CC 87 3C 23 DC 62 B8 D2 60 16 9A FA 2F 75
AB 91 6A 58 D9 74 91 88 35 D2 5E 6A 43 50 85 B2
BA DF D6 DF AA C3 59 A5 EF BB 7B CC 4B 59 D5 38
DF 9A 04 30 2E 10 C8 BC 1C BF 1A 0B 3A 51 20 EA
17 CD A7 CF AD 76 5F 56 23 47 4D 36 8C CC A8 AF
00 07 CD 9F 5E 4C 84 9F 16 7A 58 0B 14 AA BD EF
AE E7 EE F4 7C B0 FC A9 76 7B E1 FD A6 94 19 DF
B9 27 E9 DF 07 34 8B 19 66 91 AB AE B5 80 B3 2D
EF 58 53 8B 8D 23 F8 77 32 EA 63 B0 2B 4F A0 F4
87 33 60 E2 84 19 28 CD 60 DD 4C EE 8C C0 D4 C9
22 A9 61 88 D0 32 67 5C 8A C8 50 93 3C 7A FF 15
33 B9 4C 83 4A DB B6 9C 61 15 BA D4 69 2D 86 19
F9 0B 0C DF 8A 7B 9C 26 40 29 AC 18 5B 70 B8 3F
28 01 F2 F4 B3 F7 0C 59 3E A3 AE EB 61 3A 7F 1B
1D E3 3F D7 50 81 F5 92 30 5F 2E 45 26 ED C0 96
```

```
31 B1 09 58 F4 64 D8 89 F3 1B A0 10 25 0F DA 7F
13 68 EC 29 67 FC 84 EF 2A E9 AF F2 68 E0 B1 70
0A FF C6 82 0B 52 3A 3D 91 71 35 F2 DF F2 EE 06
BF E7 2B 31 24 72 1D 4A 26 C0 4E 53 A7 5E 30 E7
3A 7A 9C 4A 95 D9 1C 55 D4 95 E9 F5 1D D0 B5 E9
D8 3C 6D 5E 8C E8 03 AA 62 B8 D6 54 DB 53 D0 9B
8D CF F2 73 CD FE B5 73 FA D8 BC D4 55 78 BE C2
E7 70 D0 1E FD E8 6E 72 1A 3F 7C 6C CE 27 5D AB
E6 E2 14 3F 1A F1 8D A7 EF DD C4 C7 B7 0B 5E 34
5D B9 3C C9 36 BE A3 23 49 1C CB 38 A3 88 F5 46
A9 FF 00 DD 4E 13 00 B9 B2 15 3D 20 41 D2 05 B4
43 E4 1B 45 A6 53 F2 A5 C4 49 2C 1A DD 54 45 12
DD A2 52 98 33 46 2B 71 A4 1A 45 BE 97 29 0B 6F
```

SHAKE-128 sample to produce 4096-bits of output

The message as a bit string

```
1 1 0 0 1
```

About to call last of the absorb phase

XORed state (in bytes)

```
F3 03 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 80 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
            00 00 00 00 00 00 00 00
```

XORed state (as lanes of integers)

```
[0, 0] = 00000000000003f3
[1, 0] = 0000000000000000
[2, 0] = 0000000000000000
[3, 0] = 0000000000000000
[4, 0] = 0000000000000000
[0, 1] = 0000000000000000
[1, 1] = 0000000000000000
[2, 1] = 0000000000000000
[3, 1] = 0000000000000000
[4, 1] = 0000000000000000
[0, 2] = 0000000000000000
[1, 2] = 0000000000000000
[2, 2] = 0000000000000000
[3, 2] = 0000000000000000
[4, 2] = 0000000000000000
[0, 3] = 0000000000000000
[1, 3] = 0000000000000000
[2, 3] = 0000000000000000
[3, 3] = 0000000000000000
[4, 3] = 0000000000000000
[0, 4] = 8000000000000000
[1, 4] = 0000000000000000
[2, 4] = 0000000000000000
[3, 4] = 0000000000000000
[4, 4] = 0000000000000000
```

Round #0

After theta

```
F3 03 00 00 00 00 00 00 F3 03 00 00 00 00 00 80
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
E7 07 00 00 00 00 00 00 00 00 00 00 00 00 00 00
F3 03 00 00 00 00 00 80 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 E7 07 00 00 00 00 00 00
00 00 00 00 00 00 00 00 F3 03 00 00 00 00 00 80
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
E7 07 00 00 00 00 00 00 00 00 00 00 00 00 00 00
F3 03 00 00 00 00 00 80 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 E7 07 00 00 00 00 00 00
00 00 00 00 00 00 00 80 F3 03 00 00 00 00 00 80
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
            E7 07 00 00 00 00 00 00
```

After rho

```
F3 03 00 00 00 00 00 00 E7 07 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 38 3F 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 38 3F 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 70 7E 00 00 00 00
00 00 00 00 00 00 00 00 00 CE 0F 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 80 F3 03 00 00 00 00 00 00 00 00 00
00 00 00 00 00 70 7E 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 E7 07 00 00 00 00 00
00 00 02 00 00 00 00 00 CE 0F 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
            00 C0 F9 01 00 00 00 00
```

After pi

```
F3 03 00 00 00 00 00 00 00 00 00 00 00 38 3F 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 C0 F9 01 00 00 00 00 00 00 00 00 00 00 00 00
00 00 70 7E 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 70 7E 00 00 00 00 00 00 00 00 00
E7 07 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 E7 07 00 00 00 00 00
00 00 02 00 00 00 00 00 00 00 00 38 3F 00 00 00
00 00 00 00 00 00 00 00 00 CE 0F 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 80 F3 03 00 00 00 00 00 00 00 00 00
            CE 0F 00 00 00 00 00 00
```

After chi

```
F3 03 00 00 00 00 00 00 00 00 00 00 00 38 3F 00
00 C0 F9 01 00 00 00 00 F3 03 00 00 00 00 00 00
00 C0 F9 01 00 38 3F 00 00 00 00 00 00 00 00 00
00 00 70 7E 00 70 7E 00 00 00 00 00 00 00 00 00
00 00 00 00 00 70 7E 00 00 00 70 7E 00 00 00 00
E7 07 00 00 00 00 00 00 00 E7 07 00 00 00 00 00
00 00 00 00 00 00 00 00 E7 E0 07 00 00 00 00 00
00 00 02 00 00 00 00 00 00 CE 0F 38 3F 00 00 00
00 00 00 00 00 00 00 00 00 CE 0F 00 00 00 00 00
00 00 00 38 3F 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 80 F3 03 00 00 00 00 00 00 00 00 00
CE 0F 00 00 80 F3 03 00 00 00 00 00 00 00 00 00
            CE 0F 00 00 00 00 00 00
```

After iota

```
F2 03 00 00 00 00 00 00 00 00 00 00 38 3F 00
00 C0 F9 01 00 00 00 00 F3 03 00 00 00 00 00
00 C0 F9 01 00 38 3F 00 00 00 00 00 00 00 00
00 00 70 7E 00 70 7E 00 00 00 00 00 00 00 00
00 00 00 00 00 70 7E 00 00 00 70 7E 00 00 00
E7 07 00 00 00 00 00 00 00 E7 07 00 00 00 00
00 00 00 00 00 00 00 00 E7 E0 07 00 00 00 00
00 00 02 00 00 00 00 00 00 CE 0F 38 3F 00 00
00 00 00 00 00 00 00 00 00 CE 0F 00 00 00 00
00 00 00 38 3F 00 00 00 00 00 00 00 00 00 00
00 00 00 00 80 F3 03 00 00 00 00 00 00 00 00
CE 0F 00 00 80 F3 03 00 00 00 00 00 00 00 00
            CE 0F 00 00 00 00 00 00
```

(Skip rounds 1 to 22)

Round #23

After theta

```
22 B2 35 3A 97 67 32 8B 25 D8 47 EF FF E1 E6 1F
61 F2 2A F1 55 B6 A2 61 5B EF 58 FA 3C E5 7D 06
04 B6 51 87 0C 89 F8 9A 51 47 E1 4F 69 AA F7 A9
F6 DB BB 5C 44 76 AF 6E F8 D0 7A 6E 83 5C B3 AD
7F 82 9C 4E D6 60 8F FD 3E B1 1B B7 C6 E1 78 5D
FD 45 12 71 C0 DF EF 29 F8 7E F7 D2 F7 BA 4C BB
1C BD F7 09 4F F5 CA 6F 9E 65 00 E6 EB FD 11 00
23 C4 D2 83 D4 7C B0 C8 CA 4C 6C B0 A1 4A 79 B2
AA ED 13 4D 1B 0D CA 7B 81 78 5E 33 F7 B0 9C 7B
56 58 FF 75 56 B6 FB 5E 27 F1 CC F8 DD DC C2 EE
32 76 AE 9C D8 F8 7C BB D9 69 77 20 8C AF 2A 66
DB 44 C6 BF 3D 51 A1 79 9F 88 9C 53 5B 0C D7 A6
            64 74 A5 78 C0 BF DF AF
```

After rho

```
22 B2 35 3A 97 67 32 8B 4A B0 8F DE FF C3 CD 3F
98 BC 4A 7C 95 AD 68 58 53 DE 67 B0 F5 8E A5 CF
48 C4 D7 24 B0 8D 3A 64 94 A6 7A 9F 1A 75 14 FE
CB 45 64 F7 EA 66 BF BD 2B 3E B4 9E DB 20 D7 6C
41 4E 27 6B B0 C7 FE 3F 8E D7 E5 13 BB 71 6B 1C
E9 2F 92 88 03 FE 7E 4F ED E2 FB DD 4B DF EB 32
4F 78 AA 57 7E E3 E8 BD FB 23 00 3C CB 00 CC D7
41 6A 3E 58 E4 11 62 E9 60 43 95 F2 64 95 99 D8
A2 69 A3 41 79 4F B5 7D CE BD 40 3C AF 99 7B 58
76 DF CB 0A EB BF CE CA EE 27 F1 CC F8 DD DC C2
F3 ED CA D8 B9 72 62 E3 65 A7 DD 81 30 BE AA 98
9B C8 F8 B7 27 2A 34 6F 88 9C 53 5B 0C D7 A6 9F
            F7 2B 19 5D 29 1E F0 EF
```

After pi

```
22 B2 35 3A 97 67 32 8B CB 45 64 F7 EA 66 BF BD
4F 78 AA 57 7E E3 E8 BD 76 DF CB 0A EB BF CE CA
F7 2B 19 5D 29 1E F0 EF 53 DE 67 B0 F5 8E A5 CF
8E D7 E5 13 BB 71 6B 1C E9 2F 92 88 03 FE 7E 4F
A2 69 A3 41 79 4F B5 7D 9B C8 F8 B7 27 2A 34 6F
4A B0 8F DE FF C3 CD 3F 2B 3E  B4 9E DB 20 D7 6C
FB 23 00 3C CB 00 CC D7 EE 27 F1 CC F8 DD DC C2
F3 ED CA D8 B9 72 62 E3 48 C4 D7 24 B0 8D 3A 64
94 A6 7A 9F 1A 75 14 FE ED E2 FB DD 4B DF EB 32
CE BD 40 3C AF 99 7B 58 88 9C 53 5B 0C D7 A6 9F
98 BC 4A 7C 95 AD 68 58 41 4E 27 6B B0 C7 FE 3F
41 6A 3E 58 E4 11 62 E9 60 43 95 F2 64 95 99 D8
            65 A7 DD 81 30 BE AA 98
```

After chi

```
26 8A BF 3A 83 E6 72 8B FB C2 25 FF 6B 7A B9 FF
CE 58 BA 02 7E E3 D8 98 76 4F EF 28 7D DE CC CA
3E 6E 59 98 41 1E 7D DB 32 F6 75 38 F5 00 B1 8C
8C 97 C4 52 C3 70 EA 2C F0 AF CA 3E 05 DE 7E 4D
E2 7F A4 41 A9 CB 34 FD 17 C9 78 B4 2D 5B 7E 7F
9A B1 8F FE FF C3 C5 AC 2F 3A 45 5E EB FD C7 6C
EA EB 0A 2C CA 22 EE F6 E6 37 F4 CA BE 5C 51 DE
D2 E3 FA D8 B9 52 70 A3 21 84 56 64 F1 07 D1 64
96 BB 7A BF BE 75 04 B6 ED E2 E8 9E 4B 99 6F B5
8E FD C4 18 1F 91 63 38 1C BE 7B C0 06 A7 A2 05
98 9C 52 6C D1 BD 68 98 61 4F A6 C9 B0 43 67 2F
44 CE 76 59 F4 3B 40 E9 F8 5B 97 8E E1 94 D9 98
            24 E5 F8 82 10 FC 3C BF
```

After iota

```
2E 0A BF BA 83 E6 72 0B FB C2 25 FF 6B 7A B9 FF
CE 58 BA 02 7E E3 D8 98 76 4F EF 28 7D DE CC CA
3E 6E 59 98 41 1E 7D DB 32 F6 75 38 F5 00 B1 8C
8C 97 C4 52 C3 70 EA 2C F0 AF CA 3E 05 DE 7E 4D
E2 7F A4 41 A9 CB 34 FD 17 C9 78 B4 2D 5B 7E 7F
9A B1 8F FE FF C3 C5 AC 2F 3A 45 5E EB FD C7 6C
EA EB 0A 2C CA 22 EE F6 E6 37 F4 CA BE 5C 51 DE
D2 E3 FA D8 B9 52 70 A3 21 84 56 64 F1 07 D1 64
96 BB 7A BF BE 75 04 B6 ED E2 E8 9E 4B 99 6F B5
8E FD C4 18 1F 91 63 38 1C BE 7B C0 06 A7 A2 05
98 9C 52 6C D1 BD 68 98 61 4F A6 C9 B0 43 67 2F
44 CE 76 59 F4 3B 40 E9 F8 5B 97 8E E1 94 D9 98
            24 E5 F8 82 10 FC 3C BF
```

After permutation

```
2E 0A BF BA 83 E6 72 0B FB C2 25 FF 6B 7A B9 FF
CE 58 BA 02 7E E3 D8 98 76 4F EF 28 7D DE CC CA
3E 6E 59 98 41 1E 7D DB 32 F6 75 38 F5 00 B1 8C
8C 97 C4 52 C3 70 EA 2C F0 AF CA 3E 05 DE 7E 4D
E2 7F A4 41 A9 CB 34 FD 17 C9 78 B4 2D 5B 7E 7F
9A B1 8F FE FF C3 C5 AC 2F 3A 45 5E EB FD C7 6C
EA EB 0A 2C CA 22 EE F6 E6 37 F4 CA BE 5C 51 DE
D2 E3 FA D8 B9 52 70 A3 21 84 56 64 F1 07 D1 64
96 BB 7A BF BE 75 04 B6 ED E2 E8 9E 4B 99 6F B5
8E FD C4 18 1F 91 63 38 1C BE 7B C0 06 A7 A2 05
98 9C 52 6C D1 BD 68 98 61 4F A6 C9 B0 43 67 2F
44 CE 76 59 F4 3B 40 E9 F8 5B 97 8E E1 94 D9 98
            24 E5 F8 82 10 FC 3C BF
```

State (as lanes of integers)

```
[0, 0] = 0b72e683babf0a2e
[1, 0] = ffb97a6bff25c2fb
[2, 0] = 98d8e37e02ba58ce
[3, 0] = caccde7d28ef4f76
[4, 0] = db7d1e4198596e3e
[0, 1] = 8cb100f53875f632
[1, 1] = 2cea70c352c4978c
[2, 1] = 4d7ede053ecaaff0
[3, 1] = fd34cba941a47fe2
[4, 1] = 7f7e5b2db478c917
[0, 2] = acc5c3fffe8fb19a
[1, 2] = 6cc7fdeb5e453a2f
[2, 2] = f6ee22ca2c0aebea
[3, 2] = de515cbecaf437e6
[4, 2] = a37052b9d8fae3d2
[0, 3] = 64d107f164568421
```

```
[1, 3] = b60475bebf7abb96
[2, 3] = b56f994b9ee8e2ed
[3, 3] = 3863911f18c4fd8e
[4, 3] = 05a2a706c07bbe1c
[0, 4] = 9868bdd16c529c98
[1, 4] = 2f6743b0c9a64f61
[2, 4] = e9403bf45976ce44
[3, 4] = 98d994e18e975bf8
[4, 4] = bf3cfc1082f8e524
```

About to call squeeze (again)

State before permutation (in bytes)

```
2E 0A BF BA 83 E6 72 0B FB C2 25 FF 6B 7A B9 FF
CE 58 BA 02 7E E3 D8 98 76 4F EF 28 7D DE CC CA
3E 6E 59 98 41 1E 7D DB 32 F6 75 38 F5 00 B1 8C
8C 97 C4 52 C3 70 EA 2C F0 AF CA 3E 05 DE 7E 4D
E2 7F A4 41 A9 CB 34 FD 17 C9 78 B4 2D 5B 7E 7F
9A B1 8F FE FF C3 C5 AC 2F 3A 45 5E EB FD C7 6C
EA EB 0A 2C CA 22 EE F6 E6 37 F4 CA BE 5C 51 DE
D2 E3 FA D8 B9 52 70 A3 21 84 56 64 F1 07 D1 64
96 BB 7A BF BE 75 04 B6 ED E2 E8 9E 4B 99 6F B5
8E FD C4 18 1F 91 63 38 1C BE 7B C0 06 A7 A2 05
98 9C 52 6C D1 BD 68 98 61 4F A6 C9 B0 43 67 2F
44 CE 76 59 F4 3B 40 E9 F8 5B 97 8E E1 94 D9 98
           24 E5 F8 82 10 FC 3C BF
```

State before permutation (as lanes of integers)

```
[0, 0] = 0b72e683babf0a2e
[1, 0] = ffb97a6bff25c2fb
[2, 0] = 98d8e37e02ba58ce
[3, 0] = caccde7d28ef4f76
[4, 0] = db7d1e4198596e3e
[0, 1] = 8cb100f53875f632
[1, 1] = 2cea70c352c4978c
[2, 1] = 4d7ede053ecaaff0
[3, 1] = fd34cba941a47fe2
[4, 1] = 7f7e5b2db478c917
[0, 2] = acc5c3fffe8fb19a
[1, 2] = 6cc7fdeb5e453a2f
[2, 2] = f6ee22ca2c0aebea
[3, 2] = de515cbecaf437e6
[4, 2] = a37052b9d8fae3d2
[0, 3] = 64d107f164568421
[1, 3] = b60475bebf7abb96
[2, 3] = b56f994b9ee8e2ed
[3, 3] = 3863911f18c4fd8e
[4, 3] = 05a2a706c07bbe1c
[0, 4] = 9868bdd16c529c98
[1, 4] = 2f6743b0c9a64f61
[2, 4] = e9403bf45976ce44
[3, 4] = 98d994e18e975bf8
[4, 4] = bf3cfc1082f8e524
```

Round #0

After theta

```
B3 22 16 06 DB 28 70 FB 3E F7 AC 24 DF 9F C9 D6
69 81 1B EC 1B BB 09 2C 8C 40 BB 93 F4 FA 71 CE
45 65 37 45 87 6D 11 3D AF DE DC 84 AD CE B3 7C
49 A2 4D 89 77 95 9A 05 57 76 6B D0 60 86 AF F9
18 70 F0 FA 20 EF 89 F9 6C C2 16 69 EB 28 12 99
```

```
07 99 26 42 A7 0D C7 5C EA 0F CC 85 5F 18 B7 45
4D 32 AB C2 AF 7A 3F 42 1C 38 A0 71 37 78 EC DA
A9 E8 94 05 7F 21 1C 45 BC AC FF D8 A9 C9 D3 94
53 8E F3 64 0A 90 74 9F 4A 3B 49 70 2E C1 BE 01
74 F2 90 A3 96 B5 DE 3C 67 B5 15 1D C0 D4 CE E3
05 B4 FB D0 89 73 6A 68 A4 7A 2F 12 04 A6 17 06
E3 17 D7 B7 91 63 91 5D 02 54 C3 35 68 B0 64 9C
            5F EE 96 5F D6 8F 50 59
```

After rho

```
B3 22 16 06 DB 28 70 FB 7D EE 59 49 BE 3F 93 AD
5A E0 06 FB C6 6E 02 4B AF 1F E7 CC 08 B4 3B 49
6C 8B E8 29 2A BB 29 3A D8 EA 3C CB F7 EA CD 4D
94 78 57 A9 59 90 24 DA FE 95 DD 1A 34 98 E1 6B
38 78 7D 90 F7 C4 7C 0C 22 91 C9 26 6C 91 B6 8E
3A C8 34 11 3A 6D 38 E6 16 A9 3F 30 17 7E 61 DC
15 7E D5 FB 11 6A 92 59 F0 D8 B5 39 70 40 E3 6E
82 BF 10 8E A2 54 74 CA B1 53 93 A7 29 79 59 FF
9E 4C 01 92 EE 73 CA 71 DF 00 A5 9D 24 38 97 60
D6 9B 87 4E 1E 72 D4 B2 E3 67 B5 15 1D C0 D4 CE
A9 A1 15 D0 EE 43 27 CE 90 EA BD 48 10 98 5E 18
FC E2 FA 36 72 2C B2 6B 54 C3 35 68 B0 64 9C 02
            54 D6 97 BB E5 97 F5 23
```

After pi

```
B3 22 16 06 DB 28 70 FB 94 78 57 A9 59 90 24 DA
15 7E D5 FB 11 6A 92 59 D6 9B 87 4E 1E 72 D4 B2
54 D6 97 BB E5 97 F5 23 AF 1F E7 CC 08 B4 3B 49
22 91 C9 26 6C 91 B6 8E 3A C8 34 11 3A 6D 38 E6
9E 4C 01 92 EE 73 CA 71 FC E2 FA 36 72 2C B2 6B
7D EE 59 49 BE 3F 93 AD FE 95 DD 1A 34 98 E1 6B
F0 D8 B5 39 70 40 E3 6E E3 67 B5 15 1D C0 D4 CE
A9 A1 15 D0 EE 43 27 CE 6C 8B E8 29 2A BB 29 3A
D8 EA 3C CB F7 EA CD 4D 16 A9 3F 30 17 7E 61 DC
DF 00 A5 9D 24 38 97 60 54 C3 35 68 B0 64 9C 02
5A E0 06 FB C6 6E 02 4B 38 78 7D 90 F7 C4 7C 0C
82 BF 10 8E A2 54 74 CA B1 53 93 A7 29 79 59 FF
            90 EA BD 48 10 98 5E 18
```

After chi

```
B2 24 96 54 DB 42 E2 FA 56 F9 55 AD 57 80 60 78
15 3A C5 4A F0 EF B3 58 75 BB 87 4A 04 5A D4 6A
50 8E D6 12 E5 07 F1 23 B7 57 D3 DD 1A D8 33 29
A6 95 C8 A4 A8 83 74 9F 5A 6A CE 35 2A 61 08 EC
9D 51 04 5A E6 E3 C3 71 FC 62 F2 14 16 2D 36 ED
7D A6 79 68 FE 7F 91 A9 FD B2 DD 1E 39 18 F5 EB
F8 58 B5 F9 92 43 C0 6E B7 29 FD 1C 0D FC 44 EF
2B B0 91 C2 EE C3 47 8C 6A 8A EB 19 2A AF 09 AA
11 EA BC 46 D7 EA 5B 6D 16 6A 2F 50 87 3A 69 DE
F7 08 6D 9C 2E A3 B6 58 C4 A3 21 AA 65 24 58 47
D8 67 06 F5 C6 7E 02 89 09 38 FE B1 FE ED 75 39
82 17 3C C6 B2 D4 72 CA FB 53 91 14 EF 1F 59 BC
            B0 F2 C4 48 21 18 22 1C
```

After iota

```
B3 24 96 54 DB 42 E2 FA 56 F9 55 AD 57 80 60 78
15 3A C5 4A F0 EF B3 58 75 BB 87 4A 04 5A D4 6A
50 8E D6 12 E5 07 F1 23 B7 57 D3 DD 1A D8 33 29
A6 95 C8 A4 A8 83 74 9F 5A 6A CE 35 2A 61 08 EC
9D 51 04 5A E6 E3 C3 71 FC 62 F2 14 16 2D 36 ED
7D A6 79 68 FE 7F 91 A9 FD B2 DD 1E 39 18 F5 EB
F8 58 B5 F9 92 43 C0 6E B7 29 FD 1C 0D FC 44 EF
2B B0 91 C2 EE C3 47 8C 6A 8A EB 19 2A AF 09 AA
11 EA BC 46 D7 EA 5B 6D 16 6A 2F 50 87 3A 69 DE
```

```
F7 08 6D 9C 2E A3 B6 58 C4 A3 21 AA 65 24 58 47
D8 67 06 F5 C6 7E 02 89 09 38 FE B1 FE ED 75 39
82 17 3C C6 B2 D4 72 CA FB 53 91 14 EF 1F 59 BC
            B0 F2 C4 48 21 18 22 1C
```

(Skip rounds 1 to 22)

Round #23

After theta

```
32 27 94 3E 45 37 CA 13 65 63 DD ED B3 8D FD BD
95 B5 6A DE 6F F2 64 5A 62 74 F1 03 67 37 B9 09
38 35 14 BD CB 14 70 24 AC 55 AB E9 DC CE 46 82
5F 20 1D 30 D8 49 FD B6 04 31 0D 87 63 9F D0 CF
FB 8C 9C 0A 10 AC 91 3E DD D8 C3 B6 1E F3 E0 02
23 26 E6 37 3A 22 35 F1 0C 4D 27 AD 49 12 B4 3A
76 3C AE A1 36 64 58 55 9A 7F 45 47 56 35 EA EB
E8 57 49 8B C0 A4 28 8A A5 79 4F ED AB 43 0C E6
95 DD 91 E4 86 6C 11 33 35 FE 10 3B 10 AA AA AD
02 31 FE A2 18 27 9A 93 97 CA E2 AE 00 92 46 78
FC A9 E2 65 1A 29 81 DD 02 98 AB A1 CB DB 32 AC
BA 3E 81 B4 91 1F 07 D1 9F EB E7 1D F5 9A 44 B3
            47 FC 16 65 EC 11 97 45
```

After rho

```
32 27 94 3E 45 37 CA 13 CB C6 BA DB 67 1B FB 7B
65 AD 9A F7 9B 3C 99 56 76 93 9B 20 46 17 3F 70
A6 80 23 C1 A9 A1 E8 5D CE ED 6C 24 C8 5A B5 9A
01 83 9D D4 6F FB 05 D2 33 41 4C C3 E1 D8 27 F4
46 4E 05 08 D6 48 9F 7D 0F 2E D0 8D 3D 6C EB 31
1F 31 31 BF D1 11 A9 89 EA 30 34 9D B4 26 49 D0
0D B5 21 C3 AA B2 E3 71 6A D4 D7 35 FF 8A 8E AC
45 60 52 14 45 F4 AB A4 DA 57 87 18 CC 4B F3 9E
92 DC 90 2D 62 A6 B2 3B D5 D6 1A 7F 88 1D 08 55
44 73 52 20 C6 5F 14 E3 78 97 CA E2 AE 00 92 46
04 76 F3 A7 8A 97 69 A4 0A 60 AE 86 2E 6F CB B0
D7 27 90 36 F2 E3 20 5A EB E7 1D F5 9A 44 B3 9F
            65 D1 11 BF 45 19 7B C4
```

After pi

```
32 27 94 3E 45 37 CA 13 01 83 9D D4 6F FB 05 D2
0D B5 21 C3 AA B2 E3 71 44 73 52 20 C6 5F 14 E3
65 D1 11 BF 45 19 7B C4 76 93 9B 20 46 17 3F 70
0F 2E D0 8D 3D 6C EB 31 1F 31 31 BF D1 11 A9 89
92 DC 90 2D 62 A6 B2 3B D7 27 90 36 F2 E3 20 5A
CB C6 BA DB 67 1B FB 7B 33 41 4C C3 E1 D8 27 F4
6A D4 D7 35 FF 8A 8E AC 78 97 CA E2 AE 00 92 46
04 76 F3 A7 8A 97 69 A4 A6 80 23 C1 A9 A1 E8 5D
CE ED 6C 24 C8 5A B5 9A EA 30 34 9D B4 26 49 D0
D5 D6 1A 7F 88 1D 08 55 EB E7 1D F5 9A 44 B3 9F
65 AD 9A F7 9B 3C 99 56 46 4E 05 08 D6 48 9F 7D
45 60 52 14 45 F4 AB A4 DA 57 87 18 CC 4B F3 9E
            0A 60 AE 86 2E 6F CB B0
```

After chi

```
3E 13 B4 3D C5 37 28 32 41 C1 CF F4 2B B6 11 50
2C 35 20 5C AB B2 88 75 56 55 D6 20 C6 79 94 F0
64 51 18 7F 6F D1 7E 04 66 82 BA 12 86 06 3F F8
8F E2 50 8D 1F CA F9 03 5A 12 31 AD 41 50 A9 C9
B2 4C 9B 2D 66 B2 AD 1B DE 0B D0 BB CB 8B E0 5B
83 52 29 EF 79 19 73 73 23 42 44 01 E1 D8 37 B6
6E B4 E6 30 FF 1D E7 0C B3 17 C2 BA CB 08 00 1D
34 77 B7 A7 0A 57 6D 20 86 90 33 58 9D 85 A0 1D
DB 2B 66 46 C0 43 B5 9F C0 11 31 1D A6 66 FA 5A
```

```
D1 D6 38 7F A9 BC 40 15 A3 8A 51 D1 DA 1E A6 1D
64 8D C8 E3 9A 88 B9 D6 DC 59 80 00 5E 43 CF 67
45 40 7A 92 67 D0 A3 84 BF DA 97 69 5D 5B E3 D8
            08 22 AB 8E 6A 2F CD 99
```

After iota

```
36 93 B4 BD C5 37 28 B2 41 C1  CF F4 2B B6 11 50
2C 35 20 5C AB B2 88 75 56 55 D6 20 C6 79 94 F0
64 51 18 7F 6F D1 7E 04 66 82 BA 12 86 06 3F F8
8F E2 50 8D 1F CA F9 03 5A 12 31 AD 41 50 A9 C9
B2 4C 9B 2D 66 B2 AD 1B DE 0B D0 BB CB 8B E0 5B
83 52 29 EF 79 19 73 73 23 42 44 01 E1 D8 37 B6
6E B4 E6 30 FF 1D E7 0C B3 17 C2 BA CB 08 00 1D
34 77 B7 A7 0A 57 6D 20 86 90 33 58 9D 85 A0 1D
DB 2B 66 46 C0 43 B5 9F C0 11 31 1D A6 66 FA 5A
D1 D6 38 7F A9 BC 40 15 A3 8A 51 D1 DA 1E A6 1D
64 8D C8 E3 9A 88 B9 D6 DC 59 80 00 5E 43 CF 67
45 40 7A 92 67 D0 A3 84 BF DA 97 69 5D 5B E3 D8
            08 22 AB 8E 6A 2F CD 99
```

After permutation

```
36 93 B4 BD C5 37 28 B2 41 C1 CF F4 2B B6 11 50
2C 35 20 5C AB B2 88 75 56 55 D6 20 C6 79 94 F0
64 51 18 7F 6F D1 7E 04 66 82 BA 12 86 06 3F F8
8F E2 50 8D 1F CA F9 03 5A 12 31 AD 41 50 A9 C9
B2 4C 9B 2D 66 B2 AD 1B DE 0B D0 BB CB 8B E0 5B
83 52 29 EF 79 19 73 73 23 42 44 01 E1 D8 37 B6
6E B4 E6 30 FF 1D E7 0C B3 17 C2 BA CB 08 00 1D
34 77 B7 A7 0A 57 6D 20 86 90 33 58 9D 85 A0 1D
DB 2B 66 46 C0 43 B5 9F C0 11 31 1D A6 66 FA 5A
D1 D6 38 7F A9 BC 40 15 A3 8A 51 D1 DA 1E A6 1D
64 8D C8 E3 9A 88 B9 D6 DC 59 80 00 5E 43 CF 67
45 40 7A 92 67 D0 A3 84 BF DA 97 69 5D 5B E3 D8
            08 22 AB 8E 6A 2F CD 99
```

State (as lanes of integers)

```
[0, 0] = b22837c5bdb49336
[1, 0] = 5011b62bf4cfc141
[2, 0] = 7588b2ab5c20352c
[3, 0] = f09479c620d65556
[4, 0] = 047ed16f7f185164
[0, 1] = f83f068612ba8266
[1, 1] = 03f9ca1f8d50e28f
[2, 1] = c9a95041ad31125a
[3, 1] = 1badb2662d9b4cb2
[4, 1] = 5be08bcbbbd00bde
[0, 2] = 73731979ef295283
[1, 2] = b637d8e101444223
[2, 2] = 0ce71dff30e6b46e
[3, 2] = 1d0008cbbac217b3
[4, 2] = 206d570aa7b77734
[0, 3] = 1da0859d58339086
[1, 3] = 9fb543c046662bdb
[2, 3] = 5afa66a61d3111c0
[3, 3] = 1540bca97f38d6d1
[4, 3] = 1da61edad1518aa3
[0, 4] = d6b9889ae3c88d64
[1, 4] = 67cf435e008059dc
[2, 4] = 84a3d067927a4045
[3, 4] = d8e35b5d6997dabf
[4, 4] = 99cd2f6a8eab2208
```

About to call squeeze (again)

State before permutation (in bytes)

```
36 93 B4 BD C5 37 28 B2 41 C1 CF F4 2B B6 11 50
2C 35 20 5C AB B2 88 75 56 55 D6 20 C6 79 94 F0
64 51 18 7F 6F D1 7E 04 66 82 BA 12 86 06 3F F8
8F E2 50 8D 1F CA F9 03 5A 12 31 AD 41 50 A9 C9
B2 4C 9B 2D 66 B2 AD 1B DE 0B D0 BB CB 8B E0 5B
83 52 29 EF 79 19 73 73 23 42 44 01 E1 D8 37 B6
6E B4 E6 30 FF 1D E7 0C B3 17 C2 BA CB 08 00 1D
34 77 B7 A7 0A 57 6D 20 86 90 33 58 9D 85 A0 1D
DB 2B 66 46 C0 43 B5 9F C0 11 31 1D A6 66 FA 5A
D1 D6 38 7F A9 BC 40 15 A3 8A 51 D1 DA 1E A6 1D
64 8D C8 E3 9A 88 B9 D6 DC 59 80 00 5E 43 CF 67
45 40 7A 92 67 D0 A3 84 BF DA 97 69 5D 5B E3 D8
            08 22 AB 8E 6A 2F CD 99
```

XState before permutation (as lanes of integers)

```
[0, 0] = b22837c5bdb49336
[1, 0] = 5011b62bf4cfc141
[2, 0] = 7588b2ab5c20352c
[3, 0] = f09479c620d65556
[4, 0] = 047ed16f7f185164
[0, 1] = f83f068612ba8266
[1, 1] = 03f9ca1f8d50e28f
[2, 1] = c9a95041ad31125a
[3, 1] = 1badb2662d9b4cb2
[4, 1] = 5be08bcbbbd00bde
[0, 2] = 73731979ef295283
[1, 2] = b637d8e101444223
[2, 2] = 0ce71dff30e6b46e
[3, 2] = 1d0008cbbac217b3
[4, 2] = 206d570aa7b77734
[0, 3] = 1da0859d58339086
[1, 3] = 9fb543c046662bdb
[2, 3] = 5afa66a61d3111c0
[3, 3] = 1540bca97f38d6d1
[4, 3] = 1da61edad1518aa3
[0, 4] = d6b9889ae3c88d64
[1, 4] = 67cf435e008059dc
[2, 4] = 84a3d067927a4045
[3, 4] = d8e35b5d6997dabf
[4, 4] = 99cd2f6a8eab2208
```

Round #0

After theta

```
C7 31 4B FD 4D 43 FB 72 4A 1A 6A 92 BE 00 52 7F
B4 22 5D 20 DF 5F 19 1F 80 9D 61 17 2E 48 3B 69
3E EF 80 29 8B BF 1E DB 97 20 45 52 0E 72 EC 38
84 39 F5 EB 8A 7C BA 2C C2 05 4C D1 35 BD 38 A3
64 84 2C 1A 8E 83 02 82 84 B5 48 ED 2F E5 80 84
72 F0 D6 AF F1 6D A0 B3 28 99 E1 67 74 6E 74 99
F6 A3 9B 4C 8B F0 76 66 65 DF 75 8D 23 39 AF 84
6E C9 2F F1 EE 39 0D FF 77 32 CC 18 15 F1 73 DD
D0 F0 C3 20 55 F5 F6 B0 58 06 4C 61 D2 8B 6B 30
07 1E 8F 48 41 8D EF 8C F9 34 C9 87 3E 70 C6 C2
95 2F 37 A3 12 FC 6A 16 D7 82 25 66 CB F5 8C 48
DD 57 07 EE 13 3D 32 EE 69 12 20 5E B5 6A 4C 41
            52 9C 33 D8 8E 41 AD 46
```

After rho

```
C7 31 4B FD 4D 43 FB 72 94 34 D4 24 7D 01 A4 FE
AD 48 17 C8 F7 57 C6 07 82 B4 93 06 D8 19 76 E1
FC F5 D8 F6 79 07 4C 59 E5 20 C7 8E 73 09 52 24
BF AE C8 A7 CB 42 98 53 A8 70 01 53 74 4D 2F CE
42 16 0D C7 41 01 41 32 0E 48 48 58 8B D4 FE 52
95 83 B7 7E 8D 6F 03 9D 65 A2 64 86 9F D1 B9 D1
64 5A 84 B7 33 B3 1F DD 72 5E 09 CB BE EB 1A 47
78 F7 9C 86 7F B7 E4 97 31 2A E2 E7 BA EF 64 98
18 A4 AA DE 1E 16 1A 7E 35 18 2C 03 A6 30 E9 C5
F1 9D F1 C0 E3 11 29 A8 C2 F9 34 C9 87 3E 70 C6
AB 59 54 BE DC 8C 4A F0 5D 0B 96 98 2D D7 33 22
FB EA C0 7D A2 47 C6 BD 12 20 5E B5 6A 4C 41 69
            AB 91 14 E7 0C B6 63 50
```

After pi

```
C7 31 4B FD 4D 43 FB 72 BF AE C8 A7 CB 42 98 53
64 5A 84 B7 33 B3 1F DD F1 9D  F1 C0 E3 11 29 A8
AB 91 14 E7 0C B6 63 50 82 B4 93 06 D8 19 76 E1
0E 48 48 58 8B D4 FE 52 95 83 B7 7E 8D 6F 03 9D
18 A4 AA DE 1E 16 1A 7E FB EA C0 7D A2 47 C6 BD
94 34 D4 24 7D 01 A4 FE A8 70 01 53 74 4D 2F CE
72 5E 09 CB BE EB 1A 47 C2 F9 34 C9 87 3E 70 C6
AB 59 54 BE DC 8C 4A F0 FC F5 D8 F6 79 07 4C 59
E5 20 C7 8E 73 09 52 24 65 A2 64 86 9F D1 B9 D1
35 18 2C 03 A6 30 E9 C5 12 20 5E B5 6A 4C 41 69
AD 48 17 C8 F7 57 C6 07 42 16 0D C7 41 01 41 32
78 F7 9C 86 7F B7 E4 97 31 2A E2 E7 BA EF 64 98
            5D 0B 96 98 2D D7 33 22
```

After chi

```
87 61 4F ED 7D F2 FC FE 2E 2B B9 E7 0B 42 B8 73
6E 5A 80 90 3F 15 5D 8D B5 BD BA D8 A2 50 B1 8A
93 1F 94 E5 8E B6 63 51 13 37 24 20 DC 32 77 6C
06 6C 40 D8 99 C4 E6 30 76 C9 F7 5F 2D 2E C7 1C
18 B0 B9 DC 46 0E 2A 3E F7 A2 88 25 A1 83 4E AF
C6 3A DC AC F7 A3 B4 FF 28 D1 35 53 75 59 4F 4E
5B 5E 49 FD E6 6B 10 77 D6 DD B4 C9 A6 3F D4 C8
83 19 55 ED DC C0 41 F0 FC 77 F8 F6 F5 D7 E5 88
F5 38 CF 8F 53 29 12 20 67 82 36 32 D7 9D B9 F9
D9 CD AC 41 B7 33 E5 D5 13 20 59 BD 68 44 53 4D
95 A9 87 C8 C9 E1 62 82 43 1E 6F A6 C1 49 41 3A
34 F6 88 9E 7A A7 F7 B5 91 6A E3 A7 68 EF A0 9D
            1F 1D 9E 9F 2D D7 32 12
```

After iota

```
86 61 4F ED 7D F2 FC FE 2E 2B B9 E7 0B 42 B8 73
6E 5A 80 90 3F 15 5D 8D B5 BD BA D8 A2 50 B1 8A
93 1F 94 E5 8E B6 63 51 13 37 24 20 DC 32 77 6C
06 6C 40 D8 99 C4 E6 30 76 C9 F7 5F 2D 2E C7 1C
18 B0 B9 DC 46 0E 2A 3E F7 A2 88 25 A1 83 4E AF
C6 3A DC AC F7 A3 B4 FF 28 D1 35 53 75 59 4F 4E
5B 5E 49 FD E6 6B 10 77 D6 DD B4 C9 A6 3F D4 C8
83 19 55 ED DC C0 41 F0 FC 77 F8 F6 F5 D7 E5 88
F5 38 CF 8F 53 29 12 20 67 82 36 32 D7 9D B9 F9
D9 CD AC 41 B7 33 E5 D5 13 20 59 BD 68 44 53 4D
95 A9 87 C8 C9 E1 62 82 43 1E 6F A6 C1 49 41 3A
34 F6 88 9E 7A A7 F7 B5 91 6A E3 A7 68 EF A0 9D
            1F 1D 9E 9F 2D D7 32 12
```

(Skip rounds 1 to 22)

Round #23

After theta

```
7F B8 94 C4 39 9B 86 70 3B 89 48 FA 32 75 C3 E2
AE 9C 8E 91 39 CC 86 AF BF 55 83 9E CB BF 14 9F
A4 CA B3 FF ED BC BA 61 7A 8E 39 31 F8 6F DF C1
7C 13 22 A8 03 C0 9A A2 9B 4F 2C 70 28 7F E9 B1
D3 93 C4 9B C6 8D 29 FE 80 5A EB 0E 25 B2 C1 D5
BD F7 12 4D 48 A2 6A 36 FF 2E 6B CE 41 28 D8 4E
E6 6E E4 AA D6 EE A9 5C 07 01 C0 18 4E C2 EF 5A
23 BF 88 3F 02 E0 71 4C 66 D0 0C B6 55 FB B2 75
7A 4A 18 37 BE 9B 10 A0 EB E8 30 1D 07 93 4F B9
0E DD 19 67 64 9B 82 63 8C D9 19 58 5A F3 79 07
78 3C 6B 24 22 3C 24 90 F6 49 11 92 3F 53 A0 72
BC F4 74 C7 D5 E0 63 F5 40 25 4E 87 22 04 58 D7
            37 17 4A B6 82 FC C4 DB
```

After rho

```
7F B8 94 C4 39 9B 86 70 77 12 91 F4 65 EA 86 C5
2B A7 63 64 0E B3 E1 AB FC 4B F1 F9 5B 35 E8 B9
E7 D5 0D 23 55 9E FD 6F 83 FF F6 1D AC E7 98 13
82 3A 00 AC 29 CA 37 21 EC E6 13 0B 1C CA 5F 7A
49 E2 4D E3 C6 14 FF E9 1B 5C 0D A8 B5 EE 50 22
E9 BD 97 68 42 12 55 B3 3B FD BB AC 39 07 A1 60
57 B5 76 4F E5 32 77 23 84 DF B5 0E 02 80 31 9C
1F 01 F0 38 A6 91 5F C4 6C AB F6 65 EB CC A0 19
E3 C6 77 13 02 54 4F 09 A7 DC 75 74 98 8E 83 C9
53 70 CC A1 3B E3 8C 6C 07 8C D9 19 58 5A F3 79
90 40 E2 F1 AC 91 88 F0 D9 27 45 48 FE 4C 81 CA
97 9E EE B8 1A 7C AC 9E 25 4E 87 22 04 58 D7 40
            F1 F6 CD 85 92 AD 20 3F
```

After pi

```
7F B8 94 C4 39 9B 86 70 82 3A 00 AC 29 CA 37 21
57 B5 76 4F E5 32 77 23 53 70 CC A1 3B E3 8C 6C
F1 F6 CD 85 92 AD 20 3F FC 4B F1 F9 5B 35 E8 B9
1B 5C 0D A8 B5 EE 50 22 E9 BD 97 68 42 12 55 B3
E3 C6 77 13 02 54 4F 09 97 9E EE B8 1A 7C AC 9E
77 12 91 F4 65 EA 86 C5 EC E6 13 0B 1C CA 5F 7A
84 DF B5 0E 02 80 31 9C 07 8C D9 19 58 5A F3 79
90 40 E2 F1 AC 91 88 F0 E7 D5 0D 23 55 9E FD 6F
83 FF F6 1D AC E7 98 13 3B FD BB AC 39 07 A1 60
A7 DC 75 74 98 8E 83 C9 25 4E 87 22 04 58 D7 40
2B A7 63 64 0E B3 E1 AB 49 E2 4D E3 C6 14 FF E9
1F 01 F0 38 A6 91 5F C4 6C AB F6 65 EB CC A0 19
            D9 27 45 48 FE 4C 81 CA
```

After chi

```
2A 3D E2 87 FD AB C6 72 82 7A 88 0C 33 0B BF 6D
F7 33 77 4B 65 3E 57 30 5D 78 DC E1 12 F1 0A 2C
71 F4 CD AD 92 ED 11 3E 1C EA 63 B9 19 25 ED 28
19 1E 6D BB B5 AA 5A 2A FD A5 1F C0 5A 3A F5 25
8B 87 66 52 43 55 0F 28 94 8A E2 B8 BE B6 BC 9C
77 0B 35 F0 67 EA A6 41 EF E6 5B 1A 44 90 9D 1B
14 9F 97 EE A6 01 39 1C 60 9E C8 1D 19 30 F5 7C
18 A4 E0 FA B4 91 D1 CA DF D5 04 83 44 9E DC 0F
07 FF B2 4D 2C 6F 9A 9A 3B FF 39 AE 3D 57 F5 60
65 4D 7D 75 C9 08 AB E6 25 64 75 3E AC 39 D7 50
3D A6 D3 7C 2E 32 E1 AF 29 48 4B A6 8F 58 5F F0
8E 05 F1 30 B2 91 5E 06 4E 2B D4 41 EB 7F C0 38
            99 67 49 CB 3E 48 9F 8A
```

After iota

```
22 BD E2 07 FD AB C6 F2 82 7A 88 0C 33 0B BF 6D
F7 33 77 4B 65 3E 57 30 5D 78 DC E1 12 F1 0A 2C
71 F4 CD AD 92 ED 11 3E 1C EA 63 B9 19 25 ED 28
19 1E 6D BB B5 AA 5A 2A FD A5 1F C0 5A 3A F5 25
8B 87 66 52 43 55 0F 28 94 8A E2 B8 BE B6 BC 9C
77 0B 35 F0 67 EA A6 41 EF E6 5B 1A 44 90 9D 1B
14 9F 97 EE A6 01 39 1C 60 9E C8 1D 19 30 F5 7C
18 A4 E0 FA B4 91 D1 CA DF D5 04 83 44 9E DC 0F
07 FF B2 4D 2C 6F 9A 9A 3B FF 39 AE 3D 57 F5 60
65 4D 7D 75 C9 08 AB E6 25 64 75 3E AC 39 D7 50
3D A6 D3 7C 2E 32 E1 AF 29 48 4B A6 8F 58 5F F0
8E 05 F1 30 B2 91 5E 06 4E 2B D4 41 EB 7F C0 38
            99 67 49 CB 3E 48 9F 8A
```

After permutation

```
22 BD E2 07 FD AB C6 F2 82 7A 88 0C 33 0B BF 6D
F7 33 77 4B 65 3E 57 30 5D 78 DC E1 12 F1 0A 2C
71 F4 CD AD 92 ED 11 3E 1C EA 63 B9 19 25 ED 28
19 1E 6D BB B5 AA 5A 2A FD A5 1F C0 5A 3A F5 25
8B 87 66 52 43 55 0F 28 94 8A E2 B8 BE B6 BC 9C
77 0B 35 F0 67 EA A6 41 EF E6 5B 1A 44 90 9D 1B
14 9F 97 EE A6 01 39 1C 60 9E C8 1D 19 30 F5 7C
18 A4 E0 FA B4 91 D1 CA DF D5 04 83 44 9E DC 0F
07 FF B2 4D 2C 6F 9A 9A 3B FF 39 AE 3D 57 F5 60
65 4D 7D 75 C9 08 AB E6 25 64 75 3E AC 39 D7 50
3D A6 D3 7C 2E 32 E1 AF 29 48 4B A6 8F 58 5F F0
8E 05 F1 30 B2 91 5E 06 4E 2B D4 41 EB 7F C0 38
            99 67 49 CB 3E 48 9F 8A
```

State (as lanes of integers)

```
[0, 0] = f2c6abfd07e2bd22
[1, 0] = 6dbf0b330c887a82
[2, 0] = 30573e654b7733f7
[3, 0] = 2c0af112e1dc785d
[4, 0] = 3e11ed92adcdf471
[0, 1] = 28ed2519b963ea1c
[1, 1] = 2a5aaab5bb6d1e19
[2, 1] = 25f53a5ac01fa5fd
[3, 1] = 280f55435266878b
[4, 1] = 9cbcb6beb8e28a94
[0, 2] = 41a6ea67f0350b77
[1, 2] = 1b9d90441a5be6ef
[2, 2] = 1c3901a6ee979f14
[3, 2] = 7cf530191dc89e60
[4, 2] = cad191b4fae0a418
[0, 3] = 0fdc9e448304d5df
[1, 3] = 9a9a6f2c4db2ff07
[2, 3] = 60f5573dae39ff3b
[3, 3] = e6ab08c9757d4d65
[4, 3] = 50d739ac3e756425
[0, 4] = afe1322e7cd3a63d
[1, 4] = f05f588fa64b4829
[2, 4] = 065e91b230f1058e
[3, 4] = 38c07feb41d42b4e
[4, 4] = 8a9f483ecb496799
```

About to call squeeze (again)

State before permutation (in bytes)

```
22 BD E2 07 FD AB C6 F2 82 7A 88 0C 33 0B BF 6D
F7 33 77 4B 65 3E 57 30 5D 78 DC E1 12 F1 0A 2C
71 F4 CD AD 92 ED 11 3E 1C EA 63 B9 19 25 ED 28
19 1E 6D BB B5 AA 5A 2A FD A5 1F C0 5A 3A F5 25
8B 87 66 52 43 55 0F 28 94 8A E2 B8 BE B6 BC 9C
77 0B 35 F0 67 EA A6 41 EF E6 5B 1A 44 90 9D 1B
14 9F 97 EE A6 01 39 1C 60 9E C8 1D 19 30 F5 7C
18 A4 E0 FA B4 91 D1 CA DF D5 04 83 44 9E DC 0F
07 FF B2 4D 2C 6F 9A 9A 3B FF 39 AE 3D 57 F5 60
65 4D 7D 75 C9 08 AB E6 25 64 75 3E AC 39 D7 50
3D A6 D3 7C 2E 32 E1 AF 29 48 4B A6 8F 58 5F F0
8E 05 F1 30 B2 91 5E 06 4E 2B D4 41 EB 7F C0 38
            99 67 49 CB 3E 48 9F 8A
```

State before permutation (as lanes of integers)

```
[0, 0] = f2c6abfd07e2bd22
[1, 0] = 6dbf0b330c887a82
[2, 0] = 30573e654b7733f7
[3, 0] = 2c0af112e1dc785d
[4, 0] = 3e11ed92adcdf471
[0, 1] = 28ed2519b963ea1c
[1, 1] = 2a5aaab5bb6d1e19
[2, 1] = 25f53a5ac01fa5fd
[3, 1] = 280f55435266878b
[4, 1] = 9cbcb6beb8e28a94
[0, 2] = 41a6ea67f0350b77
[1, 2] = 1b9d90441a5be6ef
[2, 2] = 1c3901a6ee979f14
[3, 2] = 7cf530191dc89e60
[4, 2] = cad191b4fae0a418
[0, 3] = 0fdc9e448304d5df
[1, 3] = 9a9a6f2c4db2ff07
[2, 3] = 60f5573dae39ff3b
[3, 3] = e6ab08c9757d4d65
[4, 3] = 50d739ac3e756425
[0, 4] = afe1322e7cd3a63d
[1, 4] = f05f588fa64b4829
[2, 4] = 065e91b230f1058e
[3, 4] = 38c07feb41d42b4e
[4, 4] = 8a9f483ecb496799
```

Round #0

After theta

```
D7 0E 9F 91 35 1C 88 2D 7F B2 84 4B F7 45 6E 88
96 09 86 38 D1 FE DD 4B 75 39 0C 2F 10 44 53 27
BA AC D0 55 2B 9F EB EF E9 59 1E 2F D1 92 A3 F7
E4 D6 61 FC 71 E4 8B CF 9C 9F EE B3 EE FA 7F 5E
A3 C6 B6 9C 41 E0 56 23 5F D2 FF 40 07 C4 46 4D
82 B8 48 66 AF 5D E8 9E 12 2E 57 5D 80 DE 4C FE
75 A5 66 9D 12 C1 B3 67 48 DF 18 D3 1B 85 AC 77
D3 FC FD 02 0D E3 2B 1B 2A 66 79 15 8C 29 92 D0
FA 37 BE 0A E8 21 4B 7F 5A C5 C8 DD 89 97 7F 1B
4D 0C AD BB CB BD F2 ED EE 3C 68 C6 15 4B 2D 81
C8 15 AE EA E6 85 AF 70 D4 80 47 E1 4B 16 8E 15
EF 3F 00 43 06 51 D4 7D 66 6A 04 8F E9 CA 99 33
            52 3F 54 33 87 3A 65 5B
```

After rho

```
D7 0E 9F 91 35 1C 88 2D FF 64 09 97 EE 8B DC 10
65 82 21 4E B4 7F F7 92 41 34 75 52 97 C3 F0 02
F9 5C 7F D7 65 85 AE 5A 12 2D 39 7A 9F 9E E5 F1
C6 1F 47 BE F8 4C 6E 1D 17 E7 A7 FB AC BB FE 9F
63 5B CE 20 70 AB 91 51 6C D4 F4 25 FD 0F 74 40
14 C4 45 32 7B ED 42 F7 F9 4B B8 5C 75 01 7A 33
EB 94 08 9E 3D AB 2B 35 0A 59 EF 90 BE 31 A6 37
81 86 F1 95 8D 69 FE 7E 2A 18 53 24 A1 55 CC F2
57 01 3D 64 E9 4F FF C6 BF 0D AD 62 E4 EE C4 CB
57 BE BD 89 A1 75 77 B9 81 EE 3C 68 C6 15 4B 2D
BE C2 21 57 B8 AA 9B 17 50 03 1E 85 2F 59 38 56
FD 07 60 C8 20 8A BA EF 6A 04 8F E9 CA 99 33 66
            D9 96 D4 0F D5 CC A1 4E
```

After pi

```
D7 0E 9F 91 35 1C 88 2D C6 1F 47 BE F8 4C 6E 1D
EB 94 08 9E 3D AB 2B 35 57 BE BD 89 A1 75 77 B9
D9 96 D4 0F D5 CC A1 4E 41 34 75 52 97 C3 F0 02
6C D4 F4 25 FD 0F 74 40 14 C4 45 32 7B ED 42 F7
57 01 3D 64 E9 4F FF C6 FD 07 60 C8 20 8A BA EF
FF 64 09 97 EE 8B DC 10 17 E7 A7 FB AC BB FE 9F
0A 59 EF 90 BE 31 A6 37 81 EE 3C 68 C6 15 4B 2D
BE C2 21 57 B8 AA 9B 17 F9 5C 7F D7 65 85 AE 5A
12 2D 39 7A 9F 9E E5 F1 F9 4B B8 5C 75 01 7A 33
BF 0D AD 62 E4 EE C4 CB 6A 04 8F E9 CA 99 33 66
65 82 21 4E B4 7F F7 92 63 5B CE 20 70 AB 91 51
81 86 F1 95 8D 69 FE 7E 2A 18 53 24 A1 55 CC F2
            50 03 1E 85 2F 59 38 56
```

After chi

```
FE 8E 97 91 30 BF 89 0D D2 35 F2 BF 78 18 3A 95
63 94 48 98 69 23 AB 73 51 B6 B6 19 81 65 7F 98
D9 87 94 21 1D 8C C7 5E 51 34 74 40 95 23 F2 B5
2F D5 CC 61 7D 0D C9 40 BC C2 05 BA 7B 6D 42 DE
57 31 28 76 7E 0E BF C6 D1 C7 E0 ED 48 86 BE AF
F7 7C 41 97 FC 8B DC 30 96 41 B7 93 EC BF B7 97
34 59 EE 87 86 9B 36 25 C0 CA 34 E8 80 14 0F 2D
BE 41 87 3F B8 9A B9 98 10 1E FF D3 05 84 B4 58
14 29 3C 58 1F 70 61 39 B9 4B BA D5 7F 10 49 17
2E 55 DD 74 C1 EA 48 D3 68 25 8F C1 50 83 72 C7
E5 06 10 DB 39 3F 99 BC 49 43 CC 00 50 BF 91 D1
D1 85 FD 14 83 61 CE 7A 0F 98 72 6E 31 73 0B 72
            52 5A D0 A5 6F D9 38 17
```

After iota

```
FF 8E 97 91 30 BF 89 0D D2 35 F2 BF 78 18 3A 95
63 94 48 98 69 23 AB 73 51 B6 B6 19 81 65 7F 98
D9 87 94 21 1D 8C C7 5E 51 34 74 40 95 23 F2 B5
2F D5 CC 61 7D 0D C9 40 BC C2 05 BA 7B 6D 42 DE
57 31 28 76 7E 0E BF C6 D1 C7 E0 ED 48 86 BE AF
F7 7C 41 97 FC 8B DC 30 96 41 B7 93 EC BF B7 97
34 59 EE 87 86 9B 36 25 C0 CA 34 E8 80 14 0F 2D
BE 41 87 3F B8 9A B9 98 10 1E FF D3 05 84 B4 58
14 29 3C 58 1F 70 61 39 B9 4B BA D5 7F 10 49 17
2E 55 DD 74 C1 EA 48 D3 68 25 8F C1 50 83 72 C7
E5 06 10 DB 39 3F 99 BC 49 43 CC 00 50 BF 91 D1
D1 85 FD 14 83 61 CE 7A 0F 98 72 6E 31 73 0B 72
            52 5A D0 A5 6F D9 38 17
```

(Skip rounds 1 to 22)

Round #23

After theta

```
37 E8 EC 6A 7B 06 DA 58 CD F9 4D 54 60 33 DE 0F
0E 9D 66 56 32 64 53 73 0F A4 CA 2B 43 63 1C A7
E8 B3 06 EE F5 CA 0D 83 42 AD 23 B3 3A B8 5F E7
99 EB AB DF E1 6E 21 66 41 57 4A 94 20 47 29 06
36 0F 73 FE AF 49 5A 68 BE 60 D0 B4 B7 2C 98 0B
8C 86 9F C1 BF 2A C3 86 98 A9 EF FC 60 69 05 C4
F0 7B 93 6D 1C 8D 4E 5B 80 21 76 E4 EF CA 54 37
2A 09 9B 04 16 2E 65 6A D7 EE 90 D2 3C 62 6F C1
B4 E1 C8 B7 2B E9 E4 EF 03 35 0A 7C 6E 7F 0E 40
FE F9 A0 31 7A 7E BC 8B 46 68 9C 0E 43 96 BA 1E
A2 7A 2C 3B E9 E1 C7 A3 31 3B B1 00 C2 8C C8 4A
BE B9 41 20 3B 91 2D E0 40 15 75 78 DE BA 92 38
            53 43 0B BF 4A 54 00 EB
```

After rho

```
37 E8 EC 6A 7B 06 DA 58 9A F3 9B A8 C0 66 BC 1F
43 A7 99 95 0C D9 D4 9C 34 C6 71 FA 40 AA BC 32
57 6E 18 44 9F 35 70 AF AB 83 FB 75 2E D4 3A 32
FA 1D EE 16 62 96 B9 BE 41 D0 95 12 25 C8 51 8A
87 39 FF D7 24 2D 34 9B 82 B9 E0 0B 06 4D 7B CB
64 34 FC 0C FE 55 19 36 10 63 A6 BE F3 83 A5 15
6C E3 68 74 DA 82 DF 9B 95 A9 6E 00 43 EC C8 DF
02 0B 97 32 35 95 84 4D A5 79 C4 DE 82 AF DD 21
F9 76 25 9D FC 9D 36 1C 07 A0 81 1A 05 3E B7 3F
8F 77 D1 3F 1F 34 46 CF 1E 46 68 9C 0E 43 96 BA
1F 8F 8A EA B1 EC A4 87 C5 EC C4 02 08 33 22 2B
37 37 08 64 27 B2 05 DC 15 75 78 DE BA 92 38 40
            C0 FA D4 D0 C2 AF 12 15
```

After pi

```
37 E8 EC 6A 7B 06 DA 58 FA 1D EE 16 62 96 B9 BE
6C E3 68 74 DA 82 DF 9B 8F 77 D1 3F 1F 34 46 CF
C0 FA D4 D0 C2 AF 12 15 34 C6 71 FA 40 AA BC 32
82 B9 E0 0B 06 4D 7B CB 64 34 FC 0C FE 55 19 36
F9 76 25 9D FC 9D 36 1C 37 37 08 64 27 B2 05 DC
9A F3 9B A8 C0 66 BC 1F 41 D0 95 12 25 C8 51 8A
95 A9 6E 00 43 EC C8 DF 1E 46 68 9C 0E 43 96 BA
1F 8F 8A EA B1 EC A4 87 57 6E 18 44 9F 35 70 AF
AB 83 FB 75 2E D4 3A 32 10 63 A6 BE F3 83 A5 15
07 A0 81 1A 05 3E B7 3F 15 75 78 DE BA 92 38 40
43 A7 99 95 0C D9 D4 9C 87 39 FF D7 24 2D 34 9B
02 0B 97 32 35 95 84 4D A5 79 C4 DE 82 AF DD 21
            C5 EC C4 02 08 33 22 2B
```

After chi

```
33 0A EC 0A E3 06 9C 59 79 09 7F 1D 67 A2 B9 FA
2C 6B 6C B4 1A 09 CF 8B B8 77 F9 15 26 34 8E 87
08 EF D6 C4 C2 3F 33 B3 50 C2 6D FE B8 BA BC 06
1B FB E1 9A 06 C5 5D C3 62 35 F4 6C FD 77 18 F6
F9 B6 54 07 BC 95 8E 3E B5 0E 88 65 21 F7 46 15
0E DA F1 A8 82 42 34 4A 4B 96 95 8E 29 CB 47 AA
94 20 EC 62 F2 40 E8 DA 9E 36 79 9C 4E 41 8E A2
5E 8F 8E F8 94 64 E5 07 47 0E 1C CE 4E 36 F5 AA
AC 03 FA 75 2A E8 28 18 00 36 DE 7A 49 03 AD 55
45 AA 81 1A 00 1B F7 90 BD F4 9B EF 9A 52 32 50
43 A5 99 B5 1D 49 54 D8 22 49 BF 1B A6 07 6D BB
42 8F 97 32 3D 85 A6 47 A7 7A DD 4B 86 67 09 B5
            41 F4 A2 40 28 17 02 28
```

After iota

```
3B 8A EC 8A E3 06 9C D9 79 09 7F 1D 67 A2 B9 FA
2C 6B 6C B4 1A 09 CF 8B B8 77 F9 15 26 34 8E 87
08 EF D6 C4 C2 3F 33 B3 50 C2 6D FE B8 BA BC 06
1B FB E1 9A 06 C5 5D C3 62 35 F4 6C FD 77 18 F6
F9 B6 54 07 BC 95 8E 3E B5 0E 88 65 21 F7 46 15
0E DA F1 A8 82 42 34 4A 4B 96 95 8E 29 CB 47 AA
94 20 EC 62 F2 40 E8 DA 9E 36 79 9C 4E 41 8E A2
5E 8F 8E F8 94 64 E5 07 47 0E 1C CE 4E 36 F5 AA
AC 03 FA 75 2A E8 28 18 00 36 DE 7A 49 03 AD 55
45 AA 81 1A 00 1B F7 90 BD F4 9B EF 9A 52 32 50
43 A5 99 B5 1D 49 54 D8 22 49 BF 1B A6 07 6D BB
42 8F 97 32 3D 85 A6 47 A7 7A DD 4B 86 67 09 B5
            41 F4 A2 40 28 17 02 28
```

After permutation

```
   3B 8A EC 8A E3 06 9C D9 79 09 7F 1D 67 A2 B9 FA
   2C 6B 6C B4 1A 09 CF 8B B8 77 F9 15 26 34 8E 87
   08 EF D6 C4 C2 3F 33 B3 50 C2 6D FE B8 BA BC 06
1B FB E1 9A 06 C5 5D C3 62 35 F4 6C FD 77 18 F6
F9 B6 54 07 BC 95 8E 3E B5 0E 88 65 21 F7 46 15
0E DA F1 A8 82 42 34 4A 4B 96 95 8E 29 CB 47 AA
94 20 EC 62 F2 40 E8 DA 9E 36 79 9C 4E 41 8E A2
5E 8F 8E F8 94 64 E5 07 47 0E 1C CE 4E 36 F5 AA
AC 03 FA 75 2A E8 28 18 00 36 DE 7A 49 03 AD 55
45 AA 81 1A 00 1B F7 90 BD F4 9B EF 9A 52 32 50
43 A5 99 B5 1D 49 54 D8 22 49 BF 1B A6 07 6D BB
42 8F 97 32 3D 85 A6 47 A7 7A DD 4B 86 67 09 B5
            41 F4 A2 40 28 17 02 28
```

State (as lanes of integers)

```
[0, 0] = d99c06e38aec8a3b
[1, 0] = fab9a2671d7f0979
[2, 0] = 8bcf091ab46c6b2c
[3, 0] = 878e342615f977b8
[4, 0] = b3333fc2c4d6ef08
[0, 1] = 06bcbab8fe6dc250
[1, 1] = c35dc5069ae1fb1b
[2, 1] = f61877fd6cf43562
[3, 1] = 3e8e95bc0754b6f9
[4, 1] = 1546f72165880eb5
[0, 2] = 4a344282a8f1da0e
[1, 2] = aa47cb298e95964b
[2, 2] = dae840f262ec2094
[3, 2] = a28e414e9c79369e
[4, 2] = 07e56494f88e8f5e
[0, 3] = aaf5364ece1c0e47
[1, 3] = 1828e82a75fa03ac
[2, 3] = 55ad03497ade3600
[3, 3] = 90f71b001a81aa45
[4, 3] = 5032529aef9bf4bd
[0, 4] = d854491db599a543
[1, 4] = bb6d07a61bbf4922
[2, 4] = 47a6853d32978f42
[3, 4] = b50967864bdd7aa7
[4, 4] = 2802172840a2f441
```

The hash value is

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

SHAKE-128 sample to produce 4096-bits of output

The message as a bit string

```
1 1 0 0 1 0 1 0 0 0 0 1 1 0 1 0 1 1 0 1 1 1 1 0 1 0 0 1 1 0
```

About to call last of the absorb phase

XORed state (in bytes)

```
53 58 7B D9 07 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 80 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
            00 00 00 00 00 00 00 00
```


XORed state (as lanes of integers)

```
[0, 0] = 00000007d97b5853
[1, 0] = 0000000000000000
[2, 0] = 0000000000000000
[3, 0] = 0000000000000000
[4, 0] = 0000000000000000
[0, 1] = 0000000000000000
[1, 1] = 0000000000000000
[2, 1] = 0000000000000000
[3, 1] = 0000000000000000
[4, 1] = 0000000000000000
[0, 2] = 0000000000000000
[1, 2] = 0000000000000000
[2, 2] = 0000000000000000
[3, 2] = 0000000000000000
[4, 2] = 0000000000000000
[0, 3] = 0000000000000000
[1, 3] = 0000000000000000
[2, 3] = 0000000000000000
[3, 3] = 0000000000000000
[4, 3] = 0000000000000000
[0, 4] = 8000000000000000
[1, 4] = 0000000000000000
[2, 4] = 0000000000000000
[3, 4] = 0000000000000000
[4, 4] = 0000000000000000
```

Round #0

After theta

```
53 58 7B D9 07 00 00 00 53 58 7B D9 07 00 00 80
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
A7 B0 F6 B2 0F 00 00 00 00 00 00 00 00 00 00 00
53 58 7B D9 07 00 00 80 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 A7 B0 F6 B2 0F 00 00 00
00 00 00 00 00 00 00 00 53 58 7B D9 07 00 00 80
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
A7 B0 F6 B2 0F 00 00 00 00 00 00 00 00 00 00 00
53 58 7B D9 07 00 00 80 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 A7 B0 F6 B2 0F 00 00 00
00 00 00 00 00 00 00 80 53 58 7B D9 07 00 00 80
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
            A7 B0 F6 B2 0F 00 00 00
```

After rho

```
53 58 7B D9 07 00 00 00 A7 B0 F6 B2 0F 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 38 85 B5 97 7D 00 00 00 00 00 00 00 00
97 7D 00 00 00 38 85 B5 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 70 0A 6B 2F FB 00
00 00 00 00 00 00 00 00 00 4E 61 ED 65 1F 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
D9 07 00 00 80 53 58 7B 00 00 00 00 00 00 00 00
2F FB 00 00 00 70 0A 6B 00 00 00 00 00 00 00 00
```

```
00 00 00 00 00 00 00 00 00 A7 B0 F6 B2 0F 00 00
00 00 02 00 00 00 00 00 4E 61 ED 65 1F 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
            00 C0 29 AC BD EC 03 00
```

After pi

```
53 58 7B D9 07 00 00 00 97 7D 00 00 00 38 85 B5
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 C0 29 AC BD EC 03 00 00 00 00 00 00 00 00 00
00 00 70 0A 6B 2F FB 00 00 00 00 00 00 00 00 00
2F FB 00 00 00 70 0A 6B 00 00 00 00 00 00 00 00
A7 B0 F6 B2 0F 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 A7 B0 F6 B2 0F 00 00
00 00 02 00 00 00 00 00 00 00 00 38 85 B5 97 7D
00 00 00 00 00 00 00 00 00 4E 61 ED 65 1F 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
D9 07 00 00 80 53 58 7B 00 00 00 00 00 00 00 00
            4E 61 ED 65 1F 00 00 00
```

After chi

```
53 58 7B D9 07 00 00 00 97 7D 00 00 00 38 85 B5
00 C0 29 AC BD EC 03 00 53 18 52 51 02 00 00 00
84 E5 29 AC BD D4 86 B5 00 00 00 00 00 00 00 00
2F FB 70 0A 6B 5F F1 6B 00 00 00 00 00 00 00 00
2F FB 00 00 00 70 0A 6B 00 00 70 0A 6B 2F FB 00
A7 B0 F6 B2 0F 00 00 00 00 A7 B0 F6 B2 0F 00 00
00 00 02 00 00 00 00 00 A7 17 44 44 BD 0F 00 00
00 00 02 00 00 00 00 00 00 4E 61 D5 E0 AA 97 7D
00 00 00 00 00 00 00 00 00 4E 61 ED 65 1F 00 00
00 00 00 38 85 B5 97 7D 00 00 00 00 00 00 00 00
D9 07 00 00 80 53 58 7B 00 00 00 00 00 00 00 00
97 66 ED 65 9F 53 58 7B 00 00 00 00 00 00 00 00
            4E 61 ED 65 1F 00 00 00
```

After iota

```
52 58 7B D9 07 00 00 00 97 7D 00 00 00 38 85 B5
00 C0 29 AC BD EC 03 00 53 18 52 51 02 00 00 00
84 E5 29 AC BD D4 86 B5 00 00 00 00 00 00 00 00
2F FB 70 0A 6B 5F F1 6B 00 00 00 00 00 00 00 00
2F FB 00 00 00 70 0A 6B 00 00 70 0A 6B 2F FB 00
A7 B0 F6 B2 0F 00 00 00 00 A7 B0 F6 B2 0F 00 00
00 00 02 00 00 00 00 00 A7 17 44 44 BD 0F 00 00
00 00 02 00 00 00 00 00 00 4E 61 D5 E0 AA 97 7D
00 00 00 00 00 00 00 00 00 4E 61 ED 65 1F 00 00
00 00 00 38 85 B5 97 7D 00 00 00 00 00 00 00 00
D9 07 00 00 80 53 58 7B 00 00 00 00 00 00 00 00
97 66 ED 65 9F 53 58 7B 00 00 00 00 00 00 00 00
            4E 61 ED 65 1F 00 00 00
```

(Skip rounds 1 to 22)

Round #23

After theta

```
E5 C9 38 91 7E 2D CB B6 4A 58 42 73 14 82 E1 30
C6 50 6D 1E 06 82 8D 5E 8B F9 05 58 45 03 D5 87
8E 5B 12 B3 03 98 A7 EF A3 87 68 10 6A CF 6C B1
4E 6B 71 A4 46 0A C2 25 DA DB 48 F1 BA 33 88 15
3C 04 56 F1 82 E8 B3 83 7E D0 A1 5C 3A 51 4D 4B
FB 44 D7 40 4E 41 AF AD 87 22 12 4D 83 EA 79 D4
2A C6 4E D0 A7 90 BE 27 E7 B4 40 C6 63 09 3B 93
36 ED 8D 06 58 2D 32 E0 26 54 B6 49 05 CD FC 47
4F 83 EA 78 1E F1 51 EB 2F B3 24 89 85 66 CF B6
B2 6B 35 F6 19 C3 E1 AC DF 6F 1B 5E E3 06 89 82
27 71 C4 F3 B6 99 32 7C 4C 8E F3 6D 8D 18 5A 13
60 56 56 76 79 A3 F4 B6 97 2F 9A CC 07 CF FB A1
            08 96 F2 AF 4E B2 8B 8F
```

After rho

```
E5 C9 38 91 7E 2D CB B6 94 B0 84 E6 28 04 C3 61
31 54 9B 87 81 60 A3 97 34 50 7D B8 98 5F 80 55
C0 3C 7D 77 DC 92 98 1D A1 F6 CC 16 3B 7A 88 06
47 6A A4 20 5C E2 B4 16 85 F6 36 52 BC EE 0C 62
02 AB 78 41 F4 D9 41 1E D5 B4 E4 07 1D CA A5 13
DD 27 BA 06 72 0A 7A 6D 51 1F 8A 48 34 0D AA E7
82 3E 85 F4 3D 51 31 76 12 76 26 CF 69 81 8C C7
03 AC 16 19 70 9B F6 46 93 0A 9A F9 8F 4C A8 6C
1D CF 23 3E 6A FD 69 50 67 DB 97 59 92 C4 42 B3
38 9C 55 76 AD C6 3E 63 82 DF 6F 1B 5E E3 06 89
CA F0 9D C4 11 CF DB 66 30 39 CE B7 35 62 68 4D
CC CA CA 2E 6F 94 DE 16 2F 9A CC 07 CF FB A1 97
            E2 23 82 A5 FC AB 93 EC
```

After pi

```
E5 C9 38 91 7E 2D CB B6 47 6A A4 20 5C E2 B4 16
82 3E 85 F4 3D 51 31 76 38 9C 55 76 AD C6 3E 63
E2 23 82 A5 FC AB 93 EC 34 50 7D B8 98 5F 80 55
D5 B4 E4 07 1D CA A5 13 DD 27 BA 06 72 0A 7A 6D
1D CF 23 3E 6A FD 69 50 CC CA CA 2E 6F 94 DE 16
94 B0 84 E6 28 04 C3 61 85 F6 36 52 BC EE 0C 62
12 76 26 CF 69 81 8C C7 82 DF 6F 1B 5E E3 06 89
CA F0 9D C4 11 CF DB 66 C0 3C 7D 77 DC 92 98 1D
A1 F6 CC 16 3B 7A 88 06 51 1F 8A 48 34 0D AA E7
67 DB 97 59 92 C4 42 B3 2F 9A CC 07 CF FB A1 97
31 54 9B 87 81 60 A3 97 02 AB 78 41 F4 D9 41 1E
03 AC 16 19 70 9B F6 46 93 0A 9A F9 8F 4C A8 6C
            30 39 CE B7 35 62 68 4D
```

After chi

```
65 DD 39 45 5F 3C CA D6 7F EA F4 22 DC 64 BA 17
40 1D 07 75 6D 78 B0 FA 3D 54 6D 66 AF C2 76 71
E0 01 06 85 FC 69 A7 EC 3C 53 67 B8 FA 5F DA 39
D5 7C E5 3F 15 3F A4 03 1D 27 72 06 77 0A EC 6B
2D DF 16 AE FA B6 69 11 0D 6E 4A 29 6A 14 FB 14
86 B0 84 6B 69 05 43 E4 05 7F 7F 42 AA 8C 0E 6A
5A 56 B6 0B 68 8D 55 A1 96 DF 6F 39 76 E3 06 88
```

```
CB B6 AF D4 85 25 D7 64 90 35 7F 3F D8 97 BA FC
87 36 D9 07 B9 BA C8 16 59 1F C2 4E 79 36 0B E3
A7 FF A6 29 82 C4 5A BB 0E 58 4C 07 EC 93 A1 95
30 50 9D 9F 81 62 15 D7 92 A9 F0 A1 7B 9D 49 36
23 9D 52 1F 40 B9 B6 47 92 4E 8B F9 0F 4C 2B FE
            32 92 AE F7 41 FB 28 45
```

After iota

```
6D 5D 39 C5 5F 3C CA 56 7F EA F4 22 DC 64 BA 17
40 1D 07 75 6D 78 B0 FA 3D 54 6D 66 AF C2 76 71
E0 01 06 85 FC 69 A7 EC 3C 53 67 B8 FA 5F DA 39
D5 7C E5 3F 15 3F A4 03 1D 27 72 06 77 0A EC 6B
2D DF 16 AE FA B6 69 11 0D 6E 4A 29 6A 14 FB 14
86 B0 84 6B 69 05 43 E4 05 7F 7F 42 AA 8C 0E 6A
5A 56 B6 0B 68 8D 55 A1 96 DF 6F 39 76 E3 06 88
CB B6 AF D4 85 25 D7 64 90 35 7F 3F D8 97 BA FC
87 36 D9 07 B9 BA C8 16 59 1F C2 4E 79 36 0B E3
A7 FF A6 29 82 C4 5A BB 0E 58 4C 07 EC 93 A1 95
30 50 9D 9F 81 62 15 D7 92 A9 F0 A1 7B 9D 49 36
23 9D 52 1F 40 B9 B6 47 92 4E 8B F9 0F 4C 2B FE
            32 92 AE F7 41 FB 28 45
```

After permutation

```
6D 5D 39 C5 5F 3C CA 56 7F EA F4 22 DC 64 BA 17
40 1D 07 75 6D 78 B0 FA 3D 54 6D 66 AF C2 76 71
E0 01 06 85 FC 69 A7 EC 3C 53 67 B8 FA 5F DA 39
D5 7C E5 3F 15 3F A4 03 1D 27 72 06 77 0A EC 6B
2D DF 16 AE FA B6 69 11 0D 6E 4A 29 6A 14 FB 14
86 B0 84 6B 69 05 43 E4 05 7F 7F 42 AA 8C 0E 6A
5A 56 B6 0B 68 8D 55 A1 96 DF 6F 39 76 E3 06 88
CB B6 AF D4 85 25 D7 64 90 35 7F 3F D8 97 BA FC
87 36 D9 07 B9 BA C8 16 59 1F C2 4E 79 36 0B E3
A7 FF A6 29 82 C4 5A BB 0E 58 4C 07 EC 93 A1 95
30 50 9D 9F 81 62 15 D7 92 A9 F0 A1 7B 9D 49 36
23 9D 52 1F 40 B9 B6 47 92 4E 8B F9 0F 4C 2B FE
            32 92 AE F7 41 FB 28 45
```

State (as lanes of integers)

```
[0, 0] = 56ca3c5fc5395d6d
[1, 0] = 17ba64dc22f4ea7f
[2, 0] = fab0786d75071d40
[3, 0] = 7176c2af666d543d
[4, 0] = eca769fc850601e0
[0, 1] = 39da5ffab867533c
[1, 1] = 03a43f153fe57cd5
[2, 1] = 6bec0a770672271d
[3, 1] = 1169b6faae16df2d
[4, 1] = 14fb146a294a6e0d
[0, 2] = e44305696b84b086
[1, 2] = 6a0e8caa427f7f05
[2, 2] = a1558d680bb6565a
[3, 2] = 8806e376396fdf96
[4, 2] = 64d72585d4afb6cb
[0, 3] = fcba97d83f7f3590
[1, 3] = 16c8bab907d93687
```

```
[2, 3] = e30b36794ec21f59
[3, 3] = bb5ac48229a6ffa7
[4, 3] = 95a193ec074c580e
[0, 4] = d71562819f9d5030
[1, 4] = 36499d7ba1f0a992
[2, 4] = 47b6b9401f529d23
[3, 4] = fe2b4c0ff98b4e92
[4, 4] = 4528fb41f7ae9232
```

About to call squeeze (again)

State before permutation (in bytes)

```
6D 5D 39 C5 5F 3C CA 56 7F EA F4 22 DC 64 BA 17
40 1D 07 75 6D 78 B0 FA 3D 54 6D 66 AF C2 76 71
E0 01 06 85 FC 69 A7 EC 3C 53 67 B8 FA 5F DA 39
D5 7C E5 3F 15 3F A4 03 1D 27 72 06 77 0A EC 6B
2D DF 16 AE FA B6 69 11 0D 6E 4A 29 6A 14 FB 14
86 B0 84 6B 69 05 43 E4 05 7F 7F 42 AA 8C 0E 6A
5A 56 B6 0B 68 8D 55 A1 96 DF 6F 39 76 E3 06 88
CB B6 AF D4 85 25 D7 64 90 35 7F 3F D8 97 BA FC
87 36 D9 07 B9 BA C8 16 59 1F C2 4E 79 36 0B E3
A7 FF A6 29 82 C4 5A BB 0E 58 4C 07 EC 93 A1 95
30 50 9D 9F 81 62 15 D7 92 A9 F0 A1 7B 9D 49 36
23 9D 52 1F 40 B9 B6 47 92 4E 8B F9 0F 4C 2B FE
            32 92 AE F7 41 FB 28 45
```

State before permutation (as lanes of integers)

```
[0, 0] = 56ca3c5fc5395d6d
[1, 0] = 17ba64dc22f4ea7f
[2, 0] = fab0786d75071d40
[3, 0] = 7176c2af666d543d
[4, 0] = eca769fc850601e0
[0, 1] = 39da5ffab867533c
[1, 1] = 03a43f153fe57cd5
[2, 1] = 6bec0a770672271d
[3, 1] = 1169b6faae16df2d
[4, 1] = 14fb146a294a6e0d
[0, 2] = e44305696b84b086
[1, 2] = 6a0e8caa427f7f05
[2, 2] = a1558d680bb6565a
[3, 2] = 8806e376396fdf96
[4, 2] = 64d72585d4afb6cb
[0, 3] = fcba97d83f7f3590
[1, 3] = 16c8bab907d93687
[2, 3] = e30b36794ec21f59
[3, 3] = bb5ac48229a6ffa7
[4, 3] = 95a193ec074c580e
[0, 4] = d71562819f9d5030
[1, 4] = 36499d7ba1f0a992
[2, 4] = 47b6b9401f529d23
[3, 4] = fe2b4c0ff98b4e92
[4, 4] = 4528fb41f7ae9232
```

Round #0

After theta

```
03 A3 B6 BF A2 ED EB A7 F3 ED 6B C6 DF 17 2E 9E
9D A0 33 CE 90 B7 F1 FE 74 9C 3C 5F 99 D3 C6 7D
BC 52 4E C8 79 51 36 00 52 AD E8 C2 07 8E FB C8
59 7B 7A DB 16 4C 30 8A C0 9A 46 BD 8A C5 AD 6F
64 17 47 97 CC A7 D9 1D 51 3D 02 64 EF 2C 6A F8
E8 4E 0B 11 94 D4 62 15 89 78 E0 A6 A9 FF 9A E3
87 EB 82 B0 95 42 14 A5 DF 17 3E 00 40 F2 B6 84
97 E5 E7 99 00 1D 46 88 FE CB F0 45 25 46 9B 0D
0B 31 46 E3 BA C9 5C 9F 84 A2 F6 F5 84 F9 4A E7
EE 37 F7 10 B4 D5 EA B7 52 0B 04 4A 69 AB 30 79
5E AE 12 E5 7C B3 34 26 1E AE 6F 45 78 EE DD BF
FE 20 66 A4 BD 76 F7 43 DB 86 DA C0 39 5D 9B F2
            6E C1 E6 BA C4 C3 B9 A9
```

After rho

```
03 A3 B6 BF A2 ED EB A7 E7 DB D7 8C BF 2F 5C 3C
27 E8 8C 33 E4 6D BC 7F 39 6D DC 47 C7 C9 F3 95
8B B2 01 E0 95 72 42 CE 7C E0 B8 8F 2C D5 8A 2E
B7 6D C1 04 A3 98 B5 A7 1B B0 A6 51 AF 62 71 EB
8B A3 4B E6 D3 EC 0E B2 A2 86 1F D5 23 40 F6 CE
40 77 5A 88 A0 A4 16 AB 8E 27 E2 81 9B A6 FE 6B
84 AD 14 A2 28 3D 5C 17 E4 6D 09 BF 2F 7C 00 80
4C 80 0E 23 C4 CB F2 F3 8B 4A 8C 36 1B FC 97 E1
68 5C 37 99 EB 73 21 C6 A5 73 42 51 FB 7A C2 7C
5A FD D6 FD E6 1E 82 B6 79 52 0B 04 4A 69 AB 30
D2 98 78 B9 4A 94 F3 CD 7A B8 BE 15 E1 B9 77 FF
1F C4 8C B4 D7 EE 7E C8 86 DA C0 39 5D 9B F2 DB
            6E AA 5B B0 B9 2E F1 70
```

After pi

```
03 A3 B6 BF A2 ED EB A7 B7 6D C1 04 A3 98 B5 A7
84 AD 14 A2 28 3D 5C 17 5A FD D6 FD E6 1E 82 B6
6E AA 5B B0 B9 2E F1 70 39 6D DC 47 C7 C9 F3 95
A2 86 1F D5 23 40 F6 CE 40 77 5A 88 A0 A4 16 AB
68 5C 37 99 EB 73 21 C6 1F C4 8C B4 D7 EE 7E C8
E7 DB D7 8C BF 2F 5C 3C 1B B0 A6 51 AF 62 71 EB
E4 6D 09 BF 2F 7C 00 80 79 52 0B 04 4A 69 AB 30
D2 98 78 B9 4A 94 F3 CD 8B B2 01 E0 95 72 42 CE
7C E0 B8 8F 2C D5 8A 2E 8E 27 E2 81 9B A6 FE 6B
A5 73 42 51 FB 7A C2 7C 86 DA C0 39 5D 9B F2 DB
27 E8 8C 33 E4 6D BC 7F 8B A3 4B E6 D3 EC 0E B2
4C 80 0E 23 C4 CB F2 F3 8B 4A 8C 36 1B FC 97 E1
            7A B8 BE 15 E1 B9 77 FF
```

After chi

```
03 23 A2 1D AA C8 A3 B7 ED 3D 03 59 65 9A 37 07
A0 AF 1D A2 31 1D 2D 57 5B FC 72 F2 E4 DF 88 31
DA E6 1A B0 B8 3E E5 70 79 1C 9C 4F 47 6D F3 B4
8A 8E 3A C4 68 13 D7 8A 57 F7 D2 AC B4 28 48 A3
48 75 67 DA EB 72 A0 D3 9D 46 8F 24 F7 EE 7A 82
03 96 DE 22 BF 33 5C 3C 02 A2 A4 51 EF 63 DA DB
66 E5 79 06 2F E8 50 4D 5C 11 8C 00 FF 42 A7 00
CA B8 58 E8 4A D4 D2 0E 09 B5 43 E0 06 50 36 8F
5D B0 B8 DF 4C 8D 8A 3A 8C AF 62 A9 9F 27 CE E8
```

```
AC 53 43 91 7B 1A C2 78 F2 9A 78 36 75 1E 7A FB
63 E8 88 32 E0 6E 4C 3E 08 E9 CB F2 C8 D8 0B B2
3C 30 3C 22 24 CA 92 ED 8E 0A 8C 14 1F B8 1F E1
            F2 BB FD D1 F2 39 75 7F
```

After iota

```
02 23 A2 1D AA C8 A3 B7 ED 3D 03 59 65 9A 37 07
A0 AF 1D A2 31 1D 2D 57 5B FC 72 F2 E4 DF 88 31
DA E6 1A B0 B8 3E E5 70 79 1C 9C 4F 47 6D F3 B4
8A 8E 3A C4 68 13 D7 8A 57 F7 D2 AC B4 28 48 A3
48 75 67 DA EB 72 A0 D3 9D 46 8F 24 F7 EE 7A 82
03 96 DE 22 BF 33 5C 3C 02 A2 A4 51 EF 63 DA DB
66 E5 79 06 2F E8 50 4D 5C 11 8C 00 FF 42 A7 00
CA B8 58 E8 4A D4 D2 0E 09 B5 43 E0 06 50 36 8F
5D B0 B8 DF 4C 8D 8A 3A 8C AF 62 A9 9F 27 CE E8
AC 53 43 91 7B 1A C2 78 F2 9A 78 36 75 1E 7A FB
63 E8 88 32 E0 6E 4C 3E 08 E9 CB F2 C8 D8 0B B2
3C 30 3C 22 24 CA 92 ED 8E 0A 8C 14 1F B8 1F E1
            F2 BB FD D1 F2 39 75 7F
```

(Skip rounds 1 to 22)

Round #23

After theta

```
09 F3 BB 3C 65 7E 82 3C EF 00 38 23 F6 8E C9 98
72 91 67 37 64 1A 04 F9 FB DB 6B 5A 79 80 81 4A
4B 51 05 7A 71 CC B6 8F 7D 28 B4 85 38 12 31 98
CC 6D 01 50 57 2F 91 49 F9 84 11 A9 73 A4 54 0F
DF A1 88 22 46 AF 38 AA E2 1D 4D 19 09 96 A0 D9
C6 4D 09 A8 4D 58 7A 20 F0 C3 EB 57 78 1A 3B D3
88 50 D7 04 63 E2 E6 54 BD 1B 7D FA 78 8A 4B CD
43 39 45 52 3B 7E D7 A2 55 17 A5 4D 10 CC 2E 39
50 AC CF F1 0E 03 0F 0E 58 7D 18 B1 BA A1 89 E0
24 ED 4C 92 92 90 6B 04 23 5F D5 EC E2 47 AD 9F
98 94 82 64 17 1C 1D FE 85 51 42 86 54 FC BD F3
21 2F EE F3 75 C6 67 DD 9F DB AB 48 97 89 3A 18
            B7 2E B6 63 34 C7 DE 63
```

After rho

```
09 F3 BB 3C 65 7E 82 3C DF 01 70 46 EC 1D 93 31
5C E4 D9 0D 99 06 41 BE 07 18 A8 B4 BF BD A6 95
63 B6 7D 5C 8A 2A D0 8B 88 23 11 83 D9 87 42 5B
00 75 F5 12 99 C4 DC 16 43 3E 61 44 EA 1C 29 D5
50 44 11 A3 57 1C D5 EF 09 9A 2D DE D1 94 91 60
31 6E 4A 40 6D C2 D2 03 4C C3 0F AF 5F E1 69 EC
26 18 13 37 A7 42 84 BA 14 97 9A 7B 37 FA F4 F1
A9 1D BF 6B D1 A1 9C 22 9B 20 98 5D 72 AA 2E 4A
39 DE 61 E0 C1 01 8A F5 44 70 AC 3E 8C 58 DD D0
72 8D 80 A4 9D 49 52 12 9F 23 5F D5 EC E2 47 AD
74 F8 63 52 0A 92 5D 70 17 46 09 19 52 F1 F7 CE
E4 C5 7D BE CE F8 AC 3B DB AB 48 97 89 3A 18 9F
            F7 D8 AD 8B ED 18 CD B1
```

After pi

```
09 F3 BB 3C 65 7E 82 3C 00 75 F5 12 99 C4 DC 16
26 18 13 37 A7 42 84 BA 72 8D 80 A4 9D 49 52 12
F7 D8 AD 8B ED 18 CD B1 07 18 A8 B4 BF BD A6 95
09 9A 2D DE D1 94 91 60 31 6E 4A 40 6D C2 D2 03
39 DE 61 E0 C1 01 8A F5 E4 C5 7D BE CE F8 AC 3B
DF 01 70 46 EC 1D 93 31 43 3E 61 44 EA 1C 29 D5
14 97 9A 7B 37 FA F4 F1 9F 23 5F D5 EC E2 47 AD
74 F8 63 52 0A 92 5D 70 63 B6 7D 5C 8A 2A D0 8B
88 23 11 83 D9 87 42 5B 4C C3 0F AF 5F E1 69 EC
44 70 AC 3E 8C 58 DD D0 DB AB 48 97 89 3A 18 9F
5C E4 D9 0D 99 06 41 BE 50 44 11 A3 57 1C D5 EF
A9 1D BF 6B D1 A1 9C 22 9B 20 98 5D 72 AA 2E 4A
            17 46 09 19 52 F1 F7 CE
```

After chi

```
2F FB B9 19 43 7C 82 94 50 F0 75 92 81 CD 8E 16
A3 48 3E 3C C7 52 09 1B 7A AE 92 90 9D 2F 50 1E
F7 DC E9 89 75 98 91 B3 37 7C EA B4 93 FF E4 96
01 0A 0C 7E 51 95 99 94 F5 6F 56 5E 63 3A F6 09
3A C6 E1 E0 F0 04 88 71 EC 47 78 F4 8E F8 BD 5B
CB 80 EA 7D F9 FF 47 11 C8 1E 24 C0 22 1C 2A D9
74 4F BA 79 35 EA EC A1 14 22 4F D1 08 EF C5 AC
74 C6 62 52 08 92 75 B4 27 76 73 70 8C 4A F9 2F
88 13 B1 93 59 9F D6 4B D7 48 4F 2E 5E C3 69 E3
64 64 99 76 8E 58 1D D0 53 AA 48 14 D8 BF 1A CF
F5 FD 77 45 19 A7 49 BE 42 64 11 B7 75 16 F7 A7
AD 5B BE 6B D1 F0 4D A6 D3 80 48 59 FB AC 2E 7A
            17 46 09 BB 14 E9 63 8F
```

After iota

```
27 7B B9 99 43 7C 82 14 50 F0 75 92 81 CD 8E 16
A3 48 3E 3C C7 52 09 1B 7A AE 92 90 9D 2F 50 1E
F7 DC E9 89 75 98 91 B3 37 7C EA B4 93 FF E4 96
01 0A 0C 7E 51 95 99 94 F5 6F 56 5E 63 3A F6 09
3A C6 E1 E0 F0 04 88 71 EC 47 78 F4 8E F8 BD 5B
CB 80 EA 7D F9 FF 47 11 C8 1E 24 C0 22 1C 2A D9
74 4F BA 79 35 EA EC A1 14 22 4F D1 08 EF C5 AC
74 C6 62 52 08 92 75 B4 27 76 73 70 8C 4A F9 2F
88 13 B1 93 59 9F D6 4B D7 48 4F 2E 5E C3 69 E3
64 64 99 76 8E 58 1D D0 53 AA 48 14 D8 BF 1A CF
F5 FD 77 45 19 A7 49 BE 42 64 11 B7 75 16 F7 A7
AD 5B BE 6B D1 F0 4D A6 D3 80 48 59 FB AC 2E 7A
            17 46 09 BB 14 E9 63 8F
```

After permutation

```
27 7B B9 99 43 7C 82 14 50 F0 75 92 81 CD 8E 16
A3 48 3E 3C C7 52 09 1B 7A AE 92 90 9D 2F 50 1E
F7 DC E9 89 75 98 91 B3 37 7C EA B4 93 FF E4 96
01 0A 0C 7E 51 95 99 94 F5 6F 56 5E 63 3A F6 09
3A C6 E1 E0 F0 04 88 71 EC 47 78 F4 8E F8 BD 5B
CB 80 EA 7D F9 FF 47 11 C8 1E 24 C0 22 1C 2A D9
74 4F BA 79 35 EA EC A1 14 22 4F D1 08 EF C5 AC
74 C6 62 52 08 92 75 B4 27 76 73 70 8C 4A F9 2F
88 13 B1 93 59 9F D6 4B D7 48 4F 2E 5E C3 69 E3
```

```
64 64 99 76 8E 58 1D D0 53 AA 48 14 D8 BF 1A CF
F5 FD 77 45 19 A7 49 BE 42 64 11 B7 75 16 F7 A7
AD 5B BE 6B D1 F0 4D A6 D3 80 48 59 FB AC 2E 7A
            17 46 09 BB 14 E9 63 8F
```

State (as lanes of integers)

```
[0, 0] = 14827c4399b97b27
[1, 0] = 168ecd819275f050
[2, 0] = 1b0952c73c3e48a3
[3, 0] = 1e502f9d9092ae7a
[4, 0] = b391987589e9dcf7
[0, 1] = 96e4ff93b4ea7c37
[1, 1] = 949995517e0c0a01
[2, 1] = 09f63a635e566ff5
[3, 1] = 718804f0e0e1c63a
[4, 1] = 5bbdf88ef47847ec
[0, 2] = 1147fff97dea80cb
[1, 2] = d92a1c22c0241ec8
[2, 2] = a1ecea3579ba4f74
[3, 2] = acc5ef08d14f2214
[4, 2] = b47592085262c674
[0, 3] = 2ff94a8c70737627
[1, 3] = 4bd69f5993b11388
[2, 3] = e369c35e2e4f48d7
[3, 3] = d01d588e76996464
[4, 3] = cf1abfd81448aa53
[0, 4] = be49a7194577fdf5
[1, 4] = a7f71675b7116442
[2, 4] = a64df0d16bbe5bad
[3, 4] = 7a2eacfb594880d3
[4, 4] = 8f63e914bb094617
```

About to call squeeze (again)

State before permutation (in bytes)

```
27 7B B9 99 43 7C 82 14 50 F0 75 92 81 CD 8E 16
A3 48 3E 3C C7 52 09 1B 7A AE 92 90 9D 2F 50 1E
F7 DC E9 89 75 98 91 B3 37 7C EA B4 93 FF E4 96
01 0A 0C 7E 51 95 99 94 F5 6F 56 5E 63 3A F6 09
3A C6 E1 E0 F0 04 88 71 EC 47 78 F4 8E F8 BD 5B
CB 80 EA 7D F9 FF 47 11 C8 1E 24 C0 22 1C 2A D9
74 4F BA 79 35 EA EC A1 14 22 4F D1 08 EF C5 AC
74 C6 62 52 08 92 75 B4 27 76 73 70 8C 4A F9 2F
88 13 B1 93 59 9F D6 4B D7 48 4F 2E 5E C3 69 E3
64 64 99 76 8E 58 1D D0 53 AA 48 14 D8 BF 1A CF
F5 FD 77 45 19 A7 49 BE 42 64 11 B7 75 16 F7 A7
AD 5B BE 6B D1 F0 4D A6 D3 80 48 59 FB AC 2E 7A
            17 46 09 BB 14 E9 63 8F
```

State before permutation (as lanes of integers)

```
[0, 0] = 14827c4399b97b27
[1, 0] = 168ecd819275f050
[2, 0] = 1b0952c73c3e48a3
[3, 0] = 1e502f9d9092ae7a
[4, 0] = b391987589e9dcf7
```

```
[0, 1] = 96e4ff93b4ea7c37
[1, 1] = 949995517e0c0a01
[2, 1] = 09f63a635e566ff5
[3, 1] = 718804f0e0e1c63a
[4, 1] = 5bbdf88ef47847ec
[0, 2] = 1147fff97dea80cb
[1, 2] = d92a1c22c0241ec8
[2, 2] = a1ecea3579ba4f74
[3, 2] = acc5ef08d14f2214
[4, 2] = b47592085262c674
[0, 3] = 2ff94a8c70737627
[1, 3] = 4bd69f5993b11388
[2, 3] = e369c35e2e4f48d7
[3, 3] = d01d588e76996464
[4, 3] = cf1abfd81448aa53
[0, 4] = be49a7194577fdf5
[1, 4] = a7f71675b7116442
[2, 4] = a64df0d16bbe5bad
[3, 4] = 7a2eacfb594880d3
[4, 4] = 8f63e914bb094617
```

Round #0

After theta

```
AB EC F0 08 C0 43 9B 66 E8 0A 8E 4B 01 3E 70 F8
36 86 18 29 38 FF 49 7E 74 B7 D4 CF FC D6 26 D0
06 6A 7E CC 1D 8B 9C DF BB EB A3 25 10 C0 FD E4
B9 F0 F7 A7 D1 66 67 7A 60 A1 70 4B 9C 97 B6 6C
34 DF A7 BF 91 FD FE BF 1D F1 EF B1 E6 EB B0 37
47 17 A3 EC 7A C0 5E 63 70 E4 DF 19 A2 EF D4 37
E1 81 9C 6C CA 47 AC C4 1A 3B 09 8E 69 16 B3 62
85 70 F5 17 60 81 78 D8 AB E1 3A E1 0F 75 E0 5D
30 E9 4A 4A D9 6C 28 A5 42 86 69 3B A1 6E 29 86
6A 7D DF 29 EF A1 6B 1E A2 1C DF 51 B0 AC 17 A3
79 6A 3E D4 9A 98 50 CC FA 9E EA 6E F5 E5 09 49
38 95 98 7E 2E 5D 0D C3 DD 99 0E 06 9A 55 58 B4
            E6 F0 9E FE 7C FA 6E E3
```

After rho

```
AB EC F0 08 C0 43 9B 66 D1 15 1C 97 02 7C E0 F0
8D 21 46 0A CE 7F 92 9F 6F 6D 02 4D 77 4B FD CC
58 E4 FC 36 50 F3 63 EE 02 01 DC 4F BE BB 3E 5A
7F 1A 6D 76 A6 97 0B 7F 1B 58 28 DC 12 E7 A5 2D
EF D3 DF C8 7E FF 5F 9A 0E 7B D3 11 FF 1E 6B BE
3B BA 18 65 D7 03 F6 1A DF C0 91 7F 67 88 BE 53
64 53 3E 62 25 0E 0F E4 2C 66 C5 34 76 12 1C D3
0B B0 40 3C EC 42 B8 FA C2 1F EA C0 BB 56 C3 75
49 29 9B 0D A5 14 26 5D 14 43 21 C3 B4 9D 50 B7
74 CD 43 AD EF 3B E5 3D A3 A2 1C DF 51 B0 AC 17
42 31 E7 A9 F9 50 6B 62 E9 7B AA BB D5 97 27 24
A7 12 D3 CF A5 AB 61 18 99 0E 06 9A 55 58 B4 DD
            DB B8 39 BC A7 3F 9F BE
```

After pi

```
AB EC F0 08 C0 43 9B 66 7F 1A 6D 76 A6 97 0B 7F
64 53 3E 62 25 0E 0F E4 74 CD 43 AD EF 3B E5 3D
DB B8 39 BC A7 3F 9F BE 6F 6D 02 4D 77 4B FD CC
0E 7B D3 11 FF 1E 6B BE 3B BA 18 65 D7 03 F6 1A
49 29 9B 0D A5 14 26 5D A7 12 D3 CF A5 AB 61 18
D1 15 1C 97 02 7C E0 F0 1B 58 28 DC 12 E7 A5 2D
2C 66 C5 34 76 12 1C D3 A3 A2 1C DF 51 B0 AC 17
42 31 E7 A9 F9 50 6B 62 58 E4 FC 36 50 F3 63 EE
02 01 DC 4F BE BB 3E 5A DF C0 91 7F 67 88 BE 53
14 43 21 C3 B4 9D 50 B7 99 0E 06 9A 55 58 B4 DD
8D 21 46 0A CE 7F 92 9F EF D3 DF C8 7E FF 5F 9A
0B B0 40 3C EC 42 B8 FA C2 1F EA C0 BB 56 C3 75
            E9 7B AA BB D5 97 27 24
```

After chi

```
AB AD E2 08 C1 4B 9F E6 6F 96 2C FB 6C A6 EB 66
EF 63 06 72 25 0A 15 66 54 89 83 AD AF 7B E5 7D
8F AA 34 CA 81 AB 9F A7 5E ED 0A 29 77 4A 69 CC
4E 7A 50 19 DF 0A 6B FB 9D A8 58 A7 D7 A8 B7 1A
01 44 9B 0D F7 54 BA 99 A7 00 02 DF 2D BF 63 2A
F5 33 D9 B7 66 6C F8 22 98 D8 30 17 13 47 05 29
6C 77 26 14 DE 52 5F B3 32 A6 04 C9 53 9C 2C 87
48 79 C7 E1 E9 D3 6E 6F 85 24 FD 06 11 F3 E3 EF
02 02 FC CF 2E AE 7E FE 56 CC 97 67 26 C8 1A 1B
54 A3 D9 E7 B4 3E 13 95 9B 0F 06 D3 FB 50 A8 CD
8D 01 46 3E 4E 7F 32 FF 2F DC 75 08 6D EB 1C 9F
22 D0 40 07 A8 C3 9C FA C6 1F AE C0 B1 3E 53 EE
            8B A9 33 7B E5 17 6A 24
```

After iota

```
AA AD E2 08 C1 4B 9F E6 6F 96 2C FB 6C A6 EB 66
EF 63 06 72 25 0A 15 66 54 89 83 AD AF 7B E5 7D
8F AA 34 CA 81 AB 9F A7 5E ED 0A 29 77 4A 69 CC
4E 7A 50 19 DF 0A 6B FB 9D A8 58 A7 D7 A8 B7 1A
01 44 9B 0D F7 54 BA 99 A7 00 02 DF 2D BF 63 2A
F5 33 D9 B7 66 6C F8 22 98 D8 30 17 13 47 05 29
6C 77 26 14 DE 52 5F B3 32 A6 04 C9 53 9C 2C 87
48 79 C7 E1 E9 D3 6E 6F 85 24 FD 06 11 F3 E3 EF
02 02 FC CF 2E AE 7E FE 56 CC 97 67 26 C8 1A 1B
54 A3 D9 E7 B4 3E 13 95 9B 0F 06 D3 FB 50 A8 CD
8D 01 46 3E 4E 7F 32 FF 2F DC 75 08 6D EB 1C 9F
22 D0 40 07 A8 C3 9C FA C6 1F AE C0 B1 3E 53 EE
            8B A9 33 7B E5 17 6A 24
```

(Skip rounds 1 to 22)

Round #23

After theta

```
6E E1 47 C1 F8 67 26 A8 EA D9 BA EA 82 E2 64 DC
15 5A 0C 64 0B 10 3F CA 05 64 49 91 73 CE 88 43
09 1F 7C A5 A1 B6 3E 1E FD 70 27 85 1B 63 8B 44
F5 0E F7 9F 6A 76 8F CE 9D CC F6 66 6A 4F 28 C2
04 99 7D 3D 06 C9 AD 4B E7 EF 86 0A 91 1A 76 9F
37 58 7F E7 98 74 3B 4B 27 53 05 7E AF EC 1C 78
16 56 09 A2 C6 0C 74 D3 66 72 25 BE 53 A9 82 5A
```

```
94 FB 83 EF D1 DC 63 8A E6 96 2A D7 E1 79 4A 75
E4 A9 E7 E1 25 27 7A 79 6E EB 1F 39 F0 67 39 8B
FD 13 D6 B3 D0 6E A7 F1 DF 06 4A EA 4D 3C 0E 3F
16 80 59 7C 83 4B 43 BB FD 13 03 C0 F8 BA 92 F4
71 52 21 92 2F 61 23 F8 0B 4D C9 14 A4 0F CE E1
            F6 AF A3 8E A4 15 A5 B4
```

After rho

```
6E E1 47 C1 F8 67 26 A8 D5 B3 75 D5 05 C5 C9 B8
85 16 03 D9 02 C4 8F 72 E7 8C 38 54 40 96 14 39
B5 F5 F1 48 F8 E0 2B 0D B8 31 B6 48 D4 0F 77 52
FF A9 66 F7 E8 5C EF 70 70 27 B3 BD 99 DA 13 8A
CC BE 1E 83 E4 D6 25 82 61 F7 79 FE 6E A8 10 A9
BA C1 FA 3B C7 A4 DB 59 E0 9D 4C 15 F8 BD B2 73
10 35 66 A0 9B B6 B0 4A 52 05 B5 CC E4 4A 7C A7
F7 68 EE 31 45 CA FD C1 AE C3 F3 94 EA CC 2D 55
3C BC E4 44 2F 8F 3C F5 9C 45 B7 F5 8F 1C F8 B3
ED 34 BE 7F C2 7A 16 DA 3F DF 06 4A EA 4D 3C 0E
0D ED 5A 00 66 F1 0D 2E F7 4F 0C 00 E3 EB 4A D2
4E 2A 44 F2 25 6C 04 3F 4D C9 14 A4 0F CE E1 0B
            29 AD FD EB A8 23 69 45
```

After pi

```
6E E1 47 C1 F8 67 26 A8 FF A9 66 F7 E8 5C EF 70
10 35 66 A0 9B B6 B0 4A ED 34 BE 7F C2 7A 16 DA
29 AD FD EB A8 23 69 45 E7 8C 38 54 40 96 14 39
61 F7 79 FE 6E A8 10 A9 BA C1 FA 3B C7 A4 DB 59
3C BC E4 44 2F 8F 3C F5 4E 2A 44 F2 25 6C 04 3F
D5 B3 75 D5 05 C5 C9 B8 70 27 B3 BD 99 DA 13 8A
52 05 B5 CC E4 4A 7C A7 3F DF 06 4A EA 4D 3C 0E
0D ED 5A 00 66 F1 0D 2E B5 F5 F1 48 F8 E0 2B 0D
B8 31 B6 48 D4 0F 77 52 E0 9D 4C 15 F8 BD B2 73
9C 45 B7 F5 8F 1C F8 B3 4D C9 14 A4 0F CE E1 0B
85 16 03 D9 02 C4 8F 72 CC BE 1E 83 E4 D6 25 82
F7 68 EE 31 45 CA FD C1 AE C3 F3 94 EA CC 2D 55
            F7 4F 0C 00 E3 EB 4A D2
```

After chi

```
6E F5 47 C1 EB C5 36 A2 12 A9 FE A8 A8 14 E9 E0
10 BC 27 20 B3 B7 D9 4F AB 74 BC 7F 92 3E 10 72
B8 A5 DD DD A8 3B A0 15 7D 8C BA 55 C1 92 DF 69
65 CB 7D BA 46 A3 34 0D F8 C3 FA 89 C7 C4 DB 53
9D 38 DC 40 6F 1D 2C F5 4E 59 05 58 0B 44 04 BF
D7 B3 71 95 61 C5 A5 9D 5D FD B1 BF 93 DF 13 82
52 25 ED CC E0 FA 7D 87 EF CD 23 9F EB 49 FC 9E
2D E9 D8 28 FE EB 1F 2C F5 79 B9 5D D0 50 AB 2C
A4 71 05 A8 D3 0F 3F D2 A1 15 4C 15 F8 7F B3 7B
2C 71 56 BD 7F 3C F2 B7 45 C9 12 A4 0B C1 B5 59
B6 56 E3 E9 03 CC 57 33 C4 3D 0F 07 4E D2 25 96
A6 64 E2 31 44 E9 BF 43 AE D3 F0 4D EA C8 A8 75
            BF E7 10 02 07 F9 6A 52
```

After iota

```
66 75 47 41 EB C5 36 22 12 A9 FE A8 A8 14 E9 E0
10 BC 27 20 B3 B7 D9 4F AB 74 BC 7F 92 3E 10 72
B8 A5 DD DD A8 3B A0 15 7D 8C BA 55 C1 92 DF 69
65 CB 7D BA 46 A3 34 0D F8 C3 FA 89 C7 C4 DB 53
```

```
9D 38 DC 40 6F 1D 2C F5 4E 59 05 58 0B 44 04 BF
D7 B3 71 95 61 C5 A5 9D 5D FD B1 BF 93 DF 13 82
52 25 ED CC E0 FA 7D 87 EF CD 23 9F EB 49 FC 9E
2D E9 D8 28 FE EB 1F 2C F5 79 B9 5D D0 50 AB 2C
A4 71 05 A8 D3 0F 3F D2 A1 15 4C 15 F8 7F B3 7B
2C 71 56 BD 7F 3C F2 B7 45 C9 12 A4 0B C1 B5 59
B6 56 E3 E9 03 CC 57 33 C4 3D 0F 07 4E D2 25 96
A6 64 E2 31 44 E9 BF 43 AE D3 F0 4D EA C8 A8 75
            BF E7 10 02 07 F9 6A 52
```

After permutation

```
66 75 47 41 EB C5 36 22 12 A9 FE A8 A8 14 E9 E0
10 BC 27 20 B3 B7 D9 4F AB 74 BC 7F 92 3E 10 72
B8 A5 DD DD A8 3B A0 15 7D 8C BA 55 C1 92 DF 69
65 CB 7D BA 46 A3 34 0D F8 C3 FA 89 C7 C4 DB 53
9D 38 DC 40 6F 1D 2C F5 4E 59 05 58 0B 44 04 BF
D7 B3 71 95 61 C5 A5 9D 5D FD B1 BF 93 DF 13 82
52 25 ED CC E0 FA 7D 87 EF CD 23 9F EB 49 FC 9E
2D E9 D8 28 FE EB 1F 2C F5 79 B9 5D D0 50 AB 2C
A4 71 05 A8 D3 0F 3F D2 A1 15 4C 15 F8 7F B3 7B
2C 71 56 BD 7F 3C F2 B7 45 C9 12 A4 0B C1 B5 59
B6 56 E3 E9 03 CC 57 33 C4 3D 0F 07 4E D2 25 96
A6 64 E2 31 44 E9 BF 43 AE D3 F0 4D EA C8 A8 75
            BF E7 10 02 07 F9 6A 52
```

State (as lanes of integers)

```
[0, 0] = 2236c5eb41477566
[1, 0] = e0e914a8a8fea912
[2, 0] = 4fd9b7b32027bc10
[3, 0] = 72103e927fbc74ab
[4, 0] = 15a03ba8dddda5b8
[0, 1] = 69df92c155ba8c7d
[1, 1] = 0d34a346ba7dcb65
[2, 1] = 53dbc4c789fac3f8
[3, 1] = f52c1d6f40dc389d
[4, 1] = bf04440b5805594e
[0, 2] = 9da5c5619571b3d7
[1, 2] = 8213df93bfb1fd5d
[2, 2] = 877dfae0cced2552
[3, 2] = 9efc49eb9f23cdef
[4, 2] = 2c1febfe28d8e92d
[0, 3] = 2cab50d05db979f5
[1, 3] = d23f0fd3a80571a4
[2, 3] = 7bb37ff8154c15a1
[3, 3] = b7f23c7fbd56712c
[4, 3] = 59b5c10ba412c945
[0, 4] = 3357cc03e9e356b6
[1, 4] = 9625d24e070f3dc4
[2, 4] = 43bfe94431e264a6
[3, 4] = 75a8c8ea4df0d3ae
[4, 4] = 526af9070210e7bf
```

About to call squeeze (again)

State before permutation (in bytes)

```
66 75 47 41 EB C5 36 22 12 A9 FE A8 A8 14 E9 E0
10 BC 27 20 B3 B7 D9 4F AB 74 BC 7F 92 3E 10 72
B8 A5 DD DD A8 3B A0 15 7D 8C BA 55 C1 92 DF 69
65 CB 7D BA 46 A3 34 0D F8 C3 FA 89 C7 C4 DB 53
9D 38 DC 40 6F 1D 2C F5 4E 59 05 58 0B 44 04 BF
D7 B3 71 95 61 C5 A5 9D 5D FD B1 BF 93 DF 13 82
52 25 ED CC E0 FA 7D 87 EF CD 23 9F EB 49 FC 9E
2D E9 D8 28 FE EB 1F 2C F5 79 B9 5D D0 50 AB 2C
A4 71 05 A8 D3 0F 3F D2 A1 15 4C 15 F8 7F B3 7B
2C 71 56 BD 7F 3C F2 B7 45 C9 12 A4 0B C1 B5 59
B6 56 E3 E9 03 CC 57 33 C4 3D 0F 07 4E D2 25 96
A6 64 E2 31 44 E9 BF 43 AE D3 F0 4D EA C8 A8 75
            BF E7 10 02 07 F9 6A 52
```

State before permutation (as lanes of integers)

```
[0, 0] = 2236c5eb41477566
[1, 0] = e0e914a8a8fea912
[2, 0] = 4fd9b7b32027bc10
[3, 0] = 72103e927fbc74ab
[4, 0] = 15a03ba8dddda5b8
[0, 1] = 69df92c155ba8c7d
[1, 1] = 0d34a346ba7dcb65
[2, 1] = 53dbc4c789fac3f8
[3, 1] = f52c1d6f40dc389d
[4, 1] = bf04440b5805594e
[0, 2] = 9da5c5619571b3d7
[1, 2] = 8213df93bfb1fd5d
[2, 2] = 877dfae0cced2552
[3, 2] = 9efc49eb9f23cdef
[4, 2] = 2c1febfe28d8e92d
[0, 3] = 2cab50d05db979f5
[1, 3] = d23f0fd3a80571a4
[2, 3] = 7bb37ff8154c15a1
[3, 3] = b7f23c7fbd56712c
[4, 3] = 59b5c10ba412c945
[0, 4] = 3357cc03e9e356b6
[1, 4] = 9625d24e070f3dc4
[2, 4] = 43bfe94431e264a6
[3, 4] = 75a8c8ea4df0d3ae
[4, 4] = 526af9070210e7bf
```

Round #0

After theta

```
D3 E8 34 4E 7A 02 FB F8 E6 9B 14 1E 60 24 BF 6F
ED 29 D5 83 55 3F 38 D3 55 29 26 28 18 79 AA CB
FC 4D 94 E6 1B B8 5A 5D C8 11 C9 5A 50 55 12 B3
91 F9 97 0C 8E 93 62 82 05 56 08 2A 21 4C 3A CF
63 65 46 17 E5 5A 96 4C 0A B1 4C 63 B8 C7 FE F7
62 2E 02 9A F0 02 68 47 A9 CF 5B 09 5B EF 45 0D
AF B0 1F 6F 06 72 9C 1B 11 90 B9 C8 61 0E 46 27
69 01 91 13 4D 68 E5 64 40 E4 CA 52 41 97 66 F6
50 43 EF 1E 1B 3F 69 5D 5C 80 BE B6 1E F7 52 E7
```

```
D2 2C CC EA F5 7B 48 0E 01 21 5B 9F B8 42 4F 11
03 CB 90 E6 92 0B 9A E9 30 0F E5 B1 86 E2 73 19
5B F1 10 92 A2 61 5E DF 50 8E 6A 1A 60 8F 12 CC
            FB 0F 59 39 B4 7A 90 1A
```

After rho

```
D3 E8 34 4E 7A 02 FB F8 CC 37 29 3C C0 48 7E DF
7B 4A F5 60 D5 0F CE 74 91 A7 BA 5C 95 62 82 82
C0 D5 EA E2 6F A2 34 DF 05 55 25 31 8B 1C 91 AC
C9 E0 38 29 26 18 99 7F 73 81 15 82 4A 08 93 CE
32 A3 8B 72 2D 4B A6 B1 EC 7F AF 10 CB 34 86 7B
12 73 11 D0 84 17 40 3B 35 A4 3E 6F 25 6C BD 17
78 33 90 E3 DC 78 85 FD 1C 8C 4E 22 20 73 91 C3
89 26 B4 72 B2 B4 80 C8 A5 82 2E CD EC 81 C8 95
DD 63 E3 27 AD 0B 6A E8 A9 73 2E 40 5F 5B 8F 7B
0F C9 41 9A 85 59 BD 7E 11 01 21 5B 9F B8 42 4F
68 A6 0F 2C 43 9A 4B 2E C0 3C 94 C7 1A 8A CF 65
2B 1E 42 52 34 CC EB 7B 8E 6A 1A 60 8F 12 CC 50
            A4 C6 FE 43 56 0E AD 1E
```

After pi

```
D3 E8 34 4E 7A 02 FB F8 C9 E0 38 29 26 18 99 7F
78 33 90 E3 DC 78 85 FD 0F C9 41 9A 85 59 BD 7E
A4 C6 FE 43 56 0E AD 1E 91 A7 BA 5C 95 62 82 82
EC 7F AF 10 CB 34 86 7B 12 73 11 D0 84 17 40 3B
DD 63 E3 27 AD 0B 6A E8 2B 1E 42 52 34 CC EB 7B
CC 37 29 3C C0 48 7E DF 73 81 15 82 4A 08 93 CE
1C 8C 4E 22 20 73 91 C3 11 01 21 5B 9F B8 42 4F
68 A6 0F 2C 43 9A 4B 2E C0 D5 EA E2 6F A2 34 DF
05 55 25 31 8B 1C 91 AC 35 A4 3E 6F 25 6C BD 17
A9 73 2E 40 5F 5B 8F 7B 8E 6A 1A 60 8F 12 CC 50
7B 4A F5 60 D5 0F CE 74 32 A3 8B 72 2D 4B A6 B1
89 26 B4 72 B2 B4 80 C8 A5 82 2E CD EC 81 C8 95
            C0 3C 94 C7 1A 8A CF 65
```

After chi

```
E3 FB B4 8C A2 62 FF 78 CE 28 79 31 27 19 A1 7D
D8 35 2E A2 8E 7E 85 FD 5C E1 41 96 AD 59 EF 9E
AC C6 F6 62 52 16 AD 19 83 A7 AA 9C 91 61 C2 82
21 7F 4D 37 E2 3C AC BB 30 6F 11 80 94 D3 C1 28
4D C2 5B 2B 2C 29 6A 68 47 46 47 52 7E D8 EF 02
C0 3B 63 1C E0 3B 7E DE 72 80 34 DB D5 80 D1 C2
74 2A 40 06 60 71 98 E3 95 10 01 4B 1F F8 76 9E
5B 26 1B AE 49 9A CA 2E F0 75 F0 AC 4B C2 18 CC
8D 06 25 31 D1 0F 93 C4 33 AC 2E 4F A5 6C FD 17
E9 E6 CE C2 3F FB BF F4 8B 6A 1F 71 0F 0E 4D 70
F2 4E C1 60 47 BB CE 3C 16 23 81 FF 61 4A EE A4
C9 1A 24 70 A0 BE 87 A8 9E C0 4F ED 29 84 C8 85
            C0 9D 9E D5 32 CA EF E4
```

After iota

```
E2 FB B4 8C A2 62 FF 78 CE 28 79 31 27 19 A1 7D
D8 35 2E A2 8E 7E 85 FD 5C E1 41 96 AD 59 EF 9E
AC C6 F6 62 52 16 AD 19 83 A7 AA 9C 91 61 C2 82
21 7F 4D 37 E2 3C AC BB 30 6F 11 80 94 D3 C1 28
4D C2 5B 2B 2C 29 6A 68 47 46 47 52 7E D8 EF 02
C0 3B 63 1C E0 3B 7E DE 72 80 34 DB D5 80 D1 C2
```

```
74 2A 40 06 60 71 98 E3 95 10 01 4B 1F F8 76 9E
5B 26 1B AE 49 9A CA 2E F0 75 F0 AC 4B C2 18 CC
8D 06 25 31 D1 0F 93 C4 33 AC 2E 4F A5 6C FD 17
E9 E6 CE C2 3F FB BF F4 8B 6A 1F 71 0F 0E 4D 70
F2 4E C1 60 47 BB CE 3C 16 23 81 FF 61 4A EE A4
C9 1A 24 70 A0 BE 87 A8 9E C0 4F ED 29 84 C8 85
            C0 9D 9E D5 32 CA EF E4
```

(Skip rounds 1 to 22)

Round #23

After theta

```
F9 F3 31 CD DE 7F AA 7C C7 29 EA 3A 25 16 46 21
D9 DC 2A 68 AB 06 96 C9 EA AE EB A0 89 44 A1 DF
FE A3 F1 85 FB 75 44 07 74 0B F5 B6 28 5C C2 D8
31 35 63 38 F6 C6 FE 3D 49 80 BE 20 6E EB 7A 7F
8D 5B 31 30 16 E5 3F 80 99 83 69 F0 DF D0 C1 32
C0 7C A7 42 18 2A 3E 57 DB 05 6F C2 91 67 0C 0A
D1 9D 32 23 6F 9F AF 67 28 4B 65 DC 19 C2 90 EC
08 4D 57 4A F3 90 A8 80 2E 3C 8C 93 E9 F6 8C 7D
3E 4B 4D CB 2C 79 65 62 51 1E E0 AC 22 DC B3 71
15 17 78 27 F0 30 55 4D 13 12 29 98 84 75 7D E5
83 00 8C 30 62 77 FB D5 E0 5C EA 1E 67 2D 74 A2
F0 51 87 FE C8 E8 5F BD 08 9D 84 2D 3A 0C BC 55
            CE 9E EC 8C BE 08 98 D0
```

After rho

```
F9 F3 31 CD DE 7F AA 7C 8E 53 D4 75 4A 2C 8C 42
36 B7 0A DA AA 81 65 72 48 14 FA AD EE BA 0E 9A
AF 23 3A F0 1F 8D 2F DC 8B C2 25 8C 4D B7 50 6F
86 63 6F EC DF 13 53 33 5F 12 A0 2F 88 DB BA DE
AD 18 18 8B F2 1F C0 C6 1D 2C 93 39 98 06 FF 0D
02 E6 3B 15 C2 50 F1 B9 28 6C 17 BC 09 47 9E 31
19 79 FB 7C 3D 8B EE 94 84 21 D9 51 96 CA B8 33
A5 79 48 54 40 84 A6 2B 27 D3 ED 19 FB 5C 78 18
69 99 25 AF 4C CC 67 A9 D9 B8 28 0F 70 56 11 EE
A6 AA A9 E2 02 EF 04 1E E5 13 12 29 98 84 75 7D
ED 57 0F 02 30 C2 88 DD 82 73 A9 7B 9C B5 D0 89
3E EA D0 1F 19 FD AB 17 9D 84 2D 3A 0C BC 55 08
            26 B4 B3 27 3B A3 2F 02
```

After pi

```
F9 F3 31 CD DE 7F AA 7C 86 63 6F EC DF 13 53 33
19 79 FB 7C 3D 8B EE 94 A6 AA A9 E2 02 EF 04 1E
26 B4 B3 27 3B A3 2F 02 48 14 FA AD EE BA 0E 9A
1D 2C 93 39 98 06 FF 0D 02 E6 3B 15 C2 50 F1 B9
69 99 25 AF 4C CC 67 A9 3E EA D0 1F 19 FD AB 17
8E 53 D4 75 4A 2C 8C 42 5F 12 A0 2F 88 DB BA DE
84 21 D9 51 96 CA B8 33 E5 13 12 29 98 84 75 7D
ED 57 0F 02 30 C2 88 DD AF 23 3A F0 1F 8D 2F DC
8B C2 25 8C 4D B7 50 6F 28 6C 17 BC 09 47 9E 31
D9 B8 28 0F 70 56 11 EE 9D 84 2D 3A 0C BC 55 08
36 B7 0A DA AA 81 65 72 AD 18 18 8B F2 1F C0 C6
A5 79 48 54 40 84 A6 2B 27 D3 ED 19 FB 5C 78 18
            82 73 A9 7B 9C B5 D0 89
```

After chi

```
E0 EB A1 DD FE F7 06 F8 20 E1 6F 6E DD 77 53 39
19 6D E9 79 04 8B C5 94 7F E9 A9 2A C6 B3 84 62
20 B4 FD 07 3A A3 7E 01 4A D6 D2 A9 AC EA 0E 2A
74 35 97 93 94 8A F9 0D 14 84 EB 05 D3 61 79 AF
29 8D 0F 0F AA CE 63 21 2B C2 D1 0F 09 F9 5A 12
0E 72 8D 25 5C 2C 8C 63 3E 00 A2 07 80 DF FF 92
8C 65 D4 53 B6 88 30 B3 E7 13 C2 5C D2 A8 71 7F
BC 57 2F 08 B0 11 BA 41 8F 0F 28 C0 1F CD A1 CC
5A 52 0D 8F 3D A7 51 A1 2C 68 12 8C 05 EF DA 31
FB 9B 3A CF 63 57 3B 3A 9D 44 28 36 4C 8E 05 2B
36 D6 4A 8E AA 01 43 5B AF 9A BD 82 49 47 98 D6
25 59 48 36 44 25 26 AA 13 57 EF 99 D9 5C 5D 6A
            0B 7B B9 7A CC AB 50 0D
```

After iota

```
E8 6B A1 5D FE F7 06 78 20 E1 6F 6E DD 77 53 39
19 6D E9 79 04 8B C5 94 7F E9 A9 2A C6 B3 84 62
20 B4 FD 07 3A A3 7E 01 4A D6 D2 A9 AC EA 0E 2A
74 35 97 93 94 8A F9 0D 14 84 EB 05 D3 61 79 AF
29 8D 0F 0F AA CE 63 21 2B C2 D1 0F 09 F9 5A 12
0E 72 8D 25 5C 2C 8C 63 3E 00 A2 07 80 DF FF 92
8C 65 D4 53 B6 88 30 B3 E7 13 C2 5C D2 A8 71 7F
BC 57 2F 08 B0 11 BA 41 8F 0F 28 C0 1F CD A1 CC
5A 52 0D 8F 3D A7 51 A1 2C 68 12 8C 05 EF DA 31
FB 9B 3A CF 63 57 3B 3A 9D 44 28 36 4C 8E 05 2B
36 D6 4A 8E AA 01 43 5B AF 9A BD 82 49 47 98 D6
25 59 48 36 44 25 26 AA 13 57 EF 99 D9 5C 5D 6A
            0B 7B B9 7A CC AB 50 0D
```

After permutation

```
E8 6B A1 5D FE F7 06 78 20 E1 6F 6E DD 77 53 39
19 6D E9 79 04 8B C5 94 7F E9 A9 2A C6 B3 84 62
20 B4 FD 07 3A A3 7E 01 4A D6 D2 A9 AC EA 0E 2A
74 35 97 93 94 8A F9 0D 14 84 EB 05 D3 61 79 AF
29 8D 0F 0F AA CE 63 21 2B C2 D1 0F 09 F9 5A 12
0E 72 8D 25 5C 2C 8C 63 3E 00 A2 07 80 DF FF 92
8C 65 D4 53 B6 88 30 B3 E7 13 C2 5C D2 A8 71 7F
BC 57 2F 08 B0 11 BA 41 8F 0F 28 C0 1F CD A1 CC
5A 52 0D 8F 3D A7 51 A1 2C 68 12 8C 05 EF DA 31
FB 9B 3A CF 63 57 3B 3A 9D 44 28 36 4C 8E 05 2B
36 D6 4A 8E AA 01 43 5B AF 9A BD 82 49 47 98 D6
25 59 48 36 44 25 26 AA 13 57 EF 99 D9 5C 5D 6A
            0B 7B B9 7A CC AB 50 0D
```

State (as lanes of integers)

```
[0, 0] = 7806f7fe5da16be8
[1, 0] = 395377dd6e6fe120
[2, 0] = 94c58b0479e96d19
[3, 0] = 6284b3c62aa9e97f
[4, 0] = 017ea33a07fdb420
[0, 1] = 2a0eeaaca9d2d64a
[1, 1] = 0df98a9493973574
[2, 1] = af7961d305eb8414
```

```
[3, 1] = 2163ceaa0f0f8d29
[4, 1] = 125af9090fd1c22b
[0, 2] = 638c2c5c258d720e
[1, 2] = 92ffdf8007a2003e
[2, 2] = b33088b653d4658c
[3, 2] = 7f71a8d25cc213e7
[4, 2] = 41ba11b0082f57bc
[0, 3] = cca1cd1fc0280f8f
[1, 3] = a151a73d8f0d525a
[2, 3] = 31daef058c12682c
[3, 3] = 3a3b5763cf3a9bfb
[4, 3] = 2b058e4c3628449d
[0, 4] = 5b4301aa8e4ad636
[1, 4] = d698474982bd9aaf
[2, 4] = aa26254436485925
[3, 4] = 6a5d5cd999ef5713
[4, 4] = 0d50abcc7ab97b0b
```

The hash value is

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

C.2 SHAKE-256

C.2.1 Parameters, functions and constants

C.2.1.1 Parameters

For SHAKE-128, $L_1 = r = 1\ 088$, $L_2 = b = 1\ 600$ and $c = b - r = 512$. For SHAKE-256, d is a variable to determine the output length.

C.2.1.2 Byte ordering convention

Each data input D to the round-function ϕ is a block of 1 088 bits that is XORed into the part of the state. The permutation f is then applied to the state. Because the step mappings that comprise the permutation are defined on the array form of the state, it is convenient to regard D as a sequence of 64-bit words that are XORed directly into the state array. For this purpose, when D is represented as a sequence of 136 bytes, B_0, B_1, …, B_{135}, then D should be interpreted as a sequence of 17 lane words, Z_0, Z_1, …, Z_{16}, as follows:

$$Z_i = 2^{56}B_{8i+7} + 2^{48}B_{8i+6} + 2^{40}B_{8i+5} + 2^{32}B_{8i+4} + 2^{24}B_{8i+3} + 2^{16}B_{8i+2} + 2^{8}B_{8i+1} + B_{8i}$$

for $0 \le i \le 16$.

Hence, each group of eight consecutive bytes is a word, and the bytes of the word are arranged in increasing order of significance, so that the first byte in the group becomes the least significant byte of the word.

Under this interpretation, D is XORed with the state array as follows.

If j and k are the elements of {0, 1, 2, 3, 4}, such that (j, k) is the unique pair for which $i = 5k + j$, then for $0 \le i \le 16$, $Lane'(j, k) = Z_i \oplus Lane(j, k)$, where $Lane'(j, k)$ is the updated value of the lane.

C.2.1.3 Functions

The functions, including the function *Rnd* and step mappings, for the dedicated SHAKE-256 are the same as Dedicated Hash-Function 13 and is specified in Clause 19.

C.2.1.4 Constants

The constants used for the mapping, ρ, are the offsets defined in Clause 19.

C.2.1.5 Initializing value

The initializing value is a 1 600-bit all-zero string.

C.2.2 Padding method

The data M will be padded with "1111" before applying the padding method pad10*1(x, m) specified in Clause 19, with $x = 1\ 088$.

That is, the padded data is $P = M \,||\, 1111 \,||\, 10^*1$, such that the length of P is a multiple of 1 088.

C.2.3 Description of round-function

The round-function for SHAKE-128 is the permutation KECCAK-p specified in Clause 19. Notice that KECCAK-p is considered as ϕ as defined in ISO/IEC 10118-1. However, for each execution of KECCAK-p, it iterates the *Rnd* function 24 times. That is, it executes

$$Rnd(\mathbf{A}, i_r) = \iota(\chi<\pi\{\rho\{\theta(\mathbf{A})]\}>, i_r),$$

for $i_r = 0, 1, ..., 23$.

C.2.4 Output transformation

In step h) of SPONGE[*f*, pad, *r*](*N*, *d*) specified in Clause 19, each execution of *f* in the squeezing stage for SHAKE-256 generates $r = 1088$ bits. The output is concatenated until enough bits are generated to obtain *d* bits. That is, for a given *d*, after the last data block is inputted, it generates the first *r* bits of output. Then, it executes the function *f* $\lceil d/r \rceil - 1$ times to generate a total of $\lceil d/r \rceil \cdot r$ output bits and then truncates to *d* bits.

C.2.5 Examples

NOTE 1 Data is presented in three different ways: bit strings, byte strings and "w" length words (for the lanes).

NOTE 2 Bit strings are the sequence of bits from left to right.

NOTE 3 Byte strings are the bytes from left to right and the bits within the byte are right to left.

NOTE 4 Words are the integer representation of the values in the lanes.

SHAKE-256 sample to produce 4 096-bit of output.

The message as a bit string

```
(empty message)
```

About to call last of the absorb phase

XORed state (in bytes)

```
1F 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 80 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
               00 00 00 00 00 00 00 00
```

XORed state (as lanes of integers)

```
[0, 0] = 000000000000001f
[1, 0] = 0000000000000000
[2, 0] = 0000000000000000
[3, 0] = 0000000000000000
[4, 0] = 0000000000000000
[0, 1] = 0000000000000000
[1, 1] = 0000000000000000
[2, 1] = 0000000000000000
[3, 1] = 0000000000000000
[4, 1] = 0000000000000000
[0, 2] = 0000000000000000
[1, 2] = 0000000000000000
[2, 2] = 0000000000000000
[3, 2] = 0000000000000000
[4, 2] = 0000000000000000
```

```
[0, 3] = 0000000000000000
[1, 3] = 8000000000000000
[2, 3] = 0000000000000000
[3, 3] = 0000000000000000
[4, 3] = 0000000000000000
[0, 4] = 0000000000000000
[1, 4] = 0000000000000000
[2, 4] = 0000000000000000
[3, 4] = 0000000000000000
[4, 4] = 0000000000000000
```

Round #0

After theta

```
1E 00 00 00 00 00 00 00 1F 00 00 00 00 00 00 00
00 00 00 00 00 00 00 80 00 00 00 00 00 00 00 00
3E 00 00 00 00 00 00 00 01 00 00 00 00 00 00 00
1F 00 00 00 00 00 00 00 00 00 00 00 00 00 00 80
00 00 00 00 00 00 00 00 3E 00 00 00 00 00 00 00
01 00 00 00 00 00 00 00 1F 00 00 00 00 00 00 00
00 00 00 00 00 00 00 80 00 00 00 00 00 00 00 00
3E 00 00 00 00 00 00 00 01 00 00 00 00 00 00 00
1F 00 00 00 00 00 00 80 00 00 00 00 00 00 00 80
00 00 00 00 00 00 00 00 3E 00 00 00 00 00 00 00
01 00 00 00 00 00 00 00 1F 00 00 00 00 00 00 00
00 00 00 00 00 00 00 80 00 00 00 00 00 00 00 00
               3E 00 00 00 00 00 00 00
```

After rho

```
1E 00 00 00 00 00 00 00 3E 00 00 00 00 00 00 00
00 00 00 00 00 00 00 20 00 00 00 00 00 00 00 00
00 00 00 F0 01 00 00 00 00 00 00 00 10 00 00 00
00 00 00 00 00 F0 01 00 20 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 E0 03 00 00 00 00
08 00 00 00 00 00 00 00 00 7C 00 00 00 00 00 00
00 00 00 00 00 04 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 1F 00 00 00 00 00 00 00 02 00 00
00 00 00 00 00 F0 03 00 00 40 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 3E 00 00 00 00 00 00
00 00 04 00 00 00 00 00 7C 00 00 00 00 00 00 00
00 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00
               00 80 0F 00 00 00 00 00
```

After pi

```
1E 00 00 00 00 00 00 00 00 00 00 00 F0 01 00
00 00 00 00 00 04 00 00 00 00 00 00 00 00 00 00
00 80 0F 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 E0 03 00 00 00 00 08 00 00 00 00 00 00 00
00 00 00 00 00 F0 03 00 00 00 00 00 00 00 00 10
3E 00 00 00 00 00 00 00 20 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 3E 00 00 00 00 00 00
00 00 04 00 00 00 00 00 00 00 00 F0 01 00 00 00
00 00 00 00 10 00 00 00 00 7C 00 00 00 00 00 00
00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 20 00 00 00 00 00 00 00 00
00 00 00 00 00 1F 00 00 00 00 00 00 00 02 00 00
```

```
                7C 00 00 00 00 00 00 00
```

After chi

```
1E 00 00 00 00 04 00 00 00 00 00 00 F0 01 00
00 80 0F 00 00 04 00 00 1E 00 00 00 00 00 00 00
00 80 0F 00 00 F0 01 00 08 00 00 00 00 00 00 00
00 00 E0 03 00 F0 03 00 08 00 00 00 00 00 00 10
00 00 00 00 00 F0 03 00 00 00 E0 03 00 00 00 10
3E 00 00 00 00 00 00 00 20 3E 00 00 00 00 00 00
00 00 04 00 00 00 00 00 3E 3E 00 00 00 00 00 00
00 00 04 00 00 00 00 00 00 7C 00 F0 01 00 00 00
00 00 00 00 10 00 00 00 00 7C 00 00 00 00 00 00
00 40 00 F0 01 00 00 00 00 00 00 00 10 00 00 00
00 00 00 00 00 1F 00 20 00 00 00 00 00 00 00 00
7C 00 00 00 00 1F 00 00 00 00 00 00 00 02 00 20
                7C 00 00 00 00 00 00 00
```

After iota

```
1F 00 00 00 00 04 00 00 00 00 00 00 F0 01 00
00 80 0F 00 00 04 00 00 1E 00 00 00 00 00 00 00
00 80 0F 00 00 F0 01 00 08 00 00 00 00 00 00 00
00 00 E0 03 00 F0 03 00 08 00 00 00 00 00 00 10
00 00 00 00 00 F0 03 00 00 00 E0 03 00 00 00 10
3E 00 00 00 00 00 00 00 20 3E 00 00 00 00 00 00
00 00 04 00 00 00 00 00 3E 3E 00 00 00 00 00 00
00 00 04 00 00 00 00 00 00 7C 00 F0 01 00 00 00
00 00 00 00 10 00 00 00 00 7C 00 00 00 00 00 00
00 40 00 F0 01 00 00 00 00 00 00 00 10 00 00 00
00 00 00 00 00 1F 00 20 00 00 00 00 00 00 00 00
7C 00 00 00 00 1F 00 00 00 00 00 00 00 02 00 20
                7C 00 00 00 00 00 00 00
```

(Skip rounds 1 to 22)

Round #23

After theta

```
12 BD 5D BB 89 28 9D 11 EE 0E 30 76 65 D9 8A 3D
7B 87 FC B3 DD 91 96 99 7B 44 09 E9 AE CC 20 D6
90 D5 FA 89 B4 D3 CE 1F F8 F1 96 7D AB AD 02 E0
B7 88 31 BA 31 F1 9E B7 90 13 3A 8C 32 E2 6D B5
E1 E5 C8 C2 2F 81 67 03 88 F1 A0 D9 78 AC 46 C9
21 F1 0C 64 24 57 D0 23 2D FD 7A DB F6 A1 1E 0A
77 53 B0 CF 53 72 4E 5C 69 73 52 53 A9 06 0F 63
19 92 A9 74 BC 06 1E B7 B9 EE B9 63 E8 8E 62 68
CD DD B2 F4 B0 8D 43 8B 98 F2 39 FE E4 39 C8 56
31 7A EB DF F3 A9 65 F5 6E 7C 50 4C 8E 54 0A C6
D1 21 78 57 5E 79 BE 69 EA B3 B5 E4 E8 D5 3D 7F
4F E2 5D 6A C7 F6 BD 12 58 1F DA 44 E4 78 D8 42
                19 67 A2 4E C2 23 D8 7D
```

After rho

```
12 BD 5D BB 89 28 9D 11 DC 1D 60 EC CA B2 15 7B
DE 21 FF 6C 77 A4 65 E6 CA 0C 62 BD 47 94 90 EE
9D 76 FE 80 AC D6 4F A4 B7 DA 2A 00 8E 1F 6F D9
A3 1B 13 EF 79 7B 8B 18 2D E4 84 0E A3 8C 78 5B
72 64 E1 97 C0 B3 81 F0 6A 94 8C 18 0F 9A 8D C7
```

```
09 89 67 20 23 B9 82 1E 28 B4 F4 EB 6D DB 87 7A
7D 9E 92 73 E2 BA 9B 82 0D 1E C6 D2 E6 A4 A6 52
3A 5E 03 8F DB 0C C9 54 C7 D0 1D C5 D0 72 DD 73
96 1E B6 71 68 B1 B9 5B 64 2B 4C F9 1C 7F F2 1C
B5 AC 3E 46 6F FD 7B 3E C6 6E 7C 50 4C 8E 54 0A
F9 A6 45 87 E0 5D 79 E5 A9 CF D6 92 A3 57 F7 FC
49 BC 4B ED D8 BE 57 E2 1F DA 44 E4 78 D8 42 58
            76 5F C6 99 A8 93 F0 08
```

After pi

```
12 BD 5D BB 89 28 9D 11 A3 1B 13 EF 79 7B 8B 18
7D 9E 92 73 E2 BA 9B 82 B5 AC 3E 46 6F FD 7B 3E
76 5F C6 99 A8 93 F0 08 CA 0C 62 BD 47 94 90 EE
6A 94 8C 18 0F 9A 8D C7 09 89 67 20 23 B9 82 1E
96 1E B6 71 68 B1 B9 5B 49 BC 4B ED D8 BE 57 E2
DC 1D 60 EC CA B2 15 7B 2D E4 84 0E A3 8C 78 5B
0D 1E C6 D2 E6 A4 A6 52 C6 6E 7C 50 4C 8E 54 0A
F9 A6 45 87 E0 5D 79 E5 9D 76 FE 80 AC D6 4F A4
B7 DA 2A 00 8E 1F 6F D9 28 B4 F4 EB 6D DB 87 7A
64 2B 4C F9 1C 7F F2 1C 1F DA 44 E4 78 D8 42 58
DE 21 FF 6C 77 A4 65 E6 72 64 E1 97 C0 B3 81 F0
3A 5E 03 8F DB 0C C9 54 C7 D0 1D C5 D0 72 DD 73
            A9 CF D6 92 A3 57 F7 FC
```

After chi

```
4E 39 DD AB 0B A8 8D 93 23 3B 3F EB 74 3E EB 24
3F CD 52 EA 62 B8 1B 82 B5 0C 27 64 6E D5 76 2F
D7 5D C4 DD D8 C0 F2 00 CB 05 01 9D 67 B5 92 F6
FC 82 1C 49 47 9A B4 86 40 29 2E AC B3 B7 C4 BE
14 1E 96 61 6F B1 39 57 69 2C C7 ED D0 B4 5A E3
DC 07 22 3C 8E 92 93 7B EF 84 BC 0E AB 86 28 53
34 9E C7 55 46 F5 8F B7 C2 77 5C 38 46 2C 50 10
D8 46 C1 85 C1 51 11 E5 95 52 2A 6B CD 16 CF 86
F3 D1 22 10 9E 3B 1F DD 33 64 F4 EF 0D 5B 87 3A
E4 0F F6 F9 98 79 FF B8 3D 52 44 E4 7A D1 62 01
D6 3B FD 64 6C A8 2D E2 B7 E4 FD D7 C0 C1 95 D3
12 51 C1 9D F8 09 EB D8 91 F0 34 A9 84 D2 DD 71
            89 8B D6 01 23 44 77 EC
```

After iota

```
46 B9 DD 2B 0B A8 8D 13 23 3B 3F EB 74 3E EB 24
3F CD 52 EA 62 B8 1B 82 B5 0C 27 64 6E D5 76 2F
D7 5D C4 DD D8 C0 F2 00 CB 05 01 9D 67 B5 92 F6
FC 82 1C 49 47 9A B4 86 40 29 2E AC B3 B7 C4 BE
14 1E 96 61 6F B1 39 57 69 2C C7 ED D0 B4 5A E3
DC 07 22 3C 8E 92 93 7B EF 84 BC 0E AB 86 28 53
34 9E C7 55 46 F5 8F B7 C2 77 5C 38 46 2C 50 10
D8 46 C1 85 C1 51 11 E5 95 52 2A 6B CD 16 CF 86
F3 D1 22 10 9E 3B 1F DD 33 64 F4 EF 0D 5B 87 3A
E4 0F F6 F9 98 79 FF B8 3D 52 44 E4 7A D1 62 01
D6 3B FD 64 6C A8 2D E2 B7 E4 FD D7 C0 C1 95 D3
12 51 C1 9D F8 09 EB D8 91 F0 34 A9 84 D2 DD 71
            89 8B D6 01 23 44 77 EC
```

After permutation

```
46 B9 DD 2B 0B A8 8D 13 23 3B 3F EB 74 3E EB 24
3F CD 52 EA 62 B8 1B 82 B5 0C 27 64 6E D5 76 2F
D7 5D C4 DD D8 C0 F2 00 CB 05 01 9D 67 B5 92 F6
FC 82 1C 49 47 9A B4 86 40 29 2E AC B3 B7 C4 BE
14 1E 96 61 6F B1 39 57 69 2C C7 ED D0 B4 5A E3
DC 07 22 3C 8E 92 93 7B EF 84 BC 0E AB 86 28 53
34 9E C7 55 46 F5 8F B7 C2 77 5C 38 46 2C 50 10
D8 46 C1 85 C1 51 11 E5 95 52 2A 6B CD 16 CF 86
F3 D1 22 10 9E 3B 1F DD 33 64 F4 EF 0D 5B 87 3A
E4 0F F6 F9 98 79 FF B8 3D 52 44 E4 7A D1 62 01
D6 3B FD 64 6C A8 2D E2 B7 E4 FD D7 C0 C1 95 D3
12 51 C1 9D F8 09 EB D8 91 F0 34 A9 84 D2 DD 71
            89 8B D6 01 23 44 77 EC
```

State (as lanes of integers)

```
[0, 0] = 138da80b2bddb946
[1, 0] = 24eb3e74eb3f3b23
[2, 0] = 821bb862ea52cd3f
[3, 0] = 2f76d56e64270cb5
[4, 0] = 00f2c0d8ddc45dd7
[0, 1] = f692b5679d0105cb
[1, 1] = 86b49a47491c82fc
[2, 1] = bec4b7b3ac2e2940
[3, 1] = 5739b16f61961e14
[4, 1] = e35ab4d0edc72c69
[0, 2] = 7b93928e3c2207dc
[1, 2] = 532886ab0ebc84ef
[2, 2] = b78ff54655c79e34
[3, 2] = 10502c46385c77c2
[4, 2] = e51151c185c146d8
[0, 3] = 86cf16cd6b2a5295
[1, 3] = dd1f3b9e1022d1f3
[2, 3] = 3a875b0deff46433
[3, 3] = b8ff7998f9f60fe4
[4, 3] = 0162d17ae444523d
[0, 4] = e22da86c64fd3bd6
[1, 4] = d395c1c0d7fde4b7
[2, 4] = d8eb09f89dc15112
[3, 4] = 71ddd284a934f091
[4, 4] = ec77442301d68b89
```

About to call squeeze (again)

State before permutation (in bytes)

```
46 B9 DD 2B 0B A8 8D 13 23 3B 3F EB 74 3E EB 24
3F CD 52 EA 62 B8 1B 82 B5 0C 27 64 6E D5 76 2F
D7 5D C4 DD D8 C0 F2 00 CB 05 01 9D 67 B5 92 F6
FC 82 1C 49 47 9A B4 86 40 29 2E AC B3 B7 C4 BE
14 1E 96 61 6F B1 39 57 69 2C C7 ED D0 B4 5A E3
DC 07 22 3C 8E 92 93 7B EF 84 BC 0E AB 86 28 53
34 9E C7 55 46 F5 8F B7 C2 77 5C 38 46 2C 50 10
D8 46 C1 85 C1 51 11 E5 95 52 2A 6B CD 16 CF 86
F3 D1 22 10 9E 3B 1F DD 33 64 F4 EF 0D 5B 87 3A
E4 0F F6 F9 98 79 FF B8 3D 52 44 E4 7A D1 62 01
```

```
D6 3B FD 64 6C A8 2D E2 B7 E4 FD D7 C0 C1 95 D3
12 51 C1 9D F8 09 EB D8 91 F0 34 A9 84 D2 DD 71
               89 8B D6 01 23 44 77 EC
```

State before permutation (as lanes of integers)

```
[0, 0] = 138da80b2bddb946
[1, 0] = 24eb3e74eb3f3b23
[2, 0] = 821bb862ea52cd3f
[3, 0] = 2f76d56e64270cb5
[4, 0] = 00f2c0d8ddc45dd7
[0, 1] = f692b5679d0105cb
[1, 1] = 86b49a47491c82fc
[2, 1] = bec4b7b3ac2e2940
[3, 1] = 5739b16f61961e14
[4, 1] = e35ab4d0edc72c69
[0, 2] = 7b93928e3c2207dc
[1, 2] = 532886ab0ebc84ef
[2, 2] = b78ff54655c79e34
[3, 2] = 10502c46385c77c2
[4, 2] = e51151c185c146d8
[0, 3] = 86cf16cd6b2a5295
[1, 3] = dd1f3b9e1022d1f3
[2, 3] = 3a875b0deff46433
[3, 3] = b8ff7998f9f60fe4
[4, 3] = 0162d17ae444523d
[0, 4] = e22da86c64fd3bd6
[1, 4] = d395c1c0d7fde4b7
[2, 4] = d8eb09f89dc15112
[3, 4] = 71ddd284a934f091
[4, 4] = ec77442301d68b89
```

Round #0

After theta

```
7D 47 0D AD 17 A9 DA 07 E5 77 0A AD F3 5F FC 0C
66 F1 4D 5B 12 A6 9D 3F 7A 9E 08 A5 2C 1C 13 91
E4 63 B8 BA 04 41 13 55 F0 FB D1 1B 7B B4 C5 E2
3A CE 29 0F C0 FB A3 AE 19 15 31 1D C3 A9 42 03
DB 8C B9 A0 2D 78 5C E9 5A 12 BB 8A 0C 35 BB B6
E7 F9 F2 BA 92 93 C4 6F 29 C8 89 48 2C E7 3F 7B
6D A2 D8 E4 36 EB 09 0A 0D E5 73 F9 04 E5 35 AE
EB 78 BD E2 1D D0 F0 B0 AE AC FA ED D1 17 98 92
35 9D 17 56 19 5A 08 F5 6A 58 EB 5E 7D 45 01 87
2B 9D D9 38 DA B0 9A 06 0E 6C 38 83 A6 50 83 54
ED C5 2D E2 70 A9 7A F6 71 A8 C8 91 47 A0 82 FB
4B 6D DE 2C 88 17 6D 65 5E 62 1B 68 C6 1B B8 CF
               BA B5 AA 66 FF C5 96 B9
```

After rho

```
7D 47 0D AD 17 A9 DA 07 CA EF 14 5A E7 BF F8 19
59 7C D3 96 84 69 E7 8F C2 31 11 A9 E7 89 50 CA
08 9A A8 22 1F C3 D5 25 B1 47 5B 2C 0E BF 1F BD
F2 00 BC 3F EA AA E3 9C 40 46 45 4C C7 70 AA D0
C6 5C D0 16 3C AE F4 6D B3 6B AB 25 B1 AB C8 50
3B CF 97 D7 95 9C 24 7E EC A5 20 27 22 B1 9C FF
26 B7 59 4F 50 68 13 C5 CA 6B 5C 1B CA E7 F2 09
F1 0E 68 78 D8 75 BC 5E DB A3 2F 30 25 5D 59 F5
```

```
C2 2A 43 0B A1 BE A6 F3 80 43 35 AC 75 AF BE A2
56 D3 60 A5 33 1B 47 1B 54 0E 6C 38 83 A6 50 83
EA D9 B7 17 B7 88 C3 A5 C7 A1 22 47 1E 81 0A EE
A9 CD 9B 05 F1 A2 AD 6C 62 1B 68 C6 1B B8 CF 5E
            65 AE 6E AD AA D9 7F B1
```

After pi

```
7D 47 0D AD 17 A9 DA 07 F2 00 BC 3F EA AA E3 9C
26 B7 59 4F 50 68 13 C5 56 D3 60 A5 33 1B 47 1B
65 AE 6E AD AA D9 7F B1 C2 31 11 A9 E7 89 50 CA
B3 6B AB 25 B1 AB C8 50 3B CF 97 D7 95 9C 24 7E
C2 2A 43 0B A1 BE A6 F3 A9 CD 9B 05 F1 A2 AD 6C
CA EF 14 5A E7 BF F8 19 40 46 45 4C C7 70 AA D0
CA 6B 5C 1B CA E7 F2 09 54 0E 6C 38 83 A6 50 83
EA D9 B7 17 B7 88 C3 A5 08 9A A8 22 1F C3 D5 25
B1 47 5B 2C 0E BF 1F BD EC A5 20 27 22 B1 9C FF
80 43 35 AC 75 AF BE A2 62 1B 68 C6 1B B8 CF 5E
59 7C D3 96 84 69 E7 8F C6 5C D0 16 3C AE F4 6D
F1 0E 68 78 D8 75 BC 5E DB A3 2F 30 25 5D 59 F5
            C7 A1 22 47 1E 81 0A EE
```

After chi

```
79 F0 4C ED 07 E9 CA 46 A2 40 9C 9F C9 B9 A7 86
07 9B 57 47 D8 A8 2B 65 4E 92 61 A5 26 3B C7 1D
E7 AE DE BF 42 DB 5E 29 CA B5 05 7B E3 9D 74 E4
73 4B EB 2D 91 89 4A D1 12 0A 0F D3 C5 9C 2D 72
80 1A 43 A3 A7 B7 F6 71 98 87 31 01 E1 80 25 7C
40 C6 0C 49 EF 38 A8 10 54 42 65 6C C6 70 AA 52
60 BA CF 1C FE EF 71 2D 54 28 6C 70 C3 91 68 9B
EA D9 F6 13 B7 C8 C1 65 44 3A 88 21 3F C3 55 67
B1 05 4E A4 5B B1 3D BD 8E BD 68 65 28 A1 DD A3
88 C3 B5 8C 71 EC AE 83 D3 5E 3B CA 1B 84 C5 C6
68 7E FB FE 44 38 EF 9D CC FD D7 16 19 A6 B5 CC
F5 0E 68 3F C2 F5 BE 54 C3 FF FE A0 A5 35 BC F4
            41 A1 22 47 26 07 1A 8E
```

After iota

```
78 F0 4C ED 07 E9 CA 46 A2 40 9C 9F C9 B9 A7 86
07 9B 57 47 D8 A8 2B 65 4E 92 61 A5 26 3B C7 1D
E7 AE DE BF 42 DB 5E 29 CA B5 05 7B E3 9D 74 E4
73 4B EB 2D 91 89 4A D1 12 0A 0F D3 C5 9C 2D 72
80 1A 43 A3 A7 B7 F6 71 98 87 31 01 E1 80 25 7C
40 C6 0C 49 EF 38 A8 10 54 42 65 6C C6 70 AA 52
60 BA CF 1C FE EF 71 2D 54 28 6C 70 C3 91 68 9B
EA D9 F6 13 B7 C8 C1 65 44 3A 88 21 3F C3 55 67
B1 05 4E A4 5B B1 3D BD 8E BD 68 65 28 A1 DD A3
88 C3 B5 8C 71 EC AE 83 D3 5E 3B CA 1B 84 C5 C6
68 7E FB FE 44 38 EF 9D CC FD D7 16 19 A6 B5 CC
F5 0E 68 3F C2 F5 BE 54 C3 FF FE A0 A5 35 BC F4
            41 A1 22 47 26 07 1A 8E
```

(Skip rounds 1 to 22)

Round #23

After theta

```
58 B9 7A 75 06 0A 0D 32 AA DB 84 9F F4 25 16 50
11 13 22 72 82 A3 91 B5 0F 92 96 46 40 E0 E4 5B
77 7B 46 9F 97 CD 49 9C D7 FD 96 90 94 20 01 7D
E5 AD 10 C3 57 20 90 DB E4 27 C1 55 27 F1 12 5D
41 FA 6C C1 65 24 91 16 78 37 01 F0 C2 D4 F2 BF
15 23 E6 E1 1A B1 9E DD 97 92 DA 4E 68 46 9C 4D
5A 4C 9A 5A 02 62 03 9D 7B 68 54 03 A1 B5 19 BF
21 E9 D3 FF B9 5B 4D BF 52 FE 8F 8A AD 8C 8C 3F
0B C1 5D 4A FA D1 81 78 C8 22 4E 60 45 4D C8 83
A8 86 F7 D0 0B FD 91 18 65 9C 25 70 EB 5B 52 3C
5E EB 7C E1 DA CE D2 66 AA D3 3B CA DC 76 78 67
63 F2 F5 48 72 78 4C BE 4D DF C8 8A 2D 37 EA 5B
            BF D7 42 D4 5E 14 5E 22
```

After rho

```
58 B9 7A 75 06 0A 0D 32 54 B7 09 3F E9 4B 2C A0
C4 84 88 9C E0 68 64 6D 04 4E BE F5 20 69 69 04
6C 4E E2 BC DB 33 FA BC 49 09 12 D0 77 DD 6F 09
31 7C 05 02 B9 5D DE 0A 17 F9 49 70 D5 49 BC 44
7D B6 E0 32 92 48 8B 20 2D FF 8B 77 13 00 2F 4C
AE 18 31 0F D7 88 F5 EC 36 5D 4A 6A 3B A1 19 71
D4 12 10 1B E8 D4 62 D2 6B 33 7E F7 D0 A8 06 42
FF DC AD A6 DF 90 F4 E9 15 5B 19 19 7F A4 FC 1F
4B 49 3F 3A 10 6F 21 B8 E4 41 64 11 27 B0 A2 26
3F 12 03 D5 F0 1E 7A A1 3C 65 9C 25 70 EB 5B 52
4B 9B 79 AD F3 85 6B 3B A9 4E EF 28 73 DB E1 9D
4C BE 1E 49 0E 8F C9 77 DF C8 8A 2D 37 EA 5B 4D
            97 C8 EF B5 10 B5 17 85
```

After pi

```
58 B9 7A 75 06 0A 0D 32 31 7C 05 02 B9 5D DE 0A
D4 12 10 1B E8 D4 62 D2 3F 12 03 D5 F0 1E 7A A1
97 C8 EF B5 10 B5 17 85 04 4E BE F5 20 69 69 04
2D FF 8B 77 13 00 2F 4C AE 18 31 0F D7 88 F5 EC
4B 49 3F 3A 10 6F 21 B8 4C BE 1E 49 0E 8F C9 77
54 B7 09 3F E9 4B 2C A0 17 F9 49 70 D5 49 BC 44
6B 33 7E F7 D0 A8 06 42 3C 65 9C 25 70 EB 5B 52
4B 9B 79 AD F3 85 6B 3B 6C 4E E2 BC DB 33 FA BC
49 09 12 D0 77 DD 6F 09 36 5D 4A 6A 3B A1 19 71
E4 41 64 11 27 B0 A2 26 DF C8 8A 2D 37 EA 5B 4D
C4 84 88 9C E0 68 64 6D 7D B6 E0 32 92 48 8B 20
FF DC AD A6 DF 90 F4 E9 15 5B 19 19 7F A4 FC 1F
            A9 4E EF 28 73 DB E1 9D
```

After chi

```
9C BB 6A 6C 46 8A 2D E2 1A 7C 06 C6 A9 57 C6 2B
54 DA FC 3B E8 75 67 D6 77 23 13 95 F6 14 72 93
B6 8C EA B7 A9 E0 C5 8D 86 4E 8E FD E4 E1 B9 A4
6C BE 85 47 13 67 2F 5C AA AE 31 4E D9 08 3D AB
4B 09 9F 8E 30 0F 01 B8 65 0F 1F 4B 1D 8F CF 3F
3C B5 3F B8 E9 EB 2E A2 03 BD C9 70 F5 0A E5 54
28 A9 1F 7F 53 AC 26 6B 28 41 9C 37 78 A1 5F D2
```

```
48 D3 39 ED E7 85 FB 7F 5A 1A AA 96 D3 13 EA CC
89 09 36 C1 73 CD CD 0F 2D D5 C0 46 2B EB 40 38
C4 47 04 81 EF A1 02 96 DE C9 9A 6D 13 26 5E 4C
46 CC 85 18 AD F8 10 A4 7D B5 F0 2B B2 6C 83 36
57 D8 4B 86 DF CB F5 69 51 DB 19 8D FF 84 F8 7F
            90 7C 8F 0A 61 DB 6A 9D
```

After iota

```
94 3B 6A EC 46 8A 2D 62 1A 7C 06 C6 A9 57 C6 2B
54 DA FC 3B E8 75 67 D6 77 23 13 95 F6 14 72 93
B6 8C EA B7 A9 E0 C5 8D 86 4E 8E FD E4 E1 B9 A4
6C BE 85 47 13 67 2F 5C AA AE 31 4E D9 08 3D AB
4B 09 9F 8E 30 0F 01 B8 65 0F 1F 4B 1D 8F CF 3F
3C B5 3F B8 E9 EB 2E A2 03 BD C9 70 F5 0A E5 54
28 A9 1F 7F 53 AC 26 6B 28 41 9C 37 78 A1 5F D2
48 D3 39 ED E7 85 FB 7F 5A 1A AA 96 D3 13 EA CC
89 09 36 C1 73 CD CD 0F 2D D5 C0 46 2B EB 40 38
C4 47 04 81 EF A1 02 96 DE C9 9A 6D 13 26 5E 4C
46 CC 85 18 AD F8 10 A4 7D B5 F0 2B B2 6C 83 36
57 D8 4B 86 DF CB F5 69 51 DB 19 8D FF 84 F8 7F
            90 7C 8F 0A 61 DB 6A 9D
```

After permutation

```
94 3B 6A EC 46 8A 2D 62 1A 7C 06 C6 A9 57 C6 2B
54 DA FC 3B E8 75 67 D6 77 23 13 95 F6 14 72 93
B6 8C EA B7 A9 E0 C5 8D 86 4E 8E FD E4 E1 B9 A4
6C BE 85 47 13 67 2F 5C AA AE 31 4E D9 08 3D AB
4B 09 9F 8E 30 0F 01 B8 65 0F 1F 4B 1D 8F CF 3F
3C B5 3F B8 E9 EB 2E A2 03 BD C9 70 F5 0A E5 54
28 A9 1F 7F 53 AC 26 6B 28 41 9C 37 78 A1 5F D2
48 D3 39 ED E7 85 FB 7F 5A 1A AA 96 D3 13 EA CC
89 09 36 C1 73 CD CD 0F 2D D5 C0 46 2B EB 40 38
C4 47 04 81 EF A1 02 96 DE C9 9A 6D 13 26 5E 4C
46 CC 85 18 AD F8 10 A4 7D B5 F0 2B B2 6C 83 36
57 D8 4B 86 DF CB F5 69 51 DB 19 8D FF 84 F8 7F
            90 7C 8F 0A 61 DB 6A 9D
```

State (as lanes of integers)

```
[0, 0] = 622d8a46ec6a3b94
[1, 0] = 2bc657a9c6067c1a
[2, 0] = d66775e83bfcda54
[3, 0] = 937214f695132377
[4, 0] = 8dc5e0a9b7ea8cb6
[0, 1] = a4b9e1e4fd8e4e86
[1, 1] = 5c2f67134785be6c
[2, 1] = ab3d08d94e31aeaa
[3, 1] = b8010f308e9f094b
[4, 1] = 3fcf8f1d4b1f0f65
[0, 2] = a22eebe9b83fb53c
[1, 2] = 54e50af570c9bd03
[2, 2] = 6b26ac537f1fa928
[3, 2] = d25fa178379c4128
[4, 2] = 7ffb85e7ed39d348
[0, 3] = ccea13d396aa1a5a
[1, 3] = 0fcdcd73c1360989
```

```
[2, 3] = 3840eb2b46c0d52d
[3, 3] = 9602a1ef810447c4
[4, 3] = 4c5e26136d9ac9de
[0, 4] = a410f8ad1885cc46
[1, 4] = 36836cb22bf0b57d
[2, 4] = 69f5cbdf864bd857
[3, 4] = 7ff884ff8d19db51
[4, 4] = 9d6adb610a8f7c90
```

About to call squeeze (again)

State before permutation (in bytes)

```
94 3B 6A EC 46 8A 2D 62 1A 7C 06 C6 A9 57 C6 2B
54 DA FC 3B E8 75 67 D6 77 23 13 95 F6 14 72 93
B6 8C EA B7 A9 E0 C5 8D 86 4E 8E FD E4 E1 B9 A4
6C BE 85 47 13 67 2F 5C AA AE 31 4E D9 08 3D AB
4B 09 9F 8E 30 0F 01 B8 65 0F 1F 4B 1D 8F CF 3F
3C B5 3F B8 E9 EB 2E A2 03 BD C9 70 F5 0A E5 54
28 A9 1F 7F 53 AC 26 6B 28 41 9C 37 78 A1 5F D2
48 D3 39 ED E7 85 FB 7F 5A 1A AA 96 D3 13 EA CC
89 09 36 C1 73 CD CD 0F 2D D5 C0 46 2B EB 40 38
C4 47 04 81 EF A1 02 96 DE C9 9A 6D 13 26 5E 4C
46 CC 85 18 AD F8 10 A4 7D B5 F0 2B B2 6C 83 36
57 D8 4B 86 DF CB F5 69 51 DB 19 8D FF 84 F8 7F
            90 7C 8F 0A 61 DB 6A 9D
```

State before permutation (as lanes of integers)

```
[0, 0] = 622d8a46ec6a3b94
[1, 0] = 2bc657a9c6067c1a
[2, 0] = d66775e83bfcda54
[3, 0] = 937214f695132377
[4, 0] = 8dc5e0a9b7ea8cb6
[0, 1] = a4b9e1e4fd8e4e86
[1, 1] = 5c2f67134785be6c
[2, 1] = ab3d08d94e31aeaa
[3, 1] = b8010f308e9f094b
[4, 1] = 3fcf8f1d4b1f0f65
[0, 2] = a22eebe9b83fb53c
[1, 2] = 54e50af570c9bd03
[2, 2] = 6b26ac537f1fa928
[3, 2] = d25fa178379c4128
[4, 2] = 7ffb85e7ed39d348
[0, 3] = ccea13d396aa1a5a
[1, 3] = 0fcdcd73c1360989
[2, 3] = 3840eb2b46c0d52d
[3, 3] = 9602a1ef810447c4
[4, 3] = 4c5e26136d9ac9de
[0, 4] = a410f8ad1885cc46
[1, 4] = 36836cb22bf0b57d
[2, 4] = 69f5cbdf864bd857
[3, 4] = 7ff884ff8d19db51
[4, 4] = 9d6adb610a8f7c90
```

Round #0

After theta

```
43 59 AA AD 7B AA 6D 4A 70 CB 41 75 B1 DF 15 A8
D7 F6 6B 60 3A D1 88 ED 71 38 F9 B2 22 CB 31 ED
53 57 0F D8 6D A9 93 85 51 2C 4E BC D9 C1 F9 8C
06 09 C2 F4 0B EF FC DF 29 82 A6 15 0B AC D2 90
4D 12 75 A9 E4 D0 42 C6 80 D4 FA 24 D9 C6 99 37
EB D7 FF F9 D4 CB 6E 8A 69 0A 8E C3 ED 82 36 D7
AB 85 88 24 81 08 C9 50 2E 5A 76 10 AC 7E 1C AC
AD 08 DC 82 23 CC AD 77 8D 78 6A D7 EE 33 AA E4
E3 BE 71 72 6B 45 1E 8C AE F9 57 1D F9 4F AF 03
C2 5C EE A6 3B 7E 41 E8 3B 12 7F 02 D7 6F 08 44
91 AE 45 59 90 D8 50 8C 17 02 B7 98 AA E4 50 B5
D4 F4 DC DD 0D 6F 1A 52 57 C0 F3 AA 2B 5B BB 01
            75 A7 6A 65 A5 92 3C 95
```

After rho

```
43 59 AA AD 7B AA 6D 4A E1 96 83 EA 62 BF 2B 50
B5 FD 1A 98 4E 34 62 FB B2 1C D3 1E 87 93 2F 2B
4B 9D 2C 9C BA 7A C0 6E 9B 1D 9C CF 18 C5 E2 C4
4C BF F0 CE FF 6D 90 20 64 8A A0 69 C5 02 AB 34
89 BA 54 72 68 21 E3 26 9C 79 03 48 AD 4F 92 6D
5C BF FE CF A7 5E 76 53 5C A7 29 38 0E B7 0B DA
24 09 44 48 86 5A 2D 44 FD 38 58 5D B4 EC 20 58
C1 11 E6 D6 BB 56 04 6E AE DD 67 54 C9 1B F1 D4
4E 6E AD C8 83 71 DC 37 D7 01 D7 FC AB 8E FC A7
2F 08 5D 98 CB DD 74 C7 44 3B 12 7F 02 D7 6F 08
43 31 46 BA 16 65 41 62 5E 08 DC 62 AA 92 43 D5
9A 9E BB BB E1 4D 43 8A C0 F3 AA 2B 5B BB 01 57
            4F 65 DD A9 5A 59 A9 24
```

After pi

```
43 59 AA AD 7B AA 6D 4A 4C BF F0 CE FF 6D 90 20
24 09 44 48 86 5A 2D 44 2F 08 5D 98 CB DD 74 C7
4F 65 DD A9 5A 59 A9 24 B2 1C D3 1E 87 93 2F 2B
9C 79 03 48 AD 4F 92 6D 5C BF FE CF A7 5E 76 53
4E 6E AD C8 83 71 DC 37 9A 9E BB BB E1 4D 43 8A
E1 96 83 EA 62 BF 2B 50 64 8A A0 69 C5 02 AB 34
FD 38 58 5D B4 EC 20 58 44 3B 12 7F 02 D7 6F 08
43 31 46 BA 16 65 41 62 4B 9D 2C 9C BA 7A C0 6E
9B 1D 9C CF 18 C5 E2 C4 5C A7 29 38 0E B7 0B DA
D7 01 D7 FC AB 8E FC A7 C0 F3 AA 2B 5B BB 01 57
B5 FD 1A 98 4E 34 62 FB 89 BA 54 72 68 21 E3 26
C1 11 E6 D6 BB 56 04 6E AE DD 67 54 C9 1B F1 D4
            5E 08 DC 62 AA 92 43 D5
```

After chi

```
63 59 AE AD 7B B8 40 0E 47 BF E9 5E B6 E8 C0 A3
64 6C C4 69 96 5A A4 64 2F 10 7F 9C EA 7F 30 8D
43 C3 8D EB DE 1C 39 04 F2 9A 2F 99 85 83 4B 39
9E 39 02 48 AD 6E 1A 49 CC 2F EC FC C7 52 75 DB
6E 6E ED CC 85 E3 F0 16 96 FF BB FB C9 01 D3 CE
78 A6 DB FE 52 53 2B 18 64 89 A2 4B C7 11 E4 34
FE 38 1C DD A0 CC 20 3A E4 BD 93 3F 62 4D 45 18
47 39 66 BB 93 65 C1 46 0F 3F 0D AC BC 48 C9 74
18 1D 4A 0B B9 CD 16 E1 5C 55 01 3B 5E 86 0A 8A
```

```
DC 0D D3 68 0B CE 3C 8F 50 F3 3A 68 5B 3E 23 D7
F5 FC B8 1C DD 62 66 B3 A7 76 55 72 28 28 12 B6
91 11 7E F4 99 D6 06 6F 0F 28 65 CC 8D 3F D1 FE
            56 0A 98 00 8A 93 C2 D1
```

After iota

```
62 59 AE AD 7B B8 40 0E 47 BF E9 5E B6 E8 C0 A3
64 6C C4 69 96 5A A4 64 2F 10 7F 9C EA 7F 30 8D
43 C3 8D EB DE 1C 39 04 F2 9A 2F 99 85 83 4B 39
9E 39 02 48 AD 6E 1A 49 CC 2F EC FC C7 52 75 DB
6E 6E ED CC 85 E3 F0 16 96 FF BB FB C9 01 D3 CE
78 A6 DB FE 52 53 2B 18 64 89 A2 4B C7 11 E4 34
FE 38 1C DD A0 CC 20 3A E4 BD 93 3F 62 4D 45 18
47 39 66 BB 93 65 C1 46 0F 3F 0D AC BC 48 C9 74
18 1D 4A 0B B9 CD 16 E1 5C 55 01 3B 5E 86 0A 8A
DC 0D D3 68 0B CE 3C 8F 50 F3 3A 68 5B 3E 23 D7
F5 FC B8 1C DD 62 66 B3 A7 76 55 72 28 28 12 B6
91 11 7E F4 99 D6 06 6F 0F 28 65 CC 8D 3F D1 FE
            56 0A 98 00 8A 93 C2 D1
```

(Skip rounds 1 to 22)

Round #23

After theta

```
B3 28 26 C5 75 3F AB 7A E8 63 36 F2 32 D1 04 CC
8D 13 B7 C9 DD F3 EE 58 B3 C5 57 CB 9F 10 41 BC
47 1A 06 8C B7 5F A6 16 60 A2 AD 6D F3 34 55 FB
F9 F0 B1 6E 4C 7C 9B FF CF 81 A3 3F D5 20 62 70
12 F5 0C D5 4D 03 7A 25 27 72 C9 9F 7E 5C 7D 62
5B 5A 31 FE 35 E1 28 B4 22 FF 26 8A 43 B2 24 0E
0E 69 38 D3 C4 91 22 0F 02 1B 95 4D 87 9C E9 48
B2 A1 67 E9 51 07 C9 DB 85 3F 0E BF 44 E9 BB 6D
FC 6D D1 2B EA F4 9F 26 CA 14 FA 9F 60 5F C9 EB
80 76 4B B0 B1 F0 A4 A2 64 44 4A A2 85 50 27 0E
F1 F7 66 76 C1 3B 06 40 AA 45 F4 B2 9C 70 3C 14
80 81 E9 89 E7 BC 3D 96 6B 70 6E A0 0A F2 71 03
            CF 5F 4F 2D 93 8D F8 01
```

After rho

```
B3 28 26 C5 75 3F AB 7A D1 C7 6C E4 65 A2 09 98
E3 C4 6D 72 F7 BC 3B 56 09 11 C4 3B 5B 7C B5 FC
FD 32 B5 38 D2 30 60 BC 36 4F 53 B5 0F 26 DA DA
EB C6 C4 B7 F9 9F 0F 1F DC 73 E0 E8 4F 35 88 18
7A 86 EA A6 01 BD 12 89 D5 27 76 22 97 FC E9 C7
DD D2 8A F1 AF 09 47 A1 38 88 FC 9B 28 0E C9 92
99 26 8E 14 79 70 48 C3 39 D3 91 04 36 2A 9B 0E
F4 A8 83 E4 6D D9 D0 B3 7E 89 D2 77 DB 0A 7F 1C
7A 45 9D FE D3 84 BF 2D E4 75 65 0A FD 4F B0 AF
9E 54 14 D0 6E 09 36 16 0E 64 44 4A A2 85 50 27
18 00 C5 DF 9B D9 05 EF A8 16 D1 CB 72 C2 F1 50
30 30 3D F1 9C B7 C7 12 70 6E A0 0A F2 71 03 6B
            7E C0 F3 D7 53 CB 64 23
```

After pi

```
B3 28 26 C5 75 3F AB 7A EB C6 C4 B7 F9 9F 0F 1F
99 26 8E 14 79 70 48 C3 9E 54 14 D0 6E 09 36 16
7E C0 F3 D7 53 CB 64 23 09 11 C4 3B 5B 7C B5 FC
D5 27 76 22 97 FC E9 C7 DD D2 8A F1 AF 09 47 A1
7A 45 9D FE D3 84 BF 2D 30 30 3D F1 9C B7 C7 12
D1 C7 6C E4 65 A2 09 98 DC 73 E0 E8 4F 35 88 18
39 D3 91 04 36 2A 9B 0E 0E 64 44 4A A2 85 50 27
18 00 C5 DF 9B D9 05 EF FD 32 B5 38 D2 30 60 BC
36 4F 53 B5 0F 26 DA DA 38 88 FC 9B 28 0E C9 92
E4 75 65 0A FD 4F B0 AF 70 6E A0 0A F2 71 03 6B
E3 C4 6D 72 F7 BC 3B 56 7A 86 EA A6 01 BD 12 89
F4 A8 83 E4 6D D9 D0 B3 7E 89 D2 77 DB 0A 7F 1C
            A8 16 D1 CB 72 C2 F1 50
```

After chi

```
A3 08 2C C5 75 5F EB BA ED 96 D4 77 FF 96 39 0B
F9 A6 6D 13 68 B2 08 E2 1F 7C 10 D0 4A 3D BD 4E
36 06 33 E5 DB 4B 60 26 01 C1 4C EA 73 7D B3 DC
F7 22 63 2C C7 78 51 CB DD E2 AA F0 A3 3A 07 B3
73 44 5D F4 90 CC 8F C1 E4 16 0F F1 18 37 8F 11
F0 47 7D E0 55 A8 1A 9E DA 57 A4 A2 CF B0 C8 39
29 D3 10 91 2F 72 9E C6 CF A3 6C 6A C6 A7 58 37
14 30 45 D7 91 CC 85 EF F5 B2 19 32 F2 38 61 BC
F2 3A 52 B5 DA 67 EA F7 28 82 7C 9B 2A 3E CA D2
69 65 70 3A FD 4F D0 3B 72 23 E2 8F FF 77 99 29
67 EC 6C 32 9B FC FB 64 70 87 BA B5 93 BF 3D 85
74 BE 82 6C 4D 19 50 F3 3D 49 FE 47 5E 36 75 1A
            B0 14 53 4F 72 C3 F1 D9
```

After iota

```
AB 88 2C 45 75 5F EB 3A ED 96 D4 77 FF 96 39 0B
F9 A6 6D 13 68 B2 08 E2 1F 7C 10 D0 4A 3D BD 4E
36 06 33 E5 DB 4B 60 26 01 C1 4C EA 73 7D B3 DC
F7 22 63 2C C7 78 51 CB DD E2 AA F0 A3 3A 07 B3
73 44 5D F4 90 CC 8F C1 E4 16 0F F1 18 37 8F 11
F0 47 7D E0 55 A8 1A 9E DA 57 A4 A2 CF B0 C8 39
29 D3 10 91 2F 72 9E C6 CF A3 6C 6A C6 A7 58 37
14 30 45 D7 91 CC 85 EF F5 B2 19 32 F2 38 61 BC
F2 3A 52 B5 DA 67 EA F7 28 82 7C 9B 2A 3E CA D2
69 65 70 3A FD 4F D0 3B 72 23 E2 8F FF 77 99 29
67 EC 6C 32 9B FC FB 64 70 87 BA B5 93 BF 3D 85
74 BE 82 6C 4D 19 50 F3 3D 49 FE 47 5E 36 75 1A
            B0 14 53 4F 72 C3 F1 D9
```

After permutation

```
AB 88 2C 45 75 5F EB 3A ED 96 D4 77 FF 96 39 0B
F9 A6 6D 13 68 B2 08 E2 1F 7C 10 D0 4A 3D BD 4E
36 06 33 E5 DB 4B 60 26 01 C1 4C EA 73 7D B3 DC
F7 22 63 2C C7 78 51 CB DD E2 AA F0 A3 3A 07 B3
73 44 5D F4 90 CC 8F C1 E4 16 0F F1 18 37 8F 11
F0 47 7D E0 55 A8 1A 9E DA 57 A4 A2 CF B0 C8 39
29 D3 10 91 2F 72 9E C6 CF A3 6C 6A C6 A7 58 37
14 30 45 D7 91 CC 85 EF F5 B2 19 32 F2 38 61 BC
F2 3A 52 B5 DA 67 EA F7 28 82 7C 9B 2A 3E CA D2
```

```
69 65 70 3A FD 4F D0 3B 72 23 E2 8F FF 77 99 29
67 EC 6C 32 9B FC FB 64 70 87 BA B5 93 BF 3D 85
74 BE 82 6C 4D 19 50 F3 3D 49 FE 47 5E 36 75 1A
            B0 14 53 4F 72 C3 F1 D9
```

State (as lanes of integers)

```
[0, 0] = 3aeb5f75452c88ab
[1, 0] = 0b3996ff77d496ed
[2, 0] = e208b268136da6f9
[3, 0] = 4ebd3d4ad0107c1f
[4, 0] = 26604bdbe5330636
[0, 1] = dcb37d73ea4cc101
[1, 1] = cb5178c72c6322f7
[2, 1] = b3073aa3f0aae2dd
[3, 1] = c18fcc90f45d4473
[4, 1] = 118f3718f10f16e4
[0, 2] = 9e1aa855e07d47f0
[1, 2] = 39c8b0cfa2a457da
[2, 2] = c69e722f9110d329
[3, 2] = 3758a7c66a6ca3cf
[4, 2] = ef85cc91d7453014
[0, 3] = bc6138f23219b2f5
[1, 3] = f7ea67dab5523af2
[2, 3] = d2ca3e2a9b7c8228
[3, 3] = 3bd04ffd3a706569
[4, 3] = 299977ff8fe22372
[0, 4] = 64fbfc9b326cec67
[1, 4] = 853dbf93b5ba8770
[2, 4] = f350194d6c82be74
[3, 4] = 1a75365e47fe493d
[4, 4] = d9f1c3724f5314b0
```

About to call squeeze (again)

State before permutation (in bytes)

```
AB 88 2C 45 75 5F EB 3A ED 96 D4 77 FF 96 39 0B
F9 A6 6D 13 68 B2 08 E2 1F 7C 10 D0 4A 3D BD 4E
36 06 33 E5 DB 4B 60 26 01 C1 4C EA 73 7D B3 DC
F7 22 63 2C C7 78 51 CB DD E2 AA F0 A3 3A 07 B3
73 44 5D F4 90 CC 8F C1 E4 16 0F F1 18 37 8F 11
F0 47 7D E0 55 A8 1A 9E DA 57 A4 A2 CF B0 C8 39
29 D3 10 91 2F 72 9E C6 CF A3 6C 6A C6 A7 58 37
14 30 45 D7 91 CC 85 EF F5 B2 19 32 F2 38 61 BC
F2 3A 52 B5 DA 67 EA F7 28 82 7C 9B 2A 3E CA D2
69 65 70 3A FD 4F D0 3B 72 23 E2 8F FF 77 99 29
67 EC 6C 32 9B FC FB 64 70 87 BA B5 93 BF 3D 85
74 BE 82 6C 4D 19 50 F3 3D 49 FE 47 5E 36 75 1A
            B0 14 53 4F 72 C3 F1 D9
```

State before permutation (as lanes of integers)

```
[0, 0] = 3aeb5f75452c88ab
[1, 0] = 0b3996ff77d496ed
[2, 0] = e208b268136da6f9
[3, 0] = 4ebd3d4ad0107c1f
[4, 0] = 26604bdbe5330636
```

```
[0, 1] = dcb37d73ea4cc101
[1, 1] = cb5178c72c6322f7
[2, 1] = b3073aa3f0aae2dd
[3, 1] = c18fcc90f45d4473
[4, 1] = 118f3718f10f16e4
[0, 2] = 9e1aa855e07d47f0
[1, 2] = 39c8b0cfa2a457da
[2, 2] = c69e722f9110d329
[3, 2] = 3758a7c66a6ca3cf
[4, 2] = ef85cc91d7453014
[0, 3] = bc6138f23219b2f5
[1, 3] = f7ea67dab5523af2
[2, 3] = d2ca3e2a9b7c8228
[3, 3] = 3bd04ffd3a706569
[4, 3] = 299977ff8fe22372
[0, 4] = 64fbfc9b326cec67
[1, 4] = 853dbf93b5ba8770
[2, 4] = f350194d6c82be74
[3, 4] = 1a75365e47fe493d
[4, 4] = d9f1c3724f5314b0
```

Round #0

After theta

```
2A 23 12 B5 D7 56 06 04 86 90 EF 32 C2 63 F6 C7
54 97 C9 8D A8 6B E1 5A 46 F9 A9 52 77 E9 B2 A8
50 10 4C 48 10 F8 1F FE 80 6A 72 1A D1 74 5E E2
9C 24 58 69 FA 8D 9E 07 70 D3 0E 6E 63 E3 EE 0B
2A C1 E4 76 AD 18 80 27 82 00 70 5C D3 84 F0 C9
71 EC 43 10 F7 A1 F7 A0 B1 51 9F E7 F2 45 07 F5
84 E2 B4 0F EF AB 77 7E 96 26 D5 E8 FB 73 57 D1
72 26 3A 7A 5A 7F FA 37 74 19 27 C2 50 31 8C 82
99 3C 69 F0 E7 92 25 3B 85 B3 D8 05 EA E7 23 6A
30 E0 C9 B8 C0 9B DF DD 14 35 9D 22 34 C4 E6 F1
E6 47 52 C2 39 F5 16 5A 1B 81 81 F0 AE 4A F2 49
D9 8F 26 F2 8D C0 B9 4B 64 CC 47 C5 63 E2 7A FC
            D6 02 2C E2 B9 70 8E 01
```

After rho

```
2A 23 12 B5 D7 56 06 04 0D 21 DF 65 84 C7 EC 8F
D5 65 72 23 EA 5A B8 16 97 2E 8B 6A 94 9F 2A 75
C0 FF F0 87 82 60 42 82 11 4D E7 25 0E A8 26 A7
95 A6 DF E8 79 C0 49 82 02 DC B4 83 DB D8 B8 FB
60 72 BB 56 0C C0 13 95 08 9F 2C 08 00 C7 35 4D
8D 63 1F 82 B8 0F BD 07 D4 C7 46 7D 9E CB 17 1D
7D 78 5F BD F3 23 14 A7 E7 AE A2 2D 4D AA D1 F7
3D AD 3F FD 1B 39 13 1D 84 A1 62 18 05 E9 32 4E
0D FE 5C B2 64 27 93 27 11 B5 C2 59 EC 02 F5 F3
F3 BB 1B 06 3C 19 17 78 F1 14 35 9D 22 34 C4 E6
5B 68 99 1F 49 09 E7 D4 6D 04 06 C2 BB 2A C9 27
FB D1 44 BE 11 38 77 29 CC 47 C5 63 E2 7A FC 64
            63 80 B5 00 8B 78 2E 9C
```

After pi

```
2A 23 12 B5 D7 56 06 04 95 A6 DF E8 79 C0 49 82
7D 78 5F BD F3 23 14 A7 F3 BB 1B 06 3C 19 17 78
63 80 B5 00 8B 78 2E 9C 97 2E 8B 6A 94 9F 2A 75
08 9F 2C 08 00 C7 35 4D 8D 63 1F 82 B8 0F BD 07
0D FE 5C B2 64 27 93 27 FB D1 44 BE 11 38 77 29
0D 21 DF 65 84 C7 EC 8F 02 DC B4 83 DB D8 B8 FB
E7 AE A2 2D 4D AA D1 F7 F1 14 35 9D 22 34 C4 E6
5B 68 99 1F 49 09 E7 D4 C0 FF F0 87 82 60 42 82
11 4D E7 25 0E A8 26 A7 D4 C7 46 7D 9E CB 17 1D
11 B5 C2 59 EC 02 F5 F3 CC 47 C5 63 E2 7A FC 64
D5 65 72 23 EA 5A B8 16 60 72 BB 56 0C C0 13 95
3D AD 3F FD 1B 39 13 1D 84 A1 62 18 05 E9 32 4E
            6D 04 06 C2 BB 2A C9 27
```

After chi

```
42 7B 12 A0 55 75 12 21 17 25 DF EA 75 D8 4A DA
7D 78 FB BD 70 43 3C 23 FB 98 19 B3 68 1F 17 78
F6 04 78 48 A3 F8 67 1E 12 4E 98 E8 2C 97 A2 77
08 03 6C 38 44 E7 37 6D 7F 62 1F 8E A9 17 D9 0F
09 D0 D7 F2 E0 A0 9B 73 F3 40 60 BE 11 78 62 21
E8 03 DD 49 80 E5 AD 8B 12 CC A1 13 F9 CC BC FB
ED C6 2A 2F 04 A3 F2 E7 F5 15 73 FD A6 F2 CC ED
59 B4 B9 9D 12 11 F7 A4 04 7D F0 DF 12 23 53 9A
10 7D 67 25 6E A8 C6 45 18 85 43 5F 9C B3 1F 19
11 0D F2 DD EC 02 F7 71 DD 47 C2 43 EE F2 D8 41
C8 E8 76 8A F9 63 B8 1E E0 72 FB 56 08 00 33 D7
54 A9 3B 3F A1 3B DA 3C 14 C0 12 39 45 B9 02 5E
            4D 16 8F 96 BF AA CA A6
```

After iota

```
43 7B 12 A0 55 75 12 21 17 25 DF EA 75 D8 4A DA
7D 78 FB BD 70 43 3C 23 FB 98 19 B3 68 1F 17 78
F6 04 78 48 A3 F8 67 1E 12 4E 98 E8 2C 97 A2 77
08 03 6C 38 44 E7 37 6D 7F 62 1F 8E A9 17 D9 0F
09 D0 D7 F2 E0 A0 9B 73 F3 40 60 BE 11 78 62 21
E8 03 DD 49 80 E5 AD 8B 12 CC A1 13 F9 CC BC FB
ED C6 2A 2F 04 A3 F2 E7 F5 15 73 FD A6 F2 CC ED
59 B4 B9 9D 12 11 F7 A4 04 7D F0 DF 12 23 53 9A
10 7D 67 25 6E A8 C6 45 18 85 43 5F 9C B3 1F 19
11 0D F2 DD EC 02 F7 71 DD 47 C2 43 EE F2 D8 41
C8 E8 76 8A F9 63 B8 1E E0 72 FB 56 08 00 33 D7
54 A9 3B 3F A1 3B DA 3C 14 C0 12 39 45 B9 02 5E
            4D 16 8F 96 BF AA CA A6
```

(Skip rounds 1 to 22)

Round #23

After theta

```
A2 AF 0C FF F2 B7 95 B7 92 E2 AC 2F 78 C0 CC 08
80 1D 23 23 1A 00 08 83 FB 92 91 C8 EB 77 D0 6C
D8 DC D7 76 3A 51 A1 27 9B 05 D4 67 4C B2 0B E9
74 EB F6 A8 05 CC CD EA 65 C8 5D 5A D6 32 C5 39
5A 45 20 4D 59 66 5D 4E FE 9C 58 88 D3 BC 12 A5
3E 25 20 3E 1F 6F E1 69 DD 90 E8 68 E6 68 DE BD
38 C1 FC 22 73 88 E7 78 55 69 E1 AF 45 17 93 20
```

```
2F AD 5A 68 01 30 3B C2 67 8E B1 87 19 EA 09 08
A7 0B E8 8A 74 96 95 90 98 B6 8F 55 74 44 77 93
1A 04 2F D6 4B 8E 00 33 C8 54 D8 42 8C 8D 54 5B
56 CB 31 2A 69 A8 29 E8 81 57 64 31 8A E7 26 9C
50 DD 62 C4 1B EF CD 15 06 92 5C 84 B3 61 C9 FE
            C9 8D 69 73 C0 F0 6C F0
```

After rho

```
A2 AF 0C FF F2 B7 95 B7 24 C5 59 5F F0 80 99 11
60 C7 C8 88 06 00 C2 20 7E 07 CD B6 2F 19 89 BC
89 0A 3D C1 E6 BE B6 D3 C6 24 BB 90 BE 59 40 7D
8F 5A C0 DC AC 4E B7 6E 4E 19 72 97 96 B5 4C 71
22 90 A6 2C B3 2E 27 AD 2B 51 EA CF 89 85 38 CD
F3 29 01 F1 F9 78 0B 4F F7 76 43 A2 A3 99 A3 79
17 99 43 3C C7 C3 09 E6 2E 26 41 AA D2 C2 5F 8B
B4 00 98 1D E1 97 56 2D 0F 33 D4 13 10 CE 1C 63
5D 91 CE B2 12 F2 74 01 BB 49 4C DB C7 2A 3A A2
11 60 46 83 E0 C5 7A C9 5B C8 54 D8 42 8C 8D 54
A6 A0 5B 2D C7 A8 A4 A1 06 5E 91 C5 28 9E 9B 70
AA 5B 8C 78 E3 BD B9 02 92 5C 84 B3 61 C9 FE 06
            1B 7C 72 63 DA 1C 30 3C
```

After pi

```
A2 AF 0C FF F2 B7 95 B7 8F 5A C0 DC AC 4E B7 6E
17 99 43 3C C7 C3 09 E6 11 60 46 83 E0 C5 7A C9
1B 7C 72 63 DA 1C 30 3C 7E 07 CD B6 2F 19 89 BC
2B 51 EA CF 89 85 38 CD F3 29 01 F1 F9 78 0B 4F
5D 91 CE B2 12 F2 74 01 AA 5B 8C 78 E3 BD B9 02
24 C5 59 5F F0 80 99 11 4E 19 72 97 96 B5 4C 71
2E 26 41 AA D2 C2 5F 8B 5B C8 54 D8 42 8C 8D 54
A6 A0 5B 2D C7 A8 A4 A1 89 0A 3D C1 E6 BE B6 D3
C6 24 BB 90 BE 59 40 7D F7 76 43 A2 A3 99 A3 79
BB 49 4C DB C7 2A 3A A2 92 5C 84 B3 61 C9 FE 06
60 C7 C8 88 06 00 C2 20 22 90 A6 2C B3 2E 27 AD
B4 00 98 1D E1 97 56 2D 0F 33 D4 13 10 CE 1C 63
            06 5E 91 C5 28 9E 9B 70
```

After chi

```
B2 2E 0F DF B1 36 9D 37 8F 3A C4 5F 8C 4A C5 67
1D 85 73 5C DD DB 09 D2 B1 E3 4A 1F C0 66 FF 4A
16 2C B2 63 D6 54 12 74 AE 2F CC 86 5F 61 8A BE
27 C1 24 CD 8B 07 4C CD 51 63 01 B9 18 75 82 4D
09 95 8F 34 1E F2 74 BD AB 0B AE 31 63 39 89 43
04 E3 58 77 B0 C2 8A 9B 1F D1 66 C7 96 B9 CC 25
8A 06 4A 8F 57 E2 7F 2A 5B 8D 54 8A 72 8C 94 44
EC B8 79 AD C1 9D E0 C1 B8 58 7D E3 E7 3E 15 D3
CE 2D B7 C9 FA 7B 58 FF F7 62 C3 82 83 58 67 7D
B2 4B 75 9B 41 1C 3A 73 D4 78 06 A3 79 88 BE 2A
F4 C7 D0 99 46 91 92 20 29 A3 E2 2E A3 66 2F EF
B4 4C 99 D9 C9 87 D5 3D 6F B2 9C 1B 16 CE 5C 63
            04 4E B7 E1 99 B0 BE FD
```

After iota

```
BA AE 0F 5F B1 36 9D B7 8F 3A C4 5F 8C 4A C5 67
1D 85 73 5C DD DB 09 D2 B1 E3 4A 1F C0 66 FF 4A
16 2C B2 63 D6 54 12 74 AE 2F CC 86 5F 61 8A BE
27 C1 24 CD 8B 07 4C CD 51 63 01 B9 18 75 82 4D
```

```
09 95 8F 34 1E F2 74 BD AB 0B AE 31 63 39 89 43
04 E3 58 77 B0 C2 8A 9B 1F D1 66 C7 96 B9 CC 25
8A 06 4A 8F 57 E2 7F 2A 5B 8D 54 8A 72 8C 94 44
EC B8 79 AD C1 9D E0 C1 B8 58 7D E3 E7 3E 15 D3
CE 2D B7 C9 FA 7B 58 FF F7 62 C3 82 83 58 67 7D
B2 4B 75 9B 41 1C 3A 73 D4 78 06 A3 79 88 BE 2A
F4 C7 D0 99 46 91 92 20 29 A3 E2 2E A3 66 2F EF
B4 4C 99 D9 C9 87 D5 3D 6F B2 9C 1B 16 CE 5C 63
            04 4E B7 E1 99 B0 BE FD
```

After permutation

```
BA AE 0F 5F B1 36 9D B7 8F 3A C4 5F 8C 4A C5 67
1D 85 73 5C DD DB 09 D2 B1 E3 4A 1F C0 66 FF 4A
16 2C B2 63 D6 54 12 74 AE 2F CC 86 5F 61 8A BE
27 C1 24 CD 8B 07 4C CD 51 63 01 B9 18 75 82 4D
09 95 8F 34 1E F2 74 BD AB 0B AE 31 63 39 89 43
04 E3 58 77 B0 C2 8A 9B 1F D1 66 C7 96 B9 CC 25
8A 06 4A 8F 57 E2 7F 2A 5B 8D 54 8A 72 8C 94 44
EC B8 79 AD C1 9D E0 C1 B8 58 7D E3 E7 3E 15 D3
CE 2D B7 C9 FA 7B 58 FF F7 62 C3 82 83 58 67 7D
B2 4B 75 9B 41 1C 3A 73 D4 78 06 A3 79 88 BE 2A
F4 C7 D0 99 46 91 92 20 29 A3 E2 2E A3 66 2F EF
B4 4C 99 D9 C9 87 D5 3D 6F B2 9C 1B 16 CE 5C 63
            04 4E B7 E1 99 B0 BE FD
```

State (as lanes of integers)

```
[0, 0] = b79d36b15f0faeba
[1, 0] = 67c54a8c5fc43a8f
[2, 0] = d209dbdd5c73851d
[3, 0] = 4aff66c01f4ae3b1
[4, 0] = 741254d663b22c16
[0, 1] = be8a615f86cc2fae
[1, 1] = cd4c078bcd24c127
[2, 1] = 4d827518b9016351
[3, 1] = bd74f21e348f9509
[4, 1] = 4389396331ae0bab
[0, 2] = 9b8ac2b07758e304
[1, 2] = 25ccb996c766d11f
[2, 2] = 2a7fe2578f4a068a
[3, 2] = 44948c728a548d5b
[4, 2] = c1e09dc1ad79b8ec
[0, 3] = d3153ee7e37d58b8
[1, 3] = ff587bfac9b72dce
[2, 3] = 7d67588382c362f7
[3, 3] = 733a1c419b754bb2
[4, 3] = 2abe8879a30678d4
[0, 4] = 2092914699d0c7f4
[1, 4] = ef2f66a32ee2a329
[2, 4] = 3dd587c9d9994cb4
[3, 4] = 635cce161b9cb26f
[4, 4] = fdbeb099e1b74e04
```

The hash value is

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

SHAKE-256 sample to produce 4096-bits of output

The message as a bit string

```
1 1 0 0 1
```

About to call last of the absorb phase

XORed state (in bytes)

```
F3 03 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 80 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
               00 00 00 00 00 00 00 00
```

XORed state (as lanes of integers)

```
[0, 0] = 00000000000003f3
[1, 0] = 0000000000000000
[2, 0] = 0000000000000000
[3, 0] = 0000000000000000
[4, 0] = 0000000000000000
[0, 1] = 0000000000000000
[1, 1] = 0000000000000000
[2, 1] = 0000000000000000
[3, 1] = 0000000000000000
[4, 1] = 0000000000000000
[0, 2] = 0000000000000000
[1, 2] = 0000000000000000
[2, 2] = 0000000000000000
[3, 2] = 0000000000000000
[4, 2] = 0000000000000000
[0, 3] = 0000000000000000
[1, 3] = 8000000000000000
[2, 3] = 0000000000000000
[3, 3] = 0000000000000000
[4, 3] = 0000000000000000
[0, 4] = 0000000000000000
[1, 4] = 0000000000000000
[2, 4] = 0000000000000000
[3, 4] = 0000000000000000
[4, 4] = 0000000000000000
```

Round #0

After theta

```
F2 03 00 00 00 00 00 00 F3 03 00 00 00 00 00 00
00 00 00 00 00 00 00 80 00 00 00 00 00 00 00 00
E6 07 00 00 00 00 00 00 01 00 00 00 00 00 00 00
F3 03 00 00 00 00 00 00 00 00 00 00 00 00 00 80
00 00 00 00 00 00 00 00 E6 07 00 00 00 00 00 00
01 00 00 00 00 00 00 00 F3 03 00 00 00 00 00 00
00 00 00 00 00 00 00 80 00 00 00 00 00 00 00 00
E6 07 00 00 00 00 00 00 01 00 00 00 00 00 00 00
F3 03 00 00 00 00 00 80 00 00 00 00 00 00 00 80
00 00 00 00 00 00 00 00 E6 07 00 00 00 00 00 00
01 00 00 00 00 00 00 00 F3 03 00 00 00 00 00 00
00 00 00 00 00 00 00 80 00 00 00 00 00 00 00 00
            E6 07 00 00 00 00 00 00
```

After rho

```
F2 03 00 00 00 00 00 00 E6 07 00 00 00 00 00 00
00 00 00 00 00 00 00 20 00 00 00 00 00 00 00 00
00 00 00 30 3F 00 00 00 00 00 00 00 10 00 00 00
00 00 00 00 00 30 3F 00 20 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 60 7E 00 00 00 00
08 00 00 00 00 00 00 00 00 CC 0F 00 00 00 00 00
00 00 00 00 00 04 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 F3 03 00 00 00 00 00 00 02 00 00
00 00 00 00 00 70 7E 00 00 40 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 E6 07 00 00 00 00 00
```

```
00 00 04 00 00 00 00 00 CC 0F 00 00 00 00 00 00
00 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00
            00 80 F9 01 00 00 00 00
```

After pi

```
F2 03 00 00 00 00 00 00 00 00 00 00 00 30 3F 00
00 00 00 00 00 04 00 00 00 00 00 00 00 00 00 00
00 80 F9 01 00 00 00 00 00 00 00 00 00 00 00 00
00 00 60 7E 00 00 00 00 08 00 00 00 00 00 00 00
00 00 00 00 00 70 7E 00 00 00 00 00 00 00 00 10
E6 07 00 00 00 00 00 00 20 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 E6 07 00 00 00 00 00
00 00 04 00 00 00 00 00 00 00 00 30 3F 00 00 00
00 00 00 00 10 00 00 00 00 CC 0F 00 00 00 00 00
00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 20 00 00 00 00 00 00 00 00
00 00 00 00 00 F3 03 00 00 00 00 00 00 02 00 00
            CC 0F 00 00 00 00 00 00
```

After chi

```
F2 03 00 00 00 04 00 00 00 00 00 00 00 30 3F 00
00 80 F9 01 00 04 00 00 F2 03 00 00 00 00 00 00
00 80 F9 01 00 30 3F 00 08 00 00 00 00 00 00 00
00 00 60 7E 00 70 7E 00 08 00 00 00 00 00 00 10
00 00 00 00 00 70 7E 00 00 00 60 7E 00 00 00 10
E6 07 00 00 00 00 00 00 20 E6 07 00 00 00 00 00
00 00 00 00 00 00 00 00 E6 E1 07 00 00 00 00 00
00 00 04 00 00 00 00 00 00 CC 0F 30 3F 00 00 00
00 00 00 00 10 00 00 00 00 CC 0F 00 00 00 00 00
00 40 00 30 3F 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 F3 03 20 00 00 00 00 00 00 00 00
CC 0F 00 00 00 F3 03 00 00 00 00 00 00 02 00 20
            CC 0F 00 00 00 00 00 00
```

After iota

```
F3 03 00 00 00 04 00 00 00 00 00 00 00 30 3F 00
00 80 F9 01 00 04 00 00 F2 03 00 00 00 00 00 00
00 80 F9 01 00 30 3F 00 08 00 00 00 00 00 00 00
00 00 60 7E 00 70 7E 00 08 00 00 00 00 00 00 10
00 00 00 00 00 70 7E 00 00 00 60 7E 00 00 00 10
E6 07 00 00 00 00 00 00 20 E6 07 00 00 00 00 00
00 00 00 00 00 00 00 00 E6 E1 07 00 00 00 00 00
00 00 04 00 00 00 00 00 00 CC 0F 30 3F 00 00 00
00 00 00 00 10 00 00 00 00 CC 0F 00 00 00 00 00
00 40 00 30 3F 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 F3 03 20 00 00 00 00 00 00 00 00
CC 0F 00 00 00 F3 03 00 00 00 00 00 00 02 00 20
            CC 0F 00 00 00 00 00 00
```

(Skip rounds 1 to 22)

Round #23

After theta

```
10 64 F8 8A 58 EA FD 09 4F 47 34 E5 34 17 1E 5B
E3 EE 8E 1B 3F 38 D3 9A 13 08 57 F5 1D EF 8F 0A
A9 6D 32 69 00 E7 BE BD B6 D8 49 9C 4A F7 31 15
84 D7 F2 62 62 54 94 B0 F1 67 CE 06 93 54 72 55
```

```
ED 42 49 FF EC 51 EB 31 35 98 45 D9 B6 7B 98 EF
CF 83 0D 3D 75 3D 03 93 4F CD 72 0F F6 BB 7E 08
49 25 D0 AF AC A7 6A BD 62 51 57 53 89 41 27 EF
35 65 E1 63 08 11 8D 81 03 F5 DE 49 DE 81 BC EA
8E CB 06 60 AB AE 7A A3 B5 64 48 65 97 61 22 7A
F9 65 03 3B 93 A0 A3 40 E8 3A AE 3A F3 8F F8 5F
83 9A 70 9B 51 02 A2 A5 3C 89 27 10 B3 E0 01 94
AE 25 64 44 ED CE 7E 1C BA 0C 0E DE C9 BC 3E F0
            48 88 D8 29 62 F4 34 67
```

After rho

```
10 64 F8 8A 58 EA FD 09 9E 8E 68 CA 69 2E 3C B6
B8 BB E3 C6 0F CE B4 E6 F1 FE A8 30 81 70 55 DF
38 F7 ED 4D 6D 93 49 03 A9 74 1F 53 61 8B 9D C4
2F 26 46 45 09 4B 78 2D 55 FC 99 B3 C1 24 95 5C
A1 A4 7F F6 A8 F5 98 76 87 F9 5E 83 59 94 6D BB
7C 1E 6C E8 A9 EB 19 98 21 3C 35 CB 3D D8 EF FA
7E 65 3D 55 EB 4D 2A 81 83 4E DE C5 A2 AE A6 12
31 84 88 C6 C0 9A B2 F0 93 BC 03 79 D5 07 EA BD
00 6C D5 55 6F D4 71 D9 11 BD 5A 32 A4 B2 CB 30
74 14 28 BF 6C 60 67 12 5F E8 3A AE 3A F3 8F F8
88 96 0E 6A C2 6D 46 09 F2 24 9E 40 CC 82 07 50
B5 84 8C A8 DD D9 8F C3 0C 0E DE C9 BC 3E F0 BA
            CD 19 12 22 76 8A 18 3D
```

After pi

```
10 64 F8 8A 58 EA FD 09 2F 26 46 45 09 4B 78 2D
7E 65 3D 55 EB 4D 2A 81 74 14 28 BF 6C 60 67 12
CD 19 12 22 76 8A 18 3D F1 FE A8 30 81 70 55 DF
87 F9 5E 83 59 94 6D BB 7C 1E 6C E8 A9 EB 19 98
00 6C D5 55 6F D4 71 D9 B5 84 8C A8 DD D9 8F C3
9E 8E 68 CA 69 2E 3C B6 55 FC 99 B3 C1 24 95 5C
83 4E DE C5 A2 AE A6 12 5F E8 3A AE 3A F3 8F F8
88 96 0E 6A C2 6D 46 09 38 F7 ED 4D 6D 93 49 03
A9 74 1F 53 61 8B 9D C4 21 3C 35 CB 3D D8 EF FA
11 BD 5A 32 A4 B2 CB 30 0C 0E DE C9 BC 3E F0 BA
B8 BB E3 C6 0F CE B4 E6 A1 A4 7F F6 A8 F5 98 76
31 84 88 C6 C0 9A B2 F0 93 BC 03 79 D5 07 EA BD
            F2 24 9E 40 CC 82 07 50
```

After chi

```
40 25 C1 9A BA EE FF 89 2F 36 46 EF 0D 6B 3D 3F
F7 6C 2F 55 F9 C7 32 AC 64 70 C0 37 64 00 82 12
E2 1B 14 67 77 8B 18 19 89 F8 88 58 21 1B 45 DF
87 99 CF 96 1F 80 0D FA C9 9E 64 40 39 E2 97 9A
40 16 F5 45 6F F4 21 C5 B3 85 DA 2B 85 5D A7 E3
1C 8C 2E 8E 4B A4 1E B4 09 5C B9 99 D9 75 9C B4
03 58 DA 85 62 A2 E6 13 49 E0 5A 2E 13 F1 B7 4E
C9 E6 9F 5B 42 6D C7 41 38 FF CD C5 71 C3 2B 39
B9 F5 55 63 E1 A9 9D C4 2D 3E B1 02 25 D4 DF 70
21 4C 7B 36 E5 33 C2 31 8D 0E CC DB BC 36 64 7E
A8 BB 63 C6 4F C4 96 66 23 9C 7C CF BD F0 D0 7B
51 84 14 C6 C8 1A B7 B0 9B 27 62 FF D6 4B 5A 1B
            F3 20 82 70 6C B3 0F 40
```

After iota

```
48 A5 C1 1A BA EE FF 09 2F 36 46 EF 0D 6B 3D 3F
F7 6C 2F 55 F9 C7 32 AC 64 70 C0 37 64 00 82 12
E2 1B 14 67 77 8B 18 19 89 F8 88 58 21 1B 45 DF
87 99 CF 96 1F 80 0D FA C9 9E 64 40 39 E2 97 9A
40 16 F5 45 6F F4 21 C5 B3 85 DA 2B 85 5D A7 E3
1C 8C 2E 8E 4B A4 1E B4 09 5C B9 99 D9 75 9C B4
03 58 DA 85 62 A2 E6 13 49 E0 5A 2E 13 F1 B7 4E
C9 E6 9F 5B 42 6D C7 41 38 FF CD C5 71 C3 2B 39
B9 F5 55 63 E1 A9 9D C4 2D 3E B1 02 25 D4 DF 70
21 4C 7B 36 E5 33 C2 31 8D 0E CC DB BC 36 64 7E
A8 BB 63 C6 4F C4 96 66 23 9C 7C CF BD F0 D0 7B
51 84 14 C6 C8 1A B7 B0 9B 27 62 FF D6 4B 5A 1B
            F3 20 82 70 6C B3 0F 40
```

After permutation

```
48 A5 C1 1A BA EE FF 09 2F 36 46 EF 0D 6B 3D 3F
F7 6C 2F 55 F9 C7 32 AC 64 70 C0 37 64 00 82 12
E2 1B 14 67 77 8B 18 19 89 F8 88 58 21 1B 45 DF
87 99 CF 96 1F 80 0D FA C9 9E 64 40 39 E2 97 9A
40 16 F5 45 6F F4 21 C5 B3 85 DA 2B 85 5D A7 E3
1C 8C 2E 8E 4B A4 1E B4 09 5C B9 99 D9 75 9C B4
03 58 DA 85 62 A2 E6 13 49 E0 5A 2E 13 F1 B7 4E
C9 E6 9F 5B 42 6D C7 41 38 FF CD C5 71 C3 2B 39
B9 F5 55 63 E1 A9 9D C4 2D 3E B1 02 25 D4 DF 70
21 4C 7B 36 E5 33 C2 31 8D 0E CC DB BC 36 64 7E
A8 BB 63 C6 4F C4 96 66 23 9C 7C CF BD F0 D0 7B
51 84 14 C6 C8 1A B7 B0 9B 27 62 FF D6 4B 5A 1B
            F3 20 82 70 6C B3 0F 40
```

State (as lanes of integers)

```
[0, 0] = 09ffeeba1ac1a548
[1, 0] = 3f3d6b0def46362f
[2, 0] = ac32c7f9552f6cf7
[3, 0] = 1282006437c07064
[4, 0] = 19188b7767141be2
[0, 1] = df451b215888f889
[1, 1] = fa0d801f96cf9987
[2, 1] = 9a97e23940649ec9
[3, 1] = c521f46f45f51640
[4, 1] = e3a75d852bda85b3
[0, 2] = b41ea44b8e2e8c1c
[1, 2] = b49c75d999b95c09
[2, 2] = 13e6a26285da5803
[3, 2] = 4eb7f1132e5ae049
[4, 2] = 41c76d425b9fe6c9
[0, 3] = 392bc371c5cdff38
[1, 3] = c49da9e16355f5b9
[2, 3] = 70dfd42502b13e2d
[3, 3] = 31c233e5367b4c21
[4, 3] = 7e6436bcdbcc0e8d
[0, 4] = 6696c44fc663bba8
[1, 4] = 7bd0f0bdcf7c9c23
[2, 4] = b0b71ac8c6148451
```

```
[3, 4] = 1b5a4bd6ff62279b
[4, 4] = 400fb36c708220f3
```

About to call squeeze (again)

State before permutation (in bytes)

```
48 A5 C1 1A BA EE FF 09 2F 36 46 EF 0D 6B 3D 3F
F7 6C 2F 55 F9 C7 32 AC 64 70 C0 37 64 00 82 12
E2 1B 14 67 77 8B 18 19 89 F8 88 58 21 1B 45 DF
87 99 CF 96 1F 80 0D FA C9 9E 64 40 39 E2 97 9A
40 16 F5 45 6F F4 21 C5 B3 85 DA 2B 85 5D A7 E3
1C 8C 2E 8E 4B A4 1E B4 09 5C B9 99 D9 75 9C B4
03 58 DA 85 62 A2 E6 13 49 E0 5A 2E 13 F1 B7 4E
C9 E6 9F 5B 42 6D C7 41 38 FF CD C5 71 C3 2B 39
B9 F5 55 63 E1 A9 9D C4 2D 3E B1 02 25 D4 DF 70
21 4C 7B 36 E5 33 C2 31 8D 0E CC DB BC 36 64 7E
A8 BB 63 C6 4F C4 96 66 23 9C 7C CF BD F0 D0 7B
51 84 14 C6 C8 1A B7 B0 9B 27 62 FF D6 4B 5A 1B
            F3 20 82 70 6C B3 0F 40
```

State before permutation (as lanes of integers)

```
[0, 0] = 09ffeeba1ac1a548
[1, 0] = 3f3d6b0def46362f
[2, 0] = ac32c7f9552f6cf7
[3, 0] = 1282006437c07064
[4, 0] = 19188b7767141be2
[0, 1] = df451b215888f889
[1, 1] = fa0d801f96cf9987
[2, 1] = 9a97e23940649ec9
[3, 1] = c521f46f45f51640
[4, 1] = e3a75d852bda85b3
[0, 2] = b41ea44b8e2e8c1c
[1, 2] = b49c75d999b95c09
[2, 2] = 13e6a26285da5803
[3, 2] = 4eb7f1132e5ae049
[4, 2] = 41c76d425b9fe6c9
[0, 3] = 392bc371c5cdff38
[1, 3] = c49da9e16355f5b9
[2, 3] = 70dfd42502b13e2d
[3, 3] = 31c233e5367b4c21
[4, 3] = 7e6436bcdbcc0e8d
[0, 4] = 6696c44fc663bba8
[1, 4] = 7bd0f0bdcf7c9c23
[2, 4] = b0b71ac8c6148451
[3, 4] = 1b5a4bd6ff62279b
[4, 4] = 400fb36c708220f3
```

Round #0

After theta

```
D9 C7 ED 3E F4 5F 2F 11 E1 83 E7 88 7D AF 72 C8
63 2D DB 33 39 FA CB 05 E8 CD CA 1B EA 35 8F FD
AF DC F1 6D 81 5B A6 D0 18 9A A4 7C 6F AA 95 C7
49 2C 6E F1 6F 44 42 0D 5D DF 90 26 F9 DF 6E 33
CC AB FF 69 E1 C1 2C 2A FE 42 3F 21 73 8D 19 2A
8D EE 02 AA 05 15 CE AC C7 E9 18 FE A9 B1 D3 43
97 19 2E E3 A2 9F 1F BA C5 5D 50 02 9D C4 BA A1
```

```
84 21 7A 51 B4 BD 79 88 A9 9D E1 E1 3F 72 FB 21
77 40 F4 04 91 6D D2 33 B9 7F 45 64 E5 E9 26 D9
AD F1 71 1A 6B 06 CF DE C0 C9 29 D1 4A E6 DA B7
39 D9 4F E2 01 75 46 7E ED 29 DD A8 CD 34 9F 8C
C5 C5 E0 A0 08 27 4E 19 17 9A 68 D3 58 7E 57 F4
            BE E7 67 7A 9A 63 B1 89
```

After rho

```
D9 C7 ED 3E F4 5F 2F 11 C3 07 CF 11 FB 5E E5 90
58 CB F6 4C 8E FE 72 C1 5E F3 D8 8F DE AC BC A1
DC 32 85 7E E5 8E 6F 0B F7 A6 5A 79 8C A1 49 CA
16 FF 46 24 D4 90 C4 E2 4C D7 37 A4 49 FE B7 DB
D5 FF B4 F0 60 16 15 E6 98 A1 E2 2F F4 13 32 D7
6D 74 17 50 2D A8 70 66 0F 1D A7 63 F8 A7 C6 4E
19 17 FD FC D0 BD CC 70 89 75 43 8B BB A0 04 3A
28 DA DE 3C 44 C2 10 BD C3 7F E4 F6 43 52 3B C3
9E 20 B2 4D 7A E6 0E 88 93 EC DC BF 22 B2 F2 74
E0 D9 BB 35 3E 4E 63 CD B7 C0 C9 29 D1 4A E6 DA
19 F9 E5 64 3F 89 07 D4 B6 A7 74 A3 36 D3 7C 32
B8 18 1C 14 E1 C4 29 A3 9A 68 D3 58 7E 57 F4 17
            6C A2 EF F9 99 9E E6 58
```

After pi

```
D9 C7 ED 3E F4 5F 2F 11 16 FF 46 24 D4 90 C4 E2
19 17 FD FC D0 BD CC 70 E0 D9 BB 35 3E 4E 63 CD
6C A2 EF F9 99 9E E6 58 5E F3 D8 8F DE AC BC A1
98 A1 E2 2F F4 13 32 D7 6D 74 17 50 2D A8 70 66
9E 20 B2 4D 7A E6 0E 88 B8 18 1C 14 E1 C4 29 A3
C3 07 CF 11 FB 5E E5 90 4C D7 37 A4 49 FE B7 DB
89 75 43 8B BB A0 04 3A B7 C0 C9 29 D1 4A E6 DA
19 F9 E5 64 3F 89 07 D4 DC 32 85 7E E5 8E 6F 0B
F7 A6 5A 79 8C A1 49 CA 0F 1D A7 63 F8 A7 C6 4E
93 EC DC BF 22 B2 F2 74 9A 68 D3 58 7E 57 F4 17
58 CB F6 4C 8E FE 72 C1 D5 FF B4 F0 60 16 15 E6
28 DA DE 3C 44 C2 10 BD C3 7F E4 F6 43 52 3B C3
            B6 A7 74 A3 36 D3 7C 32
```

After chi

```
D0 C7 54 E6 F4 72 27 01 F6 37 44 25 FA D2 E7 6F
15 35 B9 34 51 2D 48 60 71 9C BB 33 5A 0F 6A CC
6A 9A ED F9 99 1E 26 BA 3B A7 CD DF D7 04 FC 81
0A A1 42 22 A6 55 3C 5F 4D 6C 1B 40 AC A8 51 45
D8 C3 72 C6 64 CE 9A 88 38 18 3E 34 C1 D7 2B F5
42 27 8F 1A 49 5E E5 B0 7A 57 BF 84 09 B4 55 1B
81 4C 67 CF 95 21 05 3E 75 C6 C3 38 11 1C 06 DA
15 29 D5 C0 3F 29 15 9F D4 2B 20 7C 95 88 E9 0F
67 46 02 E5 8E B1 79 FA 07 1D A4 23 A4 E2 C2 4D
D7 FE D8 99 A3 3A F9 7C B9 EC 89 59 76 76 F4 D7
70 CB BC 40 8A 3E 72 D8 16 DA 94 32 63 06 3E A4
1C 5A CE 3D 70 43 54 8D 8B 37 66 BA CB 7E 39 02
            33 93 74 13 56 D3 79 14
```

After iota

```
D1 C7 54 E6 F4 72 27 01 F6 37 44 25 FA D2 E7 6F
15 35 B9 34 51 2D 48 60 71 9C BB 33 5A 0F 6A CC
6A 9A ED F9 99 1E 26 BA 3B A7 CD DF D7 04 FC 81
0A A1 42 22 A6 55 3C 5F 4D 6C 1B 40 AC A8 51 45
```

```
D8 C3 72 C6 64 CE 9A 88 38 18 3E 34 C1 D7 2B F5
42 27 8F 1A 49 5E E5 B0 7A 57 BF 84 09 B4 55 1B
81 4C 67 CF 95 21 05 3E 75 C6 C3 38 11 1C 06 DA
15 29 D5 C0 3F 29 15 9F D4 2B 20 7C 95 88 E9 0F
67 46 02 E5 8E B1 79 FA 07 1D A4 23 A4 E2 C2 4D
D7 FE D8 99 A3 3A F9 7C B9 EC 89 59 76 76 F4 D7
70 CB BC 40 8A 3E 72 D8 16 DA 94 32 63 06 3E A4
1C 5A CE 3D 70 43 54 8D 8B 37 66 BA CB 7E 39 02
            33 93 74 13 56 D3 79 14
```

(Skip rounds 1 to 22)

Round #23

After theta

```
2B 49 9B 82 1C 6A 2F 09 EC 3E AA 48 84 AC AC C3
59 B2 6F 09 C5 16 1E 91 BC 04 62 CF D8 D3 65 DD
4A 10 8D 9E 3A 88 C7 7D 00 AA 8F FC 22 1B B3 C9
6B 39 E0 16 20 76 42 18 15 B5 9C B6 E1 ED 68 D6
9A E5 D9 3D 79 A3 88 FE A8 AD 22 D5 D3 A7 56 0D
3F 0C 78 18 9A 92 35 4D 36 58 45 97 88 C4 AE ED
84 84 22 6D A1 7F A4 3E C4 7A 65 37 AB F9 5B F1
CE A9 58 20 C9 E3 7A 29 84 85 F6 48 2B FE 0D 4B
4E 66 6C DA 0B 5F D5 33 20 78 CB 9E 98 37 12 16
AB 34 41 D7 1E 75 87 22 7A 92 BF C6 5C 9F 3D F8
B8 74 0C 70 F0 D4 B2 A0 71 AF 4C D1 DE FF BD EA
2D 7A 06 E1 F0 3D 0E DD 61 18 64 8C B2 61 A3 81
            3F B2 AB CF 5A E5 14 00
```

After rho

```
2B 49 9B 82 1C 6A 2F 09 D9 7D 54 91 08 59 59 87
96 EC 5B 42 B1 85 47 64 3D 5D D6 CD 4B 20 F6 8C
41 3C EE 53 82 68 F4 D4 2F B2 31 9B 0C A0 FA C8
6E 01 62 27 84 B1 96 03 75 45 2D A7 6D 78 3B 9A
F2 EC 9E BC 51 44 7F CD 6A D5 80 DA 2A 52 3D 7D
FA 61 C0 C3 D0 94 AC 69 B6 DB 60 15 5D 22 12 BB
69 0B FD 23 F5 21 24 14 F3 B7 E2 89 F5 CA 6E 56
90 E4 71 BD 14 E7 54 2C 91 56 FC 1B 96 08 0B ED
4D 7B E1 AB 7A C6 C9 8C 09 0B 10 BC 65 4F CC 1B
EE 50 64 95 26 E8 DA A3 F8 7A 92 BF C6 5C 9F 3D
CB 82 E2 D2 31 C0 C1 53 C7 BD 32 45 7B FF F7 AA
45 CF 20 1C BE C7 A1 BB 18 64 8C B2 61 A3 81 61
            05 C0 8F EC EA B3 56 39
```

After pi

```
2B 49 9B 82 1C 6A 2F 09 6E 01 62 27 84 B1 96 03
69 0B FD 23 F5 21 24 14 EE 50 64 95 26 E8 DA A3
05 C0 8F EC EA B3 56 39 3D 5D D6 CD 4B 20 F6 8C
6A D5 80 DA 2A 52 3D 7D FA 61 C0 C3 D0 94 AC 69
4D 7B E1 AB 7A C6 C9 8C 45 CF 20 1C BE C7 A1 BB
D9 7D 54 91 08 59 59 87 75 45 2D A7 6D 78 3B 9A
F3 B7 E2 89 F5 CA 6E 56 F8 7A 92 BF C6 5C 9F 3D
CB 82 E2 D2 31 C0 C1 53 41 3C EE 53 82 68 F4 D4
2F B2 31 9B 0C A0 FA C8 B6 DB 60 15 5D 22 12 BB
09 0B 10 BC 65 4F CC 1B 18 64 8C B2 61 A3 81 61
96 EC 5B 42 B1 85 47 64 F2 EC 9E BC 51 44 7F CD
90 E4 71 BD 14 E7 54 2C 91 56 FC 1B 96 08 0B ED
            C7 BD 32 45 7B FF F7 AA
```

After chi

```
2A 43 06 82 6D 6A 0F 1D E8 51 62 B3 86 79 4C A0
68 8B 76 4B 3D 32 20 0C C4 59 74 97 32 A0 F3 A3
41 C0 EF C9 6A 22 C6 3B AD 7D 96 CC 9B A4 76 8C
6F CF A1 F2 00 10 7C F9 FA E5 C0 D7 54 95 8C 5A
75 6B 37 6A 3B E6 9F 88 07 4F 20 0E 9E 95 A8 CA
5B CF 96 99 98 DB 1D C3 7D 0D 3D 91 6F 6C AA B3
F0 37 82 C9 C4 4A 2E 14 E8 07 86 BE CE 45 87 B9
EF 82 CB F4 54 E0 E3 4B D1 75 AE 57 D3 6A F4 E7
26 B2 21 33 2C ED 36 C8 A6 BF EC 17 5D 82 13 DB
48 13 72 FD E7 07 B8 8F 36 E6 9D 3A 6D 23 8B 69
96 EC 3A 43 B5 26 47 44 F3 FE 12 BE D3 4C 74 0C
D6 4D 73 F9 7D 10 A0 2E 81 16 B5 19 16 08 0B A9
            A7 BD B6 F9 3B BF CF 23
```

After iota

```
22 C3 06 02 6D 6A 0F 9D E8 51 62 B3 86 79 4C A0
68 8B 76 4B 3D 32 20 0C C4 59 74 97 32 A0 F3 A3
41 C0 EF C9 6A 22 C6 3B AD 7D 96 CC 9B A4 76 8C
6F CF A1 F2 00 10 7C F9 FA E5 C0 D7 54 95 8C 5A
75 6B 37 6A 3B E6 9F 88 07 4F 20 0E 9E 95 A8 CA
5B CF 96 99 98 DB 1D C3 7D 0D 3D 91 6F 6C AA B3
F0 37 82 C9 C4 4A 2E 14 E8 07 86 BE CE 45 87 B9
EF 82 CB F4 54 E0 E3 4B D1 75 AE 57 D3 6A F4 E7
26 B2 21 33 2C ED 36 C8 A6 BF EC 17 5D 82 13 DB
48 13 72 FD E7 07 B8 8F 36 E6 9D 3A 6D 23 8B 69
96 EC 3A 43 B5 26 47 44 F3 FE 12 BE D3 4C 74 0C
D6 4D 73 F9 7D 10 A0 2E 81 16 B5 19 16 08 0B A9
            A7 BD B6 F9 3B BF CF 23
```

After permutation

```
22 C3 06 02 6D 6A 0F 9D E8 51 62 B3 86 79 4C A0
68 8B 76 4B 3D 32 20 0C C4 59 74 97 32 A0 F3 A3
41 C0 EF C9 6A 22 C6 3B AD 7D 96 CC 9B A4 76 8C
6F CF A1 F2 00 10 7C F9 FA E5 C0 D7 54 95 8C 5A
75 6B 37 6A 3B E6 9F 88 07 4F 20 0E 9E 95 A8 CA
5B CF 96 99 98 DB 1D C3 7D 0D 3D 91 6F 6C AA B3
F0 37 82 C9 C4 4A 2E 14 E8 07 86 BE CE 45 87 B9
EF 82 CB F4 54 E0 E3 4B D1 75 AE 57 D3 6A F4 E7
26 B2 21 33 2C ED 36 C8 A6 BF EC 17 5D 82 13 DB
48 13 72 FD E7 07 B8 8F 36 E6 9D 3A 6D 23 8B 69
96 EC 3A 43 B5 26 47 44 F3 FE 12 BE D3 4C 74 0C
D6 4D 73 F9 7D 10 A0 2E 81 16 B5 19 16 08 0B A9
            A7 BD B6 F9 3B BF CF 23
```

State (as lanes of integers)

```
[0, 0] = 9d0f6a6d0206c322
[1, 0] = a04c7986b36251e8
[2, 0] = 0c20323d4b768b68
[3, 0] = a3f3a032977459c4
[4, 0] = 3bc6226ac9efc041
[0, 1] = 8c76a49bcc967dad
[1, 1] = f97c1000f2a1cf6f
[2, 1] = 5a8c9554d7c0e5fa
```

```
[3, 1] = 889fe63b6a376b75
[4, 1] = caa8959e0e204f07
[0, 2] = c31ddb989996cf5b
[1, 2] = b3aa6c6f913d0d7d
[2, 2] = 142e4ac4c98237f0
[3, 2] = b98745cebe8607e8
[4, 2] = 4be3e054f4cb82ef
[0, 3] = e7f46ad357ae75d1
[1, 3] = c836ed2c3321b226
[2, 3] = db13825d17ecbfa6
[3, 3] = 8fb807e7fd721348
[4, 3] = 698b236d3a9de636
[0, 4] = 444726b5433aec96
[1, 4] = 0c744cd3be12fef3
[2, 4] = 2ea0107df9734dd6
[3, 4] = a90b081619b51681
[4, 4] = 23cfbf3bf9b6bda7
```

About to call squeeze (again)

State before permutation (in bytes)

```
22 C3 06 02 6D 6A 0F 9D E8 51 62 B3 86 79 4C A0
68 8B 76 4B 3D 32 20 0C C4 59 74 97 32 A0 F3 A3
41 C0 EF C9 6A 22 C6 3B AD 7D 96 CC 9B A4 76 8C
6F CF A1 F2 00 10 7C F9 FA E5 C0 D7 54 95 8C 5A
75 6B 37 6A 3B E6 9F 88 07 4F 20 0E 9E 95 A8 CA
5B CF 96 99 98 DB 1D C3 7D 0D 3D 91 6F 6C AA B3
F0 37 82 C9 C4 4A 2E 14 E8 07 86 BE CE 45 87 B9
EF 82 CB F4 54 E0 E3 4B D1 75 AE 57 D3 6A F4 E7
26 B2 21 33 2C ED 36 C8 A6 BF EC 17 5D 82 13 DB
48 13 72 FD E7 07 B8 8F 36 E6 9D 3A 6D 23 8B 69
96 EC 3A 43 B5 26 47 44 F3 FE 12 BE D3 4C 74 0C
D6 4D 73 F9 7D 10 A0 2E 81 16 B5 19 16 08 0B A9
            A7 BD B6 F9 3B BF CF 23
```

State before permutation (as lanes of integers)

```
[0, 0] = 9d0f6a6d0206c322
[1, 0] = a04c7986b36251e8
[2, 0] = 0c20323d4b768b68
[3, 0] = a3f3a032977459c4
[4, 0] = 3bc6226ac9efc041
[0, 1] = 8c76a49bcc967dad
[1, 1] = f97c1000f2a1cf6f
[2, 1] = 5a8c9554d7c0e5fa
[3, 1] = 889fe63b6a376b75
[4, 1] = caa8959e0e204f07
[0, 2] = c31ddb989996cf5b
[1, 2] = b3aa6c6f913d0d7d
[2, 2] = 142e4ac4c98237f0
[3, 2] = b98745cebe8607e8
[4, 2] = 4be3e054f4cb82ef
[0, 3] = e7f46ad357ae75d1
[1, 3] = c836ed2c3321b226
[2, 3] = db13825d17ecbfa6
[3, 3] = 8fb807e7fd721348
[4, 3] = 698b236d3a9de636
```

```
[0, 4] = 444726b5433aec96
[1, 4] = 0c744cd3be12fef3
[2, 4] = 2ea0107df9734dd6
[3, 4] = a90b081619b51681
[4, 4] = 23cfbf3bf9b6bda7
```

Round #0

After theta

```
44 2B B2 49 B7 E9 77 30 5E EF A7 87 95 DF F9 BF
66 35 BF 58 46 8E 48 4A A7 5E 81 CC 52 48 51 F5
F7 21 C8 E9 4C 9C 30 6C CB 95 22 87 41 27 0E 21
D9 71 64 C6 13 B6 C9 E6 F4 5B 09 C4 2F 29 E4 1C
16 6C C2 31 5B 0E 3D DE B1 AE 07 2E B8 2B 5E 9D
3D 27 22 D2 42 58 65 6E CB B3 F8 A5 7C CA 1F AC
FE 89 4B DA BF F6 46 52 8B 00 73 E5 AE AD 25 EF
59 63 EC D4 72 5E 15 1C B7 9D 1A 1C 09 E9 8C 4A
90 0C E4 07 3F 4B 83 D7 A8 01 25 04 26 3E 7B 9D
2B 14 87 A6 87 EF 1A D9 80 07 BA 1A 4B 9D 7D 3E
F0 04 8E 08 6F A5 3F E9 45 40 D7 8A C0 EA C1 13
D8 F3 BA EA 06 AC C8 68 E2 11 40 42 76 E0 A9 FF
            11 5C 91 D9 1D 01 39 74
```

After rho

```
44 2B B2 49 B7 E9 77 30 BD DE 4F 0F 2B BF F3 7F
59 CD 2F 96 91 23 92 92 85 14 55 7F EA 15 C8 2C
E2 84 61 BB 0F 41 4E 67 18 74 E2 10 B2 5C 29 72
66 3C 61 9B 6C 9E 1D 47 07 FD 56 02 F1 4B 0A 39
36 E1 98 2D 87 1E 6F 0B E2 D5 19 EB 7A E0 82 BB
EB 39 11 91 16 C2 2A 73 B0 2E CF E2 97 F2 29 7F
D2 FE B5 37 92 F2 4F 5C 5B 4B DE 17 01 E6 CA 5D
6A 39 AF 0A 8E AC 31 76 38 12 D2 19 95 6E 3B 35
FC E0 67 69 F0 1A 92 81 BD 4E D4 80 12 02 13 9F
5D 23 7B 85 E2 D0 F4 F0 3E 80 07 BA 1A 4B 9D 7D
FE A4 C3 13 38 22 BC 95 14 01 5D 2B 02 AB 07 4F
7B 5E 57 DD 80 15 19 0D 11 40 42 76 E0 A9 FF E2
            0E 5D 04 57 64 76 47 40
```

After pi

```
44 2B B2 49 B7 E9 77 30 66 3C 61 9B 6C 9E 1D 47
D2 FE B5 37 92 F2 4F 5C 5D 23 7B 85 E2 D0 F4 F0
0E 5D 04 57 64 76 47 40 85 14 55 7F EA 15 C8 2C
E2 D5 19 EB 7A E0 82 BB EB 39 11 91 16 C2 2A 73
FC E0 67 69 F0 1A 92 81 7B 5E 57 DD 80 15 19 0D
BD DE 4F 0F 2B BF F3 7F 07 FD 56 02 F1 4B 0A 39
5B 4B DE 17 01 E6 CA 5D 3E 80 07 BA 1A 4B 9D 7D
FE A4 C3 13 38 22 BC 95 E2 84 61 BB 0F 41 4E 67
18 74 E2 10 B2 5C 29 72 B0 2E CF E2 97 F2 29 7F
BD 4E D4 80 12 02 13 9F 11 40 42 76 E0 A9 FF E2
59 CD 2F 96 91 23 92 92 36 E1 98 2D 87 1E 6F 0B
6A 39 AF 0A 8E AC 31 76 38 12 D2 19 95 6E 3B 35
            14 01 5D 2B 02 AB 07 4F
```

After chi

```
D4 E9 26 6D 25 89 35 28 6B 3D 2B 1B 0C 9E AD E7
D0 A2 B1 65 96 D4 4C 5C 1D 01 C9 8D 71 59 C4 C0
2C 49 45 C5 2C 60 4F 07 8C 3C 55 6F EE 17 E0 6C
F6 15 7F 83 9A F8 12 3B E8 27 01 05 16 C7 23 7F
```

```
78 E0 67 4B 9A 1A 52 A1 19 9F 5F 5D 90 F5 1B 9E
E5 DC C7 1A 2B 1B 33 3B 23 7D 57 AA EB 42 1F 19
9B 6F 1E 16 21 C6 EA DD 3F DA 0B B6 19 D6 DE 17
FC 85 D3 13 E8 62 B4 95 42 8E 6C 59 0A E3 4E 6A
15 34 F2 10 B2 5C 3B F2 B0 2E CD 94 77 5B C5 1F
5F CA F5 09 1D 42 13 9A 09 30 C0 76 50 B5 DE F2
11 D5 08 94 99 83 82 E6 26 E3 C8 3C 96 5C 65 0A
6E 38 A2 28 8C 2D 35 3C 71 DE F0 8D 04 6E AB A5
            32 21 CD 02 04 B7 6A 46
```

After iota

```
D5 E9 26 6D 25 89 35 28 6B 3D 2B 1B 0C 9E AD E7
D0 A2 B1 65 96 D4 4C 5C 1D 01 C9 8D 71 59 C4 C0
2C 49 45 C5 2C 60 4F 07 8C 3C 55 6F EE 17 E0 6C
F6 15 7F 83 9A F8 12 3B E8 27 01 05 16 C7 23 7F
78 E0 67 4B 9A 1A 52 A1 19 9F 5F 5D 90 F5 1B 9E
E5 DC C7 1A 2B 1B 33 3B 23 7D 57 AA EB 42 1F 19
9B 6F 1E 16 21 C6 EA DD 3F DA 0B B6 19 D6 DE 17
FC 85 D3 13 E8 62 B4 95 42 8E 6C 59 0A E3 4E 6A
15 34 F2 10 B2 5C 3B F2 B0 2E CD 94 77 5B C5 1F
5F CA F5 09 1D 42 13 9A 09 30 C0 76 50 B5 DE F2
11 D5 08 94 99 83 82 E6 26 E3 C8 3C 96 5C 65 0A
6E 38 A2 28 8C 2D 35 3C 71 DE F0 8D 04 6E AB A5
            32 21 CD 02 04 B7 6A 46
```

(Skip rounds 1 to 22)

Round #23

After theta

```
C2 B2 86 B0 3C 25 DE FE 83 BD 91 6C 5C BD FA 72
E6 AB DF 4A 37 80 93 E5 A4 CC 99 39 01 93 E4 01
69 47 65 52 66 C7 42 C2 94 51 75 17 D3 08 1A 14
BA 80 92 3A FE 85 7E 7E C6 58 F9 4F A8 38 72 02
44 5F E0 DC 3B 8D B2 16 37 FC 35 43 AB 7C BA 1F
D5 06 89 0B 9F DD 34 F8 9B FC 96 15 CE 98 F5 80
E8 D7 92 E1 A3 10 A3 4C E1 46 9A E6 CC BC 35 25
A3 F2 F0 F7 C9 7D 61 73 11 FC 93 4A CC 99 15 35
74 54 FB 03 42 95 63 EE 9D A9 31 9F 1C BC A0 5D
81 07 99 65 B4 FB D3 37 81 E3 35 AA 26 0E 12 88
3D C6 44 3E 72 8C 31 86 8E E9 0B 91 CF 90 4E 77
AC B6 06 8C 54 E2 8A 52 0B 52 81 B0 A7 66 EC 47
            11 38 EA 57 8B 55 89 1C
```

After rho

```
C2 B2 86 B0 3C 25 DE FE 06 7B 23 D9 B8 7A F5 E5
F9 EA B7 D2 0D E0 64 B9 30 49 1E 40 CA 9C 99 13
3B 16 12 4E 3B 2A 93 32 31 8D A0 41 41 19 55 77
A9 E3 5F E8 E7 A7 0B 28 80 31 56 FE 13 2A 8E 9C
2F 70 EE 9D 46 59 0B A2 A7 FB 71 C3 5F 33 B4 CA
AF 36 48 5C F8 EC A6 C1 03 6E F2 5B 56 38 63 D6
0C 1F 85 18 65 42 BF 96 79 6B 4A C2 8D 34 CD 99
FB E4 BE B0 B9 51 79 F8 95 98 33 2B 6A 22 F8 27
7F 40 A8 72 CC 9D 8E 6A D0 AE CE D4 98 4F 0E 5E
7F FA 26 F0 20 B3 8C 76 88 81 E3 35 AA 26 0E 12
C6 18 F6 18 13 F9 C8 31 39 A6 2F 44 3E 43 3A DD
D5 D6 80 91 4A 5C 51 8A 52 81 B0 A7 66 EC 47 0B
            22 47 04 8E FA D5 62 55
```

After pi

```
C2 B2 86 B0 3C 25 DE FE A9 E3 5F E8 E7 A7 0B 28
0C 1F 85 18 65 42 BF 96 7F FA 26 F0 20 B3 8C 76
22 47 04 8E FA D5 62 55 30 49 1E 40 CA 9C 99 13
A7 FB 71 C3 5F 33 B4 CA AF 36 48 5C F8 EC A6 C1
7F 40 A8 72 CC 9D 8E 6A D5 D6 80 91 4A 5C 51 8A
06 7B 23 D9 B8 7A F5 E5 80 31 56 FE 13 2A 8E 9C
79 6B 4A C2 8D 34 CD 99 88 81 E3 35 AA 26 0E 12
C6 18 F6 18 13 F9 C8 31 3B 16 12 4E 3B 2A 93 32
31 8D A0 41 41 19 55 77 03 6E F2 5B 56 38 63 D6
D0 AE CE D4 98 4F 0E 5E 52 81 B0 A7 66 EC 47 0B
F9 EA B7 D2 0D E0 64 B9 2F 70 EE 9D 46 59 0B A2
FB E4 BE B0 B9 51 79 F8 95 98 33 2B 6A 22 F8 27
            39 A6 2F 44 3E 43 3A DD
```

After chi

```
C6 AE 06 A0 3C 65 6A 68 DA 03 7D 08 E7 16 0B 48
0C 1A 85 16 BF 06 DD 97 BF 4A A4 C0 24 93 10 DC
0B 06 5D C6 39 57 63 55 38 4D 16 5C 6A 50 9B 12
F7 BB D1 E1 5B 22 BC E0 2F A0 48 DD FA AC F7 41
5F 49 B6 32 4C 1D 06 7B 52 64 E1 12 5F 7F 75 42
7F 31 2B D9 34 6E B4 E4 00 B1 F7 CB 31 28 8C 9E
3F 73 5E CA 9C ED 0D B8 88 E2 E2 F4 02 24 3B D6
46 18 A2 3E 10 F9 C2 29 39 74 40 54 2D 0A B1 B2
E1 0D AC C5 C9 5E 59 7F 01 6F C2 78 30 98 22 D7
F9 B8 CC 9C 81 4D 9E 6E 52 08 10 A6 26 FD 03 4E
29 6E A7 F2 B4 E0 14 E1 2B 68 EF 96 04 7B 8B A5
D3 C2 B2 F4 AD 10 7B 20 55 D0 A3 B9 6B 82 BC 07
            3F B6 67 49 7C 5A 31 DF
```

After iota

```
CE 2E 06 20 3C 65 6A E8 DA 03 7D 08 E7 16 0B 48
0C 1A 85 16 BF 06 DD 97 BF 4A A4 C0 24 93 10 DC
0B 06 5D C6 39 57 63 55 38 4D 16 5C 6A 50 9B 12
F7 BB D1 E1 5B 22 BC E0 2F A0 48 DD FA AC F7 41
5F 49 B6 32 4C 1D 06 7B 52 64 E1 12 5F 7F 75 42
7F 31 2B D9 34 6E B4 E4 00 B1 F7 CB 31 28 8C 9E
3F 73 5E CA 9C ED 0D B8 88 E2 E2 F4 02 24 3B D6
46 18 A2 3E 10 F9 C2 29 39 74 40 54 2D 0A B1 B2
E1 0D AC C5 C9 5E 59 7F 01 6F C2 78 30 98 22 D7
F9 B8 CC 9C 81 4D 9E 6E 52 08 10 A6 26 FD 03 4E
29 6E A7 F2 B4 E0 14 E1 2B 68 EF 96 04 7B 8B A5
D3 C2 B2 F4 AD 10 7B 20 55 D0 A3 B9 6B 82 BC 07
            3F B6 67 49 7C 5A 31 DF
```

After permutation

```
CE 2E 06 20 3C 65 6A E8 DA 03 7D 08 E7 16 0B 48
0C 1A 85 16 BF 06 DD 97 BF 4A A4 C0 24 93 10 DC
0B 06 5D C6 39 57 63 55 38 4D 16 5C 6A 50 9B 12
F7 BB D1 E1 5B 22 BC E0 2F A0 48 DD FA AC F7 41
5F 49 B6 32 4C 1D 06 7B 52 64 E1 12 5F 7F 75 42
7F 31 2B D9 34 6E B4 E4 00 B1 F7 CB 31 28 8C 9E
3F 73 5E CA 9C ED 0D B8 88 E2 E2 F4 02 24 3B D6
46 18 A2 3E 10 F9 C2 29 39 74 40 54 2D 0A B1 B2
E1 0D AC C5 C9 5E 59 7F 01 6F C2 78 30 98 22 D7
```

```
F9 B8 CC 9C 81 4D 9E 6E 52 08 10 A6 26 FD 03 4E
29 6E A7 F2 B4 E0 14 E1 2B 68 EF 96 04 7B 8B A5
D3 C2 B2 F4 AD 10 7B 20 55 D0 A3 B9 6B 82 BC 07
            3F B6 67 49 7C 5A 31 DF
```

State (as lanes of integers)

```
[0, 0] = e86a653c20062ece
[1, 0] = 480b16e7087d03da
[2, 0] = 97dd06bf16851a0c
[3, 0] = dc109324c0a44abf
[4, 0] = 55635739c65d060b
[0, 1] = 129b506a5c164d38
[1, 1] = e0bc225be1d1bbf7
[2, 1] = 41f7acfadd48a02f
[3, 1] = 7b061d4c32b6495f
[4, 1] = 42757f5f12e16452
[0, 2] = e4b46e34d92b317f
[1, 2] = 9e8c2831cbf7b100
[2, 2] = b80ded9cca5e733f
[3, 2] = d63b2402f4e2e288
[4, 2] = 29c2f9103ea21846
[0, 3] = b2b10a2d54407439
[1, 3] = 7f595ec9c5ac0de1
[2, 3] = d722983078c26f01
[3, 3] = 6e9e4d819cccb8f9
[4, 3] = 4e03fd26a6100852
[0, 4] = e114e0b4f2a76e29
[1, 4] = a58b7b0496ef682b
[2, 4] = 207b10adf4b2c2d3
[3, 4] = 07bc826bb9a3d055
[4, 4] = df315a7c4967b63f
```

About to call squeeze (again)

State before permutation (in bytes)

```
CE 2E 06 20 3C 65 6A E8 DA 03 7D 08 E7 16 0B 48
0C 1A 85 16 BF 06 DD 97 BF 4A A4 C0 24 93 10 DC
0B 06 5D C6 39 57 63 55 38 4D 16 5C 6A 50 9B 12
F7 BB D1 E1 5B 22 BC E0 2F A0 48 DD FA AC F7 41
5F 49 B6 32 4C 1D 06 7B 52 64 E1 12 5F 7F 75 42
7F 31 2B D9 34 6E B4 E4 00 B1 F7 CB 31 28 8C 9E
3F 73 5E CA 9C ED 0D B8 88 E2 E2 F4 02 24 3B D6
46 18 A2 3E 10 F9 C2 29 39 74 40 54 2D 0A B1 B2
E1 0D AC C5 C9 5E 59 7F 01 6F C2 78 30 98 22 D7
F9 B8 CC 9C 81 4D 9E 6E 52 08 10 A6 26 FD 03 4E
29 6E A7 F2 B4 E0 14 E1 2B 68 EF 96 04 7B 8B A5
D3 C2 B2 F4 AD 10 7B 20 55 D0 A3 B9 6B 82 BC 07
            3F B6 67 49 7C 5A 31 DF
```

State before permutation (as lanes of integers)

```
[0, 0] = e86a653c20062ece
[1, 0] = 480b16e7087d03da
[2, 0] = 97dd06bf16851a0c
[3, 0] = dc109324c0a44abf
```

```
[4, 0] = 55635739c65d060b
[0, 1] = 129b506a5c164d38
[1, 1] = e0bc225be1d1bbf7
[2, 1] = 41f7acfadd48a02f
[3, 1] = 7b061d4c32b6495f
[4, 1] = 42757f5f12e16452
[0, 2] = e4b46e34d92b317f
[1, 2] = 9e8c2831cbf7b100
[2, 2] = b80ded9cca5e733f
[3, 2] = d63b2402f4e2e288
[4, 2] = 29c2f9103ea21846
[0, 3] = b2b10a2d54407439
[1, 3] = 7f595ec9c5ac0de1
[2, 3] = d722983078c26f01
[3, 3] = 6e9e4d819cccb8f9
[4, 3] = 4e03fd26a6100852
[0, 4] = e114e0b4f2a76e29
[1, 4] = a58b7b0496ef682b
[2, 4] = 207b10adf4b2c2d3
[3, 4] = 07bc826bb9a3d055
[4, 4] = df315a7c4967b63f
```

Round #0

After theta

```
73 33 5F C7 90 61 5E 9E DE 82 67 10 95 39 16 37
63 65 A2 20 FF F4 2A 4B 94 A6 94 47 38 B0 A2 1A
FD 1E 7A E2 4F 51 AD D6 85 50 4F BB C6 54 AF 64
F3 3A CB F9 29 0D A1 9F 40 DF 6F EB BA 5E 00 9D
74 A5 86 B5 50 3E B4 BD A4 7C C6 36 29 79 BB C1
C2 2C 72 3E 98 6A 80 92 04 30 ED D3 43 07 91 E1
50 0C 79 FC DC 1F FA 64 A3 0E D2 73 1E 07 89 10
B0 00 85 1A 66 FF 0C AA 84 69 19 B3 81 0E 85 C4
E5 8C B6 DD BB 71 44 00 6E 10 E5 4E 70 6A D5 0B
D2 54 FC 1B 9D 6E 2C A8 A4 10 37 82 50 FB CD CD
94 73 FE 15 18 E4 20 97 2F E9 F5 8E 76 54 96 DA
BC BD 95 C2 ED E2 8C FC 7E 3C 93 3E 77 A1 0E C1
            C9 AE 40 6D 0A 5C FF 5C
```

After rho

```
73 33 5F C7 90 61 5E 9E BC 05 CF 20 2A 73 2C 6E
58 99 28 C8 3F BD CA D2 03 2B AA 41 69 4A 79 84
8A 6A B5 EE F7 D0 13 7F 6B 4C F5 4A 56 08 F5 B4
9C 9F D2 10 FA 39 AF B3 27 D0 F7 DB BA AE 17 40
52 C3 5A 28 1F DA 5E BA B7 1B 4C CA 67 6C 93 92
14 66 91 F3 C1 54 03 94 86 13 C0 B4 4F 0F 1D 44
E3 E7 FE D0 27 83 62 C8 0E 12 21 46 1D A4 E7 3C
0D B3 7F 06 55 58 80 42 66 03 1D 0A 89 09 D3 32
B6 7B 37 8E 08 A0 9C D1 EA 05 37 88 72 27 38 B5
8D 05 55 9A 8A 7F A3 D3 CD A4 10 37 82 50 FB CD
83 5C 52 CE F9 57 60 90 BF A4 D7 3B DA 51 59 6A
B7 B7 52 B8 5D 9C 91 9F 3C 93 3E 77 A1 0E C1 7E
            3F 57 B2 2B 50 9B 02 D7
```

After pi

```
73 33 5F C7 90 61 5E 9E 9C 9F D2 10 FA 39 AF B3
E3 E7 FE D0 27 83 62 C8 8D 05 55 9A 8A 7F A3 D3
3F 57 B2 2B 50 9B 02 D7 03 2B AA 41 69 4A 79 84
B7 1B 4C CA 67 6C 93 92 14 66 91 F3 C1 54 03 94
B6 7B 37 8E 08 A0 9C D1 B7 B7 52 B8 5D 9C 91 9F
BC 05 CF 20 2A 73 2C 6E 27 D0 F7 DB BA AE 17 40
0E 12 21 46 1D A4 E7 3C CD A4 10 37 82 50 FB CD
83 5C 52 CE F9 57 60 90 8A 6A B5 EE F7 D0 13 7F
6B 4C F5 4A 56 08 F5 B4 86 13 C0 B4 4F 0F 1D 44
EA 05 37 88 72 27 38 B5 3C 93 3E 77 A1 0E C1 7E
58 99 28 C8 3F BD CA D2 52 C3 5A 28 1F DA 5E BA
0D B3 7F 06 55 58 80 42 66 03 1D 0A 89 09 D3 32
            BF A4 D7 3B DA 51 59 6A
```

After chi

```
10 53 73 07 95 E3 1E D6 90 9F D3 1A 72 45 2E A0
D1 B5 5C F1 77 03 62 CC CD 25 18 5E 0A 1F FF DB
B3 DB 32 3B 3A 83 A3 F6 03 4F 3B 70 E9 5A 79 80
15 02 6A C6 6F CC 0F D3 15 E2 D1 C3 94 48 02 9A
B6 73 9F CF 28 E2 F4 D1 03 A7 16 32 5B B8 13 8D
B4 07 CF 24 2F 73 CC 52 E6 74 E7 EA 38 FE 0F 81
0C 4A 63 8E 64 A3 E7 2C F1 A5 9D 17 80 70 F7 A3
80 8C 62 15 69 DB 73 90 0E 79 B5 5A FE D7 1B 3F
03 48 C2 42 66 28 D5 05 92 81 C8 C3 CE 07 DC 0E
68 6D B6 00 24 F7 2A B4 5D 97 7E 77 A1 06 25 FE
55 A9 0D CE 7F BD 4A 92 30 C3 5A 20 97 DB 0D 8A
94 17 BD 37 07 08 88 0A 26 1A 35 CA AC A5 51 A2
            BD E6 85 1B DA 13 4D 42
```

After iota

```
11 53 73 07 95 E3 1E D6 90 9F D3 1A 72 45 2E A0
D1 B5 5C F1 77 03 62 CC CD 25 18 5E 0A 1F FF DB
B3 DB 32 3B 3A 83 A3 F6 03 4F 3B 70 E9 5A 79 80
15 02 6A C6 6F CC 0F D3 15 E2 D1 C3 94 48 02 9A
B6 73 9F CF 28 E2 F4 D1 03 A7 16 32 5B B8 13 8D
B4 07 CF 24 2F 73 CC 52 E6 74 E7 EA 38 FE 0F 81
0C 4A 63 8E 64 A3 E7 2C F1 A5 9D 17 80 70 F7 A3
80 8C 62 15 69 DB 73 90 0E 79 B5 5A FE D7 1B 3F
03 48 C2 42 66 28 D5 05 92 81 C8 C3 CE 07 DC 0E
68 6D B6 00 24 F7 2A B4 5D 97 7E 77 A1 06 25 FE
55 A9 0D CE 7F BD 4A 92 30 C3 5A 20 97 DB 0D 8A
94 17 BD 37 07 08 88 0A 26 1A 35 CA AC A5 51 A2
            BD E6 85 1B DA 13 4D 42
```

(Skip rounds 1 to 22)

Round #23

After theta

```
4F BC E7 A0 3A 24 5F BF FB 42 A7 2D 76 60 EB 12
8E 99 50 1E 1A 28 3A 83 C2 A4 A9 B1 47 00 36 A8
AE B3 BA 3A 33 1E 69 A4 01 4B A2 C8 8B DC 9C C8
F4 55 44 98 9B 01 C5 1B 56 8D 81 47 0E 53 B8 98
62 90 42 BF A3 AB 6A C9 3A AA 51 95 CE E2 48 7D
38 90 8E 9C F4 4F BF 1A B1 7E 34 47 D5 2F FD 91
2E 29 7D 7D AF 8B 54 87 A8 CB 87 C6 57 F0 97 DE
```

```
D9 B7 74 32 86 76 EB D1 88 D4 D2 CC 4E 16 A5 2A
9A 03 9D 5D AA 04 D2 DA 65 C9 B2 A7 16 90 A1 AC
BD 07 8A 54 67 6C 6B 1C 6C E1 06 27 B9 B4 6B 83
06 9C 58 D8 D6 5F 2D 26 6A A2 AE D5 EE F0 89 50
67 5F 58 7A 72 82 40 FF D1 28 2D A3 2E 66 9F 88
            67 99 9C F0 B3 19 04 EA
```

After rho

```
4F BC E7 A0 3A 24 5F BF F6 85 4E 5B EC C0 D6 25
63 26 94 87 06 8A CE A0 04 60 83 2A 4C 9A 1A 7B
F1 48 23 75 9D D5 D5 99 BC C8 CD 89 1C B0 24 8A
84 B9 19 50 BC 41 5F 45 A6 55 63 E0 91 C3 14 2E
48 A1 DF D1 55 B5 64 31 8E D4 A7 A3 1A 55 E9 2C
C0 81 74 E4 A4 7F FA D5 47 C6 FA D1 1C 55 BF F4
EB 7B 5D A4 3A 74 49 E9 E0 2F BD 51 97 0F 8D AF
19 43 BB F5 E8 EC 5B 3A 99 9D 2C 4A 55 10 A9 A5
B3 4B 95 40 5A 5B 73 A0 50 D6 B2 64 D9 53 0B C8
6D 8D A3 F7 40 91 EA 8C 83 6C E1 06 27 B9 B4 6B
B5 98 18 70 62 61 5B 7F A9 89 BA 56 BB C3 27 42
EC 0B 4B 4F 4E 10 E8 FF 28 2D A3 2E 66 9F 88 D1
            81 FA 59 26 27 FC 6C 06
```

After pi

```
4F BC E7 A0 3A 24 5F BF 84 B9 19 50 BC 41 5F 45
EB 7B 5D A4 3A 74 49 E9 6D 8D A3 F7 40 91 EA 8C
81 FA 59 26 27 FC 6C 06 04 60 83 2A 4C 9A 1A 7B
8E D4 A7 A3 1A 55 E9 2C C0 81 74 E4 A4 7F FA D5
B3 4B 95 40 5A 5B 73 A0 EC 0B 4B 4F 4E 10 E8 FF
F6 85 4E 5B EC C0 D6 25 A6 55 63 E0 91 C3 14 2E
E0 2F BD 51 97 0F 8D AF 83 6C E1 06 27 B9 B4 6B
B5 98 18 70 62 61 5B 7F F1 48 23 75 9D D5 D5 99
BC C8 CD 89 1C B0 24 8A 47 C6 FA D1 1C 55 BF F4
50 D6 B2 64 D9 53 0B C8 28 2D A3 2E 66 9F 88 D1
63 26 94 87 06 8A CE A0 48 A1 DF D1 55 B5 64 31
19 43 BB F5 E8 EC 5B 3A 99 9D 2C 4A 55 10 A9 A5
            A9 89 BA 56 BB C3 27 42
```

After chi

```
24 FE A3 04 38 10 5F 17 80 3D BB 03 FC C0 FD 41
6B 09 05 A4 1D 18 4D EB 23 89 05 77 58 91 F9 35
01 FB 41 76 A3 BD 6C 46 44 61 D3 6E E8 B0 08 AA
BD 9E 26 A3 40 55 E8 0C 8C 81 3E EB A0 7F 72 8A
B3 2B 15 60 5A D1 61 A0 66 9F 6F CE 5C 55 09 FB
B6 AF D2 4A EA CC 5F A4 A5 15 23 E6 B1 73 24 6E
D4 BF A5 21 D7 4F C6 BB C1 69 A7 0D AB 39 30 6B
B5 C8 39 D0 73 62 5B 75 B2 4E 11 25 9D 90 4E ED
AC D8 CD AD DD B2 24 82 6F EF FB DB 3A D9 3F E5
81 96 B2 35 40 13 5E C0 24 AD 6F A6 66 BF A8 D3
72 64 B4 A3 AE C2 D5 AA C8 3D DB DB 40 A5 C4 B4
39 43 29 E1 42 2F 5D 78 DB BB 28 CB 51 18 61 05
            A1 08 F1 06 EA F6 07 53
```

After iota

```
2C 7E A3 84 38 10 5F 97 80 3D BB 03 FC C0 FD 41
6B 09 05 A4 1D 18 4D EB 23 89 05 77 58 91 F9 35
01 FB 41 76 A3 BD 6C 46 44 61 D3 6E E8 B0 08 AA
BD 9E 26 A3 40 55 E8 0C 8C 81 3E EB A0 7F 72 8A
```

```
B3 2B 15 60 5A D1 61 A0 66 9F 6F CE 5C 55 09 FB
B6 AF D2 4A EA CC 5F A4 A5 15 23 E6 B1 73 24 6E
D4 BF A5 21 D7 4F C6 BB C1 69 A7 0D AB 39 30 6B
B5 C8 39 D0 73 62 5B 75 B2 4E 11 25 9D 90 4E ED
AC D8 CD AD DD B2 24 82 6F EF FB DB 3A D9 3F E5
81 96 B2 35 40 13 5E C0 24 AD 6F A6 66 BF A8 D3
72 64 B4 A3 AE C2 D5 AA C8 3D DB DB 40 A5 C4 B4
39 43 29 E1 42 2F 5D 78 DB BB 28 CB 51 18 61 05
            A1 08 F1 06 EA F6 07 53
```

After permutation

```
2C 7E A3 84 38 10 5F 97 80 3D BB 03 FC C0 FD 41
6B 09 05 A4 1D 18 4D EB 23 89 05 77 58 91 F9 35
01 FB 41 76 A3 BD 6C 46 44 61 D3 6E E8 B0 08 AA
BD 9E 26 A3 40 55 E8 0C 8C 81 3E EB A0 7F 72 8A
B3 2B 15 60 5A D1 61 A0 66 9F 6F CE 5C 55 09 FB
B6 AF D2 4A EA CC 5F A4 A5 15 23 E6 B1 73 24 6E
D4 BF A5 21 D7 4F C6 BB C1 69 A7 0D AB 39 30 6B
B5 C8 39 D0 73 62 5B 75 B2 4E 11 25 9D 90 4E ED
AC D8 CD AD DD B2 24 82 6F EF FB DB 3A D9 3F E5
81 96 B2 35 40 13 5E C0 24 AD 6F A6 66 BF A8 D3
72 64 B4 A3 AE C2 D5 AA C8 3D DB DB 40 A5 C4 B4
39 43 29 E1 42 2F 5D 78 DB BB 28 CB 51 18 61 05
            A1 08 F1 06 EA F6 07 53
```

State (as lanes of integers)

```
[0, 0] = 975f103884a37e2c
[1, 0] = 41fdc0fc03bb3d80
[2, 0] = eb4d181da405096b
[3, 0] = 35f9915877058923
[4, 0] = 466cbda37641fb01
[0, 1] = aa08b0e86ed36144
[1, 1] = 0ce85540a3269ebd
[2, 1] = 8a727fa0eb3e818c
[3, 1] = a061d15a60152bb3
[4, 1] = fb09555cce6f9f66
[0, 2] = a45fccea4ad2afb6
[1, 2] = 6e2473b1e62315a5
[2, 2] = bbc64fd721a5bfd4
[3, 2] = 6b3039ab0da769c1
[4, 2] = 755b6273d039c8b5
[0, 3] = ed4e909d25114eb2
[1, 3] = 8224b2ddadcdd8ac
[2, 3] = e53fd93adbfbef6f
[3, 3] = c05e134035b29681
[4, 3] = d3a8bf66a66fad24
[0, 4] = aad5c2aea3b46472
[1, 4] = b4c4a540dbdb3dc8
[2, 4] = 785d2f42e1294339
[3, 4] = 05611851cb28bbdb
[4, 4] = 5307f6ea06f108a1
```

The hash value is

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

SHAKE-256 sample to produce 4096-bits of output

The message as a bit string

```
1 1 0 0 1 0 1 0 0 0 0 1 1 0 1 0 1 1 0 1 1 1 1 0 1 0 0 1 1 0
```

About to call last of the absorb phase

XORed state (in bytes)

```
53 58 7B D9 07 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 80 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
               00 00 00 00 00 00 00 00
```

XORed state (as lanes of integers)

```
[0, 0] = 00000007d97b5853
[1, 0] = 0000000000000000
[2, 0] = 0000000000000000
[3, 0] = 0000000000000000
[4, 0] = 0000000000000000
[0, 1] = 0000000000000000
[1, 1] = 0000000000000000
[2, 1] = 0000000000000000
[3, 1] = 0000000000000000
[4, 1] = 0000000000000000
[0, 2] = 0000000000000000
[1, 2] = 0000000000000000
[2, 2] = 0000000000000000
[3, 2] = 0000000000000000
[4, 2] = 0000000000000000
[0, 3] = 0000000000000000
[1, 3] = 8000000000000000
[2, 3] = 0000000000000000
[3, 3] = 0000000000000000
[4, 3] = 0000000000000000
[0, 4] = 0000000000000000
[1, 4] = 0000000000000000
[2, 4] = 0000000000000000
[3, 4] = 0000000000000000
[4, 4] = 0000000000000000
```

Round #0

After theta

```
52 58 7B D9 07 00 00 00 53 58 7B D9 07 00 00 00
00 00 00 00 00 00 00 80 00 00 00 00 00 00 00 00
A6 B0 F6 B2 0F 00 00 00 01 00 00 00 00 00 00 00
53 58 7B D9 07 00 00 00 00 00 00 00 00 00 00 80
00 00 00 00 00 00 00 00 A6 B0 F6 B2 0F 00 00 00
01 00 00 00 00 00 00 00 53 58 7B D9 07 00 00 00
00 00 00 00 00 00 00 80 00 00 00 00 00 00 00 00
A6 B0 F6 B2 0F 00 00 00 01 00 00 00 00 00 00 00
53 58 7B D9 07 00 00 80 00 00 00 00 00 00 00 80
00 00 00 00 00 00 00 00 A6 B0 F6 B2 0F 00 00 00
01 00 00 00 00 00 00 00 53 58 7B D9 07 00 00 00
00 00 00 00 00 00 00 80 00 00 00 00 00 00 00 00
            A6 B0 F6 B2 0F 00 00 00
```

After rho

```
52 58 7B D9 07 00 00 00 A6 B0 F6 B2 0F 00 00 00
00 00 00 00 00 00 00 20 00 00 00 00 00 00 00 00
00 00 00 30 85 B5 97 7D 00 00 00 00 10 00 00 00
97 7D 00 00 00 30 85 B5 20 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 60 0A 6B 2F FB 00
08 00 00 00 00 00 00 00 00 4C 61 ED 65 1F 00 00
00 00 00 00 00 04 00 00 00 00 00 00 00 00 00 00
D9 07 00 00 00 53 58 7B 00 00 00 00 00 02 00 00
2F FB 00 00 00 70 0A 6B 00 40 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 A6 B0 F6 B2 0F 00 00
00 00 04 00 00 00 00 00 4C 61 ED 65 1F 00 00 00
```

```
00 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00
            00 80 29 AC BD EC 03 00
```

After pi

```
52 58 7B D9 07 00 00 00 97 7D 00 00 00 30 85 B5
00 00 00 00 00 04 00 00 00 00 00 00 00 00 00 00
00 80 29 AC BD EC 03 00 00 00 00 00 00 00 00 00
00 00 60 0A 6B 2F FB 00 08 00 00 00 00 00 00 00
2F FB 00 00 00 70 0A 6B 00 00 00 00 00 00 00 10
A6 B0 F6 B2 0F 00 00 00 20 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 A6 B0 F6 B2 0F 00 00
00 00 04 00 00 00 00 00 00 00 00 30 85 B5 97 7D
00 00 00 00 10 00 00 00 00 4C 61 ED 65 1F 00 00
00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 20 00 00 00 00 00 00 00 00
D9 07 00 00 00 53 58 7B 00 00 00 00 00 02 00 00
            4C 61 ED 65 1F 00 00 00
```

After chi

```
52 58 7B D9 07 04 00 00 97 7D 00 00 00 30 85 B5
00 80 29 AC BD E8 03 00 52 58 52 51 02 00 00 00
85 A5 29 AC BD DC 86 B5 08 00 00 00 00 00 00 00
27 FB 60 0A 6B 5F F1 6B 08 00 00 00 00 00 00 10
2F FB 00 00 00 70 0A 6B 00 00 60 0A 6B 2F FB 10
A6 B0 F6 B2 0F 00 00 00 20 A6 B0 F6 B2 0F 00 00
00 00 04 00 00 00 00 00 A6 16 42 44 BD 0F 00 00
00 00 04 00 00 00 00 00 00 4C 61 DD E0 AA 97 7D
00 00 00 00 10 00 00 00 00 4C 61 ED 65 1F 00 00
00 40 00 30 85 B5 97 7D 00 00 00 00 10 00 00 00
D9 07 00 00 00 53 58 5B 00 00 00 00 00 00 00 00
95 66 ED 65 1F 53 58 7B 00 00 00 00 00 02 00 20
            4C 61 ED 65 1F 00 00 00
```

After iota

```
53 58 7B D9 07 04 00 00 97 7D 00 00 00 30 85 B5
00 80 29 AC BD E8 03 00 52 58 52 51 02 00 00 00
85 A5 29 AC BD DC 86 B5 08 00 00 00 00 00 00 00
27 FB 60 0A 6B 5F F1 6B 08 00 00 00 00 00 00 10
2F FB 00 00 00 70 0A 6B 00 00 60 0A 6B 2F FB 10
A6 B0 F6 B2 0F 00 00 00 20 A6 B0 F6 B2 0F 00 00
00 00 04 00 00 00 00 00 A6 16 42 44 BD 0F 00 00
00 00 04 00 00 00 00 00 00 4C 61 DD E0 AA 97 7D
00 00 00 00 10 00 00 00 00 4C 61 ED 65 1F 00 00
00 40 00 30 85 B5 97 7D 00 00 00 00 10 00 00 00
D9 07 00 00 00 53 58 5B 00 00 00 00 00 00 00 00
95 66 ED 65 1F 53 58 7B 00 00 00 00 00 02 00 20
            4C 61 ED 65 1F 00 00 00
```

(Skip rounds 1 to 22)

Round #23

After theta

```
C6 0D 01 1F FA C7 5E 89 C5 15 2C 3E D2 26 BB 43
32 00 00 44 47 39 FA DC 70 5C C4 DC BB 3B 9C AF
92 4A 30 73 24 79 07 29 5D 38 E4 24 C0 AF 2B E7
4B F4 64 F1 02 DE A1 68 D6 58 0D 94 0D 44 29 83
E6 B5 9A C4 47 7D 46 78 10 B8 B9 2D 00 E4 78 D5
DE 66 17 D9 50 6E 09 82 1C 74 53 8B 4A F7 1B 86
88 80 06 11 3A 4D B0 41 72 25 7A B0 D9 D6 7A 9B
E9 D1 40 74 EA 5A 0C 94 DE 08 FF 3A 6D E3 55 50
E6 3F C5 29 97 CA 25 5A 8A 9A D2 97 99 75 C9 84
BA EA 54 CE 36 A5 FF 25 ED AB 49 F3 63 72 CE FA
0C EE 25 00 A9 CF 37 26 52 FA 02 83 07 D9 5F 06
C3 2A 3D B1 48 08 F8 5F 71 EF B1 AC 4F F5 86 5C
            40 A5 80 B9 9F 68 53 E2
```

After rho

```
C6 0D 01 1F FA C7 5E 89 8A 2B 58 7C A4 4D 76 87
0C 00 00 D1 51 8E 3E B7 BB C3 F9 0A C7 45 CC BD
C9 3B 48 91 54 82 99 23 02 FC BA 72 DE 85 43 4E
16 2F E0 1D 8A B6 44 4F A0 35 56 03 65 03 51 CA
5A 4D E2 A3 3E 23 3C F3 8E 57 0D 81 9B DB 02 40
F4 36 BB C8 86 72 4B 10 18 72 D0 4D 2D 2A DD 6F
88 D0 69 82 0D 42 04 34 AD F5 36 E5 4A F4 60 B3
3A 75 2D 06 CA F4 68 20 75 DA C6 AB A0 BC 11 FE
38 E5 52 B9 44 CB FC A7 64 42 45 4D E9 CB CC BA
F4 BF 44 57 9D CA D9 A6 FA ED AB 49 F3 63 72 CE
DF 98 30 B8 97 00 A4 3E 48 E9 0B 0C 1E 64 7F 19
58 A5 27 16 09 01 FF 6B EF B1 AC 4F F5 86 5C 71
            94 38 50 29 60 EE 27 DA
```

After pi

```
C6 0D 01 1F FA C7 5E 89 16 2F E0 1D 8A B6 44 4F
88 D0 69 82 0D 42 04 34 F4 BF 44 57 9D CA D9 A6
94 38 50 29 60 EE 27 DA BB C3 F9 0A C7 45 CC BD
8E 57 0D 81 9B DB 02 40 F4 36 BB C8 86 72 4B 10
38 E5 52 B9 44 CB FC A7 58 A5 27 16 09 01 FF 6B
8A 2B 58 7C A4 4D 76 87 A0 35 56 03 65 03 51 CA
AD F5 36 E5 4A F4 60 B3 FA ED AB 49 F3 63 72 CE
DF 98 30 B8 97 00 A4 3E C9 3B 48 91 54 82 99 23
02 FC BA 72 DE 85 43 4E 18 72 D0 4D 2D 2A DD 6F
64 42 45 4D E9 CB CC BA EF B1 AC 4F F5 86 5C 71
0C 00 00 D1 51 8E 3E B7 5A 4D E2 A3 3E 23 3C F3
3A 75 2D 06 CA F4 68 20 75 DA C6 AB A0 BC 11 FE
            48 E9 0B 0C 1E 64 7F 19
```

After chi

```
4E DD 08 9D FF 87 5E B9 62 00 E4 48 1A 3E 9D CD
88 D0 79 AA 6D 66 22 6C B6 BA 45 41 07 CB 81 A7
84 1A B0 29 60 DE 27 9C CB E3 4B 42 C3 65 85 AD
86 96 4D B0 DB 52 B6 E7 B4 36 9E CE 8F 72 48 58
9B A7 8A B1 82 8F FC 33 5C B1 23 97 11 9B FD 2B
87 EB 78 98 AE B9 56 B6 F2 3D DF 0B D4 00 43 86
```

```
A8 E5 26 55 4E F4 E4 83 FA CE E3 0D D3 2E 20 4F
FF 8C 36 BB D6 02 A5 76 D1 39 08 9C 75 A8 05 02
66 FC BF 72 1E 44 43 DE 93 C3 78 4F 39 2E CD 2E
64 48 05 DD E9 CB 4D B8 ED 75 1E 2D 7F 83 1E 3D
2C 30 0D D5 91 5A 7E B7 1F C7 20 0A 1E 2B 2D 2D
32 54 24 02 D4 B4 06 21 71 DA C6 7A E1 36 11 58
            1A A4 E9 2E 30 45 7F 59
```

After iota

```
46 5D 08 1D FF 87 5E 39 62 00 E4 48 1A 3E 9D CD
88 D0 79 AA 6D 66 22 6C B6 BA 45 41 07 CB 81 A7
84 1A B0 29 60 DE 27 9C CB E3 4B 42 C3 65 85 AD
86 96 4D B0 DB 52 B6 E7 B4 36 9E CE 8F 72 48 58
9B A7 8A B1 82 8F FC 33 5C B1 23 97 11 9B FD 2B
87 EB 78 98 AE B9 56 B6 F2 3D DF 0B D4 00 43 86
A8 E5 26 55 4E F4 E4 83 FA CE E3 0D D3 2E 20 4F
FF 8C 36 BB D6 02 A5 76 D1 39 08 9C 75 A8 05 02
66 FC BF 72 1E 44 43 DE 93 C3 78 4F 39 2E CD 2E
64 48 05 DD E9 CB 4D B8 ED 75 1E 2D 7F 83 1E 3D
2C 30 0D D5 91 5A 7E B7 1F C7 20 0A 1E 2B 2D 2D
32 54 24 02 D4 B4 06 21 71 DA C6 7A E1 36 11 58
            1A A4 E9 2E 30 45 7F 59
```

After permutation

```
46 5D 08 1D FF 87 5E 39 62 00 E4 48 1A 3E 9D CD
88 D0 79 AA 6D 66 22 6C B6 BA 45 41 07 CB 81 A7
84 1A B0 29 60 DE 27 9C CB E3 4B 42 C3 65 85 AD
86 96 4D B0 DB 52 B6 E7 B4 36 9E CE 8F 72 48 58
9B A7 8A B1 82 8F FC 33 5C B1 23 97 11 9B FD 2B
87 EB 78 98 AE B9 56 B6 F2 3D DF 0B D4 00 43 86
A8 E5 26 55 4E F4 E4 83 FA CE E3 0D D3 2E 20 4F
FF 8C 36 BB D6 02 A5 76 D1 39 08 9C 75 A8 05 02
66 FC BF 72 1E 44 43 DE 93 C3 78 4F 39 2E CD 2E
64 48 05 DD E9 CB 4D B8 ED 75 1E 2D 7F 83 1E 3D
2C 30 0D D5 91 5A 7E B7 1F C7 20 0A 1E 2B 2D 2D
32 54 24 02 D4 B4 06 21 71 DA C6 7A E1 36 11 58
            1A A4 E9 2E 30 45 7F 59
```

State (as lanes of integers)

```
[0, 0] = 395e87ff1d085d46
[1, 0] = cd9d3e1a48e40062
[2, 0] = 6c22666daa79d088
[3, 0] = a781cb074145bab6
[4, 0] = 9c27de6029b01a84
[0, 1] = ad8565c3424be3cb
[1, 1] = e7b652dbb04d9686
[2, 1] = 5848728fce9e36b4
[3, 1] = 33fc8f82b18aa79b
[4, 1] = 2bfd9b119723b15c
[0, 2] = b656b9ae9878eb87
[1, 2] = 864300d40bdf3df2
[2, 2] = 83e4f44e5526e5a8
[3, 2] = 4f202ed30de3cefa
[4, 2] = 76a502d6bb368cff
[0, 3] = 0205a8759c0839d1
[1, 3] = de43441e72bffc66
[2, 3] = 2ecd2e394f78c393
```

```
[3, 3] = b84dcbe9dd054864
[4, 3] = 3d1e837f2d1e75ed
[0, 4] = b77e5a91d50d302c
[1, 4] = 2d2d2b1e0a20c71f
[2, 4] = 2106b4d402245432
[3, 4] = 581136e17ac6da71
[4, 4] = 597f45302ee9a41a
```

About to call squeeze (again)

State before permutation (in bytes)

```
46 5D 08 1D FF 87 5E 39 62 00 E4 48 1A 3E 9D CD
88 D0 79 AA 6D 66 22 6C B6 BA 45 41 07 CB 81 A7
84 1A B0 29 60 DE 27 9C CB E3 4B 42 C3 65 85 AD
86 96 4D B0 DB 52 B6 E7 B4 36 9E CE 8F 72 48 58
9B A7 8A B1 82 8F FC 33 5C B1 23 97 11 9B FD 2B
87 EB 78 98 AE B9 56 B6 F2 3D DF 0B D4 00 43 86
A8 E5 26 55 4E F4 E4 83 FA CE E3 0D D3 2E 20 4F
FF 8C 36 BB D6 02 A5 76 D1 39 08 9C 75 A8 05 02
66 FC BF 72 1E 44 43 DE 93 C3 78 4F 39 2E CD 2E
64 48 05 DD E9 CB 4D B8 ED 75 1E 2D 7F 83 1E 3D
2C 30 0D D5 91 5A 7E B7 1F C7 20 0A 1E 2B 2D 2D
32 54 24 02 D4 B4 06 21 71 DA C6 7A E1 36 11 58
            1A A4 E9 2E 30 45 7F 59
```

State before permutation (as lanes of integers)

```
[0, 0] = 395e87ff1d085d46
[1, 0] = cd9d3e1a48e40062
[2, 0] = 6c22666daa79d088
[3, 0] = a781cb074145bab6
[4, 0] = 9c27de6029b01a84
[0, 1] = ad8565c3424be3cb
[1, 1] = e7b652dbb04d9686
[2, 1] = 5848728fce9e36b4
[3, 1] = 33fc8f82b18aa79b
[4, 1] = 2bfd9b119723b15c
[0, 2] = b656b9ae9878eb87
[1, 2] = 864300d40bdf3df2
[2, 2] = 83e4f44e5526e5a8
[3, 2] = 4f202ed30de3cefa
[4, 2] = 76a502d6bb368cff
[0, 3] = 0205a8759c0839d1
[1, 3] = de43441e72bffc66
[2, 3] = 2ecd2e394f78c393
[3, 3] = b84dcbe9dd054864
[4, 3] = 3d1e837f2d1e75ed
[0, 4] = b77e5a91d50d302c
[1, 4] = 2d2d2b1e0a20c71f
[2, 4] = 2106b4d402245432
[3, 4] = 581136e17ac6da71
[4, 4] = 597f45302ee9a41a
```

Round #0

After theta

```
48 8B 89 0C 3C 00 4C 22 FE 74 E1 3F EE 63 E1 2A
63 C3 4E 94 C4 4B 27 45 22 C3 7D 31 96 B2 F9 55
A9 E2 23 6F D3 1B CB 88 C5 35 CA 53 00 E2 97 B6
1A E2 48 C7 2F 0F CA 00 5F 25 A9 F0 26 5F 4D 71
0F DE B2 C1 13 F6 84 C1 71 49 B0 D1 A2 5E 11 3F
89 3D F9 89 6D 3E 44 AD 6E 49 DA 7C 20 5D 3F 61
43 F6 11 6B E7 D9 E1 AA 6E B7 DB 7D 42 57 58 BD
D2 74 A5 FD 65 C7 49 62 DF EF 89 8D B6 2F 17 19
FA 88 BA 05 EA 19 3F 39 78 D0 4F 71 90 03 C8 07
F0 31 3D AD 78 B2 35 4A C0 8D 8D 6B CC 46 F2 29
22 E6 8C C4 52 DD 6C AC 83 B3 25 7D EA 76 51 CA
D9 47 13 3C 7D 99 03 08 E5 A3 FE 0A 70 4F 69 AA
            37 5C 7A 68 83 80 93 4D
```

After rho

```
48 8B 89 0C 3C 00 4C 22 FC E9 C2 7F DC C7 C2 55
D8 B0 13 25 F1 D2 49 D1 29 9B 5F 25 32 DC 17 63
DE 58 46 4C 15 1F 79 9B 05 20 7E 69 5B 5C A3 3C
74 FC F2 A0 0C A0 21 8E DC 57 49 2A BC C9 57 53
6F D9 E0 09 7B C2 E0 07 15 F1 13 97 04 1B 2D EA
4D EC C9 4F 6C F3 21 6A 84 B9 25 69 F3 81 74 FD
58 3B CF 0E 57 1D B2 8F AE B0 7A DD 6E B7 FB 84
FE B2 E3 24 31 69 BA D2 1B 6D 5F 2E 32 BE DF 13
B7 40 3D E3 27 47 1F 51 E4 03 3C E8 A7 38 C8 01
B6 46 09 3E A6 A7 15 4F 29 C0 8D 8D 6B CC 46 F2
B3 B1 8A 98 33 12 4B 75 0F CE 96 F4 A9 DB 45 29
FB 68 82 A7 2F 73 00 21 A3 FE 0A 70 4F 69 AA E5
            64 D3 0D 97 1E DA 20 E0
```

After pi

```
48 8B 89 0C 3C 00 4C 22 74 FC F2 A0 0C A0 21 8E
58 3B CF 0E 57 1D B2 8F B6 46 09 3E A6 A7 15 4F
64 D3 0D 97 1E DA 20 E0 29 9B 5F 25 32 DC 17 63
15 F1 13 97 04 1B 2D EA 4D EC C9 4F 6C F3 21 6A
B7 40 3D E3 27 47 1F 51 FB 68 82 A7 2F 73 00 21
FC E9 C2 7F DC C7 C2 55 DC 57 49 2A BC C9 57 53
AE B0 7A DD 6E B7 FB 84 29 C0 8D 8D 6B CC 46 F2
B3 B1 8A 98 33 12 4B 75 DE 58 46 4C 15 1F 79 9B
05 20 7E 69 5B 5C A3 3C 84 B9 25 69 F3 81 74 FD
E4 03 3C E8 A7 38 C8 01 A3 FE 0A 70 4F 69 AA E5
D8 B0 13 25 F1 D2 49 D1 6F D9 E0 09 7B C2 E0 07
FE B2 E3 24 31 69 BA D2 1B 6D 5F 2E 32 BE DF 13
            0F CE 96 F4 A9 DB 45 29
```

After chi

```
40 88 84 02 6F 1D DE 23 D2 B8 F2 90 AC 02 24 CE
18 AA CB 8F 4F 45 92 2F BE 4E 89 36 86 A7 59 4D
50 A7 7F 37 1E 7A 01 6C 61 97 97 6D 5A 3C 17 63
A7 F1 27 37 07 1F 33 FB 05 C4 4B 4B 64 C3 21 4A
B7 D3 60 E3 37 CB 08 13 EF 08 82 35 2B 70 28 A9
DE 49 F0 AA 9E F1 6A D1 DD 17 CC 2A BD 81 53 21
3C 81 78 CD 7E A5 F2 81 65 88 CD EA A7 09 C6 F2
B3 A7 83 98 13 1A 5E 77 5E C1 47 4C B5 9E 2D 5A
65 22 66 E9 5F 64 2B 3C 87 45 27 79 BB C0 56 19
```

```
B8 03 78 E4 B7 2E 99 1B A2 DE 32 51 05 29 28 C1
48 92 10 01 F1 FB 53 01 6E 94 FC 03 79 54 A5 06
FA 30 63 F4 B8 28 BA FA CB 5D 5E 2F 62 BE D7 C3
            28 87 76 FC A3 DB E5 2F
```

After iota

```
41 88 84 02 6F 1D DE 23 D2 B8 F2 90 AC 02 24 CE
18 AA CB 8F 4F 45 92 2F BE 4E 89 36 86 A7 59 4D
50 A7 7F 37 1E 7A 01 6C 61 97 97 6D 5A 3C 17 63
A7 F1 27 37 07 1F 33 FB 05 C4 4B 4B 64 C3 21 4A
B7 D3 60 E3 37 CB 08 13 EF 08 82 35 2B 70 28 A9
DE 49 F0 AA 9E F1 6A D1 DD 17 CC 2A BD 81 53 21
3C 81 78 CD 7E A5 F2 81 65 88 CD EA A7 09 C6 F2
B3 A7 83 98 13 1A 5E 77 5E C1 47 4C B5 9E 2D 5A
65 22 66 E9 5F 64 2B 3C 87 45 27 79 BB C0 56 19
B8 03 78 E4 B7 2E 99 1B A2 DE 32 51 05 29 28 C1
48 92 10 01 F1 FB 53 01 6E 94 FC 03 79 54 A5 06
FA 30 63 F4 B8 28 BA FA CB 5D 5E 2F 62 BE D7 C3
            28 87 76 FC A3 DB E5 2F
```

(Skip rounds 1 to 22)

Round #23

After theta

```
0C C9 81 25 5B 43 08 3E B4 D2 E9 67 CD 5A 1B 50
BF 19 18 FF A3 EF 5C 4A 9A 57 B3 58 2E 48 C5 F5
A6 43 7C 03 22 73 1A E9 9C 3C D6 E3 DF 18 A9 B3
C5 66 D4 23 DE 33 07 10 CE 30 76 AF 96 E2 5D F7
A9 E0 39 BD A3 E9 52 E6 4E F0 BE 76 85 CA 58 FF
53 8C 0B 58 67 28 C9 7E 3F DB 0E 27 0D DE 86 82
5F 1C 62 8D E1 C6 3B 0F B0 41 DA 1E B9 B2 E9 8F
91 78 2B D4 E0 30 21 D1 D5 40 C4 19 8C 3B 4F B7
89 E9 04 5D C5 1C 11 26 27 3C AE 35 4F FB 28 9B
2F E2 55 40 3C 7E 99 49 E3 F9 67 EE 3B E3 D6 90
8F A1 69 85 1D DE 53 2F 17 8A 73 6D 64 76 67 8D
08 B4 20 B1 C8 64 19 52 86 72 E7 6D BC 2D 99 09
            34 3E 17 AF D9 49 4D F0
```

After rho

```
0C C9 81 25 5B 43 08 3E 68 A5 D3 CF 9A B5 36 A0
6F 06 C6 FF E8 3B 97 D2 82 54 5C AF 79 35 8B E5
99 D3 48 37 1D E2 1B 10 FE 8D 91 3A CB C9 63 3D
3D E2 3D 73 00 51 6C 46 BD 33 8C DD AB A5 78 D7
F0 9C DE D1 74 29 F3 54 8C F5 EF 04 EF 6B 57 A8
9B 62 5C C0 3A 43 49 F6 0A FE 6C 3B 9C 34 78 1B
6B 0C 37 DE 79 F8 E2 10 65 D3 1F 61 83 B4 3D 72
6A 70 98 90 E8 48 BC 15 33 18 77 9E 6E AB 81 88
A0 AB 98 23 C2 24 31 9D 94 CD 13 1E D7 9A A7 7D
2F 33 E9 45 BC 0A 88 C7 90 E3 F9 67 EE 3B E3 D6
4F BD 3C 86 A6 15 76 78 5E 28 CE B5 91 D9 9D 35
81 16 24 16 99 2C 43 0A 72 E7 6D BC 2D 99 09 86
            13 3C 8D CF C5 6B 76 52
```

After pi

```
0C C9 81 25 5B 43 08 3E 3D E2 3D 73 00 51 6C 46
6B 0C 37 DE 79 F8 E2 10 2F 33 E9 45 BC 0A 88 C7
13 3C 8D CF C5 6B 76 52 82 54 5C AF 79 35 8B E5
8C F5 EF 04 EF 6B 57 A8 9B 62 5C C0 3A 43 49 F6
A0 AB 98 23 C2 24 31 9D 81 16 24 16 99 2C 43 0A
68 A5 D3 CF 9A B5 36 A0 BD 33 8C DD AB A5 78 D7
65 D3 1F 61 83 B4 3D 72 90 E3 F9 67 EE 3B E3 D6
4F BD 3C 86 A6 15 76 78 99 D3 48 37 1D E2 1B 10
FE 8D 91 3A CB C9 63 3D 0A FE 6C 3B 9C 34 78 1B
94 CD 13 1E D7 9A A7 7D 72 E7 6D BC 2D 99 09 86
6F 06 C6 FF E8 3B 97 D2 F0 9C DE D1 74 29 F3 54
6A 70 98 90 E8 48 BC 15 33 18 77 9E 6E AB 81 88
            5E 28 CE B5 91 D9 9D 35
```

After chi

```
4E C5 83 A9 22 EB 8A 2E 39 D1 F5 72 84 53 64 81
7B 00 33 54 38 99 94 00 23 F2 E9 65 A6 0A 80 EB
22 1E B1 9D C5 7B 12 12 91 56 4C 6F 69 35 83 B3
AC 7C 6F 27 2F 4F 67 A1 9A 76 78 D4 23 4B 0B F4
A2 EB C0 8A A2 35 B9 78 8D B7 87 16 1F 66 17 02
28 65 C0 EF 9A A5 33 80 2D 13 6C DB C7 AE BA 53
2A CF 1B E1 83 B0 29 5A B0 E3 3A 2E F6 9B E3 56
DA AF 30 96 87 15 3E 2F 99 A1 24 36 09 D6 03 12
6A 8C 82 3E 88 43 E4 59 68 DC 00 9B B4 35 70 99
1D DD 13 1D C7 F8 B5 6D 14 EB FC B4 EF 90 69 AB
65 66 C6 FF 60 7B 9B D3 E1 94 B9 DF 72 8A F2 DC
26 50 10 B1 79 18 A0 20 12 1E 77 D4 06 89 83 4A
            CE B0 D6 B5 85 D9 FD 31
```

After iota

```
46 45 83 29 22 EB 8A AE 39 D1 F5 72 84 53 64 81
7B 00 33 54 38 99 94 00 23 F2 E9 65 A6 0A 80 EB
22 1E B1 9D C5 7B 12 12 91 56 4C 6F 69 35 83 B3
AC 7C 6F 27 2F 4F 67 A1 9A 76 78 D4 23 4B 0B F4
A2 EB C0 8A A2 35 B9 78 8D B7 87 16 1F 66 17 02
28 65 C0 EF 9A A5 33 80 2D 13 6C DB C7 AE BA 53
2A CF 1B E1 83 B0 29 5A B0 E3 3A 2E F6 9B E3 56
DA AF 30 96 87 15 3E 2F 99 A1 24 36 09 D6 03 12
6A 8C 82 3E 88 43 E4 59 68 DC 00 9B B4 35 70 99
1D DD 13 1D C7 F8 B5 6D 14 EB FC B4 EF 90 69 AB
65 66 C6 FF 60 7B 9B D3 E1 94 B9 DF 72 8A F2 DC
26 50 10 B1 79 18 A0 20 12 1E 77 D4 06 89 83 4A
            CE B0 D6 B5 85 D9 FD 31
```

After permutation

```
46 45 83 29 22 EB 8A AE 39 D1 F5 72 84 53 64 81
7B 00 33 54 38 99 94 00 23 F2 E9 65 A6 0A 80 EB
22 1E B1 9D C5 7B 12 12 91 56 4C 6F 69 35 83 B3
AC 7C 6F 27 2F 4F 67 A1 9A 76 78 D4 23 4B 0B F4
A2 EB C0 8A A2 35 B9 78 8D B7 87 16 1F 66 17 02
28 65 C0 EF 9A A5 33 80 2D 13 6C DB C7 AE BA 53
2A CF 1B E1 83 B0 29 5A B0 E3 3A 2E F6 9B E3 56
DA AF 30 96 87 15 3E 2F 99 A1 24 36 09 D6 03 12
6A 8C 82 3E 88 43 E4 59 68 DC 00 9B B4 35 70 99
```

```
1D DD 13 1D C7 F8 B5 6D 14 EB FC B4 EF 90 69 AB
65 66 C6 FF 60 7B 9B D3 E1 94 B9 DF 72 8A F2 DC
26 50 10 B1 79 18 A0 20 12 1E 77 D4 06 89 83 4A
           CE B0 D6 B5 85 D9 FD 31
```

State (as lanes of integers)

```
[0, 0] = ae8aeb2229834546
[1, 0] = 8164538472f5d139
[2, 0] = 009499385433007b
[3, 0] = eb800aa665e9f223
[4, 0] = 12127bc59db11e22
[0, 1] = b38335696f4c5691
[1, 1] = a1674f2f276f7cac
[2, 1] = f40b4b23d478769a
[3, 1] = 78b935a28ac0eba2
[4, 1] = 0217661f1687b78d
[0, 2] = 8033a59aefc06528
[1, 2] = 53baaec7db6c132d
[2, 2] = 5a29b083e11bcf2a
[3, 2] = 56e39bf62e3ae3b0
[4, 2] = 2f3e15879630afda
[0, 3] = 1203d6093624a199
[1, 3] = 59e443883e828c6a
[2, 3] = 997035b49b00dc68
[3, 3] = 6db5f8c71d13dd1d
[4, 3] = ab6990efb4fceb14
[0, 4] = d39b7b60ffc66665
[1, 4] = dcf28a72dfb994e1
[2, 4] = 20a01879b1105026
[3, 4] = 4a838906d4771e12
[4, 4] = 31fdd985b5d6b0ce
```

About to call squeeze (again)

State before permutation (in bytes)

```
46 45 83 29 22 EB 8A AE 39 D1 F5 72 84 53 64 81
7B 00 33 54 38 99 94 00 23 F2 E9 65 A6 0A 80 EB
22 1E B1 9D C5 7B 12 12 91 56 4C 6F 69 35 83 B3
AC 7C 6F 27 2F 4F 67 A1 9A 76 78 D4 23 4B 0B F4
A2 EB C0 8A A2 35 B9 78 8D B7 87 16 1F 66 17 02
28 65 C0 EF 9A A5 33 80 2D 13 6C DB C7 AE BA 53
2A CF 1B E1 83 B0 29 5A B0 E3 3A 2E F6 9B E3 56
DA AF 30 96 87 15 3E 2F 99 A1 24 36 09 D6 03 12
6A 8C 82 3E 88 43 E4 59 68 DC 00 9B B4 35 70 99
1D DD 13 1D C7 F8 B5 6D 14 EB FC B4 EF 90 69 AB
65 66 C6 FF 60 7B 9B D3 E1 94 B9 DF 72 8A F2 DC
26 50 10 B1 79 18 A0 20 12 1E 77 D4 06 89 83 4A
           CE B0 D6 B5 85 D9 FD 31
```

State before permutation (as lanes of integers)

```
[0, 0] = ae8aeb2229834546
[1, 0] = 8164538472f5d139
[2, 0] = 009499385433007b
[3, 0] = eb800aa665e9f223
[4, 0] = 12127bc59db11e22
```

```
[0, 1] = b38335696f4c5691
[1, 1] = a1674f2f276f7cac
[2, 1] = f40b4b23d478769a
[3, 1] = 78b935a28ac0eba2
[4, 1] = 0217661f1687b78d
[0, 2] = 8033a59aefc06528
[1, 2] = 53baaec7db6c132d
[2, 2] = 5a29b083e11bcf2a
[3, 2] = 56e39bf62e3ae3b0
[4, 2] = 2f3e15879630afda
[0, 3] = 1203d6093624a199
[1, 3] = 59e443883e828c6a
[2, 3] = 997035b49b00dc68
[3, 3] = 6db5f8c71d13dd1d
[4, 3] = ab6990efb4fceb14
[0, 4] = d39b7b60ffc66665
[1, 4] = dcf28a72dfb994e1
[2, 4] = 20a01879b1105026
[3, 4] = 4a838906d4771e12
[4, 4] = 31fdd985b5d6b0ce
```

Round #0

After theta

```
8E 54 34 EA 39 5D 7B E6 30 0B 98 84 96 1B 0A F3
35 D4 10 2B C8 48 E2 33 F9 7C F1 16 9D C7 B8 B7
1A 45 1D 54 86 03 BB 49 59 47 FB AC 72 83 72 FB
A5 A6 02 D1 3D 07 09 D3 D4 A2 5B AB D3 9A 7D C7
78 65 D8 F9 99 F8 81 24 B5 EC 2B DF 5C 1E BE 59
E0 74 77 2C 81 13 C2 C8 24 C9 01 2D D5 E6 D4 21
64 1B 38 9E 73 61 5F 69 6A 6D 22 5D CD 56 DB 0A
E2 F4 9C 5F C4 6D 97 74 51 B0 93 F5 12 60 F2 5A
63 56 EF C8 9A 0B 8A 2B 26 08 23 E4 44 E4 06 AA
C7 53 0B 6E FC 35 8D 31 2C B0 50 7D AC E8 C0 F0
AD 77 71 3C 7B CD 6A 9B E8 4E D4 29 60 C2 9C AE
68 84 33 CE 89 C9 D6 13 C8 90 6F A7 3D 44 BB 16
            F6 EB 7A 7C C6 A1 54 6A
```

After rho

```
8E 54 34 EA 39 5D 7B E6 61 16 30 09 2D 37 14 E6
0D 35 C4 0A 32 92 F8 4C 79 8C 7B 9B CF 17 6F D1
1C D8 4D D2 28 EA A0 32 2A 37 28 B7 9F 75 B4 CF
10 DD 73 90 30 5D 6A 2A 31 B5 E8 D6 EA B4 66 DF
32 EC FC 4C FC 40 12 BC E1 9B 55 CB BE F2 CD E5
06 A7 BB 63 09 9C 10 46 87 90 24 07 B4 54 9B 53
F1 9C 0B FB 4A 23 DB C0 AD B6 15 D4 DA 44 BA 9A
2F E2 B6 4B 3A 71 7A CE EB 25 C0 E4 B5 A2 60 27
1D 59 73 41 71 65 CC EA 03 55 13 84 11 72 22 72
A6 31 E6 78 6A C1 8D BF F0 2C B0 50 7D AC E8 C0
AB 6D B6 DE C5 F1 EC 35 A2 3B 51 A7 80 09 73 BA
8D 70 C6 39 31 D9 7A 02 90 6F A7 3D 44 BB 16 C8
            95 9A FD BA 1E 9F 71 28
```

After pi

```
8E 54 34 EA 39 5D 7B E6 10 DD 73 90 30 5D 6A 2A
F1 9C 0B FB 4A 23 DB C0 A6 31 E6 78 6A C1 8D BF
95 9A FD BA 1E 9F 71 28 79 8C 7B 9B CF 17 6F D1
E1 9B 55 CB BE F2 CD E5 06 A7 BB 63 09 9C 10 46
1D 59 73 41 71 65 CC EA 8D 70 C6 39 31 D9 7A 02
61 16 30 09 2D 37 14 E6 31 B5 E8 D6 EA B4 66 DF
AD B6 15 D4 DA 44 BA 9A F0 2C B0 50 7D AC E8 C0
AB 6D B6 DE C5 F1 EC 35 1C D8 4D D2 28 EA A0 32
2A 37 28 B7 9F 75 B4 CF 87 90 24 07 B4 54 9B 53
03 55 13 84 11 72 22 72 90 6F A7 3D 44 BB 16 C8
0D 35 C4 0A 32 92 F8 4C 32 EC FC 4C FC 40 12 BC
2F E2 B6 4B 3A 71 7A CE EB 25 C0 E4 B5 A2 60 27
            A2 3B 51 A7 80 09 73 BA
```

After chi

```
6F 54 3C 81 73 7F EA 26 16 FC 97 90 10 9D 6E 15
E0 16 12 79 5E 3D AB C0 AC 75 E6 38 4B 81 87 79
85 13 BE AA 1E 9F 71 20 7F A8 D1 BB CE 1B 7F D3
F8 C3 15 CB CE 93 01 4D 86 87 3F 5B 09 04 22 46
6D D5 4A C3 BF 63 C9 3B 0D 63 C2 79 01 39 FA 26
ED 14 25 09 3D 77 8C E6 61 BD 48 D6 CF 1C 26 9F
A6 F7 13 5A 5A 15 BE AF B0 3E B0 51 55 AA F8 02
BB CC 7E 08 07 71 8E 2C 99 58 49 D2 08 EA AB 22
2A 72 3B 37 9E 57 94 EF 17 BA 80 3E F0 DD 8F DB
0F C5 5B 46 39 32 82 40 B2 48 87 18 D3 AE 02 05
00 37 C6 09 30 A3 90 0E F2 E9 BC E8 79 C2 12 9D
2F F8 A7 48 3A 78 69 56 E6 21 44 EC 87 30 E8 63
            90 F3 69 E3 4C 49 71 0A
```

After iota

```
6E 54 3C 81 73 7F EA 26 16 FC 97 90 10 9D 6E 15
E0 16 12 79 5E 3D AB C0 AC 75 E6 38 4B 81 87 79
85 13 BE AA 1E 9F 71 20 7F A8 D1 BB CE 1B 7F D3
F8 C3 15 CB CE 93 01 4D 86 87 3F 5B 09 04 22 46
6D D5 4A C3 BF 63 C9 3B 0D 63 C2 79 01 39 FA 26
ED 14 25 09 3D 77 8C E6 61 BD 48 D6 CF 1C 26 9F
A6 F7 13 5A 5A 15 BE AF B0 3E B0 51 55 AA F8 02
BB CC 7E 08 07 71 8E 2C 99 58 49 D2 08 EA AB 22
2A 72 3B 37 9E 57 94 EF 17 BA 80 3E F0 DD 8F DB
0F C5 5B 46 39 32 82 40 B2 48 87 18 D3 AE 02 05
00 37 C6 09 30 A3 90 0E F2 E9 BC E8 79 C2 12 9D
2F F8 A7 48 3A 78 69 56 E6 21 44 EC 87 30 E8 63
            90 F3 69 E3 4C 49 71 0A
```

(Skip rounds 1 to 22)

Round #23

After theta

```
97 06 A9 B2 38 5C D4 E3 8F DF B3 23 53 11 EF 32
81 7C 46 D4 7A C0 73 A0 33 81 E1 6A 8A D6 D5 53
F9 E5 9E FE 9D 56 A7 8B 74 DE 44 08 49 77 33 EF
7B EC D0 A4 D3 46 8F 5A 7A 6E 36 0A D8 B6 6A 82
40 CE 85 2A 43 E6 6C 0B 8A F1 50 21 4F 4F AA 83
98 FA 3C 4B 3A 20 4A 2B 00 89 2A E5 30 8D 3D 89
38 89 94 6C CC 54 36 8F A7 09 83 0A AD 2F F5 9D
```

```
25 96 AE AF 59 98 E4 1A F2 F2 C0 47 0A 37 B3 41
86 70 78 34 5D 42 32 98 44 B5 7E FC 0A EC B3 C7
24 01 D7 9C A2 81 5C AD 5C AE 62 DB BA 57 D7 07
A0 EC A6 81 C7 67 BD 51 AB E1 E0 F6 CF 24 26 61
A3 AD 55 F0 45 6E 49 22 D0 9F FE 2D 5F 0C 17 8A
            23 B5 A2 13 2A F3 81 F6
```

After rho

```
97 06 A9 B2 38 5C D4 E3 1E BF 67 47 A6 22 DE 65
20 9F 11 B5 1E F0 1C 68 68 5D 3D 35 13 18 AE A6
B4 3A 5D CC 2F F7 F4 EF 90 74 37 F3 4E E7 4D 84
4D 3A 6D F4 A8 B5 C7 0E A0 9E 9B 8D 02 B6 AD 9A
E7 42 95 21 73 B6 05 20 A4 3A A8 18 0F 15 F2 F4
C1 D4 E7 59 D2 01 51 5A 24 02 24 AA 94 C3 34 F6
64 63 A6 B2 79 C4 49 A4 5F EA 3B 4F 13 06 15 5A
D7 2C 4C 72 8D 12 4B D7 8F 14 6E 66 83 E4 E5 81
8F A6 4B 48 06 D3 10 0E D9 63 A2 5A 3F 7E 05 F6
90 AB 95 24 E0 9A 53 34 07 5C AE 62 DB BA 57 D7
F5 46 81 B2 9B 06 1E 9F AD 86 83 DB 3F 93 98 84
B4 B5 0A BE C8 2D 49 64 9F FE 2D 5F 0C 17 8A D0
            A0 FD 48 AD E8 84 CA 7C
```

After pi

```
97 06 A9 B2 38 5C D4 E3 4D 3A 6D F4 A8 B5 C7 0E
64 63 A6 B2 79 C4 49 A4 90 AB 95 24 E0 9A 53 34
A0 FD 48 AD E8 84 CA 7C 68 5D 3D 35 13 18 AE A6
A4 3A A8 18 0F 15 F2 F4 C1 D4 E7 59 D2 01 51 5A
8F A6 4B 48 06 D3 10 0E B4 B5 0A BE C8 2D 49 64
1E BF 67 47 A6 22 DE 65 A0 9E 9B 8D 02 B6 AD 9A
5F EA 3B 4F 13 06 15 5A 07 5C AE 62 DB BA 57 D7
F5 46 81 B2 9B 06 1E 9F B4 3A 5D CC 2F F7 F4 EF
90 74 37 F3 4E E7 4D 84 24 02 24 AA 94 C3 34 F6
D9 63 A2 5A 3F 7E 05 F6 9F FE 2D 5F 0C 17 8A D0
20 9F 11 B5 1E F0 1C 68 E7 42 95 21 73 B6 05 20
D7 2C 4C 72 8D 12 4B D7 8F 14 6E 66 83 E4 E5 81
            AD 86 83 DB 3F 93 98 84
```

After chi

```
B7 47 2B B0 69 1C DC 43 DD B2 7C F0 28 AF D5 1E
44 37 EE 3B 71 C0 C1 EC 87 A9 34 36 F0 C2 47 B7
E8 C5 0C E9 68 25 C9 70 29 99 7A 74 C3 18 AF AC
AA 18 A0 18 0B C7 F2 F0 F1 C5 E7 EF 1A 2D 18 3A
C7 EE 7E 49 15 C3 B6 8C 30 97 8A B6 C4 28 19 34
41 DF 47 05 B7 22 CE 25 A0 8A 1F AD CA 0E EF 1F
AF E8 3A DF 13 02 1D 52 0D E5 C8 27 FF 9A 97 B7
55 46 19 3A 9B 92 3F 05 90 38 5D C4 BF F7 C4 9D
49 15 B5 A3 65 DB 4C 84 22 9E 29 AF 94 C2 BE F6
F9 63 F2 DA 1C 9E 71 D9 9F BA 0F 6C 4C 17 83 D0
30 B3 59 E7 92 F0 56 BF EF 52 B7 25 71 52 A1 20
F7 AE CD EB B1 01 53 D3 8F 0D 7E 42 83 84 E1 E9
            6A C6 07 DB 5E 95 99 84
```

After iota

```
BF C7 2B 30 69 1C DC C3 DD B2 7C F0 28 AF D5 1E
44 37 EE 3B 71 C0 C1 EC 87 A9 34 36 F0 C2 47 B7
E8 C5 0C E9 68 25 C9 70 29 99 7A 74 C3 18 AF AC
AA 18 A0 18 0B C7 F2 F0 F1 C5 E7 EF 1A 2D 18 3A
```

```
C7 EE 7E 49 15 C3 B6 8C 30 97 8A B6 C4 28 19 34
41 DF 47 05 B7 22 CE 25 A0 8A 1F AD CA 0E EF 1F
AF E8 3A DF 13 02 1D 52 0D E5 C8 27 FF 9A 97 B7
55 46 19 3A 9B 92 3F 05 90 38 5D C4 BF F7 C4 9D
49 15 B5 A3 65 DB 4C 84 22 9E 29 AF 94 C2 BE F6
F9 63 F2 DA 1C 9E 71 D9 9F BA 0F 6C 4C 17 83 D0
30 B3 59 E7 92 F0 56 BF EF 52 B7 25 71 52 A1 20
F7 AE CD EB B1 01 53 D3 8F 0D 7E 42 83 84 E1 E9
            6A C6 07 DB 5E 95 99 84
```

After permutation

```
BF C7 2B 30 69 1C DC C3 DD B2 7C F0 28 AF D5 1E
44 37 EE 3B 71 C0 C1 EC 87 A9 34 36 F0 C2 47 B7
E8 C5 0C E9 68 25 C9 70 29 99 7A 74 C3 18 AF AC
AA 18 A0 18 0B C7 F2 F0 F1 C5 E7 EF 1A 2D 18 3A
C7 EE 7E 49 15 C3 B6 8C 30 97 8A B6 C4 28 19 34
41 DF 47 05 B7 22 CE 25 A0 8A 1F AD CA 0E EF 1F
AF E8 3A DF 13 02 1D 52 0D E5 C8 27 FF 9A 97 B7
55 46 19 3A 9B 92 3F 05 90 38 5D C4 BF F7 C4 9D
49 15 B5 A3 65 DB 4C 84 22 9E 29 AF 94 C2 BE F6
F9 63 F2 DA 1C 9E 71 D9 9F BA 0F 6C 4C 17 83 D0
30 B3 59 E7 92 F0 56 BF EF 52 B7 25 71 52 A1 20
F7 AE CD EB B1 01 53 D3 8F 0D 7E 42 83 84 E1 E9
            6A C6 07 DB 5E 95 99 84
```

State (as lanes of integers)

```
[0, 0] = c3dc1c69302bc7bf
[1, 0] = 1ed5af28f07cb2dd
[2, 0] = ecc1c0713bee3744
[3, 0] = b747c2f03634a987
[4, 0] = 70c92568e90cc5e8
[0, 1] = acaf18c3747a9929
[1, 1] = f0f2c70b18a018aa
[2, 1] = 3a182d1aefe7c5f1
[3, 1] = 8cb6c315497eeec7
[4, 1] = 341928c4b68a9730
[0, 2] = 25ce22b70547df41
[1, 2] = 1fef0ecaad1f8aa0
[2, 2] = 521d0213df3ae8af
[3, 2] = b7979aff27c8e50d
[4, 2] = 053f929b3a194655
[0, 3] = 9dc4f7bfc45d3890
[1, 3] = 844cdb65a3b51549
[2, 3] = f6bec294af299e22
[3, 3] = d9719e1cdaf263f9
[4, 3] = d083174c6c0fba9f
[0, 4] = bf56f092e759b330
[1, 4] = 20a1527125b752ef
[2, 4] = d35301b1ebcdaef7
[3, 4] = e9e18483427e0d8f
[4, 4] = 8499955edb07c66a
```

About to call squeeze (again)

State before permutation (in bytes)

```
BF C7 2B 30 69 1C DC C3 DD B2 7C F0 28 AF D5 1E
44 37 EE 3B 71 C0 C1 EC 87 A9 34 36 F0 C2 47 B7
E8 C5 0C E9 68 25 C9 70 29 99 7A 74 C3 18 AF AC
AA 18 A0 18 0B C7 F2 F0 F1 C5 E7 EF 1A 2D 18 3A
C7 EE 7E 49 15 C3 B6 8C 30 97 8A B6 C4 28 19 34
41 DF 47 05 B7 22 CE 25 A0 8A 1F AD CA 0E EF 1F
AF E8 3A DF 13 02 1D 52 0D E5 C8 27 FF 9A 97 B7
55 46 19 3A 9B 92 3F 05 90 38 5D C4 BF F7 C4 9D
49 15 B5 A3 65 DB 4C 84 22 9E 29 AF 94 C2 BE F6
F9 63 F2 DA 1C 9E 71 D9 9F BA 0F 6C 4C 17 83 D0
30 B3 59 E7 92 F0 56 BF EF 52 B7 25 71 52 A1 20
F7 AE CD EB B1 01 53 D3 8F 0D 7E 42 83 84 E1 E9
            6A C6 07 DB 5E 95 99 84
```

State before permutation (as lanes of integers)

```
[0, 0] = c3dc1c69302bc7bf
[1, 0] = 1ed5af28f07cb2dd
[2, 0] = ecc1c0713bee3744
[3, 0] = b747c2f03634a987
[4, 0] = 70c92568e90cc5e8
[0, 1] = acaf18c3747a9929
[1, 1] = f0f2c70b18a018aa
[2, 1] = 3a182d1aefe7c5f1
[3, 1] = 8cb6c315497eeec7
[4, 1] = 341928c4b68a9730
[0, 2] = 25ce22b70547df41
[1, 2] = 1fef0ecaad1f8aa0
[2, 2] = 521d0213df3ae8af
[3, 2] = b7979aff27c8e50d
[4, 2] = 053f929b3a194655
[0, 3] = 9dc4f7bfc45d3890
[1, 3] = 844cdb65a3b51549
[2, 3] = f6bec294af299e22
[3, 3] = d9719e1cdaf263f9
[4, 3] = d083174c6c0fba9f
[0, 4] = bf56f092e759b330
[1, 4] = 20a1527125b752ef
[2, 4] = d35301b1ebcdaef7
[3, 4] = e9e18483427e0d8f
[4, 4] = 8499955edb07c66a
```

Round #0

After theta

```
25 61 3E 65 B7 DE 62 7C 35 ED C0 0D A2 D6 A8 34
42 C8 32 78 87 2C 09 C0 B8 53 CD DC E6 D4 84 3D
3D 1D 26 ED 8D E6 61 1C B3 3F 6F 21 1D DA 11 13
42 47 1C E5 81 BE 8F DA F7 3A 3B AC EC C1 D0 16
F8 14 87 A3 03 D5 75 06 E5 4F A0 B2 21 EB B1 58
DB 79 52 50 69 E0 70 9A 48 D5 A3 50 40 77 92 35
A9 17 E6 9C E5 EE D5 7E 32 1F 31 CD E9 8C 54 3D
80 9E 33 3E 7E 51 97 69 0A 9E 48 91 61 35 7A 22
A1 4A 09 5E EF A2 31 AE 24 61 F5 EC 62 2E 76 DA
```

```
C6 99 0B 30 0A 88 B2 53 4A 62 25 68 A9 D4 2B BC
AA 15 4C B2 4C 32 E8 00 07 0D 0B D8 FB 2B DC 0A
F1 51 11 A8 47 ED 9B FF B0 F7 87 A8 95 92 22 63
               BF 1E 2D DF BB 56 31 E8
```

After rho

```
25 61 3E 65 B7 DE 62 7C 6A DA 81 1B 44 AD 51 69
10 B2 0C DE 21 4B 02 B0 4E 4D D8 83 3B D5 CC 6D
34 0F E3 E8 E9 30 69 6F D2 A1 1D 31 31 FB F3 16
51 1E E8 FB A8 2D 74 C4 C5 BD CE 0E 2B 7B 30 B4
8A C3 D1 81 EA 3A 03 7C 1E 8B 55 FE 04 2A 1B B2
DC CE 93 82 4A 03 87 D3 D6 20 55 8F 42 01 DD 49
E7 2C 77 AF F6 4B BD 30 19 A9 7A 64 3E 62 9A D3
1F BF A8 CB 34 40 CF 19 22 C3 6A F4 44 14 3C 91
C1 EB 5D 34 C6 35 54 29 3B 6D 92 B0 7A 76 31 17
51 76 CA 38 73 01 46 01 BC 4A 62 25 68 A9 D4 2B
A0 03 A8 56 30 C9 32 C9 1C 34 2C 60 EF AF 70 2B
3E 2A 02 F5 A8 7D F3 3F F7 87 A8 95 92 22 63 B0
               0C FA AF 47 CB F7 AE 55
```

After pi

```
25 61 3E 65 B7 DE 62 7C 51 1E E8 FB A8 2D 74 C4
E7 2C 77 AF F6 4B BD 30 51 76 CA 38 73 01 46 01
0C FA AF 47 CB F7 AE 55 4E 4D D8 83 3B D5 CC 6D
1E 8B 55 FE 04 2A 1B B2 DC CE 93 82 4A 03 87 D3
C1 EB 5D 34 C6 35 54 29 3E 2A 02 F5 A8 7D F3 3F
6A DA 81 1B 44 AD 51 69 C5 BD CE 0E 2B 7B 30 B4
19 A9 7A 64 3E 62 9A D3 BC 4A 62 25 68 A9 D4 2B
A0 03 A8 56 30 C9 32 C9 34 0F E3 E8 E9 30 69 6F
D2 A1 1D 31 31 FB F3 16 D6 20 55 8F 42 01 DD 49
3B 6D 92 B0 7A 76 31 17 F7 87 A8 95 92 22 63 B0
10 B2 0C DE 21 4B 02 B0 8A C3 D1 81 EA 3A 03 7C
1F BF A8 CB 34 40 CF 19 22 C3 6A F4 44 14 3C 91
               1C 34 2C 60 EF AF 70 2B
```

After chi

```
83 41 29 61 E1 9C EB 4C 41 4C 60 EB A9 2D 36 C5
EB A4 52 E8 7E BD 15 64 70 77 DA 18 47 09 06 29
5C E4 6F DD C3 D6 BA D5 8E 09 5A 83 71 D4 48 2C
1F AA 19 CA 80 1E 4B 9A E2 CE 91 43 62 4B 24 C5
81 AE 85 36 D5 B5 58 69 2E A8 07 89 AC 57 E0 AD
72 DA B1 7B 50 AD DB 2A 61 FF CE 0F 6B F2 74 9C
19 A8 F2 36 2E 22 B8 13 F6 92 63 2C 2C 8D 95 0B
25 26 E6 52 1B 9B 12 5D 30 0F A3 66 AB 30 65 26
FB EC 9F 01 09 8D D3 00 12 A2 7D 8A C2 01 9F E9
3B 65 D1 D8 13 66 39 58 35 27 B4 84 82 E9 F1 A0
05 8E 24 94 35 0B CE B1 AA 83 93 B5 AA 2E 33 FC
03 8B AC CB 9F EB 8F 33 22 41 6A 6A 44 54 3E 01
               96 75 FD 61 25 9F 71 67
```

After iota

```
82 41 29 61 E1 9C EB 4C 41 4C 60 EB A9 2D 36 C5
EB A4 52 E8 7E BD 15 64 70 77 DA 18 47 09 06 29
5C E4 6F DD C3 D6 BA D5 8E 09 5A 83 71 D4 48 2C
1F AA 19 CA 80 1E 4B 9A E2 CE 91 43 62 4B 24 C5
81 AE 85 36 D5 B5 58 69 2E A8 07 89 AC 57 E0 AD
72 DA B1 7B 50 AD DB 2A 61 FF CE 0F 6B F2 74 9C
```

```
19 A8 F2 36 2E 22 B8 13 F6 92 63 2C 2C 8D 95 0B
25 26 E6 52 1B 9B 12 5D 30 0F A3 66 AB 30 65 26
FB EC 9F 01 09 8D D3 00 12 A2 7D 8A C2 01 9F E9
3B 65 D1 D8 13 66 39 58 35 27 B4 84 82 E9 F1 A0
05 8E 24 94 35 0B CE B1 AA 83 93 B5 AA 2E 33 FC
03 8B AC CB 9F EB 8F 33 22 41 6A 6A 44 54 3E 01
            96 75 FD 61 25 9F 71 67
```

(Skip rounds 1 to 22)

Round #23

After theta

```
DC 0B 39 6D E0 BF 0E 37 86 94 6B 37 1E FC 40 22
26 33 5B 91 46 31 15 8A 23 B8 4F 9A 7E 11 15 D9
2E 1D 5D BC D4 A3 69 30 7E 0C D9 82 09 3D A6 3E
C2 A1 47 73 EB E9 70 9F 9A 80 17 78 71 2A BC B8
47 74 40 FE AA 70 F8 71 3A A9 85 D6 C6 09 6A EA
8F 1B 26 7D EE 9C C2 06 8B 13 14 4E 3D F5 61 04
8D 9C A1 47 78 04 36 D3 33 DE 3C EF 21 65 53 BB
25 D4 4B 90 58 01 D2 CD BF BB E2 CD 9F AC B6 F6
39 32 FE 4D AD B6 8D 5C F8 FC 4D 64 D9 A7 A3 3B
66 77 9C 22 EA 4F 08 3D E4 49 62 DB 2E 21 70 B4
27 98 8D 6D 44 E5 49 02 43 61 24 56 45 83 63 B3
93 05 06 CF 48 42 39 99 EB B0 02 E1 30 48 A7 21
            26 E4 BC 4F A3 7E 62 82
```

After rho

```
DC 0B 39 6D E0 BF 0E 37 0C 29 D7 6E 3C F8 81 44
C9 CC 56 A4 51 4C 85 A2 17 51 91 3D 82 FB A4 E9
1E 4D 83 71 E9 E8 E2 A5 98 D0 63 EA E3 C7 90 2D
34 B7 9E 0E F7 29 1C 7A AE 26 E0 05 5E 9C 0A 2F
3A 20 7F 55 38 FC B8 23 A0 A6 AE 93 5A 68 6D 9C
78 DC 30 E9 73 E7 14 36 11 2C 4E 50 38 F5 D4 87
3D C2 23 B0 99 6E E4 0C CA A6 76 67 BC 79 DE 43
48 AC 00 E9 E6 12 EA 25 9B 3F 59 6D ED 7F 77 C5
BF A9 D5 B6 91 2B 47 C6 D1 1D 7C FE 26 B2 EC D3
09 A1 C7 EC 8E 53 44 FD B4 E4 49 62 DB 2E 21 70
27 09 9C 60 36 B6 11 95 0E 85 91 58 15 0D 8E CD
B2 C0 E0 19 49 28 27 73 B0 02 E1 30 48 A7 21 EB
            98 A0 09 39 EF D3 A8 9F
```

After pi

```
DC 0B 39 6D E0 BF 0E 37 34 B7 9E 0E F7 29 1C 7A
3D C2 23 B0 99 6E E4 0C 09 A1 C7 EC 8E 53 44 FD
98 A0 09 39 EF D3 A8 9F 17 51 91 3D 82 FB A4 E9
A0 A6 AE 93 5A 68 6D 9C 78 DC 30 E9 73 E7 14 36
BF A9 D5 B6 91 2B 47 C6 B2 C0 E0 19 49 28 27 73
0C 29 D7 6E 3C F8 81 44 AE 26 E0 05 5E 9C 0A 2F
CA A6 76 67 BC 79 DE 43 B4 E4 49 62 DB 2E 21 70
27 09 9C 60 36 B6 11 95 1E 4D 83 71 E9 E8 E2 A5
98 D0 63 EA E3 C7 90 2D 11 2C 4E 50 38 F5 D4 87
D1 1D 7C FE 26 B2 EC D3 B0 02 E1 30 48 A7 21 EB
C9 CC 56 A4 51 4C 85 A2 3A 20 7F 55 38 FC B8 23
48 AC 00 E9 E6 12 EA 25 9B 3F 59 6D ED 7F 77 C5
            0E 85 91 58 15 0D 8E CD
```

After chi

```
D5 4B 18 DD E8 F9 EE 33 34 96 5A 42 F1 38 1C 8B
AD C2 2B A1 F8 EE 4C 0E 4D AA F7 A8 8E 7F 42 DD
B8 14 8F 3B F8 D3 B8 D7 4F 09 81 55 A3 7C B4 CB
27 87 6B 85 DA 60 2E 5C 78 9C 10 E0 3B E7 34 07
BA B8 C4 92 13 F8 C7 4E 12 66 CE 9B 11 28 6E 67
4C A9 C1 0C 9C 99 55 04 9A 66 E9 05 1D 9A 2B 1F
C9 AF E2 67 98 E9 CE C6 BC C4 0A 6C D3 66 A1 30
85 0F BC 61 74 B2 1B BE 1F 61 8F 61 F1 D8 A6 27
58 C1 53 44 E5 C5 B8 7D 31 2E CF 50 70 F0 D5 AF
DF 50 7E BF 87 FA 2E D7 30 92 81 BA 4A A0 31 E3
89 40 56 0C 97 4E C7 A6 A9 33 26 51 31 91 AD E3
4C 2C 80 F9 F6 12 62 2D 5A 77 1F C9 AD 3F 76 E7
            3C A5 B8 09 3D BD B6 CC
```

After iota

```
DD CB 18 5D E8 F9 EE B3 34 96 5A 42 F1 38 1C 8B
AD C2 2B A1 F8 EE 4C 0E 4D AA F7 A8 8E 7F 42 DD
B8 14 8F 3B F8 D3 B8 D7 4F 09 81 55 A3 7C B4 CB
27 87 6B 85 DA 60 2E 5C 78 9C 10 E0 3B E7 34 07
BA B8 C4 92 13 F8 C7 4E 12 66 CE 9B 11 28 6E 67
4C A9 C1 0C 9C 99 55 04 9A 66 E9 05 1D 9A 2B 1F
C9 AF E2 67 98 E9 CE C6 BC C4 0A 6C D3 66 A1 30
85 0F BC 61 74 B2 1B BE 1F 61 8F 61 F1 D8 A6 27
58 C1 53 44 E5 C5 B8 7D 31 2E CF 50 70 F0 D5 AF
DF 50 7E BF 87 FA 2E D7 30 92 81 BA 4A A0 31 E3
89 40 56 0C 97 4E C7 A6 A9 33 26 51 31 91 AD E3
4C 2C 80 F9 F6 12 62 2D 5A 77 1F C9 AD 3F 76 E7
            3C A5 B8 09 3D BD B6 CC
```

After permutation

```
DD CB 18 5D E8 F9 EE B3 34 96 5A 42 F1 38 1C 8B
AD C2 2B A1 F8 EE 4C 0E 4D AA F7 A8 8E 7F 42 DD
B8 14 8F 3B F8 D3 B8 D7 4F 09 81 55 A3 7C B4 CB
27 87 6B 85 DA 60 2E 5C 78 9C 10 E0 3B E7 34 07
BA B8 C4 92 13 F8 C7 4E 12 66 CE 9B 11 28 6E 67
4C A9 C1 0C 9C 99 55 04 9A 66 E9 05 1D 9A 2B 1F
C9 AF E2 67 98 E9 CE C6 BC C4 0A 6C D3 66 A1 30
85 0F BC 61 74 B2 1B BE 1F 61 8F 61 F1 D8 A6 27
58 C1 53 44 E5 C5 B8 7D 31 2E CF 50 70 F0 D5 AF
DF 50 7E BF 87 FA 2E D7 30 92 81 BA 4A A0 31 E3
89 40 56 0C 97 4E C7 A6 A9 33 26 51 31 91 AD E3
4C 2C 80 F9 F6 12 62 2D 5A 77 1F C9 AD 3F 76 E7
            3C A5 B8 09 3D BD B6 CC
```

State (as lanes of integers)

```
[0, 0] = b3eef9e85d18cbdd
[1, 0] = 8b1c38f1425a9634
[2, 0] = 0e4ceef8a12bc2ad
[3, 0] = dd427f8ea8f7aa4d
[4, 0] = d7b8d3f83b8f14b8
[0, 1] = cbb47ca35581094f
[1, 1] = 5c2e60da856b8727
[2, 1] = 0734e73be0109c78
```

```
[3, 1] = 4ec7f81392c4b8ba
[4, 1] = 676e28119bce6612
[0, 2] = 0455999c0cc1a94c
[1, 2] = 1f2b9a1d05e9669a
[2, 2] = c6cee99867e2afc9
[3, 2] = 30a166d36c0ac4bc
[4, 2] = be1bb27461bc0f85
[0, 3] = 27a6d8f1618f611f
[1, 3] = 7db8c5e54453c158
[2, 3] = afd5f07050cf2e31
[3, 3] = d72efa87bf7e50df
[4, 3] = e331a04aba819230
[0, 4] = a6c74e970c564089
[1, 4] = e3ad9131512633a9
[2, 4] = 2d6212f6f9802c4c
[3, 4] = e7763fadc91f775a
[4, 4] = ccb6bd3d09b8a53c
```

The hash value is

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

Bibliography

[1] U.S. Department of Commerce/National Institute of Standards and Technology, Secure Hash Standard (SHS), Federal Information Processing Standards Publication (FIPS PUB) 180-4, March 2012

[2] FEDERAL AGENCY ON TECHNICAL REGULATION AND METROLOGY. *Information technology — Cryptographic data security — Hash-function, National Standard of the Russian Federation GOST R 34.11-2012*. Standartinform, Moscow, 2012

[3] BARRETO P.S.L.M., RIJMEN V. The WHIRLPOOL Hashing Function, First open NESSIE Workshop, Leuven, 13–14 November 2000

[4] BERTONI G., DAEMEN J., PEETERS M., VAN ASSCHE G. Cryptographic sponge functions, January 2011, http://sponge.noekeon.org/CSF-0.1.pdf

[5] BERTONI G., DAEMEN J., PEETERS M., VAN ASSCHE G. The KECCAK reference, Version 3.0, January 2011, http://keccak.noekeon.org/Keccak-reference-3.0.pdf

[6] BOSSELAERS D.H., PRENEEL B. The new cryptographic hash-function RIPEMD-160, Dr. *Dobbs*. 1997 January, **22** (1) pp. 24–28

[7] SM3 CRYPOGRAPHIC HASH ALGORITHM. http://www.oscca.gov.cn/UpFile/20101222141857786.pdf, December 2010

[8] SM3 HASH-FUNCTION. Submitted to Internet Engineering Task Force (IETF). http://tools.ietf.org/html/draft-shen-sm3-hash-00, October 2011

[9] ISO/IEC 10118-1:2016, *Information technology — Security techniques — Hash-functions — Part 1: General*

ICS 35.030

Price based on 313 pages