ARCHIVED PUBLICATION

The attached publication,

FIPS Publication 180-2 (with Change Notice 1)
(change notice dated February 25, 2004),

was superseded on October 17, 2008 and is provided here only for historical purposes.

For the most current revision of this publication, see:
http://csrc.nist.gov/publications/PubsFIPS.html#fips180-4.

Federal Information
Processing Standards Publication 180-2
(+ Change Notice to include SHA-224)

2002 August 1

Announcing the

SECURE HASH STANDARD

Federal Information Processing Standards Publications (FIPS PUBS) are issued by the National Institute of Standards and Technology (NIST) after approval by the Secretary of Commerce pursuant to Section 5131 of the Information Technology Management Reform Act of 1996 (Public Law 104-106), and the Computer Security Act of 1987 (Public Law 100-235).

1. Name of Standard: Secure Hash Signature Standard (SHS) (FIPS PUB 180-2).

2. Category of Standard: Computer Security Standard, Cryptography.

3. Explanation: This Standard specifies four secure hash algorithms - SHA-1, SHA-256, SHA-384, and SHA-512 - for computing a condensed representation of electronic data (message). When a message of any length $< 2^{64}$ bits (for SHA-1 and SHA-256) or $< 2^{128}$ bits (for SHA-384 and SHA-512) is input to an algorithm, the result is an output called a message digest. The message digests range in length from 160 to 512 bits, depending on the algorithm. Secure hash algorithms are typically used with other cryptographic algorithms, such as digital signature algorithms and keyed-hash message authentication codes, or in the generation of random numbers (bits).

The four hash algorithms specified in this standard are called secure because, for a given algorithm, it is computationally infeasible 1) to find a message that corresponds to a given message digest, or 2) to find two different messages that produce the same message digest. Any change to a message will, with a very high probability, result in a different message digest. This will result in a verification failure when the secure hash algorithm is used with a digital signature algorithm or a keyed-hash message authentication algorithm.

This standard supersedes FIPS 180-1, adding three algorithms that are capable of producing larger message digests. The SHA-1 algorithm specified herein is the same algorithm that was specified previously in FIPS 180-1, although some of the notation has been modified to be consistent with the notation used in the SHA-256, SHA-384, and SHA-512 algorithms.

4. Approving Authority: Secretary of Commerce.

5. Maintenance Agency: U.S. Department of Commerce, National Institute of Standards and Technology (NIST), Information Technology Laboratory (ITL).

6. Applicability: This standard is applicable to all Federal departments and agencies for the protection of sensitive unclassified information that is not subject to section 2315 of Title 10, United States Code, or section 3502(2) of Title 44, United States Code. This standard shall be implemented whenever a secure hash algorithm is required for Federal applications, including use by other cryptographic algorithms and protocols. The adoption and use of this standard is available to private and commercial organizations.

7. Specifications: Federal Information Processing Standard (FIPS) 180-2, Secure Hash Standard (SHS) (affixed).

8. Implementations: The secure hash algorithms specified herein may be implemented in software, firmware, hardware or any combination thereof. Only algorithm implementations that are validated by NIST will be considered as complying with this standard. Information about the planned validation program can be obtained at http://csrc.nist.gov/cryptval/ or from the National Institute of Standards and Technology, Information Technology Laboratory, Attn: SHS Validation, 100 Bureau Drive Stop 8930, Gaithersburg, MD 20899-8930.

9. Implementation Schedule: This standard becomes effective on February 1, 2003.

10. Patents: Implementations of the secure hash algorithms in this standard may be covered by U.S. or foreign patents.

11. Export Control: Certain cryptographic devices and technical data regarding them are subject to Federal export controls. Exports of cryptographic modules implementing this standard and technical data regarding them must comply with these Federal regulations and be licensed by the Bureau of Export Administration of the U.S. Department of Commerce. Applicable Federal government export controls are specified in Title 15, Code of Federal Regulations (CFR) Part 740.17; Title 15, CFR Part 742; and Title 15, CFR Part 774, Category 5, Part 2.

12. Qualifications: While it is the intent of this standard to specify general security requirements for generating a message digest, conformance to this standard does not assure that a particular implementation is secure. The responsible authority in each agency or department shall assure that an overall implementation provides an acceptable level of security. This standard will be reviewed every five years in order to assess its adequacy.

13. Waiver Procedure. Under certain exceptional circumstances, the heads of Federal agencies, or their delegates, may approve waivers to Federal Information Processing Standards (FIPS). The heads of such agencies may redelegate such authority only to a senior official designated pursuant to Section 3506(b) of Title 44, U.S. Code. Waivers shall be granted only when compliance with this standard would

a. adversely affect the accomplishment of the mission of an operator of a Federal computer system or
b. cause a major adverse financial impact on the operator that is not offset by government-wide savings.

Agency heads may act upon a written waiver request containing the information detailed above. Agency heads may also act without a written waiver request when they determine that conditions for meeting the standard cannot be met. Agency heads may approve waivers only by a written decision that explains the basis on which the agency head made the required finding(s). A copy of each such decision, with procurement sensitive or classified portions clearly identified, shall be sent to: National Institute of Standards and Technology; ATTN: FIPS Waiver Decision, Information Technology Laboratory, 100 Bureau Drive, Stop 8900, Gaithersburg, MD 20899-8900.

In addition, a notice of each waiver granted and each delegation of authority to approve waivers shall be sent promptly to the Committee on Government Operations of the House of Representatives and the Committee on Government Affairs of the Senate and shall be published promptly in the Federal Register.

When the determination on a waiver applies to the procurement of equipment and/or services, a notice of the waiver determination must be published in the Commerce Business Daily as a part of the notice of solicitation for offers of an acquisition or, if the waiver determination is made after that notice is published, by amendment to such notice.

A copy of the waiver, any supporting documents, the document approving the waiver and any supporting and accompanying documents, with such deletions as the agency is authorized and decides to make under Section 552(b) of Title 5, U.S. Code, shall be part of the procurement documentation and retained by the agency.

14. Where to Obtain Copies of the Standard: This publication is available electronically by accessing http://csrc.nist.gov/publications/. A list of other available computer security publications, including ordering information, can be obtained from NIST Publications List 91, which is available at the same web site. Alternatively, copies of NIST computer security publications are available from: National Technical Information Service (NTIS), 5285 Port Royal Road, Springfield, VA 22161.

Federal Information
Processing Standards Publication 180-2

2002 August 1

Specifications for the

SECURE HASH STANDARD

Table Of Contents

1. INTRODUCTION

This standard specifies four secure hash algorithms, SHA-1[1], SHA-256, SHA-384, and SHA-512. All four of the algorithms are iterative, one-way hash functions that can process a message to produce a condensed representation called a *message digest*. These algorithms enable the determination of a message's integrity: any change to the message will, with a very high probability, result in a different message digest. This property is useful in the generation and verification of digital signatures and message authentication codes, and in the generation of random numbers (bits).

Each algorithm can be described in two stages: preprocessing and hash computation. Preprocessing involves padding a message, parsing the padded message into *m*-bit blocks, and setting initialization values to be used in the hash computation. The hash computation generates a *message schedule* from the padded message and uses that schedule, along with functions, constants, and word operations to iteratively generate a series of hash values. The final hash value generated by the hash computation is used to determine the message digest.

The four algorithms differ most significantly in the number of bits of security that are provided for the data being hashed – this is directly related to the message digest length. When a secure hash algorithm is used in conjunction with another algorithm, there may be requirements specified elsewhere that require the use of a secure hash algorithm with a certain number of bits of security. For example, if a message is being signed with a digital signature algorithm that provides 128 bits of security, then that signature algorithm may require the use of a secure hash algorithm that also provides 128 bits of security (e.g., SHA-256).

Additionally, the four algorithms differ in terms of the size of the blocks and words of data that are used during hashing. Figure 1 presents the basic properties of all four secure hash algorithms.

					Security[2] (bits)
-					80
-					128
-					192
-					256

Figure 1: Secure Hash Algorithm Properties

[1] The SHA-1 algorithm specified in this document is identical to the SHA-1 algorithm specified in FIPS 180-1 [180-1]. However, this specification, FIPS 180-2, uses $ROTL^n(X)$ instead of $S^n(X)$ [180-1] to denote "circular left shift by *n* bits" (i.e., "left rotation by *n* bits"). This is described in Sec. 3.2. Some other notational changes have been made in order to be consistent with the specifications for SHA-256, SHA-384, and SHA-512.

[2] In this context, "security" refers to the fact that a birthday attack [HAC] on a message digest of size *n* produces a collision with a workfactor of approximately $2^{n/2}$.

2. DEFINITIONS

2.1 Glossary of Terms and Acronyms

Bit	A binary digit having a value of 0 or 1.
Byte	A group of eight bits.
FIPS	Federal Information Processing Standard.
Word	A group of either 32 bits (4 bytes) or 64 bits (8 bytes), depending on the secure hash algorithm.

2.2 Algorithm Parameters, Symbols, and Terms

2.2.1 Parameters

The following parameters are used in the secure hash algorithm specifications in this standard.

$a, b, c, \ldots, h$	Working variables that are the w-bit words used in the computation of the hash values, $H^{(i)}$.
$H^{(i)}$	The i^{th} hash value. $H^{(0)}$ is the *initial* hash value; $H^{(N)}$ is the *final* hash value and is used to determine the message digest.
$H_j^{(i)}$	The j^{th} word of the i^{th} hash value, where $H_0^{(i)}$ is the left-most word of hash value i.
K_t	Constant value to be used for iteration t of the hash computation.
k	Number of zeroes appended to a message during the padding step.
ℓ	Length of the message, M, in bits.
m	Number of bits in a message block, $M^{(i)}$.
M	Message to be hashed.
$M^{(i)}$	Message block i, with a size of m bits.
$M_j^{(i)}$	The j^{th} word of the i^{th} message block, where $M_0^{(i)}$ is the left-most word of message block i.

n	Number of bits to be rotated or shifted when a word is operated upon.
N	Number of blocks in the padded message.
T	Temporary w-bit word used in the hash computation.
w	Number of bits in a word.
W_t	The t^{th} w-bit word of the message schedule.

2.2.2 Symbols

The following symbols are used in the secure hash algorithm specifications, and each operates on w-bit words.

$\wedge$	Bitwise AND operation.
$\vee$	Bitwise OR ("inclusive-OR") operation.
$\oplus$	Bitwise XOR ("exclusive-OR") operation.
$\neg$	Bitwise complement operation.
+	Addition modulo 2^w.
<<	Left-shift operation, where $x << n$ is obtained by discarding the left-most n bits of the word x and then padding the result with n zeroes on the right.
>>	Right-shift operation, where $x >> n$ is obtained by discarding the right-most n bits of the word x and then padding the result with n zeroes on the left.

3. NOTATION AND CONVENTIONS

3.1 Bit Strings and Integers

The following terminology related to bit strings and integers will be used.

1. A *hex digit* is an element of the set {`0, 1,…, 9, a,…, f`}. A hex digit is the representation of a 4-bit string. For example, the hex digit "`7`" represents the 4-bit string "`0111`", and the hex digit "`a`" represents the 4-bit string "`1010`".

2. A *word* is a *w*-bit string that may be represented as a sequence of hex digits. To convert a word to hex digits, each 4-bit string is converted to its hex digit equivalent, as described in (1) above. For example, the 32-bit string

   ```
   1010 0001 0000 0011 1111 1110 0010 0011
   ```

   can be expressed as "`a103fe23`", and the 64-bit string

   ```
   1010 0001 0000 0011 1111 1110 0010 0011
   0011 0010 1110 1111 0011 0000 0001 1010
   ```

   can be expressed as "`a103fe2332ef301a`".

   Throughout this specification, the "big-endian" convention is used when expressing both 32- and 64-bit words, so that within each word, the most significant bit is stored in the left-most bit position.

3. An *integer* may be represented as a word or pair of words. A word representation of the message length, ℓ, in bits, is required for the padding techniques of Sec. 5.1.

   An integer between 0 and 2^{32}-1 *inclusive* may be represented as a 32-bit word. The least significant four bits of the integer are represented by the right-most hex digit of the word representation. For example, the integer $291=2^8 + 2^5 + 2^1 + 2^0=256+32+2+1$ is represented by the hex word `00000123`.

   The same holds true for an integer between 0 and 2^{64}-1 *inclusive*, which may be represented as a 64-bit word.

   If Z is an integer, $0 \le Z < 2^{64}$, then $Z=2^{32}X + Y$, where $0 \le X < 2^{32}$ and $0 \le Y < 2^{32}$. Since X and Y can be represented as 32-bit words x and y, respectively, the integer Z can be represented as the pair of words (x, y). This property is used for SHA-1 and SHA-256.

If Z is an integer, $0 \le Z < 2^{128}$, then $Z=2^{64}X + Y$, where $0 \le X < 2^{64}$ and $0 \le Y < 2^{64}$. Since X and Y can be represented as 64-bit words x and y, respectively, the integer Z can be represented as the pair of words (x, y). This property is used for SHA-384 and SHA-512.

4. For the secure hash algorithms, the size of the *message block* - m bits - depends on the algorithm.

   a) For **SHA-1** and **SHA-256**, each message block has **512 bits**, which are represented as a sequence of sixteen **32-bit words**.

   b) For **SHA-384** and **SHA-512**, each message block has **1024 bits**, which are represented as a sequence of sixteen **64-bit words**.

3.2 Operations on Words

The following operations are applied to w-bit words in all four secure hash algorithms. SHA-1 and SHA-256 operate on 32-bit words (w=32), and SHA-384 and SHA-512 operate on 64-bit words (w=64).

1. Bitwise *logical* word operations: $\wedge$, $\vee$, $\oplus$, and (see Sec. 2.2.2).

2. Addition modulo 2^w.

   The operation $x + y$ is defined as follows. The words x and y represent integers X and Y, where $0 \le X < 2^w$ and $0 \le Y < 2^w$. For positive integers U and V, let $U \bmod V$ be the remainder upon dividing U by V. Compute

   $$Z=(X + Y) \bmod 2^w.$$

   Then $0 \le Z < 2^w$. Convert the integer Z to a word, z, and define $z=x + y$.

3. The *right shift* operation $\boldsymbol{SHR^n(x)}$, where x is a w-bit word and n is an integer with $0 \le n < w$, is defined by

   $$SHR^n(x)=x >> n.$$

   This operation is used in the SHA-256, SHA-384, and SHA-512 algorithms.

4. The *rotate right* (circular right shift) operation $\boldsymbol{ROTR^n(x)}$, where x is a w-bit word and n is an integer with $0 \le n < w$, is defined by

   $$ROTR^n(x)=(x >> n) \vee (x << w - n).$$

   Thus, $ROTR^n(x)$ is equivalent to a circular shift (rotation) of x by n positions to the right.

This operation is used by the SHA-256, SHA-384, and SHA-512 algorithms.

5. The *rotate left* (circular left shift) operation, $\boldsymbol{ROTL^n(x)}$, where x is a w-bit word and n is an integer with $0 \leq n < w$, is defined by

   $$ROTL^n(x)=(x << n) \vee (x >> w - n).$$

   Thus, $ROTL^n(x)$ is equivalent to a circular shift (rotation) of x by n positions to the left.

   This operation is used only in the SHA-1 algorithm. Note that in Ref. [180-1] this operation was referred to as "$S^n(X)$"; however, the notation has been modified for clarity and consistency with the notation used for operations in the other secure hash algorithms.

6. Note the following equivalence relationships, where w is fixed in each relationship:

   $$ROTL^n(x) \approx ROTR^{w-n}(x)$$

   $$ROTR^n(x) \approx ROTL^{w-n}(x).$$

4. FUNCTIONS AND CONSTANTS

4.1 Functions

This section defines the functions that are used by each of the algorithms. Although the SHA-256, SHA-384, and SHA-512 algorithms all use similar functions, their descriptions are separated into sections for SHA-256 (Sec. 4.1.2) and for SHA-384 and SHA-512 (Sec. 4.1.3), since the input and output for these functions are words of different sizes. Each of the algorithms include $Ch(x, y, z)$ and $Maj(x, y, z)$ functions; the exclusive-OR operation ($\oplus$) in these functions may be replaced by a bitwise OR operation ($\vee$) and produce identical results.

4.1.1 SHA-1 Functions

SHA-1 uses a sequence of logical functions, $f_0, f_1, \ldots, f_{79}$. Each function f_t, where $0 \le t < 79$, operates on three 32-bit words, x, y, and z, and produces a 32-bit word as output. The function $f_t(x, y, z)$ is defined as follows:

$$f_t(x, y, z) = \begin{cases} Ch(x, y, z)=(x \wedge y) \oplus (\ \ x \wedge z) & 0 \le t \le 19 \\ Parity(x, y, z)=x \oplus y \oplus z & 20 \le t \le 39 \\ Maj(x, y, z)=(x \wedge y) \oplus (x \wedge z) \oplus (y \wedge z) & 40 \le t \le 59 \\ Parity(x, y, z)=x \oplus y \oplus z & 60 \le t \le 79. \end{cases} \quad (4.1)$$

4.1.2 SHA-256 Functions

SHA-256 uses six logical functions, where *each function operates on 32-bit words*, which are represented as x, y, and z. The result of each function is a new 32-bit word.

$$Ch(x, y, z) = (x \wedge y) \oplus (\ \ x \wedge z) \quad (4.2)$$

$$Maj(x, y, z) = (x \wedge y) \oplus (x \wedge z) \oplus (y \wedge z) \quad (4.3)$$

$$\sum_0^{\{256\}}(x) = ROTR^2(x) \oplus ROTR^{13}(x) \oplus ROTR^{22}(x) \quad (4.4)$$

$$\sum_1^{\{256\}}(x) = ROTR^6(x) \oplus ROTR^{11}(x) \oplus ROTR^{25}(x) \quad (4.5)$$

$$s_0^{\{256\}}(x) = ROTR^7(x) \oplus ROTR^{18}(x) \oplus SHR^3(x) \quad (4.6)$$

$$s_1^{\{256\}}(x) = ROTR^{17}(x) \oplus ROTR^{19}(x) \oplus SHR^{10}(x) \quad (4.7)$$

4.1.3 SHA-384 and SHA-512 Functions

SHA-384 and SHA-512 each use six logical functions, where *each function operates on 64-bit words*, which are represented as x, y, and z. The result of each function is a new 64-bit word.

$$Ch(x,y,z) = (x \wedge y) \oplus (\ x \wedge z) \quad (4.8)$$

$$Maj(x,y,z) = (x \wedge y) \oplus (x \wedge z) \oplus (y \wedge z) \quad (4.9)$$

$$\sum_0^{\{512\}}(x) = ROTR^{28}(x) \oplus ROTR^{34}(x) \oplus ROTR^{39}(x) \quad (4.10)$$

$$\sum_1^{\{512\}}(x) = ROTR^{14}(x) \oplus ROTR^{18}(x) \oplus ROTR^{41}(x) \quad (4.11)$$

$$s_0^{\{512\}}(x) = ROTR^{1}(x) \oplus ROTR^{8}(x) \oplus SHR^{7}(x) \quad (4.12)$$

$$s_1^{\{512\}}(x) = ROTR^{19}(x) \oplus ROTR^{61}(x) \oplus SHR^{6}(x) \quad (4.13)$$

4.2 Constants

4.2.1 SHA-1 Constants

SHA-1 uses a sequence of eighty constant 32-bit words, K_0, K_1,…, K_{79}, which are given by

$$K_t = \begin{cases} \texttt{5a827999} & 0 \le t \le 19 \\ \texttt{6ed9eba1} & 20 \le t \le 39 \\ \texttt{8f1bbcdc} & 40 \le t \le 59 \\ \texttt{ca62c1d6} & 60 \le t \le 79. \end{cases} \quad (4.14)$$

4.2.2 SHA-256 Constants

SHA-256 uses a sequence of sixty-four constant 32-bit words, $K_0^{\{256\}}, K_1^{\{256\}}, \ldots, K_{63}^{\{256\}}$. These words represent the first thirty-two bits of the fractional parts of the cube roots of the first sixty-four prime numbers. In hex, these constant words are (from left to right)

```
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.
```

4.2.3 SHA-384 and SHA-512 Constants

SHA-384 and SHA-512 use the same sequence of eighty constant 64-bit words, $K_0^{\{512\}}, K_1^{\{512\}}, \ldots, K_{79}^{\{512\}}$. These words represent the first sixty-four bits of the fractional parts of the cube roots of the first eighty prime numbers. In hex, these constant words are (from left to right)

```
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.
```

5. PREPROCESSING

Preprocessing shall take place before hash computation begins. This preprocessing consists of three steps: padding the message, *M* (Sec. 5.1), parsing the padded message into message blocks (Sec. 5.2), and setting the initial hash value, $H^{(0)}$ (Sec. 5.3).

5.1 Padding the Message

The message, *M*, shall be padded before hash computation begins. The purpose of this padding is to ensure that the padded message is a multiple of 512 or 1024 bits, depending on the algorithm.

5.1.1 SHA-1 and SHA-256

Suppose that the length of the message, *M*, is ℓ bits. Append the bit "**1**" to the end of the message, followed by *k* zero bits, where *k* is the smallest, non-negative solution to the equation $\ell + 1 + k \equiv 448 \bmod 512$. Then append the 64-bit block that is equal to the number ℓ expressed using a binary representation. For example, the (8-bit ASCII) message "**abc**" has length $8 \times 3 = 24$, so the message is padded with a one bit, then $448 - (24 + 1) = 423$ zero bits, and then the message length, to become the 512-bit padded message

$$\underbrace{\texttt{01100001}}_{\text{“a”}}\ \underbrace{\texttt{01100010}}_{\text{“b”}}\ \underbrace{\texttt{01100011}}_{\text{“c”}}\ \texttt{1}\ \overbrace{\texttt{00…00}}^{423}\ \overbrace{\texttt{00…011000}}^{64}.$$

The length of the padded message should now be a multiple of 512 bits.

5.1.2 SHA-384 and SHA-512

Suppose the length of the message *M*, in bits, is ℓ bits. Append the bit "**1**" to the end of the message, followed by *k* zero bits, where *k* is the smallest non-negative solution to the equation $\ell + 1 + k \equiv 896 \bmod 1024$. Then append the 128-bit block that is equal to the number ℓ expressed using a binary representation. For example, the (8-bit ASCII) message "**abc**" has length $8 \times 3 = 24$, so the message is padded with a one bit, then $896 - (24 + 1) = 871$ zero bits, and then the message length, to become the 1024-bit padded message

$$\underbrace{\texttt{01100001}}_{\text{“a”}}\ \underbrace{\texttt{01100010}}_{\text{“b”}}\ \underbrace{\texttt{01100011}}_{\text{“c”}}\ \texttt{1}\ \overbrace{\texttt{00…00}}^{871}\ \overbrace{\texttt{00…011000}}^{128}.$$

The length of the padded message should now be a multiple of 1024 bits.

5.2 Parsing the Padded Message

After a message has been padded, it must be parsed into N m-bit blocks before the hash computation can begin.

5.2.1 SHA-1 and SHA-256

For SHA-1 and SHA-256, the padded message is parsed into N 512-bit blocks, $M^{(1)}$, $M^{(2)}$,…, $M^{(N)}$. Since the 512 bits of the input block may be expressed as sixteen 32-bit words, the first 32 bits of message block i are denoted $M_0^{(i)}$, the next 32 bits are $M_1^{(i)}$, and so on up to $M_{15}^{(i)}$.

5.2.2 SHA-384 and SHA-512

For SHA-384 and SHA-512, the padded message is parsed into N 1024-bit blocks, $M^{(1)}$, $M^{(2)}$,…, $M^{(N)}$. Since the 1024 bits of the input block may be expressed as sixteen 64-bit words, the first 64 bits of message block i are denoted $M_0^{(i)}$, the next 64 bits are $M_1^{(i)}$, and so on up to $M_{15}^{(i)}$.

5.3 Setting the Initial Hash Value ($H^{(0)}$)

Before hash computation begins for each of the secure hash algorithms, the initial hash value, $H^{(0)}$, must be set. The size and number of words in $H^{(0)}$ depends on the message digest size.

5.3.1 SHA-1

For SHA-1, the initial hash value, $H^{(0)}$, shall consist of the following five 32-bit words, in hex:

$$H_0^{(0)} = \texttt{67452301}$$
$$H_1^{(0)} = \texttt{efcdab89}$$
$$H_2^{(0)} = \texttt{98badcfe}$$
$$H_3^{(0)} = \texttt{10325476}$$
$$H_4^{(0)} = \texttt{c3d2e1f0}.$$

5.3.2 SHA-256

For SHA-256, the initial hash value, $H^{(0)}$, shall consist of the following eight 32-bit words, in hex:

$$H_0^{(0)} = \texttt{6a09e667}$$
$$H_1^{(0)} = \texttt{bb67ae85}$$
$$H_2^{(0)} = \texttt{3c6ef372}$$
$$H_3^{(0)} = \texttt{a54ff53a}$$
$$H_4^{(0)} = \texttt{510e527f}$$
$$H_5^{(0)} = \texttt{9b05688c}$$
$$H_6^{(0)} = \texttt{1f83d9ab}$$
$$H_7^{(0)} = \texttt{5be0cd19}.$$

These words were obtained by taking the first thirty-two bits of the fractional parts of the square roots of the first eight prime numbers.

5.3.3 SHA-384

For SHA-384, the initial hash value, $H^{(0)}$, shall consist of the following eight 64-bit words, in hex:

$$H_0^{(0)} = \texttt{cbbb9d5dc1059ed8}$$
$$H_1^{(0)} = \texttt{629a292a367cd507}$$
$$H_2^{(0)} = \texttt{9159015a3070dd17}$$
$$H_3^{(0)} = \texttt{152fecd8f70e5939}$$
$$H_4^{(0)} = \texttt{67332667ffc00b31}$$
$$H_5^{(0)} = \texttt{8eb44a8768581511}$$
$$H_6^{(0)} = \texttt{db0c2e0d64f98fa7}$$
$$H_7^{(0)} = \texttt{47b5481dbefa4fa4}.$$

These words were obtained by taking the first sixty-four bits of the fractional parts of the square roots of the ninth through sixteenth prime numbers.

5.3.4 SHA-512

For SHA-512, the initial hash value, $H^{(0)}$, shall consist of the following eight 64-bit words, in hex:

$$H_0^{(0)} = \texttt{6a09e667f3bcc908}$$
$$H_1^{(0)} = \texttt{bb67ae8584caa73b}$$
$$H_2^{(0)} = \texttt{3c6ef372fe94f82b}$$
$$H_3^{(0)} = \texttt{a54ff53a5f1d36f1}$$
$$H_4^{(0)} = \texttt{510e527fade682d1}$$
$$H_5^{(0)} = \texttt{9b05688c2b3e6c1f}$$
$$H_6^{(0)} = \texttt{1f83d9abfb41bd6b}$$
$$H_7^{(0)} = \texttt{5be0cd19137e2179}.$$

These words were obtained by taking the first sixty-four bits of the fractional parts of the square roots of the first eight prime numbers.

6. SECURE HASH ALGORITHMS

In the following sections, SHA-512 is described before SHA-384. That is because the SHA-384 algorithm is identical to SHA-512, with the exception of using a different initial hash value and truncating the final hash value to 384 bits.

For each of the secure hash algorithms, there may exist alternate computation methods that yield identical results; one example is the alternative SHA-1 computation described in Sec. 6.1.3. Such alternate methods may be implemented in conformance to this standard.

6.1 SHA-1

SHA-1 may be used to hash a message, M, having a length of ℓ bits, where $0 \le \ell < 2^{64}$. The algorithm uses 1) a message schedule of eighty 32-bit words, 2) five working variables of 32 bits each, and 3) a hash value of five 32-bit words. The final result of SHA-1 is a 160-bit message digest.

The words of the message schedule are labeled W_0, W_1,…, W_{79}. The five working variables are labeled ***a***, ***b***, ***c***, ***d***, and ***e***. The words of the hash value are labeled $H_0^{(i)}, H_1^{(i)}, \ldots, H_4^{(i)}$, which will hold the initial hash value, $H^{(0)}$, replaced by each successive intermediate hash value (after each message block is processed), $H^{(i)}$, and ending with the final hash value, $H^{(N)}$. SHA-1 also uses a single temporary word, T.

Appendix A gives several detailed examples of SHA-1.

6.1.1 SHA-1 Preprocessing

1. Pad the message, M, according to Sec. 5.1.1;

2. Parse the padded message into N 512-bit message blocks, $M^{(1)}$, $M^{(2)}$, …, $M^{(N)}$, according to Sec. 5.2.1; and

3. Set the initial hash value, $H^{(0)}$, as specified in Sec. 5.3.1.

6.1.2 SHA-1 Hash Computation

The SHA-1 hash computation uses functions and constants previously defined in Sec. 4.1.1 and Sec. 4.2.1, respectively. Addition (+) is performed modulo 2^{32}.

After preprocessing is completed, each message block, $M^{(1)}$, $M^{(2)}$, …, $M^{(N)}$, is processed in order, using the following steps:

For i=1 to N:
{

1. Prepare the message schedule, $\{W_t\}$:

$$W_t = \begin{cases} M_t^{(i)} & 0 \le t \le 15 \\ ROTL^1(W_{t-3} \oplus W_{t-8} \oplus W_{t-14} \oplus W_{t-16}) & 16 \le t \le 79 \end{cases}$$

2. Initialize the five working variables, ***a***, ***b***, ***c***, ***d***, and ***e***, with the $(i\text{-}1)^{st}$ hash value:

$$a = H_0^{(i-1)}$$
$$b = H_1^{(i-1)}$$
$$c = H_2^{(i-1)}$$
$$d = H_3^{(i-1)}$$
$$e = H_4^{(i-1)}$$

3. For t=0 to 79:
   {
   $$T = ROTL^5(a) + f_t(b,c,d) + e + K_t + W_t$$
   $$e = d$$
   $$d = c$$
   $$c = ROTL^{30}(b)$$
   $$b = a$$
   $$a = T$$
   }

4. Compute the i^{th} intermediate hash value $H^{(i)}$:

$$H_0^{(i)} = a + H_0^{(i-1)}$$
$$H_1^{(i)} = b + H_1^{(i-1)}$$
$$H_2^{(i)} = c + H_2^{(i-1)}$$
$$H_3^{(i)} = d + H_3^{(i-1)}$$
$$H_4^{(i)} = e + H_4^{(i-1)}$$

}

After repeating steps one through four a total of N times (i.e., after processing $M^{(N)}$), the resulting 160-bit message digest of the message, M, is

$$H_0^{(N)} \| H_1^{(N)} \| H_2^{(N)} \| H_3^{(N)} \| H_4^{(N)}.$$

6.1.3 Alternate Method for Computing a SHA-1 Message Digest

The SHA-1 hash computation method described in Sec. 6.1.2 assumes that the message schedule W_0, W_1,…, W_{79} is implemented as an array of eighty 32-bit words. This is efficient from the standpoint of the minimization of execution time, since the addresses of W_{t-3},…, W_{t-16} in step (2) of Sec. 6.1.2 are easily computed.

However, if memory is limited, an alternative is to regard $\{W_t\}$ as a circular queue that may be implemented using an array of sixteen 32-bit words, W_0, W_1,…, W_{15}. The alternate method that is described in this section yields the same message digest as the SHA-1 computation method described in Sec. 6.1.2. Although this alternate method saves sixty-four 32-bit words of storage, it is likely to lengthen the execution time due to the increased complexity of the address computations for the $\{W_t\}$ in step (3).

For this alternate SHA-1 method, let *MASK*=`0000000f` (in hex). As in Sec. 6.1.1, addition is performed modulo 2^{32}. Assuming that the preprocessing as described in Sec. 6.1.1 has been performed, the processing of $M^{(i)}$ is as follows:

For i=1 to N:
{

1. For t=0 to 15:
   {
   $$W_t = M_t^{(i)}$$
   }

2. Initialize the five working variables, ***a***, ***b***, ***c***, ***d***, and ***e***, with the (i-1)st hash value:

   $$a = H_0^{(i-1)}$$
   $$b = H_1^{(i-1)}$$
   $$c = H_2^{(i-1)}$$
   $$d = H_3^{(i-1)}$$
   $$e = H_4^{(i-1)}$$

3. For t=0 to 79:
   {
   $$s = t \wedge MASK$$

   If $t \geq 16$ then
   {
   $$W_s = ROTL^1(W_{(s+13)\wedge MASK} \oplus W_{(s+8)\wedge MASK} \oplus W_{(s+2)\wedge MASK} \oplus W_s)$$
   }

$$T = ROTL^5(a) + f_t(b,c,d) + e + K_t + W_s$$
$$e = d$$
$$d = c$$
$$c = ROTL^{30}(b)$$
$$b = a$$
$$a = T$$

}

4. Compute the i^{th} intermediate hash value $H^{(i)}$:

$$H_0^{(i)} = a + H_0^{(i-1)}$$
$$H_1^{(i)} = b + H_1^{(i-1)}$$
$$H_2^{(i)} = c + H_2^{(i-1)}$$
$$H_3^{(i)} = d + H_3^{(i-1)}$$
$$H_4^{(i)} = e + H_4^{(i-1)}$$

}

After repeating steps one through four a total of N times (i.e., after processing $M^{(N)}$), the resulting 160-bit message digest of the message, M, is

$$H_0^{(N)} \| H_1^{(N)} \| H_2^{(N)} \| H_3^{(N)} \| H_4^{(N)}.$$

6.2 SHA-256

SHA-256 may be used to hash a message, M, having a length of ℓ bits, where $0 \le \ell < 2^{64}$. The algorithm uses 1) a message schedule of sixty-four 32-bit words, 2) eight working variables of 32 bits each, and 3) a hash value of eight 32-bit words. The final result of SHA-256 is a 256-bit message digest.

The words of the message schedule are labeled W_0, W_1,…, W_{63}. The eight working variables are labeled ***a***, ***b***, ***c***, ***d***, ***e***, ***f***, ***g***, and ***h***. The words of the hash value are labeled $H_0^{(i)}, H_1^{(i)}, \ldots, H_7^{(i)}$, which will hold the initial hash value, $H^{(0)}$, replaced by each successive intermediate hash value (after each message block is processed), $H^{(i)}$, and ending with the final hash value, $H^{(N)}$. SHA-256 also uses two temporary words, T_1 and T_2.

Appendix B gives several detailed examples of SHA-256.

6.2.1 SHA-256 Preprocessing

1. Pad the message, M, according to Sec. 5.1.1;

2. Parse the padded message into N 512-bit message blocks, $M^{(1)}$, $M^{(2)}$, …, $M^{(N)}$, according to Sec. 5.2.1; and

3. Set the initial hash value, $H^{(0)}$, as specified in Sec. 5.3.2.

6.2.2 SHA-256 Hash Computation

The SHA-256 hash computation uses functions and constants previously defined in Sec. 4.1.2 and Sec. 4.2.2, respectively. Addition (+) is performed modulo 2^{32}.

After preprocessing is completed, each message block, $M^{(1)}$, $M^{(2)}$, …, $M^{(N)}$, is processed in order, using the following steps:

For i=1 to N:
{

1. Prepare the message schedule, $\{W_t\}$:

$$W_t = \begin{cases} M_t^{(i)} & 0 \le t \le 15 \\ s_1^{\{256\}}(W_{t-2}) + W_{t-7} + s_0^{\{256\}}(W_{t-15}) + W_{t-16} & 16 \le t \le 63 \end{cases}$$

2. Initialize the eight working variables, $\boldsymbol{a}$, $\boldsymbol{b}$, $\boldsymbol{c}$, $\boldsymbol{d}$, $\boldsymbol{e}$, $\boldsymbol{f}$, $\boldsymbol{g}$, and $\boldsymbol{h}$, with the (i-1)st hash value:

$$a = H_0^{(i-1)}$$
$$b = H_1^{(i-1)}$$
$$c = H_2^{(i-1)}$$
$$d = H_3^{(i-1)}$$
$$e = H_4^{(i-1)}$$
$$f = H_5^{(i-1)}$$
$$g = H_6^{(i-1)}$$
$$h = H_7^{(i-1)}$$

3. For t=0 to 63:
{

$$T_1 = h + \sum_1^{\{256\}}(e) + Ch(e, f, g) + K_t^{\{256\}} + W_t$$
$$T_2 = \sum_0^{\{256\}}(a) + Maj(a, b, c)$$
$$h = g$$
$$g = f$$
$$f = e$$
$$e = d + T_1$$
$$d = c$$
$$c = b$$
$$b = a$$
$$a = T_1 + T_2$$

}

4. Compute the i^{th} intermediate hash value $H^{(i)}$:

$$H_0^{(i)} = a + H_0^{(i-1)}$$
$$H_1^{(i)} = b + H_1^{(i-1)}$$
$$H_2^{(i)} = c + H_2^{(i-1)}$$
$$H_3^{(i)} = d + H_3^{(i-1)}$$
$$H_4^{(i)} = e + H_4^{(i-1)}$$
$$H_5^{(i)} = f + H_5^{(i-1)}$$
$$H_6^{(i)} = g + H_6^{(i-1)}$$
$$H_7^{(i)} = h + H_7^{(i-1)}$$

}

After repeating steps one through four a total of N times (i.e., after processing $M^{(N)}$), the resulting 256-bit message digest of the message, M, is

$$H_0^{(N)} \| H_1^{(N)} \| H_2^{(N)} \| H_3^{(N)} \| H_4^{(N)} \| H_5^{(N)} \| H_6^{(N)} \| H_7^{(N)} .$$

6.3 SHA-512

SHA-512 may be used to hash a message, M, having a length of ℓ bits, where $0 \le \ell < 2^{128}$. The algorithm uses 1) a message schedule of eighty 64-bit words, 2) eight working variables of 64 bits each, and 3) a hash value of eight 64-bit words. The final result of SHA-512 is a 512-bit message digest.

The words of the message schedule are labeled W_0, W_1,…, W_{79}. The eight working variables are labeled ***a***, ***b***, ***c***, ***d***, ***e***, ***f***, ***g***, and ***h***. The words of the hash value are labeled $H_0^{(i)}, H_1^{(i)}, \ldots, H_7^{(i)}$, which will hold the initial hash value, $H^{(0)}$, replaced by each successive intermediate hash value

(after each message block is processed), $H^{(i)}$, and ending with the final hash value, $H^{(N)}$. SHA-512 also uses two temporary words, T_1 and T_2.

Appendix C gives several detailed examples of SHA-512.

6.3.1 SHA-512 Preprocessing

1. Pad the message, M, according to Sec. 5.1.2;

2. Parse the padded message into N 1024-bit message blocks, $M^{(1)}$, $M^{(2)}$, …, $M^{(N)}$, according to Sec. 5.2.2; and

3. Set the initial hash value, $H^{(0)}$, as specified in Sec. 5.3.4.

6.3.2 SHA-512 Hash Computation

The SHA-512 hash computation uses functions and constants previously defined in Sec. 4.1.3 and Sec. 4.2.3, respectively. Addition (+) is performed modulo 2^{64}.

After preprocessing is completed, each message block, $M^{(1)}$, $M^{(2)}$, …, $M^{(N)}$, is processed in order, using the following steps:

For i=1 to N:
{

1. Prepare the message schedule, $\{W_t\}$:

$$W_t = \begin{cases} M_t^{(i)} & 0 \le t \le 15 \\ s_1^{\{512\}}(W_{t-2}) + W_{t-7} + s_0^{\{512\}}(W_{t-15}) + W_{t-16} & 16 \le t \le 79 \end{cases}$$

2. Initialize the eight working variables, ***a***, ***b***, ***c***, ***d***, ***e***, ***f***, ***g***, and ***h***, with the (i-1)st hash value:

$$a = H_0^{(i-1)}$$
$$b = H_1^{(i-1)}$$
$$c = H_2^{(i-1)}$$
$$d = H_3^{(i-1)}$$
$$e = H_4^{(i-1)}$$
$$f = H_5^{(i-1)}$$
$$g = H_6^{(i-1)}$$
$$h = H_7^{(i-1)}$$

3. For t=0 to 79:

{

$T_1 = h + \sum_1^{\{512\}}(e) + Ch(e, f, g) + K_t^{\{512\}} + W_t$

$T_2 = \sum_0^{\{512\}}(a) + Maj(a, b, c)$

$h = g$

$g = f$

$f = e$

$e = d + T_1$

$d = c$

$c = b$

$b = a$

$a = T_1 + T_2$

}

4. Compute the i^{th} intermediate hash value $H^{(i)}$:

$H_0^{(i)} = a + H_0^{(i-1)}$

$H_1^{(i)} = b + H_1^{(i-1)}$

$H_2^{(i)} = c + H_2^{(i-1)}$

$H_3^{(i)} = d + H_3^{(i-1)}$

$H_4^{(i)} = e + H_4^{(i-1)}$

$H_5^{(i)} = f + H_5^{(i-1)}$

$H_6^{(i)} = g + H_6^{(i-1)}$

$H_7^{(i)} = h + H_7^{(i-1)}$

}

After repeating steps one through four a total of N times (i.e., after processing $M^{(N)}$), the resulting 512-bit message digest of the message, M, is

$$H_0^{(N)} \| H_1^{(N)} \| H_2^{(N)} \| H_3^{(N)} \| H_4^{(N)} \| H_5^{(N)} \| H_6^{(N)} \| H_7^{(N)} .$$

6.4 SHA-384

SHA-384 may be used to hash a message, M, having a length of ℓ bits, where $0 \le \ell < 2^{128}$. The algorithm is defined in the exact same manner as SHA-512 (Sec. 6.3), with the following two exceptions:

1. The initial hash value, $H^{(0)}$, shall be set as specified in Sec. 5.3.3; and

2. The 384-bit message digest is obtained by truncating the final hash value, $H^{(N)}$, to its left-most 384 bits:

$$H_0^{(N)} \| H_1^{(N)} \| H_2^{(N)} \| H_3^{(N)} \| H_4^{(N)} \| H_5^{(N)} .$$

Appendix D gives several detailed examples of SHA-384.

APPENDIX A: SHA-1 EXAMPLES

This appendix is for informational purposes only and is not required to meet the standard.

A.1 SHA-1 Example (One-Block Message)

Let the message, M, be the 24-bit ($\ell = 24$) ASCII string "**abc**", which is equivalent to the following binary string:

`01100001 01100010 01100011`.

The message is padded by appending a "`1`" bit, followed by 423 "`0`" bits, and ending with the hex value `00000000 00000018` (the two 32-bit word representation of the length, 24). Thus, the final padded message consists of one block (N=1).

For SHA-1, the initial hash value, $H^{(0)}$, is

$H_0^{(0)}$ = `67452301`
$H_1^{(0)}$ = `efcdab89`
$H_2^{(0)}$ = `98badcfe`
$H_3^{(0)}$ = `10325476`
$H_4^{(0)}$ = `c3d2e1f0`.

The words of the padded message block are then assigned to the words $W_0,\ldots,W_{15}$ of the message schedule:

W_0 = `61626380`
W_1 = `00000000`
W_2 = `00000000`
W_3 = `00000000`
W_4 = `00000000`
W_5 = `00000000`
W_6 = `00000000`
W_7 = `00000000`
W_8 = `00000000`
W_9 = `00000000`
W_{10} = `00000000`
W_{11} = `00000000`
W_{12} = `00000000`
W_{13} = `00000000`
W_{14} = `00000000`
W_{15} = `00000018`.

The following schedule shows the hex values for ***a***, ***b***, ***c***, ***d***, and ***e*** *after* pass t of the "for t=0 to 79" loop described in Sec. 6.1.2, step 4.

	a	***b***	***c***	***d***	***e***
t = 0 :	`0116fc33`	`67452301`	`7bf36ae2`	`98badcfe`	`10325476`
t = 1 :	`8990536d`	`0116fc33`	`59d148c0`	`7bf36ae2`	`98badcfe`
t = 2 :	`a1390f08`	`8990536d`	`c045bf0c`	`59d148c0`	`7bf36ae2`

$t = 3$:	cdd8e11b	a1390f08	626414db	c045bf0c	59d148c0
$t = 4$:	cfd499de	cdd8e11b	284e43c2	626414db	c045bf0c
$t = 5$:	3fc7ca40	cfd499de	f3763846	284e43c2	626414db
$t = 6$:	993e30c1	3fc7ca40	b3f52677	f3763846	284e43c2
$t = 7$:	9e8c07d4	993e30c1	0ff1f290	b3f52677	f3763846
$t = 8$:	4b6ae328	9e8c07d4	664f8c30	0ff1f290	b3f52677
$t = 9$:	8351f929	4b6ae328	27a301f5	664f8c30	0ff1f290
$t = 10$:	fbda9e89	8351f929	12dab8ca	27a301f5	664f8c30
$t = 11$:	63188fe4	fbda9e89	60d47e4a	12dab8ca	27a301f5
$t = 12$:	4607b664	63188fe4	7ef6a7a2	60d47e4a	12dab8ca
$t = 13$:	9128f695	4607b664	18c623f9	7ef6a7a2	60d47e4a
$t = 14$:	196bee77	9128f695	1181ed99	18c623f9	7ef6a7a2
$t = 15$:	20bdd62f	196bee77	644a3da5	1181ed99	18c623f9
$t = 16$:	4e925823	20bdd62f	c65afb9d	644a3da5	1181ed99
$t = 17$:	82aa6728	4e925823	c82f758b	c65afb9d	644a3da5
$t = 18$:	dc64901d	82aa6728	d3a49608	c82f758b	c65afb9d
$t = 19$:	fd9e1d7d	dc64901d	20aa99ca	d3a49608	c82f758b
$t = 20$:	1a37b0ca	fd9e1d7d	77192407	20aa99ca	d3a49608
$t = 21$:	33a23bfc	1a37b0ca	7f67875f	77192407	20aa99ca
$t = 22$:	21283486	33a23bfc	868dec32	7f67875f	77192407
$t = 23$:	d541f12d	21283486	0ce88eff	868dec32	7f67875f
$t = 24$:	c7567dc6	d541f12d	884a0d21	0ce88eff	868dec32
$t = 25$:	48413ba4	c7567dc6	75507c4b	884a0d21	0ce88eff
$t = 26$:	be35fbd5	48413ba4	b1d59f71	75507c4b	884a0d21
$t = 27$:	4aa84d97	be35fbd5	12104ee9	b1d59f71	75507c4b
$t = 28$:	8370b52e	4aa84d97	6f8d7ef5	12104ee9	b1d59f71
$t = 29$:	c5fbaf5d	8370b52e	d2aa1365	6f8d7ef5	12104ee9
$t = 30$:	1267b407	c5fbaf5d	a0dc2d4b	d2aa1365	6f8d7ef5
$t = 31$:	3b845d33	1267b407	717eebd7	a0dc2d4b	d2aa1365
$t = 32$:	046faa0a	3b845d33	c499ed01	717eebd7	a0dc2d4b
$t = 33$:	2c0ebc11	046faa0a	cee1174c	c499ed01	717eebd7
$t = 34$:	21796ad4	2c0ebc11	811bea82	cee1174c	c499ed01
$t = 35$:	dcbbb0cb	21796ad4	4b03af04	811bea82	cee1174c
$t = 36$:	0f511fd8	dcbbb0cb	085e5ab5	4b03af04	811bea82
$t = 37$:	dc63973f	0f511fd8	f72eec32	085e5ab5	4b03af04
$t = 38$:	4c986405	dc63973f	03d447f6	f72eec32	085e5ab5
$t = 39$:	32de1cba	4c986405	f718e5cf	03d447f6	f72eec32
$t = 40$:	fc87dedf	32de1cba	53261901	f718e5cf	03d447f6
$t = 41$:	970a0d5c	fc87dedf	8cb7872e	53261901	f718e5cf
$t = 42$:	7f193dc5	970a0d5c	ff21f7b7	8cb7872e	53261901
$t = 43$:	ee1b1aaf	7f193dc5	25c28357	ff21f7b7	8cb7872e
$t = 44$:	40f28e09	ee1b1aaf	5fc64f71	25c28357	ff21f7b7
$t = 45$:	1c51e1f2	40f28e09	fb86c6ab	5fc64f71	25c28357
$t = 46$:	a01b846c	1c51e1f2	503ca382	fb86c6ab	5fc64f71
$t = 47$:	bead02ca	a01b846c	8714787c	503ca382	fb86c6ab
$t = 48$:	baf39337	bead02ca	2806e11b	8714787c	503ca382
$t = 49$:	120731c5	baf39337	afab40b2	2806e11b	8714787c
$t = 50$:	641db2ce	120731c5	eebce4cd	afab40b2	2806e11b
$t = 51$:	3847ad66	641db2ce	4481cc71	eebce4cd	afab40b2
$t = 52$:	e490436d	3847ad66	99076cb3	4481cc71	eebce4cd
$t = 53$:	27e9f1d8	e490436d	8e11eb59	99076cb3	4481cc71
$t = 54$:	7b71f76d	27e9f1d8	792410db	8e11eb59	99076cb3
$t = 55$:	5e6456af	7b71f76d	09fa7c76	792410db	8e11eb59
$t = 56$:	c846093f	5e6456af	5edc7ddb	09fa7c76	792410db
$t = 57$:	d262ff50	c846093f	d79915ab	5edc7ddb	09fa7c76
$t = 58$:	09d785fd	d262ff50	f211824f	d79915ab	5edc7ddb

t = 59 :	3f52de5a	09d785fd	3498bfd4	f211824f	d79915ab
t = 60 :	d756c147	3f52de5a	4275e17f	3498bfd4	f211824f
t = 61 :	548c9cb2	d756c147	8fd4b796	4275e17f	3498bfd4
t = 62 :	b66c020b	548c9cb2	f5d5b051	8fd4b796	4275e17f
t = 63 :	6b61c9e1	b66c020b	9523272c	f5d5b051	8fd4b796
t = 64 :	19dfa7ac	6b61c9e1	ed9b0082	9523272c	f5d5b051
t = 65 :	101655f9	19dfa7ac	5ad87278	ed9b0082	9523272c
t = 66 :	0c3df2b4	101655f9	0677e9eb	5ad87278	ed9b0082
t = 67 :	78dd4d2b	0c3df2b4	4405957e	0677e9eb	5ad87278
t = 68 :	497093c0	78dd4d2b	030f7cad	4405957e	0677e9eb
t = 69 :	3f2588c2	497093c0	de37534a	030f7cad	4405957e
t = 70 :	c199f8c7	3f2588c2	125c24f0	de37534a	030f7cad
t = 71 :	39859de7	c199f8c7	8fc96230	125c24f0	de37534a
t = 72 :	edb42de4	39859de7	f0667e31	8fc96230	125c24f0
t = 73 :	11793f6f	edb42de4	ce616779	f0667e31	8fc96230
t = 74 :	5ee76897	11793f6f	3b6d0b79	ce616779	f0667e31
t = 75 :	63f7dab7	5ee76897	c45e4fdb	3b6d0b79	ce616779
t = 76 :	a079b7d9	63f7dab7	d7b9da25	c45e4fdb	3b6d0b79
t = 77 :	860d21cc	a079b7d9	d8fdf6ad	d7b9da25	c45e4fdb
t = 78 :	5738d5e1	860d21cc	681e6df6	d8fdf6ad	d7b9da25
t = 79 :	42541b35	5738d5e1	21834873	681e6df6	d8fdf6ad

That completes the processing of the first and only message block, $M^{(1)}$. The final hash value, $H^{(1)}$, is calculated to be

$$H_0^{(1)} = \texttt{67452301} + \texttt{42541b35} = \texttt{a9993e36}$$
$$H_1^{(1)} = \texttt{efcdab89} + \texttt{5738d5e1} = \texttt{4706816a}$$
$$H_2^{(1)} = \texttt{98badcfe} + \texttt{21834873} = \texttt{ba3e2571}$$
$$H_3^{(1)} = \texttt{10325476} + \texttt{681e6df6} = \texttt{7850c26c}$$
$$H_4^{(1)} = \texttt{c3d2e1f0} + \texttt{d8fdf6ad} = \texttt{9cd0d89d}.$$

The resulting 160-bit message digest is

```
a9993e36 4706816a ba3e2571 7850c26c 9cd0d89d.
```

A.2 SHA-1 Example (Multi-Block Message)

Let the message, *M*, be the 448-bit (ℓ = 448) ASCII string

"**abcdbcdecdefdefgefghfghighijhijkijkljklmklmnlmnomnopnopq**".

The message is padded by appending a "`1`" bit, followed by 511 "`0`" bits, and ending with the hex value `00000000 000001c0` (the two 32-bit word representation of the length, 448). Thus, the final padded message consists of two blocks (*N*=2).

For SHA-1, the initial hash value, $H^{(0)}$, is

$H_0^{(0)}$ = 67452301
$H_1^{(0)}$ = efcdab89
$H_2^{(0)}$ = 98badcfe
$H_3^{(0)}$ = 10325476
$H_4^{(0)}$ = c3d2e1f0.

The words of the first padded message block, $M^{(1)}$, are then assigned to the words $W_0,\ldots,W_{15}$ of the message schedule:

W_0 = 61626364
W_1 = 62636465
W_2 = 63646566
W_3 = 64656667
W_4 = 65666768
W_5 = 66676869
W_6 = 6768696a
W_7 = 68696a6b
W_8 = 696a6b6c
W_9 = 6a6b6c6d
W_{10} = 6b6c6d6e
W_{11} = 6c6d6e6f
W_{12} = 6d6e6f70
W_{13} = 6e6f7071
W_{14} = 80000000
W_{15} = 00000000.

The following schedule shows the hex values for ***a***, ***b***, ***c***, ***d***, and ***e*** *after* pass t of the "for t=0 to 79" loop described in Sec. 6.1.2, step 4.

	a	***b***	***c***	***d***	***e***
t = 0 :	0116fc17	67452301	7bf36ae2	98badcfe	10325476
t = 1 :	ebf3b452	0116fc17	59d148c0	7bf36ae2	98badcfe
t = 2 :	5109913a	ebf3b452	c045bf05	59d148c0	7bf36ae2
t = 3 :	2c4f6eac	5109913a	bafced14	c045bf05	59d148c0
t = 4 :	33f4ae5b	2c4f6eac	9442644e	bafced14	c045bf05
t = 5 :	96b85189	33f4ae5b	0b13dbab	9442644e	bafced14
t = 6 :	db04cb58	96b85189	ccfd2b96	0b13dbab	9442644e
t = 7 :	45833f0f	db04cb58	65ae1462	ccfd2b96	0b13dbab
t = 8 :	c565c35e	45833f0f	36c132d6	65ae1462	ccfd2b96
t = 9 :	6350afda	c565c35e	d160cfc3	36c132d6	65ae1462
t = 10 :	8993ea77	6350afda	b15970d7	d160cfc3	36c132d6
t = 11 :	e19ecaa2	8993ea77	98d42bf6	b15970d7	d160cfc3
t = 12 :	8603481e	e19ecaa2	e264fa9d	98d42bf6	b15970d7
t = 13 :	32f94a85	8603481e	b867b2a8	e264fa9d	98d42bf6
t = 14 :	b2e7a8be	32f94a85	a180d207	b867b2a8	e264fa9d
t = 15 :	42637e39	b2e7a8be	4cbe52a1	a180d207	b867b2a8
t = 16 :	6b068048	42637e39	acb9ea2f	4cbe52a1	a180d207
t = 17 :	426b9c35	6b068048	5098df8e	acb9ea2f	4cbe52a1
t = 18 :	944b1bd1	426b9c35	1ac1a012	5098df8e	acb9ea2f
t = 19 :	6c445652	944b1bd1	509ae70d	1ac1a012	5098df8e
t = 20 :	95836da5	6c445652	6512c6f4	509ae70d	1ac1a012
t = 21 :	09511177	95836da5	9b111594	6512c6f4	509ae70d
t = 22 :	e2b92dc4	09511177	6560db69	9b111594	6512c6f4
t = 23 :	fd224575	e2b92dc4	c254445d	6560db69	9b111594
t = 24 :	eeb82d9a	fd224575	38ae4b71	c254445d	6560db69
t = 25 :	5a142c1a	eeb82d9a	7f48915d	38ae4b71	c254445d

$t = 26$:	2972f7c7	5a142c1a	bbae0b66	7f48915d	38ae4b71
$t = 27$:	d526a644	2972f7c7	96850b06	bbae0b66	7f48915d
$t = 28$:	e1122421	d526a644	ca5cbdf1	96850b06	bbae0b66
$t = 29$:	05b457b2	e1122421	3549a991	ca5cbdf1	96850b06
$t = 30$:	a9c84bec	05b457b2	78448908	3549a991	ca5cbdf1
$t = 31$:	52e31f60	a9c84bec	816d15ec	78448908	3549a991
$t = 32$:	5af3242c	52e31f60	2a7212fb	816d15ec	78448908
$t = 33$:	31c756a9	5af3242c	14b8c7d8	2a7212fb	816d15ec
$t = 34$:	e9ac987c	31c756a9	16bcc90b	14b8c7d8	2a7212fb
$t = 35$:	ab7c32ee	e9ac987c	4c71d5aa	16bcc90b	14b8c7d8
$t = 36$:	5933fc99	ab7c32ee	3a6b261f	4c71d5aa	16bcc90b
$t = 37$:	43f87ae9	5933fc99	aadf0cbb	3a6b261f	4c71d5aa
$t = 38$:	24957f22	43f87ae9	564cff26	aadf0cbb	3a6b261f
$t = 39$:	adeb7478	24957f22	50fe1eba	564cff26	aadf0cbb
$t = 40$:	d70e5010	adeb7478	89255fc8	50fe1eba	564cff26
$t = 41$:	79bcfb08	d70e5010	2b7add1e	89255fc8	50fe1eba
$t = 42$:	f9bcb8de	79bcfb08	35c39404	2b7add1e	89255fc8
$t = 43$:	633e9561	f9bcb8de	1e6f3ec2	35c39404	2b7add1e
$t = 44$:	98c1ea64	633e9561	be6f2e37	1e6f3ec2	35c39404
$t = 45$:	c6ea241e	98c1ea64	58cfa558	be6f2e37	1e6f3ec2
$t = 46$:	a2ad4f02	c6ea241e	26307a99	58cfa558	be6f2e37
$t = 47$:	c8a69090	a2ad4f02	b1ba8907	26307a99	58cfa558
$t = 48$:	88341600	c8a69090	a8ab53c0	b1ba8907	26307a99
$t = 49$:	7e846f58	88341600	3229a424	a8ab53c0	b1ba8907
$t = 50$:	86e358ba	7e846f58	220d0580	3229a424	a8ab53c0
$t = 51$:	8d2e76c8	86e358ba	1fa11bd6	220d0580	3229a424
$t = 52$:	ce892e10	8d2e76c8	a1b8d62e	1fa11bd6	220d0580
$t = 53$:	edea95b1	ce892e10	234b9db2	a1b8d62e	1fa11bd6
$t = 54$:	36d1230a	edea95b1	33a24b84	234b9db2	a1b8d62e
$t = 55$:	776c3910	36d1230a	7b7aa56c	33a24b84	234b9db2
$t = 56$:	a681b723	776c3910	8db448c2	7b7aa56c	33a24b84
$t = 57$:	ac0a794f	a681b723	1ddb0e44	8db448c2	7b7aa56c
$t = 58$:	f03d3782	ac0a794f	e9a06dc8	1ddb0e44	8db448c2
$t = 59$:	9ef775c3	f03d3782	eb029e53	e9a06dc8	1ddb0e44
$t = 60$:	36254b13	9ef775c3	bc0f4de0	eb029e53	e9a06dc8
$t = 61$:	4080d4dc	36254b13	e7bddd70	bc0f4de0	eb029e53
$t = 62$:	2bfaf7a8	4080d4dc	cd8952c4	e7bddd70	bc0f4de0
$t = 63$:	513f9ca0	2bfaf7a8	10203537	cd8952c4	e7bddd70
$t = 64$:	e5895c81	513f9ca0	0afebdea	10203537	cd8952c4
$t = 65$:	1037d2d5	e5895c81	144fe728	0afebdea	10203537
$t = 66$:	14a82da9	1037d2d5	79625720	144fe728	0afebdea
$t = 67$:	6d17c9fd	14a82da9	440df4b5	79625720	144fe728
$t = 68$:	2c7b07bd	6d17c9fd	452a0b6a	440df4b5	79625720
$t = 69$:	fdf6efff	2c7b07bd	5b45f27f	452a0b6a	440df4b5
$t = 70$:	112b96e3	fdf6efff	4b1ec1ef	5b45f27f	452a0b6a
$t = 71$:	84065712	112b96e3	ff7dbbff	4b1ec1ef	5b45f27f
$t = 72$:	ab89fb71	84065712	c44ae5b8	ff7dbbff	4b1ec1ef
$t = 73$:	c5210e35	ab89fb71	a10195c4	c44ae5b8	ff7dbbff
$t = 74$:	352d9f4b	c5210e35	6ae27edc	a10195c4	c44ae5b8
$t = 75$:	1a0e0e0a	352d9f4b	7148438d	6ae27edc	a10195c4
$t = 76$:	d0d47349	1a0e0e0a	cd4b67d2	7148438d	6ae27edc
$t = 77$:	ad38620d	d0d47349	86838382	cd4b67d2	7148438d
$t = 78$:	d3ad7c25	ad38620d	74351cd2	86838382	cd4b67d2
$t = 79$:	8ce34517	d3ad7c25	6b4e1883	74351cd2	86838382

That completes the processing of the first message block, $M^{(1)}$. The first intermediate hash value, $H^{(1)}$, is calculated to be

$$H_0^{(1)} = \texttt{67452301} + \texttt{8ce34517} = \texttt{f4286818}$$
$$H_1^{(1)} = \texttt{efcdab89} + \texttt{d3ad7c25} = \texttt{c37b27ae}$$
$$H_2^{(1)} = \texttt{98badcfe} + \texttt{6b4e1883} = \texttt{0408f581}$$
$$H_3^{(1)} = \texttt{10325476} + \texttt{74351cd2} = \texttt{84677148}$$
$$H_4^{(1)} = \texttt{c3d2e1f0} + \texttt{86838382} = \texttt{4a566572}.$$

The words of the *second* padded message block, $M^{(2)}$, are then assigned to the words $W_0,\ldots,W_{15}$ of the message schedule:

W_0 = 00000000
W_1 = 00000000
W_2 = 00000000
W_3 = 00000000
W_4 = 00000000
W_5 = 00000000
W_6 = 00000000
W_7 = 00000000
W_8 = 00000000
W_9 = 00000000
W_{10} = 00000000
W_{11} = 00000000
W_{12} = 00000000
W_{13} = 00000000
W_{14} = 00000000
W_{15} = 000001c0.

The following schedule shows the hex values for ***a***, ***b***, ***c***, ***d***, and ***e*** *after* pass t of the "for t=0 to 79" loop described in Sec. 6.1.2, step 4.

	a	***b***	***c***	***d***	***e***
t = 0:	2df257e9	f4286818	b0dec9eb	0408f581	84677148
t = 1:	4d3dc58f	2df257e9	3d0a1a06	b0dec9eb	0408f581
t = 2:	c352bb05	4d3dc58f	4b7c95fa	3d0a1a06	b0dec9eb
t = 3:	eef743c6	c352bb05	d34f7163	4b7c95fa	3d0a1a06
t = 4:	41e34277	eef743c6	70d4aec1	d34f7163	4b7c95fa
t = 5:	5443915c	41e34277	bbbdd0f1	70d4aec1	d34f7163
t = 6:	e7fa0377	5443915c	d078d09d	bbbdd0f1	70d4aec1
t = 7:	c6946813	e7fa0377	1510e457	d078d09d	bbbdd0f1
t = 8:	fdde1de1	c6946813	f9fe80dd	1510e457	d078d09d
t = 9:	b8538aca	fdde1de1	f1a51a04	f9fe80dd	1510e457
t = 10:	6ba94f63	b8538aca	7f778778	f1a51a04	f9fe80dd
t = 11:	43a2792f	6ba94f63	ae14e2b2	7f778778	f1a51a04
t = 12:	fecd7bbf	43a2792f	daea53d8	ae14e2b2	7f778778
t = 13:	a2604ca8	fecd7bbf	d0e89e4b	daea53d8	ae14e2b2
t = 14:	258b0baa	a2604ca8	ffb35eef	d0e89e4b	daea53d8
t = 15:	d9772360	258b0baa	2898132a	ffb35eef	d0e89e4b
t = 16:	5507db6e	d9772360	8962c2ea	2898132a	ffb35eef
t = 17:	a51b58bc	5507db6e	365dc8d8	8962c2ea	2898132a
t = 18:	c2eb709f	a51b58bc	9541f6db	365dc8d8	8962c2ea
t = 19:	d8992153	c2eb709f	2946d62f	9541f6db	365dc8d8
t = 20:	37482f5f	d8992153	f0badc27	2946d62f	9541f6db
t = 21:	ee8700bd	37482f5f	f6264854	f0badc27	2946d62f

$t = 22$:	9ad594b9	ee8700bd	cdd20bd7	f6264854	f0badc27
$t = 23$:	8fbaa5b9	9ad594b9	7ba1c02f	cdd20bd7	f6264854
$t = 24$:	88fb5867	8fbaa5b9	66b5652e	7ba1c02f	cdd20bd7
$t = 25$:	eec50521	88fb5867	63eea96e	66b5652e	7ba1c02f
$t = 26$:	50bce434	eec50521	e23ed619	63eea96e	66b5652e
$t = 27$:	5c416daf	50bce434	7bb14148	e23ed619	63eea96e
$t = 28$:	2429be5f	5c416daf	142f390d	7bb14148	e23ed619
$t = 29$:	0a2fb108	2429be5f	d7105b6b	142f390d	7bb14148
$t = 30$:	17986223	0a2fb108	c90a6f97	d7105b6b	142f390d
$t = 31$:	8a4af384	17986223	028bec42	c90a6f97	d7105b6b
$t = 32$:	6b629993	8a4af384	c5e61888	028bec42	c90a6f97
$t = 33$:	f15f04f3	6b629993	2292bce1	c5e61888	028bec42
$t = 34$:	295cc25b	f15f04f3	dad8a664	2292bce1	c5e61888
$t = 35$:	696da404	295cc25b	fc57c13c	dad8a664	2292bce1
$t = 36$:	cef5ae12	696da404	ca573096	fc57c13c	dad8a664
$t = 37$:	87d5b80c	cef5ae12	1a5b6901	ca573096	fc57c13c
$t = 38$:	84e2a5f2	87d5b80c	b3bd6b84	1a5b6901	ca573096
$t = 39$:	03bb6310	84e2a5f2	21f56e03	b3bd6b84	1a5b6901
$t = 40$:	c2d8f75f	03bb6310	a138a97c	21f56e03	b3bd6b84
$t = 41$:	bfb25768	c2d8f75f	00eed8c4	a138a97c	21f56e03
$t = 42$:	28589152	bfb25768	f0b63dd7	00eed8c4	a138a97c
$t = 43$:	ec1d3d61	28589152	2fec95da	f0b63dd7	00eed8c4
$t = 44$:	3caed7af	ec1d3d61	8a162454	2fec95da	f0b63dd7
$t = 45$:	c3d033ea	3caed7af	7b074f58	8a162454	2fec95da
$t = 46$:	7316056a	c3d033ea	cf2bb5eb	7b074f58	8a162454
$t = 47$:	46f93b68	7316056a	b0f40cfa	cf2bb5eb	7b074f58
$t = 48$:	dc8e7f26	46f93b68	9cc5815a	b0f40cfa	cf2bb5eb
$t = 49$:	850d411c	dc8e7f26	11be4eda	9cc5815a	b0f40cfa
$t = 50$:	7e4672c0	850d411c	b7239fc9	11be4eda	9cc5815a
$t = 51$:	89fbd41d	7e4672c0	21435047	b7239fc9	11be4eda
$t = 52$:	1797e228	89fbd41d	1f919cb0	21435047	b7239fc9
$t = 53$:	431d65bc	1797e228	627ef507	1f919cb0	21435047
$t = 54$:	2bdbb8cb	431d65bc	05e5f88a	627ef507	1f919cb0
$t = 55$:	6da72e7f	2bdbb8cb	10c7596f	05e5f88a	627ef507
$t = 56$:	a8495a9b	6da72e7f	caf6ee32	10c7596f	05e5f88a
$t = 57$:	e785655a	a8495a9b	db69cb9f	caf6ee32	10c7596f
$t = 58$:	5b086c42	e785655a	ea1256a6	db69cb9f	caf6ee32
$t = 59$:	a65818f7	5b086c42	b9e15956	ea1256a6	db69cb9f
$t = 60$:	7aab101b	a65818f7	96c21b10	b9e15956	ea1256a6
$t = 61$:	93614c9c	7aab101b	e996063d	96c21b10	b9e15956
$t = 62$:	f66d9bf4	93614c9c	deaac406	e996063d	96c21b10
$t = 63$:	d504902b	f66d9bf4	24d85327	deaac406	e996063d
$t = 64$:	60a9da62	d504902b	3d9b66fd	24d85327	deaac406
$t = 65$:	8b687819	60a9da62	f541240a	3d9b66fd	24d85327
$t = 66$:	083e90c3	8b687819	982a7698	f541240a	3d9b66fd
$t = 67$:	f6226bbf	083e90c3	62da1e06	982a7698	f541240a
$t = 68$:	76c0563b	f6226bbf	c20fa430	62da1e06	982a7698
$t = 69$:	989dd165	76c0563b	fd889aef	c20fa430	62da1e06
$t = 70$:	8b2c7573	989dd165	ddb0158e	fd889aef	c20fa430
$t = 71$:	ae1b8e7b	8b2c7573	66277459	ddb0158e	fd889aef
$t = 72$:	ca1840de	ae1b8e7b	e2cb1d5c	66277459	ddb0158e
$t = 73$:	16f3babb	ca1840de	eb86e39e	e2cb1d5c	66277459
$t = 74$:	d28d83ad	16f3babb	b2861037	eb86e39e	e2cb1d5c
$t = 75$:	6bc02dfe	d28d83ad	c5bceeae	b2861037	eb86e39e
$t = 76$:	d3a6e275	6bc02dfe	74a360eb	c5bceeae	b2861037
$t = 77$:	da955482	d3a6e275	9af00b7f	74a360eb	c5bceeae

$t = 78$:	58c0aac0	da955482	74e9b89d	9af00b7f	74a360eb
$t = 79$:	906fd62c	58c0aac0	b6a55520	74e9b89d	9af00b7f

That completes the processing of the second and final message block, $M^{(2)}$. The final hash value, $H^{(2)}$, is calculated to be

$$H_0^{(1)} = \texttt{f4286818} + \texttt{906fd62c} = \texttt{84983e44}$$
$$H_1^{(1)} = \texttt{c37b27ae} + \texttt{58c0aac0} = \texttt{1c3bd26e}$$
$$H_2^{(1)} = \texttt{0408f581} + \texttt{b6a55520} = \texttt{baae4aa1}$$
$$H_3^{(1)} = \texttt{84677148} + \texttt{74e9b89d} = \texttt{f95129e5}$$
$$H_4^{(1)} = \texttt{4a566572} + \texttt{9af00b7f} = \texttt{e54670f1}.$$

The resulting 160-bit message digest is

```
84983e44 1c3bd26e baae4aa1 f95129e5 e54670f1.
```

A.3 SHA-1 Example (Long Message)

Let the message M be the binary-coded form of the ASCII string which consists of 1,000,000 repetitions of the character "**a**". The resulting SHA-1 message digest is

```
34aa973c d4c4daa4 f61eeb2b dbad2731 6534016f.
```

APPENDIX B: SHA-256 EXAMPLES

This appendix is for informational purposes only and is not required to meet the standard.

B.1 SHA-256 Example (One-Block Message)

Let the message, *M*, be the 24-bit ($\ell = 24$) ASCII string "**abc**", which is equivalent to the following binary string:

`01100001 01100010 01100011`.

The message is padded by appending a "`1`" bit, followed by 423 "`0`" bits, and ending with the hex value `00000000 00000018` (the two 32-bit word representation of the length, 24). Thus, the final padded message consists of one block (N=1).

For SHA-256, the initial hash value, $H^{(0)}$, is

$H_0^{(0)}$ = `6a09e667`
$H_1^{(0)}$ = `bb67ae85`
$H_2^{(0)}$ = `3c6ef372`
$H_3^{(0)}$ = `a54ff53a`
$H_4^{(0)}$ = `510e527f`
$H_5^{(0)}$ = `9b05688c`
$H_6^{(0)}$ = `1f83d9ab`
$H_7^{(0)}$ = `5be0cd19`.

The words of the padded message block are then assigned to the words $W_0,\ldots,W_{15}$ of the message schedule:

W_0 = `61626380`
W_1 = `00000000`
W_2 = `00000000`
W_3 = `00000000`
W_4 = `00000000`
W_5 = `00000000`
W_6 = `00000000`
W_7 = `00000000`
W_8 = `00000000`
W_9 = `00000000`
W_{10} = `00000000`
W_{11} = `00000000`
W_{12} = `00000000`
W_{13} = `00000000`
W_{14} = `00000000`
W_{15} = `00000018`.

The following schedule shows the hex values for ***a***, ***b***, ***c***, ***d***, ***e***, ***f***, ***g***, and ***h*** *after* pass t of the "for t=0 to 63" loop described in Sec. 6.2.2, step 4.

	a	*b*	*c*	*d*	*e*	*f*	*g*	*h*
$t = 0$:	5d6aebcd	6a09e667	bb67ae85	3c6ef372	fa2a4622	510e527f	9b05688c	1f83d9ab
$t = 1$:	5a6ad9ad	5d6aebcd	6a09e667	bb67ae85	78ce7989	fa2a4622	510e527f	9b05688c
$t = 2$:	c8c347a7	5a6ad9ad	5d6aebcd	6a09e667	f92939eb	78ce7989	fa2a4622	510e527f
$t = 3$:	d550f666	c8c347a7	5a6ad9ad	5d6aebcd	24e00850	f92939eb	78ce7989	fa2a4622
$t = 4$:	04409a6a	d550f666	c8c347a7	5a6ad9ad	43ada245	24e00850	f92939eb	78ce7989
$t = 5$:	2b4209f5	04409a6a	d550f666	c8c347a7	714260ad	43ada245	24e00850	f92939eb
$t = 6$:	e5030380	2b4209f5	04409a6a	d550f666	9b27a401	714260ad	43ada245	24e00850
$t = 7$:	85a07b5f	e5030380	2b4209f5	04409a6a	0c657a79	9b27a401	714260ad	43ada245
$t = 8$:	8e04ecb9	85a07b5f	e5030380	2b4209f5	32ca2d8c	0c657a79	9b27a401	714260ad
$t = 9$:	8c87346b	8e04ecb9	85a07b5f	e5030380	1cc92596	32ca2d8c	0c657a79	9b27a401
$t = 10$:	4798a3f4	8c87346b	8e04ecb9	85a07b5f	436b23e8	1cc92596	32ca2d8c	0c657a79
$t = 11$:	f71fc5a9	4798a3f4	8c87346b	8e04ecb9	816fd6e9	436b23e8	1cc92596	32ca2d8c
$t = 12$:	87912990	f71fc5a9	4798a3f4	8c87346b	1e578218	816fd6e9	436b23e8	1cc92596
$t = 13$:	d932eb16	87912990	f71fc5a9	4798a3f4	745a48de	1e578218	816fd6e9	436b23e8
$t = 14$:	c0645fde	d932eb16	87912990	f71fc5a9	0b92f20c	745a48de	1e578218	816fd6e9
$t = 15$:	b0fa238e	c0645fde	d932eb16	87912990	07590dcd	0b92f20c	745a48de	1e578218
$t = 16$:	21da9a9b	b0fa238e	c0645fde	d932eb16	8034229c	07590dcd	0b92f20c	745a48de
$t = 17$:	c2fbd9d1	21da9a9b	b0fa238e	c0645fde	846ee454	8034229c	07590dcd	0b92f20c
$t = 18$:	fe777bbf	c2fbd9d1	21da9a9b	b0fa238e	cc899961	846ee454	8034229c	07590dcd
$t = 19$:	e1f20c33	fe777bbf	c2fbd9d1	21da9a9b	b0638179	cc899961	846ee454	8034229c
$t = 20$:	9dc68b63	e1f20c33	fe777bbf	c2fbd9d1	8ada8930	b0638179	cc899961	846ee454
$t = 21$:	c2606d6d	9dc68b63	e1f20c33	fe777bbf	e1257970	8ada8930	b0638179	cc899961
$t = 22$:	a7a3623f	c2606d6d	9dc68b63	e1f20c33	49f5114a	e1257970	8ada8930	b0638179
$t = 23$:	c5d53d8d	a7a3623f	c2606d6d	9dc68b63	aa47c347	49f5114a	e1257970	8ada8930
$t = 24$:	1c2c2838	c5d53d8d	a7a3623f	c2606d6d	2823ef91	aa47c347	49f5114a	e1257970
$t = 25$:	cde8037d	1c2c2838	c5d53d8d	a7a3623f	14383d8e	2823ef91	aa47c347	49f5114a
$t = 26$:	b62ec4bc	cde8037d	1c2c2838	c5d53d8d	c74c6516	14383d8e	2823ef91	aa47c347
$t = 27$:	77d37528	b62ec4bc	cde8037d	1c2c2838	edffbff8	c74c6516	14383d8e	2823ef91
$t = 28$:	363482c9	77d37528	b62ec4bc	cde8037d	6112a3b7	edffbff8	c74c6516	14383d8e
$t = 29$:	a0060b30	363482c9	77d37528	b62ec4bc	ade79437	6112a3b7	edffbff8	c74c6516
$t = 30$:	ea992a22	a0060b30	363482c9	77d37528	0109ab3a	ade79437	6112a3b7	edffbff8
$t = 31$:	73b33bf5	ea992a22	a0060b30	363482c9	ba591112	0109ab3a	ade79437	6112a3b7
$t = 32$:	98e12507	73b33bf5	ea992a22	a0060b30	9cd9f5f6	ba591112	0109ab3a	ade79437
$t = 33$:	fe604df5	98e12507	73b33bf5	ea992a22	59249dd3	9cd9f5f6	ba591112	0109ab3a
$t = 34$:	a9a7738c	fe604df5	98e12507	73b33bf5	085f3833	59249dd3	9cd9f5f6	ba591112
$t = 35$:	65a0cfe4	a9a7738c	fe604df5	98e12507	f4b002d6	085f3833	59249dd3	9cd9f5f6
$t = 36$:	41a65cb1	65a0cfe4	a9a7738c	fe604df5	0772a26b	f4b002d6	085f3833	59249dd3
$t = 37$:	34df1604	41a65cb1	65a0cfe4	a9a7738c	a507a53d	0772a26b	f4b002d6	085f3833
$t = 38$:	6dc57a8a	34df1604	41a65cb1	65a0cfe4	f0781bc8	a507a53d	0772a26b	f4b002d6
$t = 39$:	79ea687a	6dc57a8a	34df1604	41a65cb1	1efbc0a0	f0781bc8	a507a53d	0772a26b
$t = 40$:	d6670766	79ea687a	6dc57a8a	34df1604	26352d63	1efbc0a0	f0781bc8	a507a53d
$t = 41$:	df46652f	d6670766	79ea687a	6dc57a8a	838b2711	26352d63	1efbc0a0	f0781bc8
$t = 42$:	17aa0dfe	df46652f	d6670766	79ea687a	decd4715	838b2711	26352d63	1efbc0a0
$t = 43$:	9d4baf93	17aa0dfe	df46652f	d6670766	fda24c2e	decd4715	838b2711	26352d63
$t = 44$:	26628815	9d4baf93	17aa0dfe	df46652f	a80f11f0	fda24c2e	decd4715	838b2711
$t = 45$:	72ab4b91	26628815	9d4baf93	17aa0dfe	b7755da1	a80f11f0	fda24c2e	decd4715
$t = 46$:	a14c14b0	72ab4b91	26628815	9d4baf93	d57b94a9	b7755da1	a80f11f0	fda24c2e
$t = 47$:	4172328d	a14c14b0	72ab4b91	26628815	fecf0bc6	d57b94a9	b7755da1	a80f11f0
$t = 48$:	05757ceb	4172328d	a14c14b0	72ab4b91	bd714038	fecf0bc6	d57b94a9	b7755da1
$t = 49$:	f11bfaa8	05757ceb	4172328d	a14c14b0	6e5c390c	bd714038	fecf0bc6	d57b94a9
$t = 50$:	7a0508a1	f11bfaa8	05757ceb	4172328d	52f1ccf7	6e5c390c	bd714038	fecf0bc6
$t = 51$:	886e7a22	7a0508a1	f11bfaa8	05757ceb	49231c1e	52f1ccf7	6e5c390c	bd714038

t = 52 :	101fd28f	886e7a22	7a0508a1	f11bfaa8	529e7d00	49231c1e	52f1ccf7	6e5c390c
t = 53 :	f5702fdb	101fd28f	886e7a22	7a0508a1	9f4787c3	529e7d00	49231c1e	52f1ccf7
t = 54 :	3ec45cdb	f5702fdb	101fd28f	886e7a22	e50e1b4f	9f4787c3	529e7d00	49231c1e
t = 55 :	38cc9913	3ec45cdb	f5702fdb	101fd28f	54cb266b	e50e1b4f	9f4787c3	529e7d00
t = 56 :	fcd1887b	38cc9913	3ec45cdb	f5702fdb	9b5e906c	54cb266b	e50e1b4f	9f4787c3
t = 57 :	c062d46f	fcd1887b	38cc9913	3ec45cdb	7e44008e	9b5e906c	54cb266b	e50e1b4f
t = 58 :	ffb70472	c062d46f	fcd1887b	38cc9913	6d83bfc6	7e44008e	9b5e906c	54cb266b
t = 59 :	b6ae8fff	ffb70472	c062d46f	fcd1887b	b21bad3d	6d83bfc6	7e44008e	9b5e906c
t = 60 :	b85e2ce9	b6ae8fff	ffb70472	c062d46f	961f4894	b21bad3d	6d83bfc6	7e44008e
t = 61 :	04d24d6c	b85e2ce9	b6ae8fff	ffb70472	948d25b6	961f4894	b21bad3d	6d83bfc6
t = 62 :	d39a2165	04d24d6c	b85e2ce9	b6ae8fff	fb121210	948d25b6	961f4894	b21bad3d
t = 63 :	506e3058	d39a2165	04d24d6c	b85e2ce9	5ef50f24	fb121210	948d25b6	961f4894

That completes the processing of the first and only message block, $M^{(1)}$. The final hash value, $H^{(1)}$, is calculated to be

$$H_0^{(1)} = \texttt{6a09e667} + \texttt{506e3058} = \texttt{ba7816bf}$$
$$H_1^{(1)} = \texttt{bb67ae85} + \texttt{d39a2165} = \texttt{8f01cfea}$$
$$H_2^{(1)} = \texttt{3c6ef372} + \texttt{04d24d6c} = \texttt{414140de}$$
$$H_3^{(1)} = \texttt{a54ff53a} + \texttt{b85e2ce9} = \texttt{5dae2223}$$
$$H_4^{(1)} = \texttt{510e527f} + \texttt{5ef50f24} = \texttt{b00361a3}$$
$$H_5^{(1)} = \texttt{9b05688c} + \texttt{fb121210} = \texttt{96177a9c}$$
$$H_6^{(1)} = \texttt{1f83d9ab} + \texttt{948d25b6} = \texttt{b410ff61}$$
$$H_7^{(1)} = \texttt{5be0cd19} + \texttt{961f4894} = \texttt{f20015ad.}$$

The resulting 256-bit message digest is

```
ba7816bf 8f01cfea 414140de 5dae2223 b00361a3 96177a9c b410ff61 f20015ad.
```

B.2 SHA-256 Example (Multi-Block Message)

Let the message, *M*, be the 448-bit (ℓ = 448) ASCII string

"**abcdbcdecdefdefgefghfghighijhijkijkljklmklmnlmnomnopnopq**".

The message is padded by appending a "`1`" bit, followed by 511 "`0`" bits, and ending with the hex value `00000000 000001c0` (the two 32-bit word representation of the length, 448). Thus, the final padded message consists of two blocks (*N*=2).

For SHA-256, the initial hash value, $H^{(0)}$, is

$$H_0^{(0)} = \texttt{6a09e667}$$
$$H_1^{(0)} = \texttt{bb67ae85}$$
$$H_2^{(0)} = \texttt{3c6ef372}$$

$H_3^{(0)}$ = a54ff53a
$H_4^{(0)}$ = 510e527f
$H_5^{(0)}$ = 9b05688c
$H_6^{(0)}$ = 1f83d9ab
$H_7^{(0)}$ = 5be0cd19.

The words of the first padded message block, $M^{(1)}$, are then assigned to the words $W_0,\ldots,W_{15}$ of the message schedule:

W_0 = 61626364
W_1 = 62636465
W_2 = 63646566
W_3 = 64656667
W_4 = 65666768
W_5 = 66676869
W_6 = 6768696a
W_7 = 68696a6b
W_8 = 696a6b6c
W_9 = 6a6b6c6d
W_{10} = 6b6c6d6e
W_{11} = 6c6d6e6f
W_{12} = 6d6e6f70
W_{13} = 6e6f7071
W_{14} = 80000000
W_{15} = 00000000.

The following schedule shows the hex values for ***a***, ***b***, ***c***, ***d***, ***e***, ***f***, ***g***, and ***h*** *after* pass t of the "for t=0 to 63" loop described in Sec. 6.2.2, step 4.

	a	***b***	***c***	***d***	***e***	***f***	***g***	***h***
t = 0 :	5d6aebb1	6a09e667	bb67ae85	3c6ef372	fa2a4606	510e527f	9b05688c	1f83d9ab
t = 1 :	2f2d5fcf	5d6aebb1	6a09e667	bb67ae85	4eb1cfce	fa2a4606	510e527f	9b05688c
t = 2 :	97651825	2f2d5fcf	5d6aebb1	6a09e667	62d5c49e	4eb1cfce	fa2a4606	510e527f
t = 3 :	4a8d64d5	97651825	2f2d5fcf	5d6aebb1	6494841b	62d5c49e	4eb1cfce	fa2a4606
t = 4 :	f921c212	4a8d64d5	97651825	2f2d5fcf	05c4f88a	6494841b	62d5c49e	4eb1cfce
t = 5 :	55c8ef48	f921c212	4a8d64d5	97651825	7ff91c94	05c4f88a	6494841b	62d5c49e
t = 6 :	485835b7	55c8ef48	f921c212	4a8d64d5	39a5b2ca	7ff91c94	05c4f88a	6494841b
t = 7 :	d237e6db	485835b7	55c8ef48	f921c212	a401d211	39a5b2ca	7ff91c94	05c4f88a
t = 8 :	359f2bce	d237e6db	485835b7	55c8ef48	c09ffec4	a401d211	39a5b2ca	7ff91c94
t = 9 :	3a474b2b	359f2bce	d237e6db	485835b7	9037b3b8	c09ffec4	a401d211	39a5b2ca
t = 10 :	b8e2b4cb	3a474b2b	359f2bce	d237e6db	443ed29e	9037b3b8	c09ffec4	a401d211
t = 11 :	1762215c	b8e2b4cb	3a474b2b	359f2bce	ee1c97a8	443ed29e	9037b3b8	c09ffec4
t = 12 :	101a4861	1762215c	b8e2b4cb	3a474b2b	839a0fc9	ee1c97a8	443ed29e	9037b3b8
t = 13 :	d68e6457	101a4861	1762215c	b8e2b4cb	9243f8af	839a0fc9	ee1c97a8	443ed29e
t = 14 :	dd16cbb3	d68e6457	101a4861	1762215c	9162aded	9243f8af	839a0fc9	ee1c97a8
t = 15 :	c3486194	dd16cbb3	d68e6457	101a4861	1496a54f	9162aded	9243f8af	839a0fc9
t = 16 :	b9dcacb1	c3486194	dd16cbb3	d68e6457	d4f64250	1496a54f	9162aded	9243f8af
t = 17 :	046a193e	b9dcacb1	c3486194	dd16cbb3	885370b6	d4f64250	1496a54f	9162aded
t = 18 :	f402f058	046a193e	b9dcacb1	c3486194	6f433549	885370b6	d4f64250	1496a54f
t = 19 :	2139187b	f402f058	046a193e	b9dcacb1	7c304206	6f433549	885370b6	d4f64250
t = 20 :	d70ac17d	2139187b	f402f058	046a193e	7cc6b262	7c304206	6f433549	885370b6
t = 21 :	1b2b66b8	d70ac17d	2139187b	f402f058	d560b028	7cc6b262	7c304206	6f433549
t = 22 :	ae2e2d4f	1b2b66b8	d70ac17d	2139187b	f074fc95	d560b028	7cc6b262	7c304206
t = 23 :	59fce6b9	ae2e2d4f	1b2b66b8	d70ac17d	a2c7d51d	f074fc95	d560b028	7cc6b262
t = 24 :	4a885065	59fce6b9	ae2e2d4f	1b2b66b8	763597fb	a2c7d51d	f074fc95	d560b028

$t = 25$:	573221da	4a885065	59fce6b9	ae2e2d4f	36e74eb4	763597fb	a2c7d51d	f074fc95
$t = 26$:	128661da	573221da	4a885065	59fce6b9	1162d575	36e74eb4	763597fb	a2c7d51d
$t = 27$:	73f858af	128661da	573221da	4a885065	e77c797f	1162d575	36e74eb4	763597fb
$t = 28$:	74bcf468	73f858af	128661da	573221da	72abaecd	e77c797f	1162d575	36e74eb4
$t = 29$:	df7151a0	74bcf468	73f858af	128661da	7629c961	72abaecd	e77c797f	1162d575
$t = 30$:	eb43f3ed	df7151a0	74bcf468	73f858af	0635d880	7629c961	72abaecd	e77c797f
$t = 31$:	5581ab07	eb43f3ed	df7151a0	74bcf468	df980085	0635d880	7629c961	72abaecd
$t = 32$:	9fc905c8	5581ab07	eb43f3ed	df7151a0	a94d2af1	df980085	0635d880	7629c961
$t = 33$:	9ce5a62f	9fc905c8	5581ab07	eb43f3ed	6ef3b6bd	a94d2af1	df980085	0635d880
$t = 34$:	1df8e885	9ce5a62f	9fc905c8	5581ab07	2a9e048e	6ef3b6bd	a94d2af1	df980085
$t = 35$:	0786dce8	1df8e885	9ce5a62f	9fc905c8	de2a21d1	2a9e048e	6ef3b6bd	a94d2af1
$t = 36$:	2c55d3a6	0786dce8	1df8e885	9ce5a62f	b067c1af	de2a21d1	2a9e048e	6ef3b6bd
$t = 37$:	a985b4be	2c55d3a6	0786dce8	1df8e885	f72bf353	b067c1af	de2a21d1	2a9e048e
$t = 38$:	91ac9d5d	a985b4be	2c55d3a6	0786dce8	68d8d590	f72bf353	b067c1af	de2a21d1
$t = 39$:	7e4d30b8	91ac9d5d	a985b4be	2c55d3a6	9f5b9b6d	68d8d590	f72bf353	b067c1af
$t = 40$:	7e056794	7e4d30b8	91ac9d5d	a985b4be	423b26c0	9f5b9b6d	68d8d590	f72bf353
$t = 41$:	508a16ab	7e056794	7e4d30b8	91ac9d5d	45459d97	423b26c0	9f5b9b6d	68d8d590
$t = 42$:	b62c7013	508a16ab	7e056794	7e4d30b8	80a92a00	45459d97	423b26c0	9f5b9b6d
$t = 43$:	167361de	b62c7013	508a16ab	7e056794	41dd3844	80a92a00	45459d97	423b26c0
$t = 44$:	de71e2f2	167361de	b62c7013	508a16ab	ff61c636	41dd3844	80a92a00	45459d97
$t = 45$:	18f0d19d	de71e2f2	167361de	b62c7013	6b88472c	ff61c636	41dd3844	80a92a00
$t = 46$:	165be9cd	18f0d19d	de71e2f2	167361de	a483f080	6b88472c	ff61c636	41dd3844
$t = 47$:	13d82741	165be9cd	18f0d19d	de71e2f2	a7802a4d	a483f080	6b88472c	ff61c636
$t = 48$:	017b9d99	13d82741	165be9cd	18f0d19d	aeb10b60	a7802a4d	a483f080	6b88472c
$t = 49$:	543c99a1	017b9d99	13d82741	165be9cd	16f134b6	aeb10b60	a7802a4d	a483f080
$t = 50$:	758ca97a	543c99a1	017b9d99	13d82741	100cf2ea	16f134b6	aeb10b60	a7802a4d
$t = 51$:	81c1cde0	758ca97a	543c99a1	017b9d99	5c47eb7b	100cf2ea	16f134b6	aeb10b60
$t = 52$:	b8d55619	81c1cde0	758ca97a	543c99a1	1c806a61	5c47eb7b	100cf2ea	16f134b6
$t = 53$:	1d6de87a	b8d55619	81c1cde0	758ca97a	3443bed4	1c806a61	5c47eb7b	100cf2ea
$t = 54$:	f907b313	1d6de87a	b8d55619	81c1cde0	61a41711	3443bed4	1c806a61	5c47eb7b
$t = 55$:	9e57c4a0	f907b313	1d6de87a	b8d55619	eec13548	61a41711	3443bed4	1c806a61
$t = 56$:	71629856	9e57c4a0	f907b313	1d6de87a	2f6c8c4e	eec13548	61a41711	3443bed4
$t = 57$:	7c015a2c	71629856	9e57c4a0	f907b313	cb9d3dd0	2f6c8c4e	eec13548	61a41711
$t = 58$:	921fccb6	7c015a2c	71629856	9e57c4a0	43d8a034	cb9d3dd0	2f6c8c4e	eec13548
$t = 59$:	e18f259a	921fccb6	7c015a2c	71629856	51e15869	43d8a034	cb9d3dd0	2f6c8c4e
$t = 60$:	bcfce922	e18f259a	921fccb6	7c015a2c	962d8621	51e15869	43d8a034	cb9d3dd0
$t = 61$:	f6f443f8	bcfce922	e18f259a	921fccb6	acc75916	962d8621	51e15869	43d8a034
$t = 62$:	86126910	f6f443f8	bcfce922	e18f259a	2fc08f85	acc75916	962d8621	51e15869
$t = 63$:	1bdc6f6f	86126910	f6f443f8	bcfce922	25d2430a	2fc08f85	acc75916	962d8621

That completes the processing of the first message block, $M^{(1)}$. The first intermediate hash value, $H^{(1)}$, is calculated to be

$$H_0^{(1)} = \texttt{6a09e667} + \texttt{1bdc6f6f} = \texttt{85e655d6}$$
$$H_1^{(1)} = \texttt{bb67ae85} + \texttt{86126910} = \texttt{417a1795}$$
$$H_2^{(1)} = \texttt{3c6ef372} + \texttt{f6f443f8} = \texttt{3363376a}$$
$$H_3^{(1)} = \texttt{a54ff53a} + \texttt{bcfce922} = \texttt{624cde5c}$$
$$H_4^{(1)} = \texttt{510e527f} + \texttt{25d2430a} = \texttt{76e09589}$$
$$H_5^{(1)} = \texttt{9b05688c} + \texttt{2fc08f85} = \texttt{cac5f811}$$
$$H_6^{(1)} = \texttt{1f83d9ab} + \texttt{acc75916} = \texttt{cc4b32c1}$$

$H_7^{(1)}$ = 5be0cd19 + 962d8621 = f20e533a.

The words of the *second* padded message block, $M^{(2)}$, are then assigned to the words $W_0,\ldots,W_{15}$ of the message schedule:

W_0 = 00000000
W_1 = 00000000
W_2 = 00000000
W_3 = 00000000
W_4 = 00000000
W_5 = 00000000
W_6 = 00000000
W_7 = 00000000
W_8 = 00000000
W_9 = 00000000
W_{10} = 00000000
W_{11} = 00000000
W_{12} = 00000000
W_{13} = 00000000
W_{14} = 00000000
W_{15} = 000001c0.

The following schedule shows the hex values for ***a***, ***b***, ***c***, ***d***, ***e***, ***f***, ***g***, and ***h*** *after* pass t of the "for t=0 to 63" loop described in Sec. 6.2.2, step 4.

	a	***b***	***c***	***d***	***e***	***f***	***g***	***h***
t = 0:	7c20c838	85e655d6	417a1795	3363376a	4670ae6e	76e09589	cac5f811	cc4b32c1
t = 1:	7c3c0f86	7c20c838	85e655d6	417a1795	8c51be64	4670ae6e	76e09589	cac5f811
t = 2:	fd1eebdc	7c3c0f86	7c20c838	85e655d6	af71b9ea	8c51be64	4670ae6e	76e09589
t = 3:	f268faa9	fd1eebdc	7c3c0f86	7c20c838	e20362ef	af71b9ea	8c51be64	4670ae6e
t = 4:	185a5d79	f268faa9	fd1eebdc	7c3c0f86	8dff3001	e20362ef	af71b9ea	8c51be64
t = 5:	3eeb6c06	185a5d79	f268faa9	fd1eebdc	fe20cda6	8dff3001	e20362ef	af71b9ea
t = 6:	89bba3f1	3eeb6c06	185a5d79	f268faa9	0a34df03	fe20cda6	8dff3001	e20362ef
t = 7:	bf9a93a0	89bba3f1	3eeb6c06	185a5d79	059abdd1	0a34df03	fe20cda6	8dff3001
t = 8:	2c096744	bf9a93a0	89bba3f1	3eeb6c06	abfa465b	059abdd1	0a34df03	fe20cda6
t = 9:	2d964e86	2c096744	bf9a93a0	89bba3f1	aa27ed82	abfa465b	059abdd1	0a34df03
t = 10:	5b35025b	2d964e86	2c096744	bf9a93a0	10e77723	aa27ed82	abfa465b	059abdd1
t = 11:	5eb4ec40	5b35025b	2d964e86	2c096744	e11b4548	10e77723	aa27ed82	abfa465b
t = 12:	35ee996d	5eb4ec40	5b35025b	2d964e86	5c24e2a2	e11b4548	10e77723	aa27ed82
t = 13:	d74080fa	35ee996d	5eb4ec40	5b35025b	68aa893f	5c24e2a2	e11b4548	10e77723
t = 14:	0cea5cbc	d74080fa	35ee996d	5eb4ec40	60356548	68aa893f	5c24e2a2	e11b4548
t = 15:	16a8cc79	0cea5cbc	d74080fa	35ee996d	0fcb1f6f	60356548	68aa893f	5c24e2a2
t = 16:	f16f634e	16a8cc79	0cea5cbc	d74080fa	8b21cdc1	0fcb1f6f	60356548	68aa893f
t = 17:	23dcb6c2	f16f634e	16a8cc79	0cea5cbc	ca9182d3	8b21cdc1	0fcb1f6f	60356548
t = 18:	dcff40fd	23dcb6c2	f16f634e	16a8cc79	69bf7b95	ca9182d3	8b21cdc1	0fcb1f6f
t = 19:	76f1a2bc	dcff40fd	23dcb6c2	f16f634e	0dc84bb1	69bf7b95	ca9182d3	8b21cdc1
t = 20:	20aad899	76f1a2bc	dcff40fd	23dcb6c2	cc4769f2	0dc84bb1	69bf7b95	ca9182d3
t = 21:	d44dc81a	20aad899	76f1a2bc	dcff40fd	5bace62d	cc4769f2	0dc84bb1	69bf7b95
t = 22:	f13ae55b	d44dc81a	20aad899	76f1a2bc	966aa287	5bace62d	cc4769f2	0dc84bb1
t = 23:	a4195b91	f13ae55b	d44dc81a	20aad899	eddbd6ed	966aa287	5bace62d	cc4769f2
t = 24:	4984fa79	a4195b91	f13ae55b	d44dc81a	a530d939	eddbd6ed	966aa287	5bace62d
t = 25:	aa6cb982	4984fa79	a4195b91	f13ae55b	0b5eeea4	a530d939	eddbd6ed	966aa287
t = 26:	9450fbbc	aa6cb982	4984fa79	a4195b91	09166dda	0b5eeea4	a530d939	eddbd6ed
t = 27:	0d936bab	9450fbbc	aa6cb982	4984fa79	6e495d4b	09166dda	0b5eeea4	a530d939
t = 28:	d958b529	0d936bab	9450fbbc	aa6cb982	c2fa99b1	6e495d4b	09166dda	0b5eeea4
t = 29:	1cfa5eb0	d958b529	0d936bab	9450fbbc	6c49db9f	c2fa99b1	6e495d4b	09166dda
t = 30:	02ef3a5f	1cfa5eb0	d958b529	0d936bab	5da10665	6c49db9f	c2fa99b1	6e495d4b
t = 31:	b0eab1c5	02ef3a5f	1cfa5eb0	d958b529	f6d93952	5da10665	6c49db9f	c2fa99b1

t = 32 :	0bfba73c	b0eab1c5	02ef3a5f	1cfa5eb0	8b99e3a9	f6d93952	5da10665	6c49db9f
t = 33 :	4bd1df96	0bfba73c	b0eab1c5	02ef3a5f	905e44ac	8b99e3a9	f6d93952	5da10665
t = 34 :	9907f1b6	4bd1df96	0bfba73c	b0eab1c5	66c3043d	905e44ac	8b99e3a9	f6d93952
t = 35 :	ecde4e0d	9907f1b6	4bd1df96	0bfba73c	5dc119e6	66c3043d	905e44ac	8b99e3a9
t = 36 :	2f11c939	ecde4e0d	9907f1b6	4bd1df96	fed4ce1d	5dc119e6	66c3043d	905e44ac
t = 37 :	d949682b	2f11c939	ecde4e0d	9907f1b6	32d99008	fed4ce1d	5dc119e6	66c3043d
t = 38 :	adca7a96	d949682b	2f11c939	ecde4e0d	c6cce4ff	32d99008	fed4ce1d	5dc119e6
t = 39 :	221b8a5a	adca7a96	d949682b	2f11c939	0b82c5eb	c6cce4ff	32d99008	fed4ce1d
t = 40 :	12d97845	221b8a5a	adca7a96	d949682b	e4213ca2	0b82c5eb	c6cce4ff	32d99008
t = 41 :	2c794876	12d97845	221b8a5a	adca7a96	ff6759ba	e4213ca2	0b82c5eb	c6cce4ff
t = 42 :	8300fca2	2c794876	12d97845	221b8a5a	e0e3457c	ff6759ba	e4213ca2	0b82c5eb
t = 43 :	f2ad6322	8300fca2	2c794876	12d97845	cc48c7f3	e0e3457c	ff6759ba	e4213ca2
t = 44 :	0f154e11	f2ad6322	8300fca2	2c794876	6f9517cb	cc48c7f3	e0e3457c	ff6759ba
t = 45 :	104a7db4	0f154e11	f2ad6322	8300fca2	5348e8f6	6f9517cb	cc48c7f3	e0e3457c
t = 46 :	0b3303a7	104a7db4	0f154e11	f2ad6322	bbe1c39a	5348e8f6	6f9517cb	cc48c7f3
t = 47 :	d7354d5b	0b3303a7	104a7db4	0f154e11	aad55b6b	bbe1c39a	5348e8f6	6f9517cb
t = 48 :	b736d7a6	d7354d5b	0b3303a7	104a7db4	68f25260	aad55b6b	bbe1c39a	5348e8f6
t = 49 :	2748e5ec	b736d7a6	d7354d5b	0b3303a7	d4b58576	68f25260	aad55b6b	bbe1c39a
t = 50 :	d8aabcf9	2748e5ec	b736d7a6	d7354d5b	27844711	d4b58576	68f25260	aad55b6b
t = 51 :	1a6bcf6a	d8aabcf9	2748e5ec	b736d7a6	ff5e99d0	27844711	d4b58576	68f25260
t = 52 :	4eca6fa0	1a6bcf6a	d8aabcf9	2748e5ec	989ed071	ff5e99d0	27844711	d4b58576
t = 53 :	ec02560a	4eca6fa0	1a6bcf6a	d8aabcf9	7151df8e	989ed071	ff5e99d0	27844711
t = 54 :	d9f0c115	ec02560a	4eca6fa0	1a6bcf6a	624150c4	7151df8e	989ed071	ff5e99d0
t = 55 :	92952710	d9f0c115	ec02560a	4eca6fa0	226806d6	624150c4	7151df8e	989ed071
t = 56 :	20d4d0e4	92952710	d9f0c115	ec02560a	4e515a4d	226806d6	624150c4	7151df8e
t = 57 :	4348eb1f	20d4d0e4	92952710	d9f0c115	c21eddf9	4e515a4d	226806d6	624150c4
t = 58 :	286fe5f0	4348eb1f	20d4d0e4	92952710	54076664	c21eddf9	4e515a4d	226806d6
t = 59 :	1c4cddd9	286fe5f0	4348eb1f	20d4d0e4	f487a853	54076664	c21eddf9	4e515a4d
t = 60 :	a9f181dd	1c4cddd9	286fe5f0	4348eb1f	27ccb387	f487a853	54076664	c21eddf9
t = 61 :	b25cef29	a9f181dd	1c4cddd9	286fe5f0	2aa1bb13	27ccb387	f487a853	54076664
t = 62 :	908c2123	b25cef29	a9f181dd	1c4cddd9	9a392956	2aa1bb13	27ccb387	f487a853
t = 63 :	9ea7148b	908c2123	b25cef29	a9f181dd	2c5c4ed0	9a392956	2aa1bb13	27ccb387

That completes the processing of the second and final message block, $M^{(2)}$. The final hash value, $H^{(2)}$, is calculated to be

$$H_0^{(2)} = \texttt{85e655d6} + \texttt{9ea7148b} = \texttt{248d6a61}$$
$$H_1^{(2)} = \texttt{417a1795} + \texttt{908c2123} = \texttt{d20638b8}$$
$$H_2^{(2)} = \texttt{3363376a} + \texttt{b25cef29} = \texttt{e5c02693}$$
$$H_3^{(2)} = \texttt{624cde5c} + \texttt{a9f181dd} = \texttt{0c3e6039}$$
$$H_4^{(2)} = \texttt{76e09589} + \texttt{2c5c4ed0} = \texttt{a33ce459}$$
$$H_5^{(2)} = \texttt{cac5f811} + \texttt{9a392956} = \texttt{64ff2167}$$
$$H_6^{(2)} = \texttt{cc4b32c1} + \texttt{2aa1bb13} = \texttt{f6ecedd4}$$
$$H_7^{(2)} = \texttt{f20e533a} + \texttt{27ccb387} = \texttt{19db06c1}.$$

The resulting 256-bit message digest is

```
248d6a61 d20638b8 e5c02693 0c3e6039 a33ce459 64ff2167 f6ecedd4 19db06c1.
```

B.3 SHA-256 Example (Long Message)

Let the message *M* be the binary-coded form of the ASCII string which consists of 1,000,000 repetitions of the character "**a**". The resulting SHA-256 message digest is

```
cdc76e5c 9914fb92 81a1c7e2 84d73e67 f1809a48 a497200e 046d39cc c7112cd0.
```

APPENDIX C: SHA-512 EXAMPLES

This appendix is for informational purposes only and is not required to meet the standard.

C.1 SHA-512 Example (One-Block Message)

Let the message, M, be the 24-bit ($\ell = 24$) ASCII string "**abc**", which is equivalent to the following binary string:

01100001 01100010 01100011.

The message is padded by appending a "1" bit, followed by 871 "0" bits, and ending with the hex value

0000000000000000 0000000000000018

(the two 64-bit word representation of the length, 24). Thus, the final padded message consists of one block (N=1).

For SHA-512, the initial hash value, $H^{(0)}$, is

$H_0^{(0)}$ = 6a09e667f3bcc908
$H_1^{(0)}$ = bb67ae8584caa73b
$H_2^{(0)}$ = 3c6ef372fe94f82b
$H_3^{(0)}$ = a54ff53a5f1d36f1
$H_4^{(0)}$ = 510e527fade682d1
$H_5^{(0)}$ = 9b05688c2b3e6c1f
$H_6^{(0)}$ = 1f83d9abfb41bd6b
$H_7^{(0)}$ = 5be0cd19137e2179.

The words of the padded message block are then assigned to the words $W_0,\ldots,W_{15}$ of the message schedule:

W_0 = 6162638000000000
W_1 = 0000000000000000
W_2 = 0000000000000000
W_3 = 0000000000000000
W_4 = 0000000000000000
W_5 = 0000000000000000
W_6 = 0000000000000000
W_7 = 0000000000000000
W_8 = 0000000000000000
W_9 = 0000000000000000
W_{10} = 0000000000000000
W_{11} = 0000000000000000
W_{12} = 0000000000000000
W_{13} = 0000000000000000
W_{14} = 0000000000000000
W_{15} = 0000000000000018.

The following schedule shows the hex values for ***a***, ***b***, ***c***, ***d***, ***e***, ***f***, ***g***, and ***h*** *after* pass *t* of the "for *t*=0 to 79" loop described in Sec. 6.3.2, step 4.

	a / ***e***	***b*** / ***f***	***c*** / ***g***	***d*** / ***h***
t = 0 :	f6afceb8bcfcddf5	6a09e667f3bcc908	bb67ae8584caa73b	3c6ef372fe94f82b
	58cb02347ab51f91	510e527fade682d1	9b05688c2b3e6c1f	1f83d9abfb41bd6b
t = 1 :	1320f8c9fb872cc0	f6afceb8bcfcddf5	6a09e667f3bcc908	bb67ae8584caa73b
	c3d4ebfd48650ffa	58cb02347ab51f91	510e527fade682d1	9b05688c2b3e6c1f
t = 2 :	ebcffc07203d91f3	1320f8c9fb872cc0	f6afceb8bcfcddf5	6a09e667f3bcc908
	dfa9b239f2697812	c3d4ebfd48650ffa	58cb02347ab51f91	510e527fade682d1
t = 3 :	5a83cb3e80050e82	ebcffc07203d91f3	1320f8c9fb872cc0	f6afceb8bcfcddf5
	0b47b4bb1928990e	dfa9b239f2697812	c3d4ebfd48650ffa	58cb02347ab51f91
t = 4 :	b680953951604860	5a83cb3e80050e82	ebcffc07203d91f3	1320f8c9fb872cc0
	745aca4a342ed2e2	0b47b4bb1928990e	dfa9b239f2697812	c3d4ebfd48650ffa
t = 5 :	af573b02403e89cd	b680953951604860	5a83cb3e80050e82	ebcffc07203d91f3
	96f60209b6dc35ba	745aca4a342ed2e2	0b47b4bb1928990e	dfa9b239f2697812
t = 6 :	c4875b0c7abc076b	af573b02403e89cd	b680953951604860	5a83cb3e80050e82
	5a6c781f54dcc00c	96f60209b6dc35ba	745aca4a342ed2e2	0b47b4bb1928990e
t = 7 :	8093d195e0054fa3	c4875b0c7abc076b	af573b02403e89cd	b680953951604860
	86f67263a0f0ec0a	5a6c781f54dcc00c	96f60209b6dc35ba	745aca4a342ed2e2
t = 8 :	f1eca5544cb89225	8093d195e0054fa3	c4875b0c7abc076b	af573b02403e89cd
	d0403c398fc40002	86f67263a0f0ec0a	5a6c781f54dcc00c	96f60209b6dc35ba
t = 9 :	81782d4a5db48f03	f1eca5544cb89225	8093d195e0054fa3	c4875b0c7abc076b
	00091f460be46c52	d0403c398fc40002	86f67263a0f0ec0a	5a6c781f54dcc00c
t = 10 :	69854c4aa0f25b59	81782d4a5db48f03	f1eca5544cb89225	8093d195e0054fa3
	d375471bde1ba3f4	00091f460be46c52	d0403c398fc40002	86f67263a0f0ec0a
t = 11 :	db0a9963f80c2eaa	69854c4aa0f25b59	81782d4a5db48f03	f1eca5544cb89225
	475975b91a7a462c	d375471bde1ba3f4	00091f460be46c52	d0403c398fc40002
t = 12 :	5e41214388186c14	db0a9963f80c2eaa	69854c4aa0f25b59	81782d4a5db48f03
	cdf3bff2883fc9d9	475975b91a7a462c	d375471bde1ba3f4	00091f460be46c52
t = 13 :	44249631255d2ca0	5e41214388186c14	db0a9963f80c2eaa	69854c4aa0f25b59
	860acf9effba6f61	cdf3bff2883fc9d9	475975b91a7a462c	d375471bde1ba3f4
t = 14 :	fa967eed85a08028	44249631255d2ca0	5e41214388186c14	db0a9963f80c2eaa
	874bfe5f6aae9f2f	860acf9effba6f61	cdf3bff2883fc9d9	475975b91a7a462c
t = 15 :	0ae07c86b1181c75	fa967eed85a08028	44249631255d2ca0	5e41214388186c14
	a77b7c035dd4c161	874bfe5f6aae9f2f	860acf9effba6f61	cdf3bff2883fc9d9
t = 16 :	caf81a425d800537	0ae07c86b1181c75	fa967eed85a08028	44249631255d2ca0
	2deecc6b39d64d78	a77b7c035dd4c161	874bfe5f6aae9f2f	860acf9effba6f61
t = 17 :	4725be249ad19e6b	caf81a425d800537	0ae07c86b1181c75	fa967eed85a08028
	f47e8353f8047455	2deecc6b39d64d78	a77b7c035dd4c161	874bfe5f6aae9f2f
t = 18 :	3c4b4104168e3edb	4725be249ad19e6b	caf81a425d800537	0ae07c86b1181c75
	29695fd88d81dbd0	f47e8353f8047455	2deecc6b39d64d78	a77b7c035dd4c161
t = 19 :	9a3fb4d38ab6cf06	3c4b4104168e3edb	4725be249ad19e6b	caf81a425d800537
	f14998dd5f70767e	29695fd88d81dbd0	f47e8353f8047455	2deecc6b39d64d78

$t = 20$:	8dc5ae65569d3855	9a3fb4d38ab6cf06	3c4b4104168e3edb	4725be249ad19e6b
	4bb9e66d1145bfdc	f14998dd5f70767e	29695fd88d81dbd0	f47e8353f8047455
$t = 21$:	da34d6673d452dcf	8dc5ae65569d3855	9a3fb4d38ab6cf06	3c4b4104168e3edb
	8e30ff09ad488753	4bb9e66d1145bfdc	f14998dd5f70767e	29695fd88d81dbd0
$t = 22$:	3e2644567b709a78	da34d6673d452dcf	8dc5ae65569d3855	9a3fb4d38ab6cf06
	0ac2b11da8f571c6	8e30ff09ad488753	4bb9e66d1145bfdc	f14998dd5f70767e
$t = 23$:	4f6877b58fe55484	3e2644567b709a78	da34d6673d452dcf	8dc5ae65569d3855
	c66005f87db55233	0ac2b11da8f571c6	8e30ff09ad488753	4bb9e66d1145bfdc
$t = 24$:	9aff71163fa3a940	4f6877b58fe55484	3e2644567b709a78	da34d6673d452dcf
	d3ecf13769180e6f	c66005f87db55233	0ac2b11da8f571c6	8e30ff09ad488753
$t = 25$:	0bc5f791f8e6816b	9aff71163fa3a940	4f6877b58fe55484	3e2644567b709a78
	6ddf1fd7edcce336	d3ecf13769180e6f	c66005f87db55233	0ac2b11da8f571c6
$t = 26$:	884c3bc27bc4f941	0bc5f791f8e6816b	9aff71163fa3a940	4f6877b58fe55484
	e6e48c9a8e948365	6ddf1fd7edcce336	d3ecf13769180e6f	c66005f87db55233
$t = 27$:	eab4a9e5771b8d09	884c3bc27bc4f941	0bc5f791f8e6816b	9aff71163fa3a940
	09068a4e255a0dac	e6e48c9a8e948365	6ddf1fd7edcce336	d3ecf13769180e6f
$t = 28$:	e62349090f47d30a	eab4a9e5771b8d09	884c3bc27bc4f941	0bc5f791f8e6816b
	0fcdf99710f21584	09068a4e255a0dac	e6e48c9a8e948365	6ddf1fd7edcce336
$t = 29$:	74bf40f869094c63	e62349090f47d30a	eab4a9e5771b8d09	884c3bc27bc4f941
	f0aec2fe1437f085	0fcdf99710f21584	09068a4e255a0dac	e6e48c9a8e948365
$t = 30$:	4c4fbbb75f1873a6	74bf40f869094c63	e62349090f47d30a	eab4a9e5771b8d09
	73e025d91b9efea3	f0aec2fe1437f085	0fcdf99710f21584	09068a4e255a0dac
$t = 31$:	ff4d3f1f0d46a736	4c4fbbb75f1873a6	74bf40f869094c63	e62349090f47d30a
	3cd388e119e8162e	73e025d91b9efea3	f0aec2fe1437f085	0fcdf99710f21584
$t = 32$:	a0509015ca08c8d4	ff4d3f1f0d46a736	4c4fbbb75f1873a6	74bf40f869094c63
	e1034573654a106f	3cd388e119e8162e	73e025d91b9efea3	f0aec2fe1437f085
$t = 33$:	60d4e6995ed91fe6	a0509015ca08c8d4	ff4d3f1f0d46a736	4c4fbbb75f1873a6
	efabbd8bf47c041a	e1034573654a106f	3cd388e119e8162e	73e025d91b9efea3
$t = 34$:	2c59ec7743632621	60d4e6995ed91fe6	a0509015ca08c8d4	ff4d3f1f0d46a736
	0fbae670fa780fd3	efabbd8bf47c041a	e1034573654a106f	3cd388e119e8162e
$t = 35$:	1a081afc59fdbc2c	2c59ec7743632621	60d4e6995ed91fe6	a0509015ca08c8d4
	f098082f502b44cd	0fbae670fa780fd3	efabbd8bf47c041a	e1034573654a106f
$t = 36$:	88df85b0bbe77514	1a081afc59fdbc2c	2c59ec7743632621	60d4e6995ed91fe6
	8fbfd0162bbf4675	f098082f502b44cd	0fbae670fa780fd3	efabbd8bf47c041a
$t = 37$:	002bb8e4cd989567	88df85b0bbe77514	1a081afc59fdbc2c	2c59ec7743632621
	66adcfa249ac7bbd	8fbfd0162bbf4675	f098082f502b44cd	0fbae670fa780fd3
$t = 38$:	b3bb8542b3376de5	002bb8e4cd989567	88df85b0bbe77514	1a081afc59fdbc2c
	b49596c20feba7de	66adcfa249ac7bbd	8fbfd0162bbf4675	f098082f502b44cd
$t = 39$:	8e01e125b855d225	b3bb8542b3376de5	002bb8e4cd989567	88df85b0bbe77514
	0c710a47ba6a567b	b49596c20feba7de	66adcfa249ac7bbd	8fbfd0162bbf4675
$t = 40$:	b01521dd6a6be12c	8e01e125b855d225	b3bb8542b3376de5	002bb8e4cd989567
	169008b3a4bb170b	0c710a47ba6a567b	b49596c20feba7de	66adcfa249ac7bbd
$t = 41$:	e96f89dd48cbd851	b01521dd6a6be12c	8e01e125b855d225	b3bb8542b3376de5
	f0996439e7b50cb1	169008b3a4bb170b	0c710a47ba6a567b	b49596c20feba7de
$t = 42$:	bc05ba8de5d3c480	e96f89dd48cbd851	b01521dd6a6be12c	8e01e125b855d225
	639cb938e14dc190	f0996439e7b50cb1	169008b3a4bb170b	0c710a47ba6a567b
$t = 43$:	35d7e7f41defcbd5	bc05ba8de5d3c480	e96f89dd48cbd851	b01521dd6a6be12c

	cc5100997f5710f2	639cb938e14dc190	f0996439e7b50cb1	169008b3a4bb170b
$t = 44$:	c47c9d5c7ea8a234	35d7e7f41defcbd5	bc05ba8de5d3c480	e96f89dd48cbd851
	858d832ae0e8911c	cc5100997f5710f2	639cb938e14dc190	f0996439e7b50cb1
$t = 45$:	021fbadbabab5ac6	c47c9d5c7ea8a234	35d7e7f41defcbd5	bc05ba8de5d3c480
	e95c2a57572d64d9	858d832ae0e8911c	cc5100997f5710f2	639cb938e14dc190
$t = 46$:	f61e672694de2d67	021fbadbabab5ac6	c47c9d5c7ea8a234	35d7e7f41defcbd5
	c6bc35740d8daa9a	e95c2a57572d64d9	858d832ae0e8911c	cc5100997f5710f2
$t = 47$:	6b69fc1bb482feac	f61e672694de2d67	021fbadbabab5ac6	c47c9d5c7ea8a234
	35264334c03ac8ad	c6bc35740d8daa9a	e95c2a57572d64d9	858d832ae0e8911c
$t = 48$:	571f323d96b3a047	6b69fc1bb482feac	f61e672694de2d67	021fbadbabab5ac6
	271580ed6c3e5650	35264334c03ac8ad	c6bc35740d8daa9a	e95c2a57572d64d9
$t = 49$:	ca9bd862c5050918	571f323d96b3a047	6b69fc1bb482feac	f61e672694de2d67
	dfe091dab182e645	271580ed6c3e5650	35264334c03ac8ad	c6bc35740d8daa9a
$t = 50$:	813a43dd2c502043	ca9bd862c5050918	571f323d96b3a047	6b69fc1bb482feac
	07a0d8ef821c5e1a	dfe091dab182e645	271580ed6c3e5650	35264334c03ac8ad
$t = 51$:	d43f83727325dd77	813a43dd2c502043	ca9bd862c5050918	571f323d96b3a047
	483f80a82eaee23e	07a0d8ef821c5e1a	dfe091dab182e645	271580ed6c3e5650
$t = 52$:	03df11b32d42e203	d43f83727325dd77	813a43dd2c502043	ca9bd862c5050918
	504f94e40591cffa	483f80a82eaee23e	07a0d8ef821c5e1a	dfe091dab182e645
$t = 53$:	d63f68037ddf06aa	03df11b32d42e203	d43f83727325dd77	813a43dd2c502043
	a6781efe1aa1ce02	504f94e40591cffa	483f80a82eaee23e	07a0d8ef821c5e1a
$t = 54$:	f650857b5babda4d	d63f68037ddf06aa	03df11b32d42e203	d43f83727325dd77
	9ccfb31a86df0f86	a6781efe1aa1ce02	504f94e40591cffa	483f80a82eaee23e
$t = 55$:	63b460e42748817e	f650857b5babda4d	d63f68037ddf06aa	03df11b32d42e203
	c6b4dd2a9931c509	9ccfb31a86df0f86	a6781efe1aa1ce02	504f94e40591cffa
$t = 56$:	7a52912943d52b05	63b460e42748817e	f650857b5babda4d	d63f68037ddf06aa
	d2e89bbd91e00be0	c6b4dd2a9931c509	9ccfb31a86df0f86	a6781efe1aa1ce02
$t = 57$:	4b81c3aec976ea4b	7a52912943d52b05	63b460e42748817e	f650857b5babda4d
	70505988124351ac	d2e89bbd91e00be0	c6b4dd2a9931c509	9ccfb31a86df0f86
$t = 58$:	581ecb3355dcd9b8	4b81c3aec976ea4b	7a52912943d52b05	63b460e42748817e
	6a3c9b0f71c8bf36	70505988124351ac	d2e89bbd91e00be0	c6b4dd2a9931c509
$t = 59$:	2c074484ef1eac8c	581ecb3355dcd9b8	4b81c3aec976ea4b	7a52912943d52b05
	4797cde4ed370692	6a3c9b0f71c8bf36	70505988124351ac	d2e89bbd91e00be0
$t = 60$:	3857dfd2fc37d3ba	2c074484ef1eac8c	581ecb3355dcd9b8	4b81c3aec976ea4b
	a6af4e9c9f807e51	4797cde4ed370692	6a3c9b0f71c8bf36	70505988124351ac
$t = 61$:	cfcd928c5424e2b6	3857dfd2fc37d3ba	2c074484ef1eac8c	581ecb3355dcd9b8
	09aee5bda1644de5	a6af4e9c9f807e51	4797cde4ed370692	6a3c9b0f71c8bf36
$t = 62$:	a81dedbb9f19e643	cfcd928c5424e2b6	3857dfd2fc37d3ba	2c074484ef1eac8c
	84058865d60a05fa	09aee5bda1644de5	a6af4e9c9f807e51	4797cde4ed370692
$t = 63$:	ab44e86276478d85	a81dedbb9f19e643	cfcd928c5424e2b6	3857dfd2fc37d3ba
	cd881ee59ca6bc53	84058865d60a05fa	09aee5bda1644de5	a6af4e9c9f807e51
$t = 64$:	5a806d7e9821a501	ab44e86276478d85	a81dedbb9f19e643	cfcd928c5424e2b6
	aa84b086688a5c45	cd881ee59ca6bc53	84058865d60a05fa	09aee5bda1644de5
$t = 65$:	eeb9c21bb0102598	5a806d7e9821a501	ab44e86276478d85	a81dedbb9f19e643
	3b5fed0d6a1f96e1	aa84b086688a5c45	cd881ee59ca6bc53	84058865d60a05fa
$t = 66$:	46c4210ab2cc155d	eeb9c21bb0102598	5a806d7e9821a501	ab44e86276478d85
	29fab5a7bff53366	3b5fed0d6a1f96e1	aa84b086688a5c45	cd881ee59ca6bc53

t = 67 :	54ba35cf56a0340e	46c4210ab2cc155d	eeb9c21bb0102598	5a806d7e9821a501
	1c66f46d95690bcf	29fab5a7bff53366	3b5fed0d6a1f96e1	aa84b086688a5c45
t = 68 :	181839d609c79748	54ba35cf56a0340e	46c4210ab2cc155d	eeb9c21bb0102598
	0ada78ba2d446140	1c66f46d95690bcf	29fab5a7bff53366	3b5fed0d6a1f96e1
t = 69 :	fb6aaae5d0b6a447	181839d609c79748	54ba35cf56a0340e	46c4210ab2cc155d
	e3711cb6564d112d	0ada78ba2d446140	1c66f46d95690bcf	29fab5a7bff53366
t = 70 :	7652c579cb60f19c	fb6aaae5d0b6a447	181839d609c79748	54ba35cf56a0340e
	aff62c9665ff80fa	e3711cb6564d112d	0ada78ba2d446140	1c66f46d95690bcf
t = 71 :	f15e9664b2803575	7652c579cb60f19c	fb6aaae5d0b6a447	181839d609c79748
	947c3dfafee570ef	aff62c9665ff80fa	e3711cb6564d112d	0ada78ba2d446140
t = 72 :	358406d165aee9ab	f15e9664b2803575	7652c579cb60f19c	fb6aaae5d0b6a447
	8c7b5fd91a794ca0	947c3dfafee570ef	aff62c9665ff80fa	e3711cb6564d112d
t = 73 :	20878dcd29cdfaf5	358406d165aee9ab	f15e9664b2803575	7652c579cb60f19c
	054d3536539948d0	8c7b5fd91a794ca0	947c3dfafee570ef	aff62c9665ff80fa
t = 74 :	33d48dabb5521de2	20878dcd29cdfaf5	358406d165aee9ab	f15e9664b2803575
	2ba18245b50de4cf	054d3536539948d0	8c7b5fd91a794ca0	947c3dfafee570ef
t = 75 :	c8960e6be864b916	33d48dabb5521de2	20878dcd29cdfaf5	358406d165aee9ab
	995019a6ff3ba3de	2ba18245b50de4cf	054d3536539948d0	8c7b5fd91a794ca0
t = 76 :	654ef9abec389ca9	c8960e6be864b916	33d48dabb5521de2	20878dcd29cdfaf5
	ceb9fc3691ce8326	995019a6ff3ba3de	2ba18245b50de4cf	054d3536539948d0
t = 77 :	d67806db8b148677	654ef9abec389ca9	c8960e6be864b916	33d48dabb5521de2
	25c96a7768fb2aa3	ceb9fc3691ce8326	995019a6ff3ba3de	2ba18245b50de4cf
t = 78 :	10d9c4c4295599f6	d67806db8b148677	654ef9abec389ca9	c8960e6be864b916
	9bb4d39778c07f9e	25c96a7768fb2aa3	ceb9fc3691ce8326	995019a6ff3ba3de
t = 79 :	73a54f399fa4b1b2	10d9c4c4295599f6	d67806db8b148677	654ef9abec389ca9
	d08446aa79693ed7	9bb4d39778c07f9e	25c96a7768fb2aa3	ceb9fc3691ce8326

That completes the processing of the first and only message block, $M^{(1)}$. The final hash value, $H^{(1)}$, is calculated to be

$$
\begin{aligned}
H_0^{(1)} &= \texttt{6a09e667f3bcc908} + \texttt{73a54f399fa4b1b2} = \texttt{ddaf35a193617aba} \\
H_1^{(1)} &= \texttt{bb67ae8584caa73b} + \texttt{10d9c4c4295599f6} = \texttt{cc417349ae204131} \\
H_2^{(1)} &= \texttt{3c6ef372fe94f82b} + \texttt{d67806db8b148677} = \texttt{12e6fa4e89a97ea2} \\
H_3^{(1)} &= \texttt{a54ff53a5f1d36f1} + \texttt{654ef9abec389ca9} = \texttt{0a9eeee64b55d39a} \\
H_4^{(1)} &= \texttt{510e527fade682d1} + \texttt{d08446aa79693ed7} = \texttt{2192992a274fc1a8} \\
H_5^{(1)} &= \texttt{9b05688c2b3e6c1f} + \texttt{9bb4d39778c07f9e} = \texttt{36ba3c23a3feebbd} \\
H_6^{(1)} &= \texttt{1f83d9abfb41bd6b} + \texttt{25c96a7768fb2aa3} = \texttt{454d4423643ce80e} \\
H_7^{(1)} &= \texttt{5be0cd19137e2179} + \texttt{ceb9fc3691ce8326} = \texttt{2a9ac94fa54ca49f.}
\end{aligned}
$$

The resulting 512-bit message digest is

```
ddaf35a193617aba cc417349ae204131 12e6fa4e89a97ea2 0a9eeee64b55d39a
2192992a274fc1a8 36ba3c23a3feebbd 454d4423643ce80e 2a9ac94fa54ca49f.
```

C.2 SHA-512 Example (Multi-Block Message)

Let the message, M, be the 896-bit ($\ell = 896$) ASCII string

"**abcdefghbcdefghicdefghijdefghijkefghijklfghijklmghijklmn**
hijklmnoijklmnopjklmnopqklmnopqrlmnopqrsmnopqrstnopqrstu".

The message is padded by appending a "`1`" bit, followed by 1023 "`0`" bits, and ending with the hex value

`0000000000000000 0000000000000380`

(the two 64-bit word representation of the length, 896). Thus, the final padded message consists of two blocks (N=2).

For SHA-512, the initial hash value, $H^{(0)}$, is

$H_0^{(0)}$ = `6a09e667f3bcc908`
$H_1^{(0)}$ = `bb67ae8584caa73b`
$H_2^{(0)}$ = `3c6ef372fe94f82b`
$H_3^{(0)}$ = `a54ff53a5f1d36f1`
$H_4^{(0)}$ = `510e527fade682d1`
$H_5^{(0)}$ = `9b05688c2b3e6c1f`
$H_6^{(0)}$ = `1f83d9abfb41bd6b`
$H_7^{(0)}$ = `5be0cd19137e2179`.

The words of the padded message block are then assigned to the words $W_0,\ldots,W_{15}$ of the message schedule:

W_0 = `6162636465666768`
W_1 = `6263646566676869`
W_2 = `636465666768696a`
W_3 = `6465666768696a6b`
W_4 = `65666768696a6b6c`
W_5 = `666768696a6b6c6d`
W_6 = `6768696a6b6c6d6e`
W_7 = `68696a6b6c6d6e6f`
W_8 = `696a6b6c6d6e6f70`
W_9 = `6a6b6c6d6e6f7071`
W_{10} = `6b6c6d6e6f707172`
W_{11} = `6c6d6e6f70717273`
W_{12} = `6d6e6f7071727374`
W_{13} = `6e6f707172737475`
W_{14} = `8000000000000000`
W_{15} = `0000000000000000`.

The following schedule shows the hex values for ***a***, ***b***, ***c***, ***d***, ***e***, ***f***, ***g***, and ***h*** *after* pass t of the "for t=0 to 79" loop described in Sec. 6.3.2, step 4.

	a / ***e***	***b*** / ***f***	***c*** / ***g***	***d*** / ***h***
$t = 0$:	f6afce9d2263455d	6a09e667f3bcc908	bb67ae8584caa73b	3c6ef372fe94f82b
	58cb0218e01b86f9	510e527fade682d1	9b05688c2b3e6c1f	1f83d9abfb41bd6b
$t = 1$:	0b7056a534ae5f62	f6afce9d2263455d	6a09e667f3bcc908	bb67ae8584caa73b
	f8c7198fe39e4c8c	58cb0218e01b86f9	510e527fade682d1	9b05688c2b3e6c1f
$t = 2$:	2ca82233760c9942	0b7056a534ae5f62	f6afce9d2263455d	6a09e667f3bcc908
	303eccccd65953de	f8c7198fe39e4c8c	58cb0218e01b86f9	510e527fade682d1
$t = 3$:	a023f17ce52cda7b	2ca82233760c9942	0b7056a534ae5f62	f6afce9d2263455d
	ffdee5eedcc9ca42	303eccccd65953de	f8c7198fe39e4c8c	58cb0218e01b86f9
$t = 4$:	8f0a67d9d591a1a7	a023f17ce52cda7b	2ca82233760c9942	0b7056a534ae5f62
	cb4cfbb166505f2f	ffdee5eedcc9ca42	303eccccd65953de	f8c7198fe39e4c8c
$t = 5$:	b466267371acc493	8f0a67d9d591a1a7	a023f17ce52cda7b	2ca82233760c9942
	73d6c84c54d399ee	cb4cfbb166505f2f	ffdee5eedcc9ca42	303eccccd65953de
$t = 6$:	658269f1a312fccd	b466267371acc493	8f0a67d9d591a1a7	a023f17ce52cda7b
	cdc40314975fb275	73d6c84c54d399ee	cb4cfbb166505f2f	ffdee5eedcc9ca42
$t = 7$:	65e3519c5b88181b	658269f1a312fccd	b466267371acc493	8f0a67d9d591a1a7
	a657850ab3970c5a	cdc40314975fb275	73d6c84c54d399ee	cb4cfbb166505f2f
$t = 8$:	56604fbb4b6393ec	65e3519c5b88181b	658269f1a312fccd	b466267371acc493
	e8b3be22fbe64df7	a657850ab3970c5a	cdc40314975fb275	73d6c84c54d399ee
$t = 9$:	c4562769a37d02c0	56604fbb4b6393ec	65e3519c5b88181b	658269f1a312fccd
	0062e70a1ef705c1	e8b3be22fbe64df7	a657850ab3970c5a	cdc40314975fb275
$t = 10$:	27c0b4c9186e1736	c4562769a37d02c0	56604fbb4b6393ec	65e3519c5b88181b
	bc9740477a18ae2d	0062e70a1ef705c1	e8b3be22fbe64df7	a657850ab3970c5a
$t = 11$:	f17f52fb02f4eb74	27c0b4c9186e1736	c4562769a37d02c0	56604fbb4b6393ec
	be58522cb9590ee1	bc9740477a18ae2d	0062e70a1ef705c1	e8b3be22fbe64df7
$t = 12$:	f2c245ac903d4a35	f17f52fb02f4eb74	27c0b4c9186e1736	c4562769a37d02c0
	49d5fa3a16dcd502	be58522cb9590ee1	bc9740477a18ae2d	0062e70a1ef705c1
$t = 13$:	9b04175ea8090daa	f2c245ac903d4a35	f17f52fb02f4eb74	27c0b4c9186e1736
	ec9c5e98ff98760d	49d5fa3a16dcd502	be58522cb9590ee1	bc9740477a18ae2d
$t = 14$:	481b8a6ee5e07031	9b04175ea8090daa	f2c245ac903d4a35	f17f52fb02f4eb74
	e4d35b613a5ac420	ec9c5e98ff98760d	49d5fa3a16dcd502	be58522cb9590ee1
$t = 15$:	9356ac3ec3e51459	481b8a6ee5e07031	9b04175ea8090daa	f2c245ac903d4a35
	701f17d27582443b	e4d35b613a5ac420	ec9c5e98ff98760d	49d5fa3a16dcd502
$t = 16$:	b889ed34abd7aa37	9356ac3ec3e51459	481b8a6ee5e07031	9b04175ea8090daa
	1d05d9ba779a1a78	701f17d27582443b	e4d35b613a5ac420	ec9c5e98ff98760d
$t = 17$:	bf537b1f3edc7381	b889ed34abd7aa37	9356ac3ec3e51459	481b8a6ee5e07031
	c362ff9cf932951d	1d05d9ba779a1a78	701f17d27582443b	e4d35b613a5ac420
$t = 18$:	d4e44d54e8242ad8	bf537b1f3edc7381	b889ed34abd7aa37	9356ac3ec3e51459
	459e4e6888919f36	c362ff9cf932951d	1d05d9ba779a1a78	701f17d27582443b
$t = 19$:	05f3fba454e5de3d	d4e44d54e8242ad8	bf537b1f3edc7381	b889ed34abd7aa37
	caed4b5fa322b984	459e4e6888919f36	c362ff9cf932951d	1d05d9ba779a1a78
$t = 20$:	cdb73772dc0248bf	05f3fba454e5de3d	d4e44d54e8242ad8	bf537b1f3edc7381
	dc8049afa6acd502	caed4b5fa322b984	459e4e6888919f36	c362ff9cf932951d
$t = 21$:	1d47a3268ff677ed	cdb73772dc0248bf	05f3fba454e5de3d	d4e44d54e8242ad8

	8407818e9b28cc12	dc8049afa6acd502	caed4b5fa322b984	459e4e6888919f36
$t = 22$:	af4e23eb622d0df4	1d47a3268ff677ed	cdb73772dc0248bf	05f3fba454e5de3d
	64b5ae5424598428	8407818e9b28cc12	dc8049afa6acd502	caed4b5fa322b984
$t = 23$:	be50606778de14a6	af4e23eb622d0df4	1d47a3268ff677ed	cdb73772dc0248bf
	0a5d727cc92e7adb	64b5ae5424598428	8407818e9b28cc12	dc8049afa6acd502
$t = 24$:	821e44f6678ac478	be50606778de14a6	af4e23eb622d0df4	1d47a3268ff677ed
	f367e596d0a038a5	0a5d727cc92e7adb	64b5ae5424598428	8407818e9b28cc12
$t = 25$:	0c852b1359a77c18	821e44f6678ac478	be50606778de14a6	af4e23eb622d0df4
	6dec8a3396a80c3f	f367e596d0a038a5	0a5d727cc92e7adb	64b5ae5424598428
$t = 26$:	ebb574fad4b7a7e4	0c852b1359a77c18	821e44f6678ac478	be50606778de14a6
	a241e7efc1eb6ff9	6dec8a3396a80c3f	f367e596d0a038a5	0a5d727cc92e7adb
$t = 27$:	a092821c3cdf08da	ebb574fad4b7a7e4	0c852b1359a77c18	821e44f6678ac478
	c84e849917a7c08e	a241e7efc1eb6ff9	6dec8a3396a80c3f	f367e596d0a038a5
$t = 28$:	82ba2e1a2df2a4f1	a092821c3cdf08da	ebb574fad4b7a7e4	0c852b1359a77c18
	61845f6924789851	c84e849917a7c08e	a241e7efc1eb6ff9	6dec8a3396a80c3f
$t = 29$:	1959ad991c63d06a	82ba2e1a2df2a4f1	a092821c3cdf08da	ebb574fad4b7a7e4
	231faf24910a891a	61845f6924789851	c84e849917a7c08e	a241e7efc1eb6ff9
$t = 30$:	9b32d4cacd9a625b	1959ad991c63d06a	82ba2e1a2df2a4f1	a092821c3cdf08da
	533066919d608799	231faf24910a891a	61845f6924789851	c84e849917a7c08e
$t = 31$:	dc55339f4d841965	9b32d4cacd9a625b	1959ad991c63d06a	82ba2e1a2df2a4f1
	e2517f359998a58d	533066919d608799	231faf24910a891a	61845f6924789851
$t = 32$:	fdebb1283b12514f	dc55339f4d841965	9b32d4cacd9a625b	1959ad991c63d06a
	b1989170a183c661	e2517f359998a58d	533066919d608799	231faf24910a891a
$t = 33$:	b44c7975a83e3334	fdebb1283b12514f	dc55339f4d841965	9b32d4cacd9a625b
	009ad175b8d588a4	b1989170a183c661	e2517f359998a58d	533066919d608799
$t = 34$:	0bac61bfc53d18b7	b44c7975a83e3334	fdebb1283b12514f	dc55339f4d841965
	a7d5416d690557b8	009ad175b8d588a4	b1989170a183c661	e2517f359998a58d
$t = 35$:	392893c22e75856a	0bac61bfc53d18b7	b44c7975a83e3334	fdebb1283b12514f
	7a7c9eb7bc813248	a7d5416d690557b8	009ad175b8d588a4	b1989170a183c661
$t = 36$:	824408631432e09b	392893c22e75856a	0bac61bfc53d18b7	b44c7975a83e3334
	5e696a9fda56d6bf	7a7c9eb7bc813248	a7d5416d690557b8	009ad175b8d588a4
$t = 37$:	a64162f151a8c1cb	824408631432e09b	392893c22e75856a	0bac61bfc53d18b7
	0f57062401dc680b	5e696a9fda56d6bf	7a7c9eb7bc813248	a7d5416d690557b8
$t = 38$:	922537abad1e95a1	a64162f151a8c1cb	824408631432e09b	392893c22e75856a
	4f4c193d435ff721	0f57062401dc680b	5e696a9fda56d6bf	7a7c9eb7bc813248
$t = 39$:	b80591f6fbfadcde	922537abad1e95a1	a64162f151a8c1cb	824408631432e09b
	00f4407c0f37237e	4f4c193d435ff721	0f57062401dc680b	5e696a9fda56d6bf
$t = 40$:	08f151f4b8d0fa2e	b80591f6fbfadcde	922537abad1e95a1	a64162f151a8c1cb
	ec8b96fe402094cd	00f4407c0f37237e	4f4c193d435ff721	0f57062401dc680b
$t = 41$:	12b5fcc2b68f65c0	08f151f4b8d0fa2e	b80591f6fbfadcde	922537abad1e95a1
	d688101dfd24a148	ec8b96fe402094cd	00f4407c0f37237e	4f4c193d435ff721
$t = 42$:	a71bf5bd64289948	12b5fcc2b68f65c0	08f151f4b8d0fa2e	b80591f6fbfadcde
	e052bfb7a6945939	d688101dfd24a148	ec8b96fe402094cd	00f4407c0f37237e
$t = 43$:	890c2cd670c4aea3	a71bf5bd64289948	12b5fcc2b68f65c0	08f151f4b8d0fa2e
	dd13e4edeeff00e7	e052bfb7a6945939	d688101dfd24a148	ec8b96fe402094cd
$t = 44$:	ca61990b43297ffc	890c2cd670c4aea3	a71bf5bd64289948	12b5fcc2b68f65c0

	139aa55c51d9ee5f	dd13e4edeeff00e7	e052bfb7a6945939	d688101dfd24a148
$t = 45$:	7196e8fa538ba4bf	ca61990b43297ffc	890c2cd670c4aea3	a71bf5bd64289948
	046735513cdd14d3	139aa55c51d9ee5f	dd13e4edeeff00e7	e052bfb7a6945939
$t = 46$:	1f0720944dbeb6a4	7196e8fa538ba4bf	ca61990b43297ffc	890c2cd670c4aea3
	a41eb7e5a27588e3	046735513cdd14d3	139aa55c51d9ee5f	dd13e4edeeff00e7
$t = 47$:	d6d4f8608b8ab199	1f0720944dbeb6a4	7196e8fa538ba4bf	ca61990b43297ffc
	24b9c216f915da60	a41eb7e5a27588e3	046735513cdd14d3	139aa55c51d9ee5f
$t = 48$:	88761eb67845978e	d6d4f8608b8ab199	1f0720944dbeb6a4	7196e8fa538ba4bf
	9fe22e39448d50ed	24b9c216f915da60	a41eb7e5a27588e3	046735513cdd14d3
$t = 49$:	7d40e6be47d85702	88761eb67845978e	d6d4f8608b8ab199	1f0720944dbeb6a4
	d9c900e01968c33e	9fe22e39448d50ed	24b9c216f915da60	a41eb7e5a27588e3
$t = 50$:	7d0d988df5768598	7d40e6be47d85702	88761eb67845978e	d6d4f8608b8ab199
	2ec2e522a7c7d12c	d9c900e01968c33e	9fe22e39448d50ed	24b9c216f915da60
$t = 51$:	48a8b60575b37f31	7d0d988df5768598	7d40e6be47d85702	88761eb67845978e
	7059f9bc8c88a373	2ec2e522a7c7d12c	d9c900e01968c33e	9fe22e39448d50ed
$t = 52$:	6bc425af294bbf79	48a8b60575b37f31	7d0d988df5768598	7d40e6be47d85702
	6a8143b1716ee33d	7059f9bc8c88a373	2ec2e522a7c7d12c	d9c900e01968c33e
$t = 53$:	307a456158ee8849	6bc425af294bbf79	48a8b60575b37f31	7d0d988df5768598
	4372e85c16ee4440	6a8143b1716ee33d	7059f9bc8c88a373	2ec2e522a7c7d12c
$t = 54$:	af36382c8fd716be	307a456158ee8849	6bc425af294bbf79	48a8b60575b37f31
	a8f8b0033187a916	4372e85c16ee4440	6a8143b1716ee33d	7059f9bc8c88a373
$t = 55$:	810ebee951c64ca1	af36382c8fd716be	307a456158ee8849	6bc425af294bbf79
	16a64f5997b9cca6	a8f8b0033187a916	4372e85c16ee4440	6a8143b1716ee33d
$t = 56$:	2dd7659f1b4d13cd	810ebee951c64ca1	af36382c8fd716be	307a456158ee8849
	5da6793bb7286a4b	16a64f5997b9cca6	a8f8b0033187a916	4372e85c16ee4440
$t = 57$:	5ac712acff4b98be	2dd7659f1b4d13cd	810ebee951c64ca1	af36382c8fd716be
	91f6395b301adbfd	5da6793bb7286a4b	16a64f5997b9cca6	a8f8b0033187a916
$t = 58$:	c1af358833cb03c0	5ac712acff4b98be	2dd7659f1b4d13cd	810ebee951c64ca1
	d4883c0c21dda190	91f6395b301adbfd	5da6793bb7286a4b	16a64f5997b9cca6
$t = 59$:	88a306074d388c7d	c1af358833cb03c0	5ac712acff4b98be	2dd7659f1b4d13cd
	9fc52468b897f9c8	d4883c0c21dda190	91f6395b301adbfd	5da6793bb7286a4b
$t = 60$:	f11bfd0cf67d3040	88a306074d388c7d	c1af358833cb03c0	5ac712acff4b98be
	47efb6407f74d318	9fc52468b897f9c8	d4883c0c21dda190	91f6395b301adbfd
$t = 61$:	1f065e7828ed4e1b	f11bfd0cf67d3040	88a306074d388c7d	c1af358833cb03c0
	7481899904a4ce23	47efb6407f74d318	9fc52468b897f9c8	d4883c0c21dda190
$t = 62$:	aebde39f2bc42ec1	1f065e7828ed4e1b	f11bfd0cf67d3040	88a306074d388c7d
	62ab526ff177a988	7481899904a4ce23	47efb6407f74d318	9fc52468b897f9c8
$t = 63$:	d35a94706e3e5df2	aebde39f2bc42ec1	1f065e7828ed4e1b	f11bfd0cf67d3040
	53f92b648d5d815c	62ab526ff177a988	7481899904a4ce23	47efb6407f74d318
$t = 64$:	d72d727c53e09ab9	d35a94706e3e5df2	aebde39f2bc42ec1	1f065e7828ed4e1b
	10746426ba9824f4	53f92b648d5d815c	62ab526ff177a988	7481899904a4ce23
$t = 65$:	3a7235e5a4051d94	d72d727c53e09ab9	d35a94706e3e5df2	aebde39f2bc42ec1
	afe455daec5c2b00	10746426ba9824f4	53f92b648d5d815c	62ab526ff177a988
$t = 66$:	f7f510fe73ef7e76	3a7235e5a4051d94	d72d727c53e09ab9	d35a94706e3e5df2
	f1202c0bb7c4583f	afe455daec5c2b00	10746426ba9824f4	53f92b648d5d815c
$t = 67$:	23c2acfb393523e9	f7f510fe73ef7e76	3a7235e5a4051d94	d72d727c53e09ab9
	a0bc2a61044ac12e	f1202c0bb7c4583f	afe455daec5c2b00	10746426ba9824f4

$t = 68$:	0307d241a1ed7121	23c2acfb393523e9	f7f510fe73ef7e76	3a7235e5a4051d94
	fad5f38f1e0aea12	a0bc2a61044ac12e	f1202c0bb7c4583f	afe455daec5c2b00
$t = 69$:	191814d82f0a16fb	0307d241a1ed7121	23c2acfb393523e9	f7f510fe73ef7e76
	39d325086e66e200	fad5f38f1e0aea12	a0bc2a61044ac12e	f1202c0bb7c4583f
$t = 70$:	0a1ed41b6da18c01	191814d82f0a16fb	0307d241a1ed7121	23c2acfb393523e9
	b3d3521e166e5df1	39d325086e66e200	fad5f38f1e0aea12	a0bc2a61044ac12e
$t = 71$:	8a3f07db93f6c827	0a1ed41b6da18c01	191814d82f0a16fb	0307d241a1ed7121
	6b370074be040ed7	b3d3521e166e5df1	39d325086e66e200	fad5f38f1e0aea12
$t = 72$:	002744d87ef80d28	8a3f07db93f6c827	0a1ed41b6da18c01	191814d82f0a16fb
	8c5a245de2d72fe6	6b370074be040ed7	b3d3521e166e5df1	39d325086e66e200
$t = 73$:	778dc7880a4a2aa0	002744d87ef80d28	8a3f07db93f6c827	0a1ed41b6da18c01
	45a375b466e5e342	8c5a245de2d72fe6	6b370074be040ed7	b3d3521e166e5df1
$t = 74$:	a3f11de5ede05b11	778dc7880a4a2aa0	002744d87ef80d28	8a3f07db93f6c827
	f5bbf52f1ab7cc05	45a375b466e5e342	8c5a245de2d72fe6	6b370074be040ed7
$t = 75$:	629c8ae6ecd8af4b	a3f11de5ede05b11	778dc7880a4a2aa0	002744d87ef80d28
	5a8fe5919d3cf136	f5bbf52f1ab7cc05	45a375b466e5e342	8c5a245de2d72fe6
$t = 76$:	c9a8c1e2d063ce94	629c8ae6ecd8af4b	a3f11de5ede05b11	778dc7880a4a2aa0
	aacd089bfae8faf9	5a8fe5919d3cf136	f5bbf52f1ab7cc05	45a375b466e5e342
$t = 77$:	c517cba6a09bb26a	c9a8c1e2d063ce94	629c8ae6ecd8af4b	a3f11de5ede05b11
	e1682bd33c8f8e23	aacd089bfae8faf9	5a8fe5919d3cf136	f5bbf52f1ab7cc05
$t = 78$:	11e3570e06e3b74e	c517cba6a09bb26a	c9a8c1e2d063ce94	629c8ae6ecd8af4b
	075aabbade34fd01	e1682bd33c8f8e23	aacd089bfae8faf9	5a8fe5919d3cf136
$t = 79$:	d90f1b1237b3a561	11e3570e06e3b74e	c517cba6a09bb26a	c9a8c1e2d063ce94
	867983f69d3a3ad1	075aabbade34fd01	e1682bd33c8f8e23	aacd089bfae8faf9

That completes the processing of the first message block, $M^{(1)}$. The intermediate hash value, $H^{(1)}$, is calculated to be

$$H_0^{(1)} = \texttt{6a09e667f3bcc908} + \texttt{d90f1b1237b3a561} = \texttt{4319017a2b706e69}$$
$$H_1^{(1)} = \texttt{bb67ae8584caa73b} + \texttt{11e3570e06e3b74e} = \texttt{cd4b05938bae5e89}$$
$$H_2^{(1)} = \texttt{3c6ef372fe94f82b} + \texttt{c517cba6a09bb26a} = \texttt{0186bf199f30aa95}$$
$$H_3^{(1)} = \texttt{a54ff53a5f1d36f1} + \texttt{c9a8c1e2d063ce94} = \texttt{6ef8b71d2f810585}$$
$$H_4^{(1)} = \texttt{510e527fade682d1} + \texttt{867983f69d3a3ad1} = \texttt{d787d6764b20bda2}$$
$$H_5^{(1)} = \texttt{9b05688c2b3e6c1f} + \texttt{075aabbade34fd01} = \texttt{a260144709736920}$$
$$H_6^{(1)} = \texttt{1f83d9abfb41bd6b} + \texttt{e1682bd33c8f8e23} = \texttt{00ec057f37d14b8e}$$
$$H_7^{(1)} = \texttt{5be0cd19137e2179} + \texttt{aacd089bfae8faf9} = \texttt{06add5b50e671c72}.$$

The words of the *second* padded message block, $M^{(2)}$, are then assigned to the words $W_0,\ldots,W_{15}$ of the message schedule:

W_0 = 0000000000000000	W_8 = 0000000000000000
W_1 = 0000000000000000	W_9 = 0000000000000000
W_2 = 0000000000000000	W_{10} = 0000000000000000
W_3 = 0000000000000000	W_{11} = 0000000000000000
W_4 = 0000000000000000	W_{12} = 0000000000000000
W_5 = 0000000000000000	W_{13} = 0000000000000000
W_6 = 0000000000000000	W_{14} = 0000000000000000
W_7 = 0000000000000000	W_{15} = 0000000000000380.

The following schedule shows the hex values for ***a***, ***b***, ***c***, ***d***, ***e***, ***f***, ***g***, and ***h*** *after* pass *t* of the "for *t*=0 to 79" loop described in Sec. 6.1.2, step 4.

	a / ***e***	***b*** / ***f***	***c*** / ***g***	***d*** / ***h***
t = 0 :	b8fdb92bdfb187e8 1d5f4d5ad031b8e6	4319017a2b706e69 d787d6764b20bda2	cd4b05938bae5e89 a260144709736920	0186bf199f30aa95 00ec057f37d14b8e
t = 1 :	6eb90718369c5cd7 4b9b4877d987b0fe	b8fdb92bdfb187e8 1d5f4d5ad031b8e6	4319017a2b706e69 d787d6764b20bda2	cd4b05938bae5e89 a260144709736920
t = 2 :	c83451f2335d5144 d6b67350e0781e99	6eb90718369c5cd7 4b9b4877d987b0fe	b8fdb92bdfb187e8 1d5f4d5ad031b8e6	4319017a2b706e69 d787d6764b20bda2
t = 3 :	28ec1deb2a9ee6e3 25e3136be5999b8c	c83451f2335d5144 d6b67350e0781e99	6eb90718369c5cd7 4b9b4877d987b0fe	b8fdb92bdfb187e8 1d5f4d5ad031b8e6
t = 4 :	806abd86c0479e5b 1b8f7670eab1cf89	28ec1deb2a9ee6e3 25e3136be5999b8c	c83451f2335d5144 d6b67350e0781e99	6eb90718369c5cd7 4b9b4877d987b0fe
t = 5 :	234788f8a54aed38 4fabe51c67d5d156	806abd86c0479e5b 1b8f7670eab1cf89	28ec1deb2a9ee6e3 25e3136be5999b8c	c83451f2335d5144 d6b67350e0781e99
t = 6 :	01264f18257b5e2c 1c3506096b99de50	234788f8a54aed38 4fabe51c67d5d156	806abd86c0479e5b 1b8f7670eab1cf89	28ec1deb2a9ee6e3 25e3136be5999b8c
t = 7 :	5b14f38104dde991 13f8bfdc4001c362	01264f18257b5e2c 1c3506096b99de50	234788f8a54aed38 4fabe51c67d5d156	806abd86c0479e5b 1b8f7670eab1cf89
t = 8 :	f522574a41b2aac6 63a5f09617622ed2	5b14f38104dde991 13f8bfdc4001c362	01264f18257b5e2c 1c3506096b99de50	234788f8a54aed38 4fabe51c67d5d156
t = 9 :	6ec258b855afae5a 211e271d92770b36	f522574a41b2aac6 63a5f09617622ed2	5b14f38104dde991 13f8bfdc4001c362	01264f18257b5e2c 1c3506096b99de50
t = 10 :	9364214ba48b416c d64dcb6ec0fe5bac	6ec258b855afae5a 211e271d92770b36	f522574a41b2aac6 63a5f09617622ed2	5b14f38104dde991 13f8bfdc4001c362
t = 11 :	082ba62147ecbbd5 34fe78473b61266e	9364214ba48b416c d64dcb6ec0fe5bac	6ec258b855afae5a 211e271d92770b36	f522574a41b2aac6 63a5f09617622ed2
t = 12 :	5790f6ba82bba809 d491e309141dcaa3	082ba62147ecbbd5 34fe78473b61266e	9364214ba48b416c d64dcb6ec0fe5bac	6ec258b855afae5a 211e271d92770b36
t = 13 :	a6b8aefd086d33ce 044943c2992cc0f0	5790f6ba82bba809 d491e309141dcaa3	082ba62147ecbbd5 34fe78473b61266e	9364214ba48b416c d64dcb6ec0fe5bac
t = 14 :	bf2324a9a363abe7 0cf5f4bde5977c54	a6b8aefd086d33ce 044943c2992cc0f0	5790f6ba82bba809 d491e309141dcaa3	082ba62147ecbbd5 34fe78473b61266e
t = 15 :	00e8e32076a61aff	bf2324a9a363abe7	a6b8aefd086d33ce	5790f6ba82bba809

	43bf4eb269a2650c	0cf5f4bde5977c54	044943c2992cc0f0	d491e309141dcaa3
$t = 16$:	f0376dff66fff4a7	00e8e32076a61aff	bf2324a9a363abe7	a6b8aefd086d33ce
	69fa5896969e85b8	43bf4eb269a2650c	0cf5f4bde5977c54	044943c2992cc0f0
$t = 17$:	2fad194272cda857	f0376dff66fff4a7	00e8e32076a61aff	bf2324a9a363abe7
	ddb519d663b7b6ec	69fa5896969e85b8	43bf4eb269a2650c	0cf5f4bde5977c54
$t = 18$:	9ae56936e95325ac	2fad194272cda857	f0376dff66fff4a7	00e8e32076a61aff
	04ceb04676619057	ddb519d663b7b6ec	69fa5896969e85b8	43bf4eb269a2650c
$t = 19$:	d94ccb853f53433b	9ae56936e95325ac	2fad194272cda857	f0376dff66fff4a7
	dcdc0f45813fb5a2	04ceb04676619057	ddb519d663b7b6ec	69fa5896969e85b8
$t = 20$:	837f8075d2945995	d94ccb853f53433b	9ae56936e95325ac	2fad194272cda857
	272b5f79a91419d8	dcdc0f45813fb5a2	04ceb04676619057	ddb519d663b7b6ec
$t = 21$:	786bde689f7aa62d	837f8075d2945995	d94ccb853f53433b	9ae56936e95325ac
	566586e69ad3f487	272b5f79a91419d8	dcdc0f45813fb5a2	04ceb04676619057
$t = 22$:	276457f01812aa6f	786bde689f7aa62d	837f8075d2945995	d94ccb853f53433b
	e78fb8b0dfbbc62f	566586e69ad3f487	272b5f79a91419d8	dcdc0f45813fb5a2
$t = 23$:	0de519f5d6c2c298	276457f01812aa6f	786bde689f7aa62d	837f8075d2945995
	5ca3e5cd1a30b954	e78fb8b0dfbbc62f	566586e69ad3f487	272b5f79a91419d8
$t = 24$:	54314dff825e2b22	0de519f5d6c2c298	276457f01812aa6f	786bde689f7aa62d
	b81a51e0c96ccf77	5ca3e5cd1a30b954	e78fb8b0dfbbc62f	566586e69ad3f487
$t = 25$:	5d3f98dd7b29c363	54314dff825e2b22	0de519f5d6c2c298	276457f01812aa6f
	95d49494f5a0d14a	b81a51e0c96ccf77	5ca3e5cd1a30b954	e78fb8b0dfbbc62f
$t = 26$:	5e9da426aa7d4a58	5d3f98dd7b29c363	54314dff825e2b22	0de519f5d6c2c298
	d22cccad2e391cd4	95d49494f5a0d14a	b81a51e0c96ccf77	5ca3e5cd1a30b954
$t = 27$:	3b62dd973298ea43	5e9da426aa7d4a58	5d3f98dd7b29c363	54314dff825e2b22
	aceb5d06101e514e	d22cccad2e391cd4	95d49494f5a0d14a	b81a51e0c96ccf77
$t = 28$:	fd258ff809b2253d	3b62dd973298ea43	5e9da426aa7d4a58	5d3f98dd7b29c363
	26c991e85352da6f	aceb5d06101e514e	d22cccad2e391cd4	95d49494f5a0d14a
$t = 29$:	b462a20846af417d	fd258ff809b2253d	3b62dd973298ea43	5e9da426aa7d4a58
	291eee54c034c326	26c991e85352da6f	aceb5d06101e514e	d22cccad2e391cd4
$t = 30$:	d5471e3dc7171224	b462a20846af417d	fd258ff809b2253d	3b62dd973298ea43
	0aaf99c59e7fadbd	291eee54c034c326	26c991e85352da6f	aceb5d06101e514e
$t = 31$:	9ace856ba1290e6e	d5471e3dc7171224	b462a20846af417d	fd258ff809b2253d
	658f0bea63804d05	0aaf99c59e7fadbd	291eee54c034c326	26c991e85352da6f
$t = 32$:	80a0d154506b37c4	9ace856ba1290e6e	d5471e3dc7171224	b462a20846af417d
	bbe6e3b3bb7fefab	658f0bea63804d05	0aaf99c59e7fadbd	291eee54c034c326
$t = 33$:	fb90a8a76dea1bfe	80a0d154506b37c4	9ace856ba1290e6e	d5471e3dc7171224
	65234d5b5049e665	bbe6e3b3bb7fefab	658f0bea63804d05	0aaf99c59e7fadbd
$t = 34$:	f517b690d940a294	fb90a8a76dea1bfe	80a0d154506b37c4	9ace856ba1290e6e
	e4dd663f44d313bc	65234d5b5049e665	bbe6e3b3bb7fefab	658f0bea63804d05
$t = 35$:	b70883992932880d	f517b690d940a294	fb90a8a76dea1bfe	80a0d154506b37c4
	dc5dd7c12b1cb6e3	e4dd663f44d313bc	65234d5b5049e665	bbe6e3b3bb7fefab
$t = 36$:	b2a2be77b0fcf3bf	b70883992932880d	f517b690d940a294	fb90a8a76dea1bfe
	50fca57291e19874	dc5dd7c12b1cb6e3	e4dd663f44d313bc	65234d5b5049e665
$t = 37$:	8575839b0f08472b	b2a2be77b0fcf3bf	b70883992932880d	f517b690d940a294
	bd7176bd099bb2f2	50fca57291e19874	dc5dd7c12b1cb6e3	e4dd663f44d313bc
$t = 38$:	4405d2765de0adfc	8575839b0f08472b	b2a2be77b0fcf3bf	b70883992932880d

	7ca4916f2cd8db10	bd7176bd099bb2f2	50fca57291e19874	dc5dd7c12b1cb6e3
$t = 39$:	eec6fca5aa657661	4405d2765de0adfc	8575839b0f08472b	b2a2be77b0fcf3bf
	7be0b7e70bdabe53	7ca4916f2cd8db10	bd7176bd099bb2f2	50fca57291e19874
$t = 40$:	bb3fcd7585b59e32	eec6fca5aa657661	4405d2765de0adfc	8575839b0f08472b
	2201c7cbd34e31fe	7be0b7e70bdabe53	7ca4916f2cd8db10	bd7176bd099bb2f2
$t = 41$:	0e109efc47927341	bb3fcd7585b59e32	eec6fca5aa657661	4405d2765de0adfc
	d43e5686506fa05d	2201c7cbd34e31fe	7be0b7e70bdabe53	7ca4916f2cd8db10
$t = 42$:	55c0dba83bcdc6e0	0e109efc47927341	bb3fcd7585b59e32	eec6fca5aa657661
	5b634502f1671535	d43e5686506fa05d	2201c7cbd34e31fe	7be0b7e70bdabe53
$t = 43$:	f5756f847bfaef67	55c0dba83bcdc6e0	0e109efc47927341	bb3fcd7585b59e32
	e2d307fd94f4818a	5b634502f1671535	d43e5686506fa05d	2201c7cbd34e31fe
$t = 44$:	f1438c9cf271c06e	f5756f847bfaef67	55c0dba83bcdc6e0	0e109efc47927341
	ad8ac1ed966b2dc6	e2d307fd94f4818a	5b634502f1671535	d43e5686506fa05d
$t = 45$:	a7dcaffdbefb9d4a	f1438c9cf271c06e	f5756f847bfaef67	55c0dba83bcdc6e0
	9e46e9f915099c34	ad8ac1ed966b2dc6	e2d307fd94f4818a	5b634502f1671535
$t = 46$:	985ba373680b8e94	a7dcaffdbefb9d4a	f1438c9cf271c06e	f5756f847bfaef67
	7d4c0abc676b1a8b	9e46e9f915099c34	ad8ac1ed966b2dc6	e2d307fd94f4818a
$t = 47$:	807f45784852303f	985ba373680b8e94	a7dcaffdbefb9d4a	f1438c9cf271c06e
	082ee70d3f352aac	7d4c0abc676b1a8b	9e46e9f915099c34	ad8ac1ed966b2dc6
$t = 48$:	d9c523173b1a1e05	807f45784852303f	985ba373680b8e94	a7dcaffdbefb9d4a
	e301dca32c44ca05	082ee70d3f352aac	7d4c0abc676b1a8b	9e46e9f915099c34
$t = 49$:	b6df019ca515cafb	d9c523173b1a1e05	807f45784852303f	985ba373680b8e94
	754b3a461a665640	e301dca32c44ca05	082ee70d3f352aac	7d4c0abc676b1a8b
$t = 50$:	427a642921b2e645	b6df019ca515cafb	d9c523173b1a1e05	807f45784852303f
	08a30fefe981f2ec	754b3a461a665640	e301dca32c44ca05	082ee70d3f352aac
$t = 51$:	7aab58dbe1b9df7b	427a642921b2e645	b6df019ca515cafb	d9c523173b1a1e05
	2749c52d0b3d1225	08a30fefe981f2ec	754b3a461a665640	e301dca32c44ca05
$t = 52$:	974ddd552aec16ce	7aab58dbe1b9df7b	427a642921b2e645	b6df019ca515cafb
	a9e6cbfb416a591f	2749c52d0b3d1225	08a30fefe981f2ec	754b3a461a665640
$t = 53$:	55e0b99d4404f6ca	974ddd552aec16ce	7aab58dbe1b9df7b	427a642921b2e645
	6c24ad697b41b1b9	a9e6cbfb416a591f	2749c52d0b3d1225	08a30fefe981f2ec
$t = 54$:	901f632579ee1eee	55e0b99d4404f6ca	974ddd552aec16ce	7aab58dbe1b9df7b
	4ee99476db1bb7a9	6c24ad697b41b1b9	a9e6cbfb416a591f	2749c52d0b3d1225
$t = 55$:	f90db9f292a60463	901f632579ee1eee	55e0b99d4404f6ca	974ddd552aec16ce
	5401644992a1f8b8	4ee99476db1bb7a9	6c24ad697b41b1b9	a9e6cbfb416a591f
$t = 56$:	9b906a7df1007357	f90db9f292a60463	901f632579ee1eee	55e0b99d4404f6ca
	f5e402ee21db8915	5401644992a1f8b8	4ee99476db1bb7a9	6c24ad697b41b1b9
$t = 57$:	71a0a998fb48c0fc	9b906a7df1007357	f90db9f292a60463	901f632579ee1eee
	96bece755cd203cb	f5e402ee21db8915	5401644992a1f8b8	4ee99476db1bb7a9
$t = 58$:	c25e798e50752535	71a0a998fb48c0fc	9b906a7df1007357	f90db9f292a60463
	9d548440d8e110f2	96bece755cd203cb	f5e402ee21db8915	5401644992a1f8b8
$t = 59$:	1ce4f2591812e6ae	c25e798e50752535	71a0a998fb48c0fc	9b906a7df1007357
	b27252537a83cf27	9d548440d8e110f2	96bece755cd203cb	f5e402ee21db8915
$t = 60$:	c1700e250dc6ffed	1ce4f2591812e6ae	c25e798e50752535	71a0a998fb48c0fc
	970088839126bda5	b27252537a83cf27	9d548440d8e110f2	96bece755cd203cb
$t = 61$:	f8e6924412fd0c64	c1700e250dc6ffed	1ce4f2591812e6ae	c25e798e50752535
	d50cf4f73910e3ee	970088839126bda5	b27252537a83cf27	9d548440d8e110f2

t = 62 :	d53e0a39eee47528	f8e6924412fd0c64	c1700e250dc6ffed	1ce4f2591812e6ae
	1b6d7234ace15d7d	d50cf4f73910e3ee	970088839126bda5	b27252537a83cf27
t = 63 :	3960545ab926c0d5	d53e0a39eee47528	f8e6924412fd0c64	c1700e250dc6ffed
	9eabb5618b4fcd13	1b6d7234ace15d7d	d50cf4f73910e3ee	970088839126bda5
t = 64 :	b2c164d71abb92fe	3960545ab926c0d5	d53e0a39eee47528	f8e6924412fd0c64
	f1736fbbfb6ebe72	9eabb5618b4fcd13	1b6d7234ace15d7d	d50cf4f73910e3ee
t = 65 :	4d979e985b067e75	b2c164d71abb92fe	3960545ab926c0d5	d53e0a39eee47528
	d1fb300f35992350	f1736fbbfb6ebe72	9eabb5618b4fcd13	1b6d7234ace15d7d
t = 66 :	59d0238ce137abd7	4d979e985b067e75	b2c164d71abb92fe	3960545ab926c0d5
	5f3c64b7546e2cec	d1fb300f35992350	f1736fbbfb6ebe72	9eabb5618b4fcd13
t = 67 :	bf8d9453b9876b0a	59d0238ce137abd7	4d979e985b067e75	b2c164d71abb92fe
	6c27893a31b0e07e	5f3c64b7546e2cec	d1fb300f35992350	f1736fbbfb6ebe72
t = 68 :	c45dd4a2d2fea059	bf8d9453b9876b0a	59d0238ce137abd7	4d979e985b067e75
	48253e21b26d8cf9	6c27893a31b0e07e	5f3c64b7546e2cec	d1fb300f35992350
t = 69 :	e08471946c17b0b6	c45dd4a2d2fea059	bf8d9453b9876b0a	59d0238ce137abd7
	714e2adf4e23ff24	48253e21b26d8cf9	6c27893a31b0e07e	5f3c64b7546e2cec
t = 70 :	b4838c1c28fee7bc	e08471946c17b0b6	c45dd4a2d2fea059	bf8d9453b9876b0a
	371f12f333f7e5b9	714e2adf4e23ff24	48253e21b26d8cf9	6c27893a31b0e07e
t = 71 :	851cf60a77f6e6d1	b4838c1c28fee7bc	e08471946c17b0b6	c45dd4a2d2fea059
	a2a475deac0e8b42	371f12f333f7e5b9	714e2adf4e23ff24	48253e21b26d8cf9
t = 72 :	f53d23c50249af2d	851cf60a77f6e6d1	b4838c1c28fee7bc	e08471946c17b0b6
	1e99cae9d4cf0409	a2a475deac0e8b42	371f12f333f7e5b9	714e2adf4e23ff24
t = 73 :	b81e85d427045550	f53d23c50249af2d	851cf60a77f6e6d1	b4838c1c28fee7bc
	f5794711faa60f63	1e99cae9d4cf0409	a2a475deac0e8b42	371f12f333f7e5b9
t = 74 :	ae70c7d11ea84a83	b81e85d427045550	f53d23c50249af2d	851cf60a77f6e6d1
	dc0d633411c289b2	f5794711faa60f63	1e99cae9d4cf0409	a2a475deac0e8b42
t = 75 :	5c54592e13c76135	ae70c7d11ea84a83	b81e85d427045550	f53d23c50249af2d
	1620dd5479e94b9b	dc0d633411c289b2	f5794711faa60f63	1e99cae9d4cf0409
t = 76 :	03a0f79087078a93	5c54592e13c76135	ae70c7d11ea84a83	b81e85d427045550
	57e90fa678e4cc97	1620dd5479e94b9b	dc0d633411c289b2	f5794711faa60f63
t = 77 :	8df0baad4c6ed50c	03a0f79087078a93	5c54592e13c76135	ae70c7d11ea84a83
	c6e7246f7f0bdac6	57e90fa678e4cc97	1620dd5479e94b9b	dc0d633411c289b2
t = 78 :	bfa9f194894db5b6	8df0baad4c6ed50c	03a0f79087078a93	5c54592e13c76135
	90bb8597bb41da1a	c6e7246f7f0bdac6	57e90fa678e4cc97	1620dd5479e94b9b
t = 79 :	4b7c99fbaf72a571	bfa9f194894db5b6	8df0baad4c6ed50c	03a0f79087078a93
	78955227fde03a42	90bb8597bb41da1a	c6e7246f7f0bdac6	57e90fa678e4cc97

That completes the processing of the second and final message block, $M^{(2)}$. The final hash value, $H^{(2)}$, is calculated to be

$$H_0^{(2)} = \texttt{4319017a2b706e69} + \texttt{4b7c99fbaf72a571} = \texttt{8e959b75dae313da}$$
$$H_1^{(2)} = \texttt{cd4b05938bae5e89} + \texttt{bfa9f194894db5b6} = \texttt{8cf4f72814fc143f}$$
$$H_2^{(2)} = \texttt{0186bf199f30aa95} + \texttt{8df0baad4c6ed50c} = \texttt{8f7779c6eb9f7fa1}$$
$$H_3^{(2)} = \texttt{6ef8b71d2f810585} + \texttt{03a0f79087078a93} = \texttt{7299aeadb6889018}$$
$$H_4^{(2)} = \texttt{d787d6764b20bda2} + \texttt{78955227fde03a42} = \texttt{501d289e4900f7e4}$$

$H_5^{(2)}$ = a260144709736920 + 90bb8597bb41da1a = 331b99dec4b5433a

$H_6^{(2)}$ = 00ec057f37d14b8e + c6e7246f7f0bdac6 = c7d329eeb6dd2654

$H_7^{(2)}$ = 06add5b50e671c72 + 57e90fa678e4cc97 = 5e96e55b874be909.

The resulting 512-bit message digest is

```
8e959b75dae313da 8cf4f72814fc143f 8f7779c6eb9f7fa1 7299aeadb6889018
501d289e4900f7e4 331b99dec4b5433a c7d329eeb6dd2654 5e96e55b874be909.
```

C.3 SHA-512 Example (Long Message)

Let the message *M* be the binary-coded form of the ASCII string which consists of 1,000,000 repetitions of the character "**a**". The resulting SHA-512 message digest is

```
e718483d0ce76964 4e2e42c7bc15b463 8e1f98b13b204428 5632a803afa973eb
de0ff244877ea60a 4cb0432ce577c31b eb009c5c2c49aa2e 4eadb217ad8cc09b.
```

APPENDIX D: SHA-384 EXAMPLES

This appendix is for informational purposes only and is not required to meet the standard.

D.1 SHA-384 Example (One-Block Message)

Let the message, M, be the 24-bit ($\ell = 24$) ASCII string "**abc**", which is equivalent to the following binary string:

01100001 01100010 01100011.

The message is padded by appending a "1" bit, followed by 871 "0" bits, and ending with the hex value

0000000000000000 0000000000000018

(the two 64-bit word representation of the length, 24). Thus, the final padded message consists of one block (N=1).

For SHA-384, the initial hash value, $H^{(0)}$, is

$H_0^{(0)}$ = cbbb9d5dc1059ed8
$H_1^{(0)}$ = 629a292a367cd507
$H_2^{(0)}$ = 9159015a3070dd17
$H_3^{(0)}$ = 152fecd8f70e5939
$H_4^{(0)}$ = 67332667ffc00b31
$H_5^{(0)}$ = 8eb44a8768581511
$H_6^{(0)}$ = db0c2e0d64f98fa7
$H_7^{(0)}$ = 47b5481dbefa4fa4.

The words of the padded message block are then assigned to the words $W_0,\ldots,W_{15}$ of the message schedule:

W_0 = 6162638000000000
W_1 = 0000000000000000
W_2 = 0000000000000000
W_3 = 0000000000000000
W_4 = 0000000000000000
W_5 = 0000000000000000
W_6 = 0000000000000000
W_7 = 0000000000000000
W_8 = 0000000000000000
W_9 = 0000000000000000
W_{10} = 0000000000000000
W_{11} = 0000000000000000
W_{12} = 0000000000000000
W_{13} = 0000000000000000
W_{14} = 0000000000000000
W_{15} = 0000000000000018.

The following schedule shows the hex values for ***a***, ***b***, ***c***, ***d***, ***e***, ***f***, ***g***, and ***h*** *after* pass *t* of the "for *t*=0 to 79" loop described in Sec. 6.3.2, step 4.

	a / ***e***	***b*** / ***f***	***c*** / ***g***	***d*** / ***h***
t = 0 :	470994ad30873f88	cbbb9d5dc1059ed8	629a292a367cd507	9159015a3070dd17
	bd03f724be6075f9	67332667ffc00b31	8eb44a8768581511	db0c2e0d64f98fa7
t = 1 :	2e91230306a12ae0	470994ad30873f88	cbbb9d5dc1059ed8	629a292a367cd507
	5e1b4e1695372b9e	bd03f724be6075f9	67332667ffc00b31	8eb44a8768581511
t = 2 :	eebe5d379be707ad	2e91230306a12ae0	470994ad30873f88	cbbb9d5dc1059ed8
	54074a65aef34336	5e1b4e1695372b9e	bd03f724be6075f9	67332667ffc00b31
t = 3 :	e308483153e15ad6	eebe5d379be707ad	2e91230306a12ae0	470994ad30873f88
	086c5b2d36a89178	54074a65aef34336	5e1b4e1695372b9e	bd03f724be6075f9
t = 4 :	3a7a023c593d8479	e308483153e15ad6	eebe5d379be707ad	2e91230306a12ae0
	8aa1144850633794	086c5b2d36a89178	54074a65aef34336	5e1b4e1695372b9e
t = 5 :	333199a85f92b052	3a7a023c593d8479	e308483153e15ad6	eebe5d379be707ad
	7a6316f0ef047ce7	8aa1144850633794	086c5b2d36a89178	54074a65aef34336
t = 6 :	76f0741213dd2ef6	333199a85f92b052	3a7a023c593d8479	e308483153e15ad6
	74063cba385f0675	7a6316f0ef047ce7	8aa1144850633794	086c5b2d36a89178
t = 7 :	02f2a04d3aab1629	76f0741213dd2ef6	333199a85f92b052	3a7a023c593d8479
	1688b9bf14980fc0	74063cba385f0675	7a6316f0ef047ce7	8aa1144850633794
t = 8 :	73e5b2a1704a0349	02f2a04d3aab1629	76f0741213dd2ef6	333199a85f92b052
	fd00139f705907d0	1688b9bf14980fc0	74063cba385f0675	7a6316f0ef047ce7
t = 9 :	bf3f67ba12882648	73e5b2a1704a0349	02f2a04d3aab1629	76f0741213dd2ef6
	652e311d4f0a4257	fd00139f705907d0	1688b9bf14980fc0	74063cba385f0675
t = 10 :	33254508bb2ea48d	bf3f67ba12882648	73e5b2a1704a0349	02f2a04d3aab1629
	9e18991c4f39f0ba	652e311d4f0a4257	fd00139f705907d0	1688b9bf14980fc0
t = 11 :	c1fdb2a0205ea0e5	33254508bb2ea48d	bf3f67ba12882648	73e5b2a1704a0349
	04732e8bc4044582	9e18991c4f39f0ba	652e311d4f0a4257	fd00139f705907d0
t = 12 :	185f9ff038a50f39	c1fdb2a0205ea0e5	33254508bb2ea48d	bf3f67ba12882648
	8b4acfc4d2b8afe6	04732e8bc4044582	9e18991c4f39f0ba	652e311d4f0a4257
t = 13 :	e5f06744c0d7563a	185f9ff038a50f39	c1fdb2a0205ea0e5	33254508bb2ea48d
	2fa93d1ce9523015	8b4acfc4d2b8afe6	04732e8bc4044582	9e18991c4f39f0ba
t = 14 :	7e32dc0e9f414783	e5f06744c0d7563a	185f9ff038a50f39	c1fdb2a0205ea0e5
	3a9950aaa5e75884	2fa93d1ce9523015	8b4acfc4d2b8afe6	04732e8bc4044582
t = 15 :	1eab6159ae87ef6d	7e32dc0e9f414783	e5f06744c0d7563a	185f9ff038a50f39
	153b895cfbc436c5	3a9950aaa5e75884	2fa93d1ce9523015	8b4acfc4d2b8afe6
t = 16 :	33ef2cebbf1739aa	1eab6159ae87ef6d	7e32dc0e9f414783	e5f06744c0d7563a
	9d1a64baf1d366aa	153b895cfbc436c5	3a9950aaa5e75884	2fa93d1ce9523015
t = 17 :	7df1b65f1b87d6ca	33ef2cebbf1739aa	1eab6159ae87ef6d	7e32dc0e9f414783
	5b6e369d36e8e181	9d1a64baf1d366aa	153b895cfbc436c5	3a9950aaa5e75884
t = 18 :	63a24014a34bb0f6	7df1b65f1b87d6ca	33ef2cebbf1739aa	1eab6159ae87ef6d
	e13e610eae680d85	5b6e369d36e8e181	9d1a64baf1d366aa	153b895cfbc436c5
t = 19 :	f1aabd313309509b	63a24014a34bb0f6	7df1b65f1b87d6ca	33ef2cebbf1739aa
	674385f0d87db94f	e13e610eae680d85	5b6e369d36e8e181	9d1a64baf1d366aa

$t = 20$:	9ba737ae88a72c64	f1aabd313309509b	63a24014a34bb0f6	7df1b65f1b87d6ca
	3fc2614c43906c0f	674385f0d87db94f	e13e610eae680d85	5b6e369d36e8e181
$t = 21$:	042c2dc9a5bf558a	9ba737ae88a72c64	f1aabd313309509b	63a24014a34bb0f6
	19316bebc88e01f2	3fc2614c43906c0f	674385f0d87db94f	e13e610eae680d85
$t = 22$:	7799c75acc748c0f	042c2dc9a5bf558a	9ba737ae88a72c64	f1aabd313309509b
	a7bbd65bf64f58c8	19316bebc88e01f2	3fc2614c43906c0f	674385f0d87db94f
$t = 23$:	ccf99a80f92bf002	7799c75acc748c0f	042c2dc9a5bf558a	9ba737ae88a72c64
	e52a24fae4e8fc9b	a7bbd65bf64f58c8	19316bebc88e01f2	3fc2614c43906c0f
$t = 24$:	ae993474363efe68	ccf99a80f92bf002	7799c75acc748c0f	042c2dc9a5bf558a
	587f308d58681928	e52a24fae4e8fc9b	a7bbd65bf64f58c8	19316bebc88e01f2
$t = 25$:	335063d1a2aec92f	ae993474363efe68	ccf99a80f92bf002	7799c75acc748c0f
	c2d6d65e38c6ea79	587f308d58681928	e52a24fae4e8fc9b	a7bbd65bf64f58c8
$t = 26$:	53a78b0cca01ba37	335063d1a2aec92f	ae993474363efe68	ccf99a80f92bf002
	3b65a26c3c92c8f3	c2d6d65e38c6ea79	587f308d58681928	e52a24fae4e8fc9b
$t = 27$:	ab7ffa529f622930	53a78b0cca01ba37	335063d1a2aec92f	ae993474363efe68
	b9d8a2f2762901ea	3b65a26c3c92c8f3	c2d6d65e38c6ea79	587f308d58681928
$t = 28$:	e428bb43afe3d63e	ab7ffa529f622930	53a78b0cca01ba37	335063d1a2aec92f
	6a8527525f898726	b9d8a2f2762901ea	3b65a26c3c92c8f3	c2d6d65e38c6ea79
$t = 29$:	bbed541a5128088c	e428bb43afe3d63e	ab7ffa529f622930	53a78b0cca01ba37
	7973aadbde294be9	6a8527525f898726	b9d8a2f2762901ea	3b65a26c3c92c8f3
$t = 30$:	4c5c38df7ec8baf4	bbed541a5128088c	e428bb43afe3d63e	ab7ffa529f622930
	422ceea0200e9ee4	7973aadbde294be9	6a8527525f898726	b9d8a2f2762901ea
$t = 31$:	4ba456ec244033ed	4c5c38df7ec8baf4	bbed541a5128088c	e428bb43afe3d63e
	7cf40857056d86b0	422ceea0200e9ee4	7973aadbde294be9	6a8527525f898726
$t = 32$:	aa4a6ab2ac5f5dd8	4ba456ec244033ed	4c5c38df7ec8baf4	bbed541a5128088c
	ad2b1ecfb5bfc556	7cf40857056d86b0	422ceea0200e9ee4	7973aadbde294be9
$t = 33$:	9cb941f2ced774b3	aa4a6ab2ac5f5dd8	4ba456ec244033ed	4c5c38df7ec8baf4
	029f66c7b4569bf0	ad2b1ecfb5bfc556	7cf40857056d86b0	422ceea0200e9ee4
$t = 34$:	39265f358594de27	9cb941f2ced774b3	aa4a6ab2ac5f5dd8	4ba456ec244033ed
	3f7b1c260c82e54f	029f66c7b4569bf0	ad2b1ecfb5bfc556	7cf40857056d86b0
$t = 35$:	09cca487d39b02a1	39265f358594de27	9cb941f2ced774b3	aa4a6ab2ac5f5dd8
	4a22b37b58a5b1b0	3f7b1c260c82e54f	029f66c7b4569bf0	ad2b1ecfb5bfc556
$t = 36$:	d48d97ce438cf4f0	09cca487d39b02a1	39265f358594de27	9cb941f2ced774b3
	a239e00b8baa0410	4a22b37b58a5b1b0	3f7b1c260c82e54f	029f66c7b4569bf0
$t = 37$:	d6f41e25a8b634d6	d48d97ce438cf4f0	09cca487d39b02a1	39265f358594de27
	25755cb8179dd0b0	a239e00b8baa0410	4a22b37b58a5b1b0	3f7b1c260c82e54f
$t = 38$:	54078334358573b4	d6f41e25a8b634d6	d48d97ce438cf4f0	09cca487d39b02a1
	0e419fb0802b0efc	25755cb8179dd0b0	a239e00b8baa0410	4a22b37b58a5b1b0
$t = 39$:	db24f9a03f4fff6b	54078334358573b4	d6f41e25a8b634d6	d48d97ce438cf4f0
	d30e99b4b394b090	0e419fb0802b0efc	25755cb8179dd0b0	a239e00b8baa0410
$t = 40$:	3604c53a845efc37	db24f9a03f4fff6b	54078334358573b4	d6f41e25a8b634d6
	791b2b4af7338b99	d30e99b4b394b090	0e419fb0802b0efc	25755cb8179dd0b0
$t = 41$:	f41b1c0eee89bdc6	3604c53a845efc37	db24f9a03f4fff6b	54078334358573b4
	e319b77d9e4e87f9	791b2b4af7338b99	d30e99b4b394b090	0e419fb0802b0efc
$t = 42$:	36644ae374632e3a	f41b1c0eee89bdc6	3604c53a845efc37	db24f9a03f4fff6b
	458250878a3972b2	e319b77d9e4e87f9	791b2b4af7338b99	d30e99b4b394b090
$t = 43$:	88806f6ae9fcd65b	36644ae374632e3a	f41b1c0eee89bdc6	3604c53a845efc37

	cfde2e6ea54fa576	458250878a3972b2	e319b77d9e4e87f9	791b2b4af7338b99
$t = 44$:	51dcaa36995c301d	88806f6ae9fcd65b	36644ae374632e3a	f41b1c0eee89bdc6
	e37f778353998050	cfde2e6ea54fa576	458250878a3972b2	e319b77d9e4e87f9
$t = 45$:	ef5e3885a2f238df	51dcaa36995c301d	88806f6ae9fcd65b	36644ae374632e3a
	740e347f24e18fda	e37f778353998050	cfde2e6ea54fa576	458250878a3972b2
$t = 46$:	eb3753f4283f4818	ef5e3885a2f238df	51dcaa36995c301d	88806f6ae9fcd65b
	0ae48cf840bb8be9	740e347f24e18fda	e37f778353998050	cfde2e6ea54fa576
$t = 47$:	a6998d63a5d09e04	eb3753f4283f4818	ef5e3885a2f238df	51dcaa36995c301d
	e21095012ee0b72a	0ae48cf840bb8be9	740e347f24e18fda	e37f778353998050
$t = 48$:	d3698fb64df175b0	a6998d63a5d09e04	eb3753f4283f4818	ef5e3885a2f238df
	c2f0b90ffce80739	e21095012ee0b72a	0ae48cf840bb8be9	740e347f24e18fda
$t = 49$:	317a3b295b991914	d3698fb64df175b0	a6998d63a5d09e04	eb3753f4283f4818
	1cadff2e6cb5aa4d	c2f0b90ffce80739	e21095012ee0b72a	0ae48cf840bb8be9
$t = 50$:	0941da08148ba463	317a3b295b991914	d3698fb64df175b0	a6998d63a5d09e04
	833eb9a4bb5a073e	1cadff2e6cb5aa4d	c2f0b90ffce80739	e21095012ee0b72a
$t = 51$:	494ac238d68c3d0b	0941da08148ba463	317a3b295b991914	d3698fb64df175b0
	80c8fc138e645028	833eb9a4bb5a073e	1cadff2e6cb5aa4d	c2f0b90ffce80739
$t = 52$:	c87e9168db9e97de	494ac238d68c3d0b	0941da08148ba463	317a3b295b991914
	65cf7f6a829aca04	80c8fc138e645028	833eb9a4bb5a073e	1cadff2e6cb5aa4d
$t = 53$:	edb4448879391dbb	c87e9168db9e97de	494ac238d68c3d0b	0941da08148ba463
	7729c85475dd318f	65cf7f6a829aca04	80c8fc138e645028	833eb9a4bb5a073e
$t = 54$:	073775c2456dc7db	edb4448879391dbb	c87e9168db9e97de	494ac238d68c3d0b
	a9cca0b6266b1d77	7729c85475dd318f	65cf7f6a829aca04	80c8fc138e645028
$t = 55$:	54de8857b24afaf7	073775c2456dc7db	edb4448879391dbb	c87e9168db9e97de
	8de51cff2ae4b068	a9cca0b6266b1d77	7729c85475dd318f	65cf7f6a829aca04
$t = 56$:	8a9cdd80f7f09c05	54de8857b24afaf7	073775c2456dc7db	edb4448879391dbb
	a60ba5e9ebaeb96a	8de51cff2ae4b068	a9cca0b6266b1d77	7729c85475dd318f
$t = 57$:	3eeb22a7524d8d7f	8a9cdd80f7f09c05	54de8857b24afaf7	073775c2456dc7db
	e2e6830b139df58f	a60ba5e9ebaeb96a	8de51cff2ae4b068	a9cca0b6266b1d77
$t = 58$:	0ed77c9cde8883d3	3eeb22a7524d8d7f	8a9cdd80f7f09c05	54de8857b24afaf7
	38413a2052387a9e	e2e6830b139df58f	a60ba5e9ebaeb96a	8de51cff2ae4b068
$t = 59$:	e64e4135f9d30dbc	0ed77c9cde8883d3	3eeb22a7524d8d7f	8a9cdd80f7f09c05
	45b640454c75c349	38413a2052387a9e	e2e6830b139df58f	a60ba5e9ebaeb96a
$t = 60$:	1ca93a293d544328	e64e4135f9d30dbc	0ed77c9cde8883d3	3eeb22a7524d8d7f
	efbef83a35c0319e	45b640454c75c349	38413a2052387a9e	e2e6830b139df58f
$t = 61$:	3dc764f89e54043a	1ca93a293d544328	e64e4135f9d30dbc	0ed77c9cde8883d3
	a57784945550cf94	efbef83a35c0319e	45b640454c75c349	38413a2052387a9e
$t = 62$:	56fb5883f1c87a05	3dc764f89e54043a	1ca93a293d544328	e64e4135f9d30dbc
	f5198a41eb80e022	a57784945550cf94	efbef83a35c0319e	45b640454c75c349
$t = 63$:	24a1124262a331c7	56fb5883f1c87a05	3dc764f89e54043a	1ca93a293d544328
	06edacae6e7b54ad	f5198a41eb80e022	a57784945550cf94	efbef83a35c0319e
$t = 64$:	eb85d19201c89694	24a1124262a331c7	56fb5883f1c87a05	3dc764f89e54043a
	9ced24983eec8723	06edacae6e7b54ad	f5198a41eb80e022	a57784945550cf94
$t = 65$:	cc981ab3a59c1db4	eb85d19201c89694	24a1124262a331c7	56fb5883f1c87a05
	eac5516336bc8882	9ced24983eec8723	06edacae6e7b54ad	f5198a41eb80e022
$t = 66$:	ceef5d997e148b44	cc981ab3a59c1db4	eb85d19201c89694	24a1124262a331c7
	617bbf70bb165212	eac5516336bc8882	9ced24983eec8723	06edacae6e7b54ad

$t = 67$:	689edf608a8e3f14	ceef5d997e148b44	cc981ab3a59c1db4	eb85d19201c89694
	3280d88472c100fd	617bbf70bb165212	eac5516336bc8882	9ced24983eec8723
$t = 68$:	1e6e0255ab88079f	689edf608a8e3f14	ceef5d997e148b44	cc981ab3a59c1db4
	f2001138439902b1	3280d88472c100fd	617bbf70bb165212	eac5516336bc8882
$t = 69$:	8c5d3b7fdad66e70	1e6e0255ab88079f	689edf608a8e3f14	ceef5d997e148b44
	90d18ec8b69f0345	f2001138439902b1	3280d88472c100fd	617bbf70bb165212
$t = 70$:	32e5ed8655871e9b	8c5d3b7fdad66e70	1e6e0255ab88079f	689edf608a8e3f14
	51105f6241313777	90d18ec8b69f0345	f2001138439902b1	3280d88472c100fd
$t = 71$:	bcd5061679be7336	32e5ed8655871e9b	8c5d3b7fdad66e70	1e6e0255ab88079f
	454b99f654443ad0	51105f6241313777	90d18ec8b69f0345	f2001138439902b1
$t = 72$:	e7d913b6678e78ef	bcd5061679be7336	32e5ed8655871e9b	8c5d3b7fdad66e70
	1ff613b5aa63776e	454b99f654443ad0	51105f6241313777	90d18ec8b69f0345
$t = 73$:	e6b8cb8dfa3475ab	e7d913b6678e78ef	bcd5061679be7336	32e5ed8655871e9b
	2e75f34303d39bb0	1ff613b5aa63776e	454b99f654443ad0	51105f6241313777
$t = 74$:	fdd4a30e168c4ae5	e6b8cb8dfa3475ab	e7d913b6678e78ef	bcd5061679be7336
	83a35dbe2a64fc26	2e75f34303d39bb0	1ff613b5aa63776e	454b99f654443ad0
$t = 75$:	12aeb6268dfa3e14	fdd4a30e168c4ae5	e6b8cb8dfa3475ab	e7d913b6678e78ef
	f660943b276786f7	83a35dbe2a64fc26	2e75f34303d39bb0	1ff613b5aa63776e
$t = 76$:	055b73814cf102b4	12aeb6268dfa3e14	fdd4a30e168c4ae5	e6b8cb8dfa3475ab
	c4b149710f5d6a71	f660943b276786f7	83a35dbe2a64fc26	2e75f34303d39bb0
$t = 77$:	95d33150de6df44c	055b73814cf102b4	12aeb6268dfa3e14	fdd4a30e168c4ae5
	c7f7bff08ebf0d30	c4b149710f5d6a71	f660943b276786f7	83a35dbe2a64fc26
$t = 78$:	5306143f64497b00	95d33150de6df44c	055b73814cf102b4	12aeb6268dfa3e14
	ca06a219cc701096	c7f7bff08ebf0d30	c4b149710f5d6a71	f660943b276786f7
$t = 79$:	ff44d7e1849dbfb3	5306143f64497b00	95d33150de6df44c	055b73814cf102b4
	1952e0c3a227c0f2	ca06a219cc701096	c7f7bff08ebf0d30	c4b149710f5d6a71

That completes the processing of the first and only message block, $M^{(1)}$. The final hash value, $H^{(1)}$, is calculated to be

$$H_0^{(1)} = \texttt{cbbb9d5dc1059ed8} + \texttt{ff44d7e1849dbfb3} = \texttt{cb00753f45a35e8b}$$
$$H_1^{(1)} = \texttt{629a292a367cd507} + \texttt{5306143f64497b00} = \texttt{b5a03d699ac65007}$$
$$H_2^{(1)} = \texttt{9159015a3070dd17} + \texttt{95d33150de6df44c} = \texttt{272c32ab0eded163}$$
$$H_3^{(1)} = \texttt{152fecd8f70e5939} + \texttt{055b73814cf102b4} = \texttt{1a8b605a43ff5bed}$$
$$H_4^{(1)} = \texttt{67332667ffc00b31} + \texttt{1952e0c3a227c0f2} = \texttt{8086072ba1e7cc23}$$
$$H_5^{(1)} = \texttt{8eb44a8768581511} + \texttt{ca06a219cc701096} = \texttt{58baeca134c825a7}$$
$$H_6^{(1)} = \texttt{db0c2e0d64f98fa7} + \texttt{c7f7bff08ebf0d30} = \texttt{a303edfdf3b89cd7}$$
$$H_7^{(1)} = \texttt{47b5481dbefa4fa4} + \texttt{c4b149710f5d6a71} = \texttt{0c66918ece57ba15.}$$

The final hash value is truncated to its left-most 384 bits (i.e., $H_0^{(1)}, \ldots, H_5^{(1)}$), resulting in the 384-bit message digest

```
cb00753f45a35e8b b5a03d699ac65007 272c32ab0eded163 1a8b605a43ff5bed
8086072ba1e7cc23 58baeca134c825a7.
```

D.2 SHA-384 Example (Multi-Block Message)

Let the message, *M*, be the 896-bit ($\ell = 896$) ASCII string

"**abcdefghbcdefghicdefghijdefghijkefghijklfghijklmghijklmn**
hijklmnoijklmnopjklmnopqklmnopqrlmnopqrsmnopqrstnopqrstu".

The message is padded by appending a "1" bit, followed by 1023 "0" bits, and ending with the hex value

0000000000000000 0000000000000380

(the two 64-bit word representation of the length, 896). Thus, the final padded message consists of two blocks (*N*=2).

For SHA-384, the initial hash value, $H^{(0)}$, is

$H_0^{(0)}$ = cbbb9d5dc1059ed8
$H_1^{(0)}$ = 629a292a367cd507
$H_2^{(0)}$ = 9159015a3070dd17
$H_3^{(0)}$ = 152fecd8f70e5939
$H_4^{(0)}$ = 67332667ffc00b31
$H_5^{(0)}$ = 8eb44a8768581511
$H_6^{(0)}$ = db0c2e0d64f98fa7
$H_7^{(0)}$ = 47b5481dbefa4fa4.

The words of the padded message block are then assigned to the words $W_0,\ldots,W_{15}$ of the message schedule:

W_0 = 6162636465666768
W_1 = 6263646566676869
W_2 = 636465666768696a
W_3 = 6465666768696a6b
W_4 = 65666768696a6b6c
W_5 = 666768696a6b6c6d
W_6 = 6768696a6b6c6d6e
W_7 = 68696a6b6c6d6e6f
W_8 = 696a6b6c6d6e6f70
W_9 = 6a6b6c6d6e6f7071
W_{10} = 6b6c6d6e6f707172
W_{11} = 6c6d6e6f70717273
W_{12} = 6d6e6f7071727374
W_{13} = 6e6f707172737475
W_{14} = 8000000000000000
W_{15} = 0000000000000000.

The following schedule shows the hex values for ***a***, ***b***, ***c***, ***d***, ***e***, ***f***, ***g***, and ***h*** *after* pass *t* of the "for *t*=0 to 79" loop described in Sec. 6.3.2, step 4.

	a / ***e***	***b*** / ***f***	***c*** / ***g***	***d*** / ***h***
$t = 0$:	4709949195eda6f0	cbbb9d5dc1059ed8	629a292a367cd507	9159015a3070dd17
	bd03f70923c6dd61	67332667ffc00b31	8eb44a8768581511	db0c2e0d64f98fa7
$t = 1$:	78d3f8bc03a38303	4709949195eda6f0	cbbb9d5dc1059ed8	629a292a367cd507
	ae067f071cd18a36	bd03f70923c6dd61	67332667ffc00b31	8eb44a8768581511
$t = 2$:	ed59d30beff95306	78d3f8bc03a38303	4709949195eda6f0	cbbb9d5dc1059ed8
	c180c7a74ed5cf1f	ae067f071cd18a36	bd03f70923c6dd61	67332667ffc00b31
$t = 3$:	8e7fe2aba3168f2b	ed59d30beff95306	78d3f8bc03a38303	4709949195eda6f0
	d92d19667920b327	c180c7a74ed5cf1f	ae067f071cd18a36	bd03f70923c6dd61
$t = 4$:	1174f9b374a9263a	8e7fe2aba3168f2b	ed59d30beff95306	78d3f8bc03a38303
	dd371f2d13661c52	d92d19667920b327	c180c7a74ed5cf1f	ae067f071cd18a36
$t = 5$:	27aaafb7fbef806b	1174f9b374a9263a	8e7fe2aba3168f2b	ed59d30beff95306
	21af3c6430a9af9c	dd371f2d13661c52	d92d19667920b327	c180c7a74ed5cf1f
$t = 6$:	b352d03a0bd34d65	27aaafb7fbef806b	1174f9b374a9263a	8e7fe2aba3168f2b
	69397de9a30e1473	21af3c6430a9af9c	dd371f2d13661c52	d92d19667920b327
$t = 7$:	412db7f990563d7c	b352d03a0bd34d65	27aaafb7fbef806b	1174f9b374a9263a
	5062fd5924e2b62e	69397de9a30e1473	21af3c6430a9af9c	dd371f2d13661c52
$t = 8$:	0f79040546e6edf7	412db7f990563d7c	b352d03a0bd34d65	27aaafb7fbef806b
	6b6c511b25a6bdbc	5062fd5924e2b62e	69397de9a30e1473	21af3c6430a9af9c
$t = 9$:	ebf02410f67b8ee7	0f79040546e6edf7	412db7f990563d7c	b352d03a0bd34d65
	dac695b91543ae80	6b6c511b25a6bdbc	5062fd5924e2b62e	69397de9a30e1473
$t = 10$:	97aa05d89b8dbe6d	ebf02410f67b8ee7	0f79040546e6edf7	412db7f990563d7c
	83b8b72646c0b598	dac695b91543ae80	6b6c511b25a6bdbc	5062fd5924e2b62e
$t = 11$:	23d0a36b692118eb	97aa05d89b8dbe6d	ebf02410f67b8ee7	0f79040546e6edf7
	a5f6c5155e221e8c	83b8b72646c0b598	dac695b91543ae80	6b6c511b25a6bdbc
$t = 12$:	e1041368d2fca1a2	23d0a36b692118eb	97aa05d89b8dbe6d	ebf02410f67b8ee7
	ae01675bfb003180	a5f6c5155e221e8c	83b8b72646c0b598	dac695b91543ae80
$t = 13$:	45bd6f69efec540d	e1041368d2fca1a2	23d0a36b692118eb	97aa05d89b8dbe6d
	c35cc50c1cf7ef98	ae01675bfb003180	a5f6c5155e221e8c	83b8b72646c0b598
$t = 14$:	c237fa23abb9bc16	45bd6f69efec540d	e1041368d2fca1a2	23d0a36b692118eb
	a16c4f134b28923e	c35cc50c1cf7ef98	ae01675bfb003180	a5f6c5155e221e8c
$t = 15$:	b4092df1c0f81853	c237fa23abb9bc16	45bd6f69efec540d	e1041368d2fca1a2
	008178e17fa649f2	a16c4f134b28923e	c35cc50c1cf7ef98	ae01675bfb003180
$t = 16$:	21e5c91d11809c13	b4092df1c0f81853	c237fa23abb9bc16	45bd6f69efec540d
	a26dfa04ed8c9b63	008178e17fa649f2	a16c4f134b28923e	c35cc50c1cf7ef98
$t = 17$:	2c957137cd4304a5	21e5c91d11809c13	b4092df1c0f81853	c237fa23abb9bc16
	6be210614b10949b	a26dfa04ed8c9b63	008178e17fa649f2	a16c4f134b28923e
$t = 18$:	2180e61afe322bc7	2c957137cd4304a5	21e5c91d11809c13	b4092df1c0f81853
	76396996200065f7	6be210614b10949b	a26dfa04ed8c9b63	008178e17fa649f2
$t = 19$:	f2911c11c96e5ff5	2180e61afe322bc7	2c957137cd4304a5	21e5c91d11809c13
	1bc2160f4f3711dc	76396996200065f7	6be210614b10949b	a26dfa04ed8c9b63
$t = 20$:	5eab10b19a5143a8	f2911c11c96e5ff5	2180e61afe322bc7	2c957137cd4304a5
	98d2b19d201f2bb6	1bc2160f4f3711dc	76396996200065f7	6be210614b10949b
$t = 21$:	29c5348d87cd5590	5eab10b19a5143a8	f2911c11c96e5ff5	2180e61afe322bc7

	4324c8caccf7753c	98d2b19d201f2bb6	1bc2160f4f3711dc	76396996200065f7
$t = 22$:	33c6b4a0166b7c9c	29c5348d87cd5590	5eab10b19a5143a8	f2911c11c96e5ff5
	d49cef5bd2dec121	4324c8caccf7753c	98d2b19d201f2bb6	1bc2160f4f3711dc
$t = 23$:	1db4ee606d2a7a96	33c6b4a0166b7c9c	29c5348d87cd5590	5eab10b19a5143a8
	b17d15b397521ab3	d49cef5bd2dec121	4324c8caccf7753c	98d2b19d201f2bb6
$t = 24$:	5cef5b2f00142660	1db4ee606d2a7a96	33c6b4a0166b7c9c	29c5348d87cd5590
	789e540f22e13932	b17d15b397521ab3	d49cef5bd2dec121	4324c8caccf7753c
$t = 25$:	ff74f4a162435903	5cef5b2f00142660	1db4ee606d2a7a96	33c6b4a0166b7c9c
	6c0be33dcc6e7572	789e540f22e13932	b17d15b397521ab3	d49cef5bd2dec121
$t = 26$:	41740b736e9676a9	ff74f4a162435903	5cef5b2f00142660	1db4ee606d2a7a96
	d8e401251592da6c	6c0be33dcc6e7572	789e540f22e13932	b17d15b397521ab3
$t = 27$:	931059fe9279ff1d	41740b736e9676a9	ff74f4a162435903	5cef5b2f00142660
	7f31116887eea596	d8e401251592da6c	6c0be33dcc6e7572	789e540f22e13932
$t = 28$:	356d08d982e2ead4	931059fe9279ff1d	41740b736e9676a9	ff74f4a162435903
	40c28c34b1bbe906	7f31116887eea596	d8e401251592da6c	6c0be33dcc6e7572
$t = 29$:	89dc825e7235c74b	356d08d982e2ead4	931059fe9279ff1d	41740b736e9676a9
	7a499ae05da50bf2	40c28c34b1bbe906	7f31116887eea596	d8e401251592da6c
$t = 30$:	97901f333e662fdc	89dc825e7235c74b	356d08d982e2ead4	931059fe9279ff1d
	4472b2e331ddfab4	7a499ae05da50bf2	40c28c34b1bbe906	7f31116887eea596
$t = 31$:	69c8f40eb38b6022	97901f333e662fdc	89dc825e7235c74b	356d08d982e2ead4
	177589502dd39aa2	4472b2e331ddfab4	7a499ae05da50bf2	40c28c34b1bbe906
$t = 32$:	4920943ffe52b207	69c8f40eb38b6022	97901f333e662fdc	89dc825e7235c74b
	6b813a0d0cdf4991	177589502dd39aa2	4472b2e331ddfab4	7a499ae05da50bf2
$t = 33$:	b4cb0df332d108ab	4920943ffe52b207	69c8f40eb38b6022	97901f333e662fdc
	8fe3d28097f18618	6b813a0d0cdf4991	177589502dd39aa2	4472b2e331ddfab4
$t = 34$:	e7748fbf744a5240	b4cb0df332d108ab	4920943ffe52b207	69c8f40eb38b6022
	0d7ab03208f1d7a5	8fe3d28097f18618	6b813a0d0cdf4991	177589502dd39aa2
$t = 35$:	7416ca18d9e265e0	e7748fbf744a5240	b4cb0df332d108ab	4920943ffe52b207
	11200c2d47c082f8	0d7ab03208f1d7a5	8fe3d28097f18618	6b813a0d0cdf4991
$t = 36$:	75476f5456e82f9c	7416ca18d9e265e0	e7748fbf744a5240	b4cb0df332d108ab
	3024702447f76224	11200c2d47c082f8	0d7ab03208f1d7a5	8fe3d28097f18618
$t = 37$:	f638a568b53a2f8f	75476f5456e82f9c	7416ca18d9e265e0	e7748fbf744a5240
	6217c1c02153302c	3024702447f76224	11200c2d47c082f8	0d7ab03208f1d7a5
$t = 38$:	c418f6f90602c79a	f638a568b53a2f8f	75476f5456e82f9c	7416ca18d9e265e0
	87f0901c227adbb3	6217c1c02153302c	3024702447f76224	11200c2d47c082f8
$t = 39$:	4f1f4f21df3dcf43	c418f6f90602c79a	f638a568b53a2f8f	75476f5456e82f9c
	fb7c63fcddf4a1c2	87f0901c227adbb3	6217c1c02153302c	3024702447f76224
$t = 40$:	13eb82e4b98d0e67	4f1f4f21df3dcf43	c418f6f90602c79a	f638a568b53a2f8f
	fb6c0e54d48d4f2d	fb7c63fcddf4a1c2	87f0901c227adbb3	6217c1c02153302c
$t = 41$:	820e75046567bace	13eb82e4b98d0e67	4f1f4f21df3dcf43	c418f6f90602c79a
	b16a9397472f0123	fb6c0e54d48d4f2d	fb7c63fcddf4a1c2	87f0901c227adbb3
$t = 42$:	741fa5dc290dd02c	820e75046567bace	13eb82e4b98d0e67	4f1f4f21df3dcf43
	ed40c88214823792	b16a9397472f0123	fb6c0e54d48d4f2d	fb7c63fcddf4a1c2
$t = 43$:	a4809bf6da6aa8bd	741fa5dc290dd02c	820e75046567bace	13eb82e4b98d0e67
	bec3d7e88c855194	ed40c88214823792	b16a9397472f0123	fb6c0e54d48d4f2d
$t = 44$:	d70b1aa4c800979c	a4809bf6da6aa8bd	741fa5dc290dd02c	820e75046567bace

	4962f310bdbd54b0	bec3d7e88c855194	ed40c88214823792	b16a9397472f0123
$t = 45$:	9a195492cfdb4745	d70b1aa4c800979c	a4809bf6da6aa8bd	741fa5dc290dd02c
	2c82d09cf05cf687	4962f310bdbd54b0	bec3d7e88c855194	ed40c88214823792
$t = 46$:	b7e68364f07f017e	9a195492cfdb4745	d70b1aa4c800979c	a4809bf6da6aa8bd
	2a1ffb84031b1b6c	2c82d09cf05cf687	4962f310bdbd54b0	bec3d7e88c855194
$t = 47$:	0e574b8e0b35e452	b7e68364f07f017e	9a195492cfdb4745	d70b1aa4c800979c
	29bdab29ee472a23	2a1ffb84031b1b6c	2c82d09cf05cf687	4962f310bdbd54b0
$t = 48$:	c176009cf82fa842	0e574b8e0b35e452	b7e68364f07f017e	9a195492cfdb4745
	cca47fbe31b335f4	29bdab29ee472a23	2a1ffb84031b1b6c	2c82d09cf05cf687
$t = 49$:	5d4f78c7a9bdbed2	c176009cf82fa842	0e574b8e0b35e452	b7e68364f07f017e
	eaf198615e99ffdc	cca47fbe31b335f4	29bdab29ee472a23	2a1ffb84031b1b6c
$t = 50$:	51ab3be828d8d13c	5d4f78c7a9bdbed2	c176009cf82fa842	0e574b8e0b35e452
	bd527cd188fb59ae	eaf198615e99ffdc	cca47fbe31b335f4	29bdab29ee472a23
$t = 51$:	4d639ef80d0f6d3e	51ab3be828d8d13c	5d4f78c7a9bdbed2	c176009cf82fa842
	b2611b90f90d732f	bd527cd188fb59ae	eaf198615e99ffdc	cca47fbe31b335f4
$t = 52$:	bba9c9efe0fbc6c8	4d639ef80d0f6d3e	51ab3be828d8d13c	5d4f78c7a9bdbed2
	fc0579337591a2c9	b2611b90f90d732f	bd527cd188fb59ae	eaf198615e99ffdc
$t = 53$:	3405d7cad2e8a689	bba9c9efe0fbc6c8	4d639ef80d0f6d3e	51ab3be828d8d13c
	0f6649f64ec8e109	fc0579337591a2c9	b2611b90f90d732f	bd527cd188fb59ae
$t = 54$:	ea54d908505798b3	3405d7cad2e8a689	bba9c9efe0fbc6c8	4d639ef80d0f6d3e
	ef48a48999108077	0f6649f64ec8e109	fc0579337591a2c9	b2611b90f90d732f
$t = 55$:	be31d1c0ccc143bc	ea54d908505798b3	3405d7cad2e8a689	bba9c9efe0fbc6c8
	4fc2d4cad0c91afc	ef48a48999108077	0f6649f64ec8e109	fc0579337591a2c9
$t = 56$:	285a76d23f6a0073	be31d1c0ccc143bc	ea54d908505798b3	3405d7cad2e8a689
	a730855599b738a3	4fc2d4cad0c91afc	ef48a48999108077	0f6649f64ec8e109
$t = 57$:	a714ceff14bebc24	285a76d23f6a0073	be31d1c0ccc143bc	ea54d908505798b3
	53c581dae1831d80	a730855599b738a3	4fc2d4cad0c91afc	ef48a48999108077
$t = 58$:	697ca14913a50a26	a714ceff14bebc24	285a76d23f6a0073	be31d1c0ccc143bc
	34d39344354aacd2	53c581dae1831d80	a730855599b738a3	4fc2d4cad0c91afc
$t = 59$:	3a38fa3775d7007c	697ca14913a50a26	a714ceff14bebc24	285a76d23f6a0073
	e26f3a21e9a27691	34d39344354aacd2	53c581dae1831d80	a730855599b738a3
$t = 60$:	44ea14d8e450c844	3a38fa3775d7007c	697ca14913a50a26	a714ceff14bebc24
	5319374fb88dd485	e26f3a21e9a27691	34d39344354aacd2	53c581dae1831d80
$t = 61$:	0928b75c925f91e2	44ea14d8e450c844	3a38fa3775d7007c	697ca14913a50a26
	79f4be3c5a372911	5319374fb88dd485	e26f3a21e9a27691	34d39344354aacd2
$t = 62$:	6db5469fa19c0e27	0928b75c925f91e2	44ea14d8e450c844	3a38fa3775d7007c
	16beec0fec168e79	79f4be3c5a372911	5319374fb88dd485	e26f3a21e9a27691
$t = 63$:	384e3159898a7362	6db5469fa19c0e27	0928b75c925f91e2	44ea14d8e450c844
	55fa3ad1102298a8	16beec0fec168e79	79f4be3c5a372911	5319374fb88dd485
$t = 64$:	483c64d3fdebf828	384e3159898a7362	6db5469fa19c0e27	0928b75c925f91e2
	1a238431921ea75e	55fa3ad1102298a8	16beec0fec168e79	79f4be3c5a372911
$t = 65$:	c9464988a1939bcf	483c64d3fdebf828	384e3159898a7362	6db5469fa19c0e27
	e3f3f08ac90f86cd	1a238431921ea75e	55fa3ad1102298a8	16beec0fec168e79
$t = 66$:	98bc93bca795059c	c9464988a1939bcf	483c64d3fdebf828	384e3159898a7362
	9e04fb49a5fd91de	e3f3f08ac90f86cd	1a238431921ea75e	55fa3ad1102298a8
$t = 67$:	b6fc101ad1d74e20	98bc93bca795059c	c9464988a1939bcf	483c64d3fdebf828
	fd13cd3620f6c1f4	9e04fb49a5fd91de	e3f3f08ac90f86cd	1a238431921ea75e

$t = 68$:	fac26e6e4da4705d	b6fc101ad1d74e20	98bc93bca795059c	c9464988a1939bcf
	0d60228aa6e55b6e	fd13cd3620f6c1f4	9e04fb49a5fd91de	e3f3f08ac90f86cd
$t = 69$:	2a630c58cc27fcaa	fac26e6e4da4705d	b6fc101ad1d74e20	98bc93bca795059c
	a2f7f27a3ec25aba	0d60228aa6e55b6e	fd13cd3620f6c1f4	9e04fb49a5fd91de
$t = 70$:	159a02d4faee11b4	2a630c58cc27fcaa	fac26e6e4da4705d	b6fc101ad1d74e20
	b2860fc55bdedaa6	a2f7f27a3ec25aba	0d60228aa6e55b6e	fd13cd3620f6c1f4
$t = 71$:	9d38bdb9df22b557	159a02d4faee11b4	2a630c58cc27fcaa	fac26e6e4da4705d
	dfc37c68af65f8bc	b2860fc55bdedaa6	a2f7f27a3ec25aba	0d60228aa6e55b6e
$t = 72$:	d42c3a57cfa78513	9d38bdb9df22b557	159a02d4faee11b4	2a630c58cc27fcaa
	bb56dea6a325ba32	dfc37c68af65f8bc	b2860fc55bdedaa6	a2f7f27a3ec25aba
$t = 73$:	abab4b0ca75a17c7	d42c3a57cfa78513	9d38bdb9df22b557	159a02d4faee11b4
	9ac71d1c037a8bbd	bb56dea6a325ba32	dfc37c68af65f8bc	b2860fc55bdedaa6
$t = 74$:	500f7b61186f6c2e	abab4b0ca75a17c7	d42c3a57cfa78513	9d38bdb9df22b557
	8347f5736531b3ec	9ac71d1c037a8bbd	bb56dea6a325ba32	dfc37c68af65f8bc
$t = 75$:	4abe0af6a67db2fe	500f7b61186f6c2e	abab4b0ca75a17c7	d42c3a57cfa78513
	14e986342ddced0f	8347f5736531b3ec	9ac71d1c037a8bbd	bb56dea6a325ba32
$t = 76$:	e1053fc85f9e56be	4abe0af6a67db2fe	500f7b61186f6c2e	abab4b0ca75a17c7
	4779767cc2ec5321	14e986342ddced0f	8347f5736531b3ec	9ac71d1c037a8bbd
$t = 77$:	7001201948fb3d71	e1053fc85f9e56be	4abe0af6a67db2fe	500f7b61186f6c2e
	5cdf6c58fc052572	4779767cc2ec5321	14e986342ddced0f	8347f5736531b3ec
$t = 78$:	88146da76ff6f23a	7001201948fb3d71	e1053fc85f9e56be	4abe0af6a67db2fe
	8901cffe7a74db98	5cdf6c58fc052572	4779767cc2ec5321	14e986342ddced0f
$t = 79$:	5ec3802b9ecfef33	88146da76ff6f23a	7001201948fb3d71	e1053fc85f9e56be
	5f2eead69efb4233	8901cffe7a74db98	5cdf6c58fc052572	4779767cc2ec5321

That completes the processing of the first message block, $M^{(1)}$. The intermediate hash value, $H^{(1)}$, is calculated to be

$$H_0^{(1)} = \texttt{cbbb9d5dc1059ed8} + \texttt{5ec3802b9ecfef33} = \texttt{2a7f1d895fd58e0b}$$
$$H_1^{(1)} = \texttt{629a292a367cd507} + \texttt{88146da76ff6f23a} = \texttt{eaae96d1a673c741}$$
$$H_2^{(1)} = \texttt{9159015a3070dd17} + \texttt{7001201948fb3d71} = \texttt{015a2173796c1a88}$$
$$H_3^{(1)} = \texttt{152fecd8f70e5939} + \texttt{e1053fc85f9e56be} = \texttt{f6352ca156acaff7}$$
$$H_4^{(1)} = \texttt{67332667ffc00b31} + \texttt{5f2eead69efb4233} = \texttt{c662113e9ebb4d64}$$
$$H_5^{(1)} = \texttt{8eb44a8768581511} + \texttt{8901cffe7a74db98} = \texttt{17b61a85e2ccf0a9}$$
$$H_6^{(1)} = \texttt{db0c2e0d64f98fa7} + \texttt{5cdf6c58fc052572} = \texttt{37eb9a6660feb519}$$
$$H_7^{(1)} = \texttt{47b5481dbefa4fa4} + \texttt{4779767cc2ec5321} = \texttt{8f2ebe9a81e6a2c5}.$$

The words of the *second* padded message block, $M^{(2)}$, are then assigned to the words $W_0,\ldots,W_{15}$ of the message schedule:

W_0 = 0000000000000000	W_8 = 0000000000000000
W_1 = 0000000000000000	W_9 = 0000000000000000
W_2 = 0000000000000000	W_{10} = 0000000000000000
W_3 = 0000000000000000	W_{11} = 0000000000000000
W_4 = 0000000000000000	W_{12} = 0000000000000000
W_5 = 0000000000000000	W_{13} = 0000000000000000
W_6 = 0000000000000000	W_{14} = 0000000000000000
W_7 = 0000000000000000	W_{15} = 0000000000000380.

The following schedule shows the hex values for ***a***, ***b***, ***c***, ***d***, ***e***, ***f***, ***g***, and ***h*** *after* pass *t* of the "for *t*=0 to 79" loop described in Sec. 6.3.2, step 4.

	a / ***e***	***b*** / ***f***	***c*** / ***g***	***d*** / ***h***
t = 0 :	657a3c2ca9639d40 791f2ad0055fdd62	2a7f1d895fd58e0b c662113e9ebb4d64	eaae96d1a673c741 17b61a85e2ccf0a9	015a2173796c1a88 37eb9a6660feb519
t = 1 :	2a4ad5d9b9fd6d86 dbf2e656b5be3f14	657a3c2ca9639d40 791f2ad0055fdd62	2a7f1d895fd58e0b c662113e9ebb4d64	eaae96d1a673c741 17b61a85e2ccf0a9
t = 2 :	f0aa6758653d1664 6e0466c82f4fd35d	2a4ad5d9b9fd6d86 dbf2e656b5be3f14	657a3c2ca9639d40 791f2ad0055fdd62	2a7f1d895fd58e0b c662113e9ebb4d64
t = 3 :	43a76f011a73d317 1367bd36d15e8b40	f0aa6758653d1664 6e0466c82f4fd35d	2a4ad5d9b9fd6d86 dbf2e656b5be3f14	657a3c2ca9639d40 791f2ad0055fdd62
t = 4 :	d802c2dfd7cc48f6 f73d759b839a2a21	43a76f011a73d317 1367bd36d15e8b40	f0aa6758653d1664 6e0466c82f4fd35d	2a4ad5d9b9fd6d86 dbf2e656b5be3f14
t = 5 :	481208e5e8314602 6b2271a46f14c843	d802c2dfd7cc48f6 f73d759b839a2a21	43a76f011a73d317 1367bd36d15e8b40	f0aa6758653d1664 6e0466c82f4fd35d
t = 6 :	af9f8112df35cf33 257f4a7d524d7b0b	481208e5e8314602 6b2271a46f14c843	d802c2dfd7cc48f6 f73d759b839a2a21	43a76f011a73d317 1367bd36d15e8b40
t = 7 :	6730781342d1131b 81957ad408cec995	af9f8112df35cf33 257f4a7d524d7b0b	481208e5e8314602 6b2271a46f14c843	d802c2dfd7cc48f6 f73d759b839a2a21
t = 8 :	82e64c677356a82e 10b62fdce4ebaa51	6730781342d1131b 81957ad408cec995	af9f8112df35cf33 257f4a7d524d7b0b	481208e5e8314602 6b2271a46f14c843
t = 9 :	203578820a8f27d0 9937b3a0cb9248a1	82e64c677356a82e 10b62fdce4ebaa51	6730781342d1131b 81957ad408cec995	af9f8112df35cf33 257f4a7d524d7b0b
t = 10 :	0bac2a84c29a1e2b 6ad288dab3de0d53	203578820a8f27d0 9937b3a0cb9248a1	82e64c677356a82e 10b62fdce4ebaa51	6730781342d1131b 81957ad408cec995
t = 11 :	dd3ff8a140485c25 3149b728123c465e	0bac2a84c29a1e2b 6ad288dab3de0d53	203578820a8f27d0 9937b3a0cb9248a1	82e64c677356a82e 10b62fdce4ebaa51
t = 12 :	e826239f830c5346 4bb7b199c4ced186	dd3ff8a140485c25 3149b728123c465e	0bac2a84c29a1e2b 6ad288dab3de0d53	203578820a8f27d0 9937b3a0cb9248a1
t = 13 :	32215ce49aae40f8 9a2872c72d790d49	e826239f830c5346 4bb7b199c4ced186	dd3ff8a140485c25 3149b728123c465e	0bac2a84c29a1e2b 6ad288dab3de0d53
t = 14 :	859533bac457f94e 539f225d25ebeb4c	32215ce49aae40f8 9a2872c72d790d49	e826239f830c5346 4bb7b199c4ced186	dd3ff8a140485c25 3149b728123c465e
t = 15 :	a88704d9962849f3	859533bac457f94e	32215ce49aae40f8	e826239f830c5346

	63bf0472ef24f7a5	539f225d25ebeb4c	9a2872c72d790d49	4bb7b199c4ced186
$t = 16$:	3aa5c566a6cfad1c	a88704d9962849f3	859533bac457f94e	32215ce49aae40f8
	ce23f6380ead33c2	63bf0472ef24f7a5	539f225d25ebeb4c	9a2872c72d790d49
$t = 17$:	2e9c483a7c08c9c1	3aa5c566a6cfad1c	a88704d9962849f3	859533bac457f94e
	b033f945f3e6b4a2	ce23f6380ead33c2	63bf0472ef24f7a5	539f225d25ebeb4c
$t = 18$:	5a68585ae0835231	2e9c483a7c08c9c1	3aa5c566a6cfad1c	a88704d9962849f3
	8a0187a9ce93d875	b033f945f3e6b4a2	ce23f6380ead33c2	63bf0472ef24f7a5
$t = 19$:	cf9cd481e6407ced	5a68585ae0835231	2e9c483a7c08c9c1	3aa5c566a6cfad1c
	37a29fa30531bac7	8a0187a9ce93d875	b033f945f3e6b4a2	ce23f6380ead33c2
$t = 20$:	3f463f864f6474d9	cf9cd481e6407ced	5a68585ae0835231	2e9c483a7c08c9c1
	0cf45bb3c07e847d	37a29fa30531bac7	8a0187a9ce93d875	b033f945f3e6b4a2
$t = 21$:	cea26288dff931a5	3f463f864f6474d9	cf9cd481e6407ced	5a68585ae0835231
	34f1b5f46bf48a73	0cf45bb3c07e847d	37a29fa30531bac7	8a0187a9ce93d875
$t = 22$:	89634cd0f4f6c08a	cea26288dff931a5	3f463f864f6474d9	cf9cd481e6407ced
	3a728a543405a8e4	34f1b5f46bf48a73	0cf45bb3c07e847d	37a29fa30531bac7
$t = 23$:	625fa38464e5c880	89634cd0f4f6c08a	cea26288dff931a5	3f463f864f6474d9
	cee1b47a49b2fc42	3a728a543405a8e4	34f1b5f46bf48a73	0cf45bb3c07e847d
$t = 24$:	7dd21453a15a3b92	625fa38464e5c880	89634cd0f4f6c08a	cea26288dff931a5
	9308bfa1be1f800b	cee1b47a49b2fc42	3a728a543405a8e4	34f1b5f46bf48a73
$t = 25$:	3d76277bc8cb0601	7dd21453a15a3b92	625fa38464e5c880	89634cd0f4f6c08a
	480e017f5d1f0b1e	9308bfa1be1f800b	cee1b47a49b2fc42	3a728a543405a8e4
$t = 26$:	c8d904196f5a1f54	3d76277bc8cb0601	7dd21453a15a3b92	625fa38464e5c880
	4bd2f1f6e940c332	480e017f5d1f0b1e	9308bfa1be1f800b	cee1b47a49b2fc42
$t = 27$:	b033139b58b6e423	c8d904196f5a1f54	3d76277bc8cb0601	7dd21453a15a3b92
	f816ec1cbe0adafb	4bd2f1f6e940c332	480e017f5d1f0b1e	9308bfa1be1f800b
$t = 28$:	097768182cb65f57	b033139b58b6e423	c8d904196f5a1f54	3d76277bc8cb0601
	62e3de54dcd8f974	f816ec1cbe0adafb	4bd2f1f6e940c332	480e017f5d1f0b1e
$t = 29$:	3196649ab5f5cc39	097768182cb65f57	b033139b58b6e423	c8d904196f5a1f54
	f6887de116d0bd8f	62e3de54dcd8f974	f816ec1cbe0adafb	4bd2f1f6e940c332
$t = 30$:	f78d3d221d16965f	3196649ab5f5cc39	097768182cb65f57	b033139b58b6e423
	c7e4859c2858ed3c	f6887de116d0bd8f	62e3de54dcd8f974	f816ec1cbe0adafb
$t = 31$:	f58e9876b4984b51	f78d3d221d16965f	3196649ab5f5cc39	097768182cb65f57
	621352b394b8ca02	c7e4859c2858ed3c	f6887de116d0bd8f	62e3de54dcd8f974
$t = 32$:	38fbf0e726e04f78	f58e9876b4984b51	f78d3d221d16965f	3196649ab5f5cc39
	4319856f17a0a430	621352b394b8ca02	c7e4859c2858ed3c	f6887de116d0bd8f
$t = 33$:	f4be0b32a57597a2	38fbf0e726e04f78	f58e9876b4984b51	f78d3d221d16965f
	c6d392a3b4eb0ed8	4319856f17a0a430	621352b394b8ca02	c7e4859c2858ed3c
$t = 34$:	f8a6b3fe2e4f0634	f4be0b32a57597a2	38fbf0e726e04f78	f58e9876b4984b51
	602663c0f34eff33	c6d392a3b4eb0ed8	4319856f17a0a430	621352b394b8ca02
$t = 35$:	9bc3871be8046113	f8a6b3fe2e4f0634	f4be0b32a57597a2	38fbf0e726e04f78
	05542ecd9883c6ba	602663c0f34eff33	c6d392a3b4eb0ed8	4319856f17a0a430
$t = 36$:	f1bd2d46be619585	9bc3871be8046113	f8a6b3fe2e4f0634	f4be0b32a57597a2
	e47b9933bafdc655	05542ecd9883c6ba	602663c0f34eff33	c6d392a3b4eb0ed8
$t = 37$:	24c84b58d119affe	f1bd2d46be619585	9bc3871be8046113	f8a6b3fe2e4f0634
	5ae0b1175beb5d2b	e47b9933bafdc655	05542ecd9883c6ba	602663c0f34eff33
$t = 38$:	ec6d3abc2b291fd3	24c84b58d119affe	f1bd2d46be619585	9bc3871be8046113

	9ecc381d277748a3	5ae0b1175beb5d2b	e47b9933bafdc655	05542ecd9883c6ba
$t = 39$:	e266c1f77d5ee90e	ec6d3abc2b291fd3	24c84b58d119affe	f1bd2d46be619585
	d92f34c110296b32	9ecc381d277748a3	5ae0b1175beb5d2b	e47b9933bafdc655
$t = 40$:	5adbaa463642b570	e266c1f77d5ee90e	ec6d3abc2b291fd3	24c84b58d119affe
	83e8f410f859388e	d92f34c110296b32	9ecc381d277748a3	5ae0b1175beb5d2b
$t = 41$:	50fdb7bb2e499a34	5adbaa463642b570	e266c1f77d5ee90e	ec6d3abc2b291fd3
	257ed8ea645e933a	83e8f410f859388e	d92f34c110296b32	9ecc381d277748a3
$t = 42$:	06514212bb7fa152	50fdb7bb2e499a34	5adbaa463642b570	e266c1f77d5ee90e
	466781db35181abe	257ed8ea645e933a	83e8f410f859388e	d92f34c110296b32
$t = 43$:	673ed5a55ff2b07d	06514212bb7fa152	50fdb7bb2e499a34	5adbaa463642b570
	ba78f3545e7914f0	466781db35181abe	257ed8ea645e933a	83e8f410f859388e
$t = 44$:	125e2e5118393e2b	673ed5a55ff2b07d	06514212bb7fa152	50fdb7bb2e499a34
	4453b23a3e13b090	ba78f3545e7914f0	466781db35181abe	257ed8ea645e933a
$t = 45$:	07ee813df5910cec	125e2e5118393e2b	673ed5a55ff2b07d	06514212bb7fa152
	eae013a0510d23cc	4453b23a3e13b090	ba78f3545e7914f0	466781db35181abe
$t = 46$:	0a0508f0a1d719c3	07ee813df5910cec	125e2e5118393e2b	673ed5a55ff2b07d
	a93815eb58891016	eae013a0510d23cc	4453b23a3e13b090	ba78f3545e7914f0
$t = 47$:	0fc8f3b3efcb1b96	0a0508f0a1d719c3	07ee813df5910cec	125e2e5118393e2b
	a071cc73b966e801	a93815eb58891016	eae013a0510d23cc	4453b23a3e13b090
$t = 48$:	02aa5b28199f304a	0fc8f3b3efcb1b96	0a0508f0a1d719c3	07ee813df5910cec
	a49f1e14f8a2be7a	a071cc73b966e801	a93815eb58891016	eae013a0510d23cc
$t = 49$:	9223e1b34382f104	02aa5b28199f304a	0fc8f3b3efcb1b96	0a0508f0a1d719c3
	bfe2106e512a7331	a49f1e14f8a2be7a	a071cc73b966e801	a93815eb58891016
$t = 50$:	e01a1e47ee8d5656	9223e1b34382f104	02aa5b28199f304a	0fc8f3b3efcb1b96
	592b899b35469a78	bfe2106e512a7331	a49f1e14f8a2be7a	a071cc73b966e801
$t = 51$:	fa7b17aad857c2f4	e01a1e47ee8d5656	9223e1b34382f104	02aa5b28199f304a
	eb6e85e4682c1671	592b899b35469a78	bfe2106e512a7331	a49f1e14f8a2be7a
$t = 52$:	0c523b7a3c84ab77	fa7b17aad857c2f4	e01a1e47ee8d5656	9223e1b34382f104
	b5e80e871ac0c005	eb6e85e4682c1671	592b899b35469a78	bfe2106e512a7331
$t = 53$:	c773d8b69da1fde2	0c523b7a3c84ab77	fa7b17aad857c2f4	e01a1e47ee8d5656
	be2b0602fc6f8f65	b5e80e871ac0c005	eb6e85e4682c1671	592b899b35469a78
$t = 54$:	c6b1bc79a4f23679	c773d8b69da1fde2	0c523b7a3c84ab77	fa7b17aad857c2f4
	c80bdc57f38a05e4	be2b0602fc6f8f65	b5e80e871ac0c005	eb6e85e4682c1671
$t = 55$:	bef9bb0fe467fd60	c6b1bc79a4f23679	c773d8b69da1fde2	0c523b7a3c84ab77
	1dab0bd116e434e5	c80bdc57f38a05e4	be2b0602fc6f8f65	b5e80e871ac0c005
$t = 56$:	8e3db3e380ec7f22	bef9bb0fe467fd60	c6b1bc79a4f23679	c773d8b69da1fde2
	32ef50751734ffee	1dab0bd116e434e5	c80bdc57f38a05e4	be2b0602fc6f8f65
$t = 57$:	1003ec42412c7b7d	8e3db3e380ec7f22	bef9bb0fe467fd60	c6b1bc79a4f23679
	1ec0d46f349fd058	32ef50751734ffee	1dab0bd116e434e5	c80bdc57f38a05e4
$t = 58$:	375facc76291f85e	1003ec42412c7b7d	8e3db3e380ec7f22	bef9bb0fe467fd60
	59c8bc0488f9768b	1ec0d46f349fd058	32ef50751734ffee	1dab0bd116e434e5
$t = 59$:	bd113d92e0354fb9	375facc76291f85e	1003ec42412c7b7d	8e3db3e380ec7f22
	e66c73db3fad397d	59c8bc0488f9768b	1ec0d46f349fd058	32ef50751734ffee
$t = 60$:	2f61d4fd8e36d9d4	bd113d92e0354fb9	375facc76291f85e	1003ec42412c7b7d
	e9f21933e1c02948	e66c73db3fad397d	59c8bc0488f9768b	1ec0d46f349fd058
$t = 61$:	1b1ad88b92701ae2	2f61d4fd8e36d9d4	bd113d92e0354fb9	375facc76291f85e
	6fd0c1719bcac335	e9f21933e1c02948	e66c73db3fad397d	59c8bc0488f9768b

t = 62 :	93d09fc06a19c5da	1b1ad88b92701ae2	2f61d4fd8e36d9d4	bd113d92e0354fb9
	b765273f571a571e	6fd0c1719bcac335	e9f21933e1c02948	e66c73db3fad397d
t = 63 :	04bea2ce99cc3bf6	93d09fc06a19c5da	1b1ad88b92701ae2	2f61d4fd8e36d9d4
	6ab0e443c2f63714	b765273f571a571e	6fd0c1719bcac335	e9f21933e1c02948
t = 64 :	02ebfc0a13492f52	04bea2ce99cc3bf6	93d09fc06a19c5da	1b1ad88b92701ae2
	77300c52e05af415	6ab0e443c2f63714	b765273f571a571e	6fd0c1719bcac335
t = 65 :	1bf525abce8d6f04	02ebfc0a13492f52	04bea2ce99cc3bf6	93d09fc06a19c5da
	8faf12c33bb371b9	77300c52e05af415	6ab0e443c2f63714	b765273f571a571e
t = 66 :	b6a36a3431547328	1bf525abce8d6f04	02ebfc0a13492f52	04bea2ce99cc3bf6
	fa8bb40b4e08100f	8faf12c33bb371b9	77300c52e05af415	6ab0e443c2f63714
t = 67 :	ffdaf83202af0d72	b6a36a3431547328	1bf525abce8d6f04	02ebfc0a13492f52
	8045a82f723a9b4e	fa8bb40b4e08100f	8faf12c33bb371b9	77300c52e05af415
t = 68 :	12737373d2985232	ffdaf83202af0d72	b6a36a3431547328	1bf525abce8d6f04
	870dbce23bad8988	8045a82f723a9b4e	fa8bb40b4e08100f	8faf12c33bb371b9
t = 69 :	6189f68162b256b5	12737373d2985232	ffdaf83202af0d72	b6a36a3431547328
	8c059af157146580	870dbce23bad8988	8045a82f723a9b4e	fa8bb40b4e08100f
t = 70 :	20b0a9a1d21c482d	6189f68162b256b5	12737373d2985232	ffdaf83202af0d72
	f22b874c96785ec8	8c059af157146580	870dbce23bad8988	8045a82f723a9b4e
t = 71 :	ef6d863c2127b394	20b0a9a1d21c482d	6189f68162b256b5	12737373d2985232
	b7aee28337d69dab	f22b874c96785ec8	8c059af157146580	870dbce23bad8988
t = 72 :	d3efe8b442689074	ef6d863c2127b394	20b0a9a1d21c482d	6189f68162b256b5
	22491ab9cdecb6b0	b7aee28337d69dab	f22b874c96785ec8	8c059af157146580
t = 73 :	4694354944a9f487	d3efe8b442689074	ef6d863c2127b394	20b0a9a1d21c482d
	659890a5818d0c50	22491ab9cdecb6b0	b7aee28337d69dab	f22b874c96785ec8
t = 74 :	b93c2403773dd08c	4694354944a9f487	d3efe8b442689074	ef6d863c2127b394
	88c2c2ac52c4f679	659890a5818d0c50	22491ab9cdecb6b0	b7aee28337d69dab
t = 75 :	025848e3ab6b69d3	b93c2403773dd08c	4694354944a9f487	d3efe8b442689074
	750da3d4e16a1b64	88c2c2ac52c4f679	659890a5818d0c50	22491ab9cdecb6b0
t = 76 :	396b53e58d04471b	025848e3ab6b69d3	b93c2403773dd08c	4694354944a9f487
	700486bf252cba75	750da3d4e16a1b64	88c2c2ac52c4f679	659890a5818d0c50
t = 77 :	51b6f9a3c1ceeb4a	396b53e58d04471b	025848e3ab6b69d3	b93c2403773dd08c
	e6b3850de8ae6230	700486bf252cba75	750da3d4e16a1b64	88c2c2ac52c4f679
t = 78 :	526a98f5dc595406	51b6f9a3c1ceeb4a	396b53e58d04471b	025848e3ab6b69d3
	4f0dcf74aea76f90	e6b3850de8ae6230	700486bf252cba75	750da3d4e16a1b64
t = 79 :	deb3eeaa973bb9dd	526a98f5dc595406	51b6f9a3c1ceeb4a	396b53e58d04471b
	3665b5dbb6c2e055	4f0dcf74aea76f90	e6b3850de8ae6230	700486bf252cba75

That completes the processing of the second and final message block, $M^{(2)}$. The final hash value, $H^{(2)}$, is calculated to be

$$H_0^{(2)} = \texttt{2a7f1d895fd58e0b} + \texttt{deb3eeaa973bb9dd} = \texttt{09330c33f71147e8}$$
$$H_1^{(2)} = \texttt{eaae96d1a673c741} + \texttt{526a98f5dc595406} = \texttt{3d192fc782cd1b47}$$
$$H_2^{(2)} = \texttt{015a2173796c1a88} + \texttt{51b6f9a3c1ceeb4a} = \texttt{53111b173b3b05d2}$$
$$H_3^{(2)} = \texttt{f6352ca156acaff7} + \texttt{396b53e58d04471b} = \texttt{2fa08086e3b0f712}$$
$$H_4^{(2)} = \texttt{c662113e9ebb4d64} + \texttt{3665b5dbb6c2e055} = \texttt{fcc7c71a557e2db9}$$

$H_5^{(2)}$ = 17b61a85e2ccf0a9 + 4f0dcf74aea76f90 = 66c3e9fa91746039

$H_6^{(2)}$ = 37eb9a6660feb519 + e6b3850de8ae6230 = 1e9f1f7449ad1749

$H_7^{(2)}$ = 8f2ebe9a81e6a2c5 + 700486bf252cba75 = ff334559a7135d3a.

The final hash value is truncated to its left-most 384 bits (i.e., $H_0^{(1)}, \ldots, H_5^{(1)}$), resulting in the 384-bit message digest

```
09330c33f71147e8 3d192fc782cd1b47 53111b173b3b05d2 2fa08086e3b0f712
fcc7c71a557e2db9 66c3e9fa91746039.
```

D.3 SHA-384 Example (Long Message)

Let the message *M* be the binary-coded form of the ASCII string which consists of 1,000,000 repetitions of the character "**a**". The resulting SHA-384 message digest is

```
9d0e1809716474cb 086e834e310a4a1c ed149e9c00f24852 7972cec5704c2a5b
07b8b3dc38ecc4eb ae97ddd87f3d8985.
```

APPENDIX E: REFERENCES

[180-1] Federal Information Processing Standards (FIPS) Publication 180-1, *Secure Hash Standard (SHS)*, U.S. DoC/NIST, April 17, 1995.

[HAC] A. Menezes, P. van Oorschot, and S. Vanstone. *Handbook of Applied Cryptography*, CRC Press, Inc., October 1997.

FIPS 180-2, SECURE HASH STANDARD

CHANGE NOTICE 1

U.S. DEPARTMENT OF COMMERCE
NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY
Gaithersburg, MD 20899

DATE OF CHANGE: 2004 February 25

Federal Information Processing Standard (FIPS) 180-2, Secure Hash Standard, specifies four secure hash functions - SHA-1, SHA-256, SHA-384, and SHA-512 - for computing a condensed representation of electronic data (a message). When a message of any length $< 2^{64}$ bits (for SHA-1 and SHA-256) or $< 2^{128}$ bits (for SHA-384 and SHA-512) is input to a hash function, the result is an output called a message digest. The message digests range in length from 160 to 512 bits, depending on the hash function.

This change notice specifies an additional hash function, SHA-224. Figure 1 of this Standard (see Section 1) specifies the basic properties of the SHA-1, SHA-256, SHA-384 and SHA-512 hash functions. The following table specifies those properties for SHA-224.

					Security (bits)
-					112

SHA-224 Specification

SHA-224 may be used to hash a message, *M*, having a length of ℓ bits, where $0 \le \ell < 2^{64}$. The function is defined in the exact same manner as SHA-256 (Section 6.2), with the following two exceptions:

1. For SHA-224, the initial hash value, $H^{(0)}$, shall consist of the following eight (8) 32-bit words:

$$H_0^{(0)} = \texttt{c1059ed8}$$
$$H_1^{(0)} = \texttt{367cd507}$$
$$H_2^{(0)} = \texttt{3070dd17}$$
$$H_3^{(0)} = \texttt{f70e5939}$$
$$H_4^{(0)} = \texttt{ffc00b31}$$
$$H_5^{(0)} = \texttt{68581511}$$
$$H_6^{(0)} = \texttt{64f98fa7}$$
$$H_7^{(0)} = \texttt{befa4fa4}$$

2. The 224-bit message digest is obtained by truncating the final hash value, $H^{(N)}$, to its left-most 224 bits:

$$H_0^{(N)} \| H_1^{(N)} \| H_2^{(N)} \| H_3^{(N)} \| H_4^{(N)} \| H_5^{(N)} \| H_6^{(N)} .$$

Truncation of the Hash Function Output

Some applications may require a hash function with an output size (i.e., message digest size) different than those provided by the hash functions in this Standard. In such cases, a truncated hash output may be used, whereby a hash function with a larger output size is applied to the data to be hashed, and the resulting output (i.e., message digest) is truncated by selecting an appropriate number of the leftmost bits. For example, if an output of 96 bits is desired, the SHA-256 hash function could be used (e.g., because it is available to the application), and the leftmost 96 bits of the output are selected as the message digest, discarding the rightmost 160 bits of the SHA-256 output.

This guidance is provided for unforeseen applications in order to provide interoperability. A standard method for truncating hash function outputs is provided strictly as a convenience for implementers and application developers. No claims are made about the suitability of truncating the hash output or about the security level obtained by truncating the hash output. The proper use of truncated hash outputs is an application-level issue.

Truncating the hash function output can impact the security of an application. For example, applications that use the truncated hash output risk attacks based on confusion between different parties about the specific amount of truncation used, and the specific hash function whose output was truncated. Any application using truncated hash output is responsible for ensuring that the truncation amount and the hash function used are known to all parties, with no chance of ambiguity.

Truncated hash output **shall not** be used in place of the full hash output by standardized applications that reference this Standard, e.g. digital signatures (FIPS 186-2) or keyed hash functions used for message authentication (FIPS 198).

SHA-224 Examples

1. SHA-224 Example (One-Block Message)

Let the message, *M*, be the 24-bit ($\ell = 24$) ASCII string "**abc**", which is equivalent to the following binary string:

```
01100001  01100010  01100011.
```

The message is padded by appending a "1" bit, followed by 423 "0" bits, and ending with the hex value `00000000 00000018` (the two 32-bit word representation of the length, 24). Thus, the final padded message consists of one block (N=1).

For SHA-224, the initial hash value, $H^{(0)}$, is

$$H_0^{(0)} = \texttt{c1059ed8}$$
$$H_1^{(0)} = \texttt{367cd507}$$
$$H_2^{(0)} = \texttt{3070dd17}$$
$$H_3^{(0)} = \texttt{f70e5939}$$
$$H_4^{(0)} = \texttt{ffc00b31}$$
$$H_5^{(0)} = \texttt{68581511}$$
$$H_6^{(0)} = \texttt{64f98fa7}$$
$$H_7^{(0)} = \texttt{befa4fa4}.$$

The words of the padded message block are then assigned to the words $W_0,\ldots,W_{15}$ of the message schedule:

$$W_0 = \texttt{61626380} \qquad W_8 = \texttt{00000000}$$
$$W_1 = \texttt{00000000} \qquad W_9 = \texttt{00000000}$$
$$W_2 = \texttt{00000000} \qquad W_{10} = \texttt{00000000}$$
$$W_3 = \texttt{00000000} \qquad W_{11} = \texttt{00000000}$$
$$W_4 = \texttt{00000000} \qquad W_{12} = \texttt{00000000}$$
$$W_5 = \texttt{00000000} \qquad W_{13} = \texttt{00000000}$$
$$W_6 = \texttt{00000000} \qquad W_{14} = \texttt{00000000}$$
$$W_7 = \texttt{00000000} \qquad W_{15} = \texttt{00000018}.$$

The following schedule shows the hex values for ***a***, ***b***, ***c***, ***d***, ***e***, ***f***, ***g***, and ***h*** *after* pass *t* of the "for *t*=0 to 63" loop described in Sec. 6.2.2, step 4.

	a	***b***	***c***	***d***	***e***	***f***	***g***	***h***
t=00	0e96b2da	c1059ed8	367cd507	3070dd17	0434225e	ffc00b31	68581511	64f98fa7
t=01	c20dab6b	0e96b2da	c1059ed8	367cd507	9cab416f	0434225e	ffc00b31	68581511
t=02	ab113b7a	c20dab6b	0e96b2da	c1059ed8	82177fe8	9cab416f	0434225e	ffc00b31
t=03	8253cc1a	ab113b7a	c20dab6b	0e96b2da	8346b27d	82177fe8	9cab416f	0434225e
t=04	08a0dc0c	8253cc1a	ab113b7a	c20dab6b	05b557db	8346b27d	82177fe8	9cab416f
t=05	b2ca3a91	08a0dc0c	8253cc1a	ab113b7a	898dc7bb	05b557db	8346b27d	82177fe8
t=06	0b6b9023	b2ca3a91	08a0dc0c	8253cc1a	a2e49147	898dc7bb	05b557db	8346b27d
t=07	f09d116d	0b6b9023	b2ca3a91	08a0dc0c	7a84120d	a2e49147	898dc7bb	05b557db
t=08	ed6fa633	f09d116d	0b6b9023	b2ca3a91	c037faad	7a84120d	a2e49147	898dc7bb
t=09	55e6a367	ed6fa633	f09d116d	0b6b9023	aae50091	c037faad	7a84120d	a2e49147
t=10	0817e82b	55e6a367	ed6fa633	f09d116d	c8c53a2c	aae50091	c037faad	7a84120d
t=11	17142334	0817e82b	55e6a367	ed6fa633	dd4c7be9	c8c53a2c	aae50091	c037faad
t=12	fc4f023e	17142334	0817e82b	55e6a367	87bea51a	dd4c7be9	c8c53a2c	aae50091
t=13	be316902	fc4f023e	17142334	0817e82b	65141125	87bea51a	dd4c7be9	c8c53a2c
t=14	1d80d178	be316902	fc4f023e	17142334	4545f53a	65141125	87bea51a	dd4c7be9
t=15	9f341a45	1d80d178	be316902	fc4f023e	6a61c411	4545f53a	65141125	87bea51a
t=16	0f324db9	9f341a45	1d80d178	be316902	06c80d6a	6a61c411	4545f53a	65141125
t=17	ffe7012b	0f324db9	9f341a45	1d80d178	b7b601f4	06c80d6a	6a61c411	4545f53a
t=18	62932ab8	ffe7012b	0f324db9	9f341a45	763b627a	b7b601f4	06c80d6a	6a61c411
t=19	5207d867	62932ab8	ffe7012b	0f324db9	7fbba936	763b627a	b7b601f4	06c80d6a
t=20	07d55ccb	5207d867	62932ab8	ffe7012b	9ba5a6ea	7fbba936	763b627a	b7b601f4
t=21	dece98a4	07d55ccb	5207d867	62932ab8	293ffb5d	9ba5a6ea	7fbba936	763b627a

```
t=22   e62a812e  dece98a4  07d55ccb  5207d867  28fe0fd9  293ffb5d  9ba5a6ea  7fbba936
t=23   57206fb8  e62a812e  dece98a4  07d55ccb  c76084ea  28fe0fd9  293ffb5d  9ba5a6ea
t=24   6a6abcf0  57206fb8  e62a812e  dece98a4  b2614c5e  c76084ea  28fe0fd9  293ffb5d
t=25   937514f0  6a6abcf0  57206fb8  e62a812e  b42ec21c  b2614c5e  c76084ea  28fe0fd9
t=26   82af3ffb  937514f0  6a6abcf0  57206fb8  be6f6760  b42ec21c  b2614c5e  c76084ea
t=27   eca3bcd5  82af3ffb  937514f0  6a6abcf0  1dccbb10  be6f6760  b42ec21c  b2614c5e
t=28   2d1576c4  eca3bcd5  82af3ffb  937514f0  01641929  1dccbb10  be6f6760  b42ec21c
t=29   fe3c8658  2d1576c4  eca3bcd5  82af3ffb  fc4b36c5  01641929  1dccbb10  be6f6760
t=30   0d7cce07  fe3c8658  2d1576c4  eca3bcd5  a4a4a3a4  fc4b36c5  01641929  1dccbb10
t=31   cce1951d  0d7cce07  fe3c8658  2d1576c4  4be9475c  a4a4a3a4  fc4b36c5  01641929
t=32   09b76257  cce1951d  0d7cce07  fe3c8658  0ccddd86  4be9475c  a4a4a3a4  fc4b36c5
t=33   f827767e  09b76257  cce1951d  0d7cce07  db116db7  0ccddd86  4be9475c  a4a4a3a4
t=34   e4a0bb48  f827767e  09b76257  cce1951d  994e2bac  db116db7  0ccddd86  4be9475c
t=35   d8bb1041  e4a0bb48  f827767e  09b76257  5b730abb  994e2bac  db116db7  0ccddd86
t=36   2a2e32f4  d8bb1041  e4a0bb48  f827767e  22e15c59  5b730abb  994e2bac  db116db7
t=37   0d275ca8  2a2e32f4  d8bb1041  e4a0bb48  f6c39382  22e15c59  5b730abb  994e2bac
t=38   7902369c  0d275ca8  2a2e32f4  d8bb1041  d9f8c2e0  f6c39382  22e15c59  5b730abb
t=39   f3c80288  7902369c  0d275ca8  2a2e32f4  00e3a7bb  d9f8c2e0  f6c39382  22e15c59
t=40   483bba4d  f3c80288  7902369c  0d275ca8  f0a8198c  00e3a7bb  d9f8c2e0  f6c39382
t=41   d75d4d26  483bba4d  f3c80288  7902369c  fcecdcd4  f0a8198c  00e3a7bb  d9f8c2e0
t=42   0744b618  d75d4d26  483bba4d  f3c80288  03186faa  fcecdcd4  f0a8198c  00e3a7bb
t=43   9cce9f01  0744b618  d75d4d26  483bba4d  a56f6bbf  03186faa  fcecdcd4  f0a8198c
t=44   a3701bd9  9cce9f01  0744b618  d75d4d26  af1bef5f  a56f6bbf  03186faa  fcecdcd4
t=45   131d4c09  a3701bd9  9cce9f01  0744b618  ecb77e1b  af1bef5f  a56f6bbf  03186faa
t=46   fb3777d9  131d4c09  a3701bd9  9cce9f01  1d601f44  ecb77e1b  af1bef5f  a56f6bbf
t=47   847ea00e  fb3777d9  131d4c09  a3701bd9  503a7b95  1d601f44  ecb77e1b  af1bef5f
t=48   aaa69347  847ea00e  fb3777d9  131d4c09  5eeb9930  503a7b95  1d601f44  ecb77e1b
t=49   505caf28  aaa69347  847ea00e  fb3777d9  ce695893  5eeb9930  503a7b95  1d601f44
t=50   675e0b02  505caf28  aaa69347  847ea00e  c22dd75f  ce695893  5eeb9930  503a7b95
t=51   abd26099  675e0b02  505caf28  aaa69347  1409c3f8  c22dd75f  ce695893  5eeb9930
t=52   0df9857a  abd26099  675e0b02  505caf28  2d864d9f  1409c3f8  c22dd75f  ce695893
t=53   308b8799  0df9857a  abd26099  675e0b02  02524f02  2d864d9f  1409c3f8  c22dd75f
t=54   909cc059  308b8799  0df9857a  abd26099  6f2a444a  02524f02  2d864d9f  1409c3f8
t=55   8d25bd94  909cc059  308b8799  0df9857a  1273c622  6f2a444a  02524f02  2d864d9f
t=56   f32141da  8d25bd94  909cc059  308b8799  1771ed3f  1273c622  6f2a444a  02524f02
t=57   8ce24395  f32141da  8d25bd94  909cc059  f52f66a6  1771ed3f  1273c622  6f2a444a
t=58   07bcd846  8ce24395  f32141da  8d25bd94  149db547  f52f66a6  1771ed3f  1273c622
t=59   622d5e5b  07bcd846  8ce24395  f32141da  b6f4c630  149db547  f52f66a6  1771ed3f
t=60   c693fc7a  622d5e5b  07bcd846  8ce24395  13dfb889  b6f4c630  149db547  f52f66a6
t=61   55d1c760  c693fc7a  622d5e5b  07bcd846  7e730e00  13dfb889  b6f4c630  149db547
t=62   fd89031b  55d1c760  c693fc7a  622d5e5b  55489ee6  7e730e00  13dfb889  b6f4c630
t=63   6203de4a  fd89031b  55d1c760  c693fc7a  2aedb1b3  55489ee6  7e730e00  13dfb889
```

The resulting 224-bit message digest is:

```
23097d22 3405d822 8642a477 bda255b3 2aadbce4 bda0b3f7 e36c9da7.
```

2. SHA-224 Example (Multi-Block Message)

Let the message, *M*, be the 448-bit ($\ell = 448$) ASCII string

"**abcdbcdecdefdefgefghfghighijhijkijkljklmklmnlmnomnopnopq**".

The message is padded by appending a "`1`" bit, followed by 511 "`0`" bits, and ending with the hex value `00000000 000001c0` (the two 32-bit word representation of the length, 448). Thus, the final padded message consists of two blocks (*N*=2).

For SHA-224, the initial hash value, $H^{(0)}$, is

$H_0^{(0)}$ = c1059ed8
$H_1^{(0)}$ = 367cd507
$H_2^{(0)}$ = 3070dd17
$H_3^{(0)}$ = f70e5939
$H_4^{(0)}$ = ffc00b31
$H_5^{(0)}$ = 68581511
$H_6^{(0)}$ = 64f98fa7
$H_7^{(0)}$ = befa4fa4.

The words of the first padded message block, $M^{(1)}$, are then assigned to the words $W_0,\ldots,W_{15}$ of the message schedule:

W_0 = 61626364
W_1 = 62636465
W_2 = 63646566
W_3 = 64656667
W_4 = 65666768
W_5 = 66676869
W_6 = 6768696a
W_7 = 68696a6b
W_8 = 696a6b6c
W_9 = 6a6b6c6d
W_{10} = 6b6c6d6e
W_{11} = 6c6d6e6f
W_{12} = 6d6e6f70
W_{13} = 6e6f7071
W_{14} = 80000000
W_{15} = 00000000.

The following schedule shows the hex values for ***a***, ***b***, ***c***, ***d***, ***e***, ***f***, ***g***, and ***h*** *after* pass *t* of the "for *t*=0 to 63" loop described in Sec. 6.2.2, step 4.

	a	***b***	***c***	***d***	***e***	***f***	***g***	***h***
t=00	0e96b2be	c1059ed8	367cd507	3070dd17	04342242	ffc00b31	68581511	64f98fa7
t=01	51d17d7b	0e96b2be	c1059ed8	367cd507	2f8ea3d4	04342242	ffc00b31	68581511
t=02	ff1cbd7f	51d17d7b	0e96b2be	c1059ed8	79a896fa	2f8ea3d4	04342242	ffc00b31
t=03	24bcc047	ff1cbd7f	51d17d7b	0e96b2be	1f60795a	79a896fa	2f8ea3d4	04342242
t=04	7d56a6ac	24bcc047	ff1cbd7f	51d17d7b	de395286	1f60795a	79a896fa	2f8ea3d4
t=05	745beb11	7d56a6ac	24bcc047	ff1cbd7f	d863d132	de395286	1f60795a	79a896fa
t=06	0dd41573	745beb11	7d56a6ac	24bcc047	2e60d323	d863d132	de395286	1f60795a
t=07	9a2541fd	0dd41573	745beb11	7d56a6ac	08d2b348	2e60d323	d863d132	de395286
t=08	3140e909	9a2541fd	0dd41573	745beb11	95dfd707	08d2b348	2e60d323	d863d132
t=09	b2954925	3140e909	9a2541fd	0dd41573	05ef5e3d	95dfd707	08d2b348	2e60d323
t=10	b2a874fb	b2954925	3140e909	9a2541fd	9dcaf118	05ef5e3d	95dfd707	08d2b348
t=11	116ce44d	b2a874fb	b2954925	3140e909	0e6d566a	9dcaf118	05ef5e3d	95dfd707
t=12	5ff9349a	116ce44d	b2a874fb	b2954925	08eb3305	0e6d566a	9dcaf118	05ef5e3d
t=13	7fa9d65d	5ff9349a	116ce44d	b2a874fb	4657cf17	08eb3305	0e6d566a	9dcaf118
t=14	006b1b16	7fa9d65d	5ff9349a	116ce44d	08d09e8d	4657cf17	08eb3305	0e6d566a
t=15	b301c98a	006b1b16	7fa9d65d	5ff9349a	6fbefa1d	08d09e8d	4657cf17	08eb3305
t=16	e623ecc0	b301c98a	006b1b16	7fa9d65d	2b3f859c	6fbefa1d	08d09e8d	4657cf17
t=17	d9244a78	e623ecc0	b301c98a	006b1b16	e66d8d9c	2b3f859c	6fbefa1d	08d09e8d
t=18	99c72726	d9244a78	e623ecc0	b301c98a	b26a409c	e66d8d9c	2b3f859c	6fbefa1d
t=19	ab0cbed2	99c72726	d9244a78	e623ecc0	010d7c65	b26a409c	e66d8d9c	2b3f859c
t=20	78062878	ab0cbed2	99c72726	d9244a78	5678a949	010d7c65	b26a409c	e66d8d9c
t=21	d7c5c5d5	78062878	ab0cbed2	99c72726	b280360c	5678a949	010d7c65	b26a409c

t=22	bad2ee72	d7c5c5d5	78062878	ab0cbed2	0d4cd0c4	b280360c	5678a949	010d7c65
t=23	bcf47346	bad2ee72	d7c5c5d5	78062878	d6a19dc8	0d4cd0c4	b280360c	5678a949
t=24	5ecc417b	bcf47346	bad2ee72	d7c5c5d5	3337a11c	d6a19dc8	0d4cd0c4	b280360c
t=25	e15bfa57	5ecc417b	bcf47346	bad2ee72	0ce15173	3337a11c	d6a19dc8	0d4cd0c4
t=26	fae6167b	e15bfa57	5ecc417b	bcf47346	73dbe5c7	0ce15173	3337a11c	d6a19dc8
t=27	991c3f99	fae6167b	e15bfa57	5ecc417b	8602a31f	73dbe5c7	0ce15173	3337a11c
t=28	7055843b	991c3f99	fae6167b	e15bfa57	eb4de5f8	8602a31f	73dbe5c7	0ce15173
t=29	08dcfb6d	7055843b	991c3f99	fae6167b	4606d126	eb4de5f8	8602a31f	73dbe5c7
t=30	2964b340	08dcfb6d	7055843b	991c3f99	213b3e63	4606d126	eb4de5f8	8602a31f
t=31	5b3677d0	2964b340	08dcfb6d	7055843b	c9689cb0	213b3e63	4606d126	eb4de5f8
t=32	1ee0fe7d	5b3677d0	2964b340	08dcfb6d	14318a4d	c9689cb0	213b3e63	4606d126
t=33	6b918d6e	1ee0fe7d	5b3677d0	2964b340	216054a8	14318a4d	c9689cb0	213b3e63
t=34	a6710d0d	6b918d6e	1ee0fe7d	5b3677d0	bc823a58	216054a8	14318a4d	c9689cb0
t=35	5e198fed	a6710d0d	6b918d6e	1ee0fe7d	c49933fe	bc823a58	216054a8	14318a4d
t=36	136c320a	5e198fed	a6710d0d	6b918d6e	75687ccb	c49933fe	bc823a58	216054a8
t=37	40ee0c43	136c320a	5e198fed	a6710d0d	f1c2caf6	75687ccb	c49933fe	bc823a58
t=38	aa96d78c	40ee0c43	136c320a	5e198fed	f48b4ceb	f1c2caf6	75687ccb	c49933fe
t=39	27c97b86	aa96d78c	40ee0c43	136c320a	b556216a	f48b4ceb	f1c2caf6	75687ccb
t=40	b07bd327	27c97b86	aa96d78c	40ee0c43	30ec2d76	b556216a	f48b4ceb	f1c2caf6
t=41	d88d56bd	b07bd327	27c97b86	aa96d78c	dc2fa5a4	30ec2d76	b556216a	f48b4ceb
t=42	5c775077	d88d56bd	b07bd327	27c97b86	5fad6db5	dc2fa5a4	30ec2d76	b556216a
t=43	1526cca3	5c775077	d88d56bd	b07bd327	da8a0b1c	5fad6db5	dc2fa5a4	30ec2d76
t=44	c09dda14	1526cca3	5c775077	d88d56bd	d98ec23a	da8a0b1c	5fad6db5	dc2fa5a4
t=45	f885e124	c09dda14	1526cca3	5c775077	e4f23e41	d98ec23a	da8a0b1c	5fad6db5
t=46	5447f0ad	f885e124	c09dda14	1526cca3	bfb7497c	e4f23e41	d98ec23a	da8a0b1c
t=47	e6227061	5447f0ad	f885e124	c09dda14	5b09619b	bfb7497c	e4f23e41	d98ec23a
t=48	009cebea	e6227061	5447f0ad	f885e124	59ecab46	5b09619b	bfb7497c	e4f23e41
t=49	92b0d169	009cebea	e6227061	5447f0ad	9a572b85	59ecab46	5b09619b	bfb7497c
t=50	8d224e54	92b0d169	009cebea	e6227061	32144602	9a572b85	59ecab46	5b09619b
t=51	c1fcac71	8d224e54	92b0d169	009cebea	4e98a8b7	32144602	9a572b85	59ecab46
t=52	8e6ce843	c1fcac71	8d224e54	92b0d169	2c1823be	4e98a8b7	32144602	9a572b85
t=53	000f54de	8e6ce843	c1fcac71	8d224e54	f32cf2a8	2c1823be	4e98a8b7	32144602
t=54	2fe2af3a	000f54de	8e6ce843	c1fcac71	20f763ee	f32cf2a8	2c1823be	4e98a8b7
t=55	1fd539af	2fe2af3a	000f54de	8e6ce843	5acdbd62	20f763ee	f32cf2a8	2c1823be
t=56	7f86644e	1fd539af	2fe2af3a	000f54de	9fc10216	5acdbd62	20f763ee	f32cf2a8
t=57	0e08dc77	7f86644e	1fd539af	2fe2af3a	2a4ea749	9fc10216	5acdbd62	20f763ee
t=58	0b9f4851	0e08dc77	7f86644e	1fd539af	18b1dfb9	2a4ea749	9fc10216	5acdbd62
t=59	dbce97c3	0b9f4851	0e08dc77	7f86644e	6ec6ba5b	18b1dfb9	2a4ea749	9fc10216
t=60	3cd78fe1	dbce97c3	0b9f4851	0e08dc77	3e1ca2f1	6ec6ba5b	18b1dfb9	2a4ea749
t=61	35f4bf1c	3cd78fe1	dbce97c3	0b9f4851	ba1a8a1b	3e1ca2f1	6ec6ba5b	18b1dfb9
t=62	86795a7d	35f4bf1c	3cd78fe1	dbce97c3	2ce11258	ba1a8a1b	3e1ca2f1	6ec6ba5b
t=63	c14b4785	86795a7d	35f4bf1c	3cd78fe1	1108ac7f	2ce11258	ba1a8a1b	3e1ca2f1

That completes the processing of the first message block, $M^{(1)}$. The first intermediate hash value, $H^{(1)}$, is calculated to be

$$H_0^{(1)} = \texttt{8250e65d}$$
$$H_1^{(1)} = \texttt{bcf62f84}$$
$$H_2^{(1)} = \texttt{66659c33}$$
$$H_3^{(1)} = \texttt{33e5e91a}$$
$$H_4^{(1)} = \texttt{10c8b7b0}$$
$$H_5^{(1)} = \texttt{95392769}$$
$$H_6^{(1)} = \texttt{1f1419c2}$$
$$H_7^{(1)} = \texttt{fd16f295}.$$

The words of the *second* padded message block, $M^{(2)}$, are then assigned to the words $W_0,\ldots,W_{15}$ of the message schedule:

W_0 = 00000000
W_1 = 00000000
W_2 = 00000000
W_3 = 00000000
W_4 = 00000000
W_5 = 00000000
W_6 = 00000000
W_7 = 00000000
W_8 = 00000000
W_9 = 00000000
W_{10} = 00000000
W_{11} = 00000000
W_{12} = 00000000
W_{13} = 00000000
W_{14} = 00000000
W_{15} = 000001c0.

The following schedule shows the hex values for ***a***, ***b***, ***c***, ***d***, ***e***, ***f***, ***g***, and ***h*** *after* pass *t* of the "for *t*=0 to 63" loop described in Sec. 6.2.2, step 4.

	a	***b***	***c***	***d***	***e***	***f***	***g***	***h***
t=00	692e407d	8250e65d	bcf62f84	66659c33	e4be1e69	10c8b7b0	95392769	1f1419c2
t=01	608d83e1	692e407d	8250e65d	bcf62f84	3ddb8cee	e4be1e69	10c8b7b0	95392769
t=02	09bfa89f	608d83e1	692e407d	8250e65d	f5813490	3ddb8cee	e4be1e69	10c8b7b0
t=03	2375fbc5	09bfa89f	608d83e1	692e407d	c3e18529	f5813490	3ddb8cee	e4be1e69
t=04	717e79e7	2375fbc5	09bfa89f	608d83e1	77d39ccc	c3e18529	f5813490	3ddb8cee
t=05	a9319748	717e79e7	2375fbc5	09bfa89f	fdbb9913	77d39ccc	c3e18529	f5813490
t=06	27a42f04	a9319748	717e79e7	2375fbc5	b999cce4	fdbb9913	77d39ccc	c3e18529
t=07	3419081e	27a42f04	a9319748	717e79e7	54e69e21	b999cce4	fdbb9913	77d39ccc
t=08	0ab393c2	3419081e	27a42f04	a9319748	ad29647e	54e69e21	b999cce4	fdbb9913
t=09	006784eb	0ab393c2	3419081e	27a42f04	aff457e7	ad29647e	54e69e21	b999cce4
t=10	ecd5c9db	006784eb	0ab393c2	3419081e	9af42a0e	aff457e7	ad29647e	54e69e21
t=11	4762e8f0	ecd5c9db	006784eb	0ab393c2	8fb6f3d8	9af42a0e	aff457e7	ad29647e
t=12	af93b2a8	4762e8f0	ecd5c9db	006784eb	97e63d39	8fb6f3d8	9af42a0e	aff457e7
t=13	533c517c	af93b2a8	4762e8f0	ecd5c9db	7364bae6	97e63d39	8fb6f3d8	9af42a0e
t=14	03c0a51b	533c517c	af93b2a8	4762e8f0	3afb010d	7364bae6	97e63d39	8fb6f3d8
t=15	5fd065bd	03c0a51b	533c517c	af93b2a8	b8e64229	3afb010d	7364bae6	97e63d39
t=16	18b268b5	5fd065bd	03c0a51b	533c517c	38eda38d	b8e64229	3afb010d	7364bae6
t=17	b87d63b4	18b268b5	5fd065bd	03c0a51b	25c2c397	38eda38d	b8e64229	3afb010d
t=18	b1d846e0	b87d63b4	18b268b5	5fd065bd	d674405f	25c2c397	38eda38d	b8e64229
t=19	8ba0aed6	b1d846e0	b87d63b4	18b268b5	b8109422	d674405f	25c2c397	38eda38d
t=20	1485f843	8ba0aed6	b1d846e0	b87d63b4	1c58cd66	b8109422	d674405f	25c2c397
t=21	238f4cda	1485f843	8ba0aed6	b1d846e0	39b2eb5f	1c58cd66	b8109422	d674405f
t=22	7031b061	238f4cda	1485f843	8ba0aed6	4b8262ad	39b2eb5f	1c58cd66	b8109422
t=23	d4e7ec62	7031b061	238f4cda	1485f843	163c3aa0	4b8262ad	39b2eb5f	1c58cd66
t=24	66582df3	d4e7ec62	7031b061	238f4cda	c0976260	163c3aa0	4b8262ad	39b2eb5f
t=25	dedb8199	66582df3	d4e7ec62	7031b061	b73e2dec	c0976260	163c3aa0	4b8262ad
t=26	f8536917	dedb8199	66582df3	d4e7ec62	7c2af9c4	b73e2dec	c0976260	163c3aa0
t=27	d7333b8a	f8536917	dedb8199	66582df3	b2b0b71a	7c2af9c4	b73e2dec	c0976260
t=28	760847c1	d7333b8a	f8536917	dedb8199	5898eff2	b2b0b71a	7c2af9c4	b73e2dec
t=29	7eabc6d7	760847c1	d7333b8a	f8536917	24dd3883	5898eff2	b2b0b71a	7c2af9c4
t=30	90c49624	7eabc6d7	760847c1	d7333b8a	cce25e67	24dd3883	5898eff2	b2b0b71a
t=31	0b876264	90c49624	7eabc6d7	760847c1	e4e4a53b	cce25e67	24dd3883	5898eff2
t=32	04cb36c0	0b876264	90c49624	7eabc6d7	5403a391	e4e4a53b	cce25e67	24dd3883
t=33	d58cc34a	04cb36c0	0b876264	90c49624	b78767c3	5403a391	e4e4a53b	cce25e67
t=34	0ed14dd7	d58cc34a	04cb36c0	0b876264	fdcdc9d9	b78767c3	5403a391	e4e4a53b
t=35	5a89a942	0ed14dd7	d58cc34a	04cb36c0	790c4a20	fdcdc9d9	b78767c3	5403a391
t=36	4d30424c	5a89a942	0ed14dd7	d58cc34a	f95bf853	790c4a20	fdcdc9d9	b78767c3
t=37	47f58c5c	4d30424c	5a89a942	0ed14dd7	0ec9be3b	f95bf853	790c4a20	fdcdc9d9
t=38	b5ad85d7	47f58c5c	4d30424c	5a89a942	cf9f1dbe	0ec9be3b	f95bf853	790c4a20
t=39	762fecbc	b5ad85d7	47f58c5c	4d30424c	15427ed3	cf9f1dbe	0ec9be3b	f95bf853
t=40	32abe746	762fecbc	b5ad85d7	47f58c5c	4053e12e	15427ed3	cf9f1dbe	0ec9be3b

```
t=41   84adb2a0  32abe746  762fecbc  b5ad85d7  7cece4e2  4053e12e  15427ed3  cf9f1dbe
t=42   c6e1c5af  84adb2a0  32abe746  762fecbc  42f9990b  7cece4e2  4053e12e  15427ed3
t=43   35e14bfa  c6e1c5af  84adb2a0  32abe746  c9965792  42f9990b  7cece4e2  4053e12e
t=44   7410bfd8  35e14bfa  c6e1c5af  84adb2a0  ca54ce51  c9965792  42f9990b  7cece4e2
t=45   3fe9e763  7410bfd8  35e14bfa  c6e1c5af  ae7cdb66  ca54ce51  c9965792  42f9990b
t=46   853c3a00  3fe9e763  7410bfd8  35e14bfa  c2be054d  ae7cdb66  ca54ce51  c9965792
t=47   f7d035e7  853c3a00  3fe9e763  7410bfd8  f6d59d2c  c2be054d  ae7cdb66  ca54ce51
t=48   20bae2b8  f7d035e7  853c3a00  3fe9e763  cab73f06  f6d59d2c  c2be054d  ae7cdb66
t=49   ae6bf667  20bae2b8  f7d035e7  853c3a00  52384d2f  cab73f06  f6d59d2c  c2be054d
t=50   12e504e5  ae6bf667  20bae2b8  f7d035e7  f9a8377f  52384d2f  cab73f06  f6d59d2c
t=51   f3497054  12e504e5  ae6bf667  20bae2b8  d0ab7cfc  f9a8377f  52384d2f  cab73f06
t=52   9f166cdb  f3497054  12e504e5  ae6bf667  71b3459b  d0ab7cfc  f9a8377f  52384d2f
t=53   ccd8fa44  9f166cdb  f3497054  12e504e5  0f557ddd  71b3459b  d0ab7cfc  f9a8377f
t=54   f5e664bd  ccd8fa44  9f166cdb  f3497054  a679a5e9  0f557ddd  71b3459b  d0ab7cfc
t=55   d4ea8c7e  f5e664bd  ccd8fa44  9f166cdb  2958ce2a  a679a5e9  0f557ddd  71b3459b
t=56   e8c8fec7  d4ea8c7e  f5e664bd  ccd8fa44  35f6800e  2958ce2a  a679a5e9  0f557ddd
t=57   882ed69e  e8c8fec7  d4ea8c7e  f5e664bd  30267d8e  35f6800e  2958ce2a  a679a5e9
t=58   4ec725f6  882ed69e  e8c8fec7  d4ea8c7e  ce1d1ce4  30267d8e  35f6800e  2958ce2a
t=59   5c9cfc69  4ec725f6  882ed69e  e8c8fec7  c8242b92  ce1d1ce4  30267d8e  35f6800e
t=60   c9a31836  5c9cfc69  4ec725f6  882ed69e  9e40a370  c8242b92  ce1d1ce4  30267d8e
t=61   f754c16e  c9a31836  5c9cfc69  4ec725f6  333e0b63  9e40a370  c8242b92  ce1d1ce4
t=62   94314748  f754c16e  c9a31836  5c9cfc69  1fbc63b0  333e0b63  9e40a370  c8242b92
t=63   f2e7a4b9  94314748  f754c16e  c9a31836  9ffd8dac  1fbc63b0  333e0b63  9e40a370
```

The resulting 224-bit message digest is:

```
75388b16 512776cc 5dba5da1 fd890150 b0c6455c b4f58b19 52522525.
```

3. SHA-224 Example (Long Message)

Let the message *M* be the binary-coded form of the ASCII string which consists of 1,000,000 repetitions of the character "**a**". The resulting SHA-224 message digest is:

```
20794655 980c91d8 bbb4c1ea 97618a4b f03f4258 1948b2ee 4ee7ad67.
```